

COMPUTER NETWORKS (CSE232) Assignment 2

Ritika Thakur (2022408) | Swarnima Prasad (2022525)

Linux Command Line Utilities

1. `ifconfig` command:

`ifconfig` is used to configure network interfaces in Unix and Linux operating systems. It is used to view and change the configuration of the network interfaces on system. `ipconfig` for Windows.

1. Using `ifconfig` on my device outputs the following:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 172.30.159.255
    inet6 fe80::215:5dff:fe66:8087 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:87 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 302 (302.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 900 (900.0 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 4 bytes 532 (532.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 532 (532.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

`eth0` is the primary WiFi interface on my device.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 172.30.159.255
    inet6 fe80::215:5dff:fe66:8087 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:87 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 302 (302.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 900 (900.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The rectangle highlights the `ipv4` address of the `eth0` network interface which is `172.30.159.31`.
(Note: I am using the college WiFi)

2. `ifconfig -a` command is used to display all interfaces even if they are down.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 172.30.159.255
    inet6 fe80::215:5dff:fe66:8087 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:87 txqueuelen 1000 (Ethernet)
    RX packets 24 bytes 3569 (3.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15 bytes 1082 (1.0 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 4 bytes 532 (532.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 532 (532.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Now we will down `eth0` using the command `sudo ifconfig eth0 down` and use `ifconfig -a` to check if the interface is down.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 down
[sudo] password for ritika:
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig -a
eth0: flags=4096<BROADCAST,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 172.30.159.255
    ether 00:15:5d:66:80:87 txqueuelen 1000 (Ethernet)
    RX packets 32 bytes 4275 (4.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 1152 (1.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Notice how `UP`, `RUNNING` is not displayed for `eth0` anymore.

4. Now we will bring `eth0` back up using the command `sudo ifconfig eth0 up` and use `ifconfig -a` to check if the interface is up.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 up
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 172.30.159.255
    inet6 fe80::215:5dff:fe66:8087 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:87 txqueuelen 1000 (Ethernet)
    RX packets 32 bytes 4275 (4.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 1668 (1.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Notice how `UP`, `RUNNING` is displayed for `eth0` again.

An interesting observation:

Although we brought the `eth0` interface up, the internet connection was not restored.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping 8.8.8.8
ping: connect: Network is unreachable
```

This is because it takes some time for the connection to be restored and since we brought the interface down

we need to restart our WSL to access internet again.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping 8.8.8.8
ping: connect: Network is unreachable
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ exit
logout
```

```
C:\Users\Ritika>wsl --shutdown
```

```
C:\Users\Ritika>wsl
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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=112 time=34.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=40.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=51.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=45.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=112 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=112 time=34.1 ms
|
```

5. We can change the IP address of our interface using the command

```
sudo ifconfig <interface_name> <new_ip_addr>
```

My current IP address is 172.30.159.31 and I changed it to 192.168.1.10 as shown below:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 192.168.1.10
[sudo] password for ritika:
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe66:80b5 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:b5 txqueuelen 1000 (Ethernet)
    RX packets 56 bytes 8118 (8.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 2496 (2.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

We can revert back to the original IP address using the same command.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 172.30.159.3
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.0.0 broadcast 172.30.255.255
    inet6 fe80::215:5dff:fe66:80b5 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:80:b5 txqueuelen 1000 (Ethernet)
    RX packets 87 bytes 14102 (14.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31 bytes 2566 (2.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Interesting note:

The IP address change affects the internet connection and we need to restart our WSL to access the internet again.

6. We can also change the subnet mask of our interface using the command

```
sudo ifconfig <interface_name> netmask <new_subnet_mask>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 172.30.159.3 netmask 255.255.240.0
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe66:8b5e prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:8b:5e txqueuelen 1000 (Ethernet)
    RX packets 297 bytes 287771 (287.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 148 bytes 49743 (49.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

7. We can also change the broadcast address of our interface using the command

```
sudo ifconfig <interface_name> broadcast <new_broadcast_addr>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 broadcast 192.168.1.255
[sudo] password for ritika:
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe66:8b5e prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:8b:5e txqueuelen 1000 (Ethernet)
    RX packets 297 bytes 287771 (287.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 148 bytes 49743 (49.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

8. We can also change the Maximum Transmission Unit (MTU) of our interface using the command

```
sudo ifconfig <interface_name> mtu <new_mtu>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo ifconfig eth0 mtu 1400
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1400
    inet 172.30.159.3 netmask 255.255.240.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe66:8b5e prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:66:8b:5e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5 bytes 398 (398.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

9. We can use `man ifconfig` to get more information about the `ifconfig`.

2. ping command:

ping or Packet Internet Groper is a network administration utility used to check the connectivity between two devices. It sends an ICMP echo request to a host and waits for an ICMP echo reply.

1. Using **ping** to check the connectivity between my device and www.google.com:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping 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=113 time=33.4 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=113 time=26.6 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=113 time=63.6 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=4 ttl=113 time=64.2 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=5 ttl=113 time=27.2 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=6 ttl=113 time=34.5 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=7 ttl=113 time=64.3 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 26.630/44.842/64.337/16.845 ms
```

The output shows that the packets are being sent and received successfully with 0% packet loss.

2. Transmitting a specific number of packets using

```
ping -c <number_of_packets> <host>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping -c 6 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=113 time=26.6 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=113 time=27.1 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=113 time=40.5 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=4 ttl=113 time=35.6 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=5 ttl=113 time=27.0 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=6 ttl=113 time=27.1 ms
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 26.576/30.658/40.530/5.433 ms
```

3. Setting the time interval between the packets using

```
ping -i <time_interval> <host>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping -i 5 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=113 time=26.4 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=113 time=26.7 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=113 time=46.6 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=4 ttl=113 time=27.9 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=5 ttl=113 time=45.3 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=6 ttl=113 time=42.9 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 25028ms
rtt min/avg/max/mdev = 26.394/35.967/46.582/9.045 ms
```

4. Setting the packet size using

```
ping -s <packet_size> <host>
```

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping -s 100 google.com
PING google.com (142.250.206.174) 100(128) bytes of data.
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=1 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=4 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=5 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=6 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=7 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=8 ttl=113 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=9 ttl=113 (truncated)
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 26.007/40.240/74.892/15.302 ms

```

5. We can specify the interface to be used for sending the packets using

```
ping -I <interface_name> <host>
```

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ ping -c 5 -I eth0 google.com
PING google.com (142.250.206.174) from 172.30.159.3 eth0: 56(84) bytes of data.
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=1 ttl=113 time=37.4 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=113 time=124 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=113 time=81.9 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=4 ttl=113 time=67.2 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=5 ttl=113 time=38.9 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 37.366/69.880/124.102/31.964 ms

```

3. **traceroute** command:

traceroute is used for tracing the full path from your local system to another network system. It shows the number of hops taken to reach the destination and the time taken for each hop. It sends an order of UDP packets, routes three packets of data to test each hop by default.

1. Using **traceroute** to trace the path to www.google.com:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ traceroute google.com
traceroute to google.com (142.250.206.174), 30 hops max, 60 byte packets
 1  DESKTOP-V520N37.mshome.net (172.30.144.1)  0.430 ms  0.401 ms  0.396 ms
 2  192.168.32.254 (192.168.32.254)  60.797 ms  61.303 ms  60.789 ms
 3  auth.iiitd.edu.in (192.168.1.99)  18.683 ms  18.680 ms  18.672 ms
 4  103.25.231.1 (103.25.231.1)  19.117 ms  19.114 ms  19.110 ms
 5  * * *
 6  10.119.234.162 (10.119.234.162)  19.301 ms  18.541 ms  18.532 ms
 7  72.14.194.160 (72.14.194.160)  18.536 ms  72.14.195.56 (72.14.195.56)  14.120 ms  14.107 ms
 8  192.178.80.159 (192.178.80.159)  37.167 ms  142.251.54.111 (142.251.54.111)  36.854 ms  192.178.80.159 (192.178.80.159)  37.207 ms
 9  142.251.76.203 (142.251.76.203)  37.313 ms  142.251.76.201 (142.251.76.201)  57.420 ms  142.251.76.203 (142.251.76.203)  36.939 ms
10  del11s22-in-f14.1e100.net (142.250.206.174)  33.643 ms  35.614 ms  27.304 ms
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$

```

The * * * most probably suggest that the specific organization does not want to reveal details of their internal network or there might be an overload.

2. To use ICMP echo requests instead of UDP packets, we can use

```
sudo traceroute -I <host>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo traceroute -I google.com
traceroute to google.com (142.250.206.174), 30 hops max, 60 byte packets
 1  DESKTOP-V520N37.mshome.net (172.30.144.1)  0.497 ms  0.482 ms  0.481 ms
 2  192.168.32.254 (192.168.32.254)  18.404 ms  *  *
 3  *  *  *
 4  *  *  *
 5  *  *  *
 6  10.119.234.162 (10.119.234.162)  5.693 ms  5.416 ms  5.409 ms
 7  72.14.195.56 (72.14.195.56)  5.558 ms  4.752 ms  5.211 ms
 8  142.251.54.111 (142.251.54.111)  28.619 ms  28.506 ms  28.375 ms
 9  142.251.76.203 (142.251.76.203)  26.573 ms  27.781 ms  27.709 ms
10  del11s22-in-f14.1e100.net (142.250.206.174)  27.352 ms  27.351 ms  27.350 ms
```

An increase in the number of hops giving * * * is observed when using ICMP echo requests.

Interestingly, using the command given in the tutorial slides

```
traceroute --type=icmp <host>
```

or

```
sudo traceroute --type=icmp <host>
```

did not work for my WSL and gave Bad Option.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ traceroute --type=icmp google.com
Bad option '--type=icmp' (with arg 'icmp') (argc 1)
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo traceroute --type=icmp google.com
Bad option '--type=icmp' (with arg 'icmp') (argc 1)
```

3. We can specify the maximum number of hops using

```
traceroute -m <max_hops> <host>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ sudo traceroute -m 5 google.com
traceroute to google.com (142.250.206.174), 5 hops max, 60 byte packets
 1  DESKTOP-V520N37.mshome.net (172.30.144.1)  0.366 ms  0.352 ms  0.408 ms
 2  192.168.32.254 (192.168.32.254)  17.725 ms  17.719 ms  17.715 ms
 3  vpn.iiitd.edu.in (192.168.1.99)  9.226 ms  9.223 ms  9.219 ms
 4  103.25.231.1 (103.25.231.1)  9.403 ms  9.216 ms  9.391 ms
 5  *  *  *
```

4. **netstat** command:

netstat or Network Statistics is used to display network connections, routing tables, interface statistics and masquerade connections.

1. Using `netstat` to display the routing table:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node  Path
unix  2      [ ]      DGRAM      0             17790    /var/run/chrony/chronyd.sock
unix  2      [ ]      DGRAM      0             20705    /run/user/1000/systemd/notify
unix  3      [ ]      DGRAM      CONNECTED    23584    /run/systemd/notify
unix  2      [ ]      DGRAM      0             23593    /run/systemd/journal/syslog
unix  9      [ ]      DGRAM      CONNECTED    23601    /run/systemd/journal/dev-log
unix  7      [ ]      DGRAM      CONNECTED    23603    /run/systemd/journal/socket
unix  3      [ ]      STREAM     CONNECTED    22545
unix  3      [ ]      STREAM     CONNECTED    20536
unix  3      [ ]      STREAM     CONNECTED    26752
unix  3      [ ]      STREAM     CONNECTED    18013    /tmp/.X11-unix/X0
unix  3      [ ]      STREAM     CONNECTED    21605
unix  2      [ ]      DGRAM      CONNECTED    23642
unix  2      [ ]      DGRAM      CONNECTED    17834
unix  3      [ ]      STREAM     CONNECTED    17896    /run/systemd/journal/stdout
unix  3      [ ]      STREAM     CONNECTED    18652
unix  2      [ ]      DGRAM      CONNECTED    25789
unix  3      [ ]      DGRAM      CONNECTED    19541
unix  3      [ ]      STREAM     CONNECTED    32
unix  3      [ ]      STREAM     CONNECTED    17941
unix  3      [ ]      STREAM     CONNECTED    66004    /run/systemd/journal/stdout
unix  3      [ ]      STREAM     CONNECTED    23777
unix  3      [ ]      STREAM     CONNECTED    20710
unix  3      [ ]      STREAM     CONNECTED    21650
unix  3      [ ]      STREAM     CONNECTED    17362    /run/systemd/journal/stdout
unix  3      [ ]      STREAM     CONNECTED    23780
unix  3      [ ]      DGRAM      CONNECTED    20707
unix  3      [ ]      STREAM     CONNECTED    48117    /run/dbus/system_bus_socket
unix  3      [ ]      STREAM     CONNECTED    66016
unix  3      [ ]      STREAM     CONNECTED    19644    /run/dbus/system_bus_socket
unix  3      [ ]      STREAM     CONNECTED    17811
unix  3      [ ]      STREAM     CONNECTED    22667    /run/dbus/system_bus_socket
unix  3      [ ]      STREAM     CONNECTED    22544
unix  3      [ ]      STREAM     CONNECTED    17930    /run/systemd/journal/stdout
unix  3      [ ]      STREAM     CONNECTED    22659    /run/dbus/system_bus_socket
unix  3      [ ]      STREAM     CONNECTED    17246

```



```

unix 2      [ ]          STREAM     CONNECTED   19507
unix 3      [ ]          STREAM     CONNECTED   66014
unix 3      [ ]          STREAM     CONNECTED   27671
unix 3      [ ]          STREAM     CONNECTED   23727
unix 3      [ ]          STREAM     CONNECTED   150
unix 2      [ ]          DGRAM       CONNECTED   18003
unix 2      [ ]          DGRAM       CONNECTED   19675
unix 3      [ ]          STREAM     CONNECTED   24693      /run/systemd/journal/stdout
unix 3      [ ]          STREAM     CONNECTED   17810
unix 3      [ ]          STREAM     CONNECTED   20538
unix 3      [ ]          STREAM     CONNECTED   23779
unix 3      [ ]          STREAM     CONNECTED   27723
unix 3      [ ]          STREAM     CONNECTED   20632      /run/systemd/journal/stdout
unix 3      [ ]          DGRAM       CONNECTED   23585
unix 3      [ ]          STREAM     CONNECTED   21647
unix 3      [ ]          STREAM     CONNECTED   74167
unix 3      [ ]          STREAM     CONNECTED   18016      /tmp/dbus-XC920eap3G
unix 3      [ ]          STREAM     CONNECTED   24712      /run/systemd/journal/stdout
unix 3      [ ]          STREAM     CONNECTED   22647
unix 2      [ ]          DGRAM       CONNECTED   74170
unix 3      [ ]          STREAM     CONNECTED   17955
unix 3      [ ]          STREAM     CONNECTED   17348      /run/systemd/journal/stdout
unix 2      [ ]          DGRAM       CONNECTED   139
unix 2      [ ]          DGRAM       CONNECTED   17944
unix 3      [ ]          STREAM     CONNECTED   20537
unix 2      [ ]          DGRAM       CONNECTED   19645
unix 3      [ ]          STREAM     CONNECTED   18591
unix 3      [ ]          STREAM     CONNECTED   19689      /run/dbus/system_bus_socket
unix 3      [ ]          STREAM     CONNECTED   19649      /run/dbus/system_bus_socket
unix 3      [ ]          STREAM     CONNECTED   19530
unix 3      [ ]          STREAM     CONNECTED   19648      /run/dbus/system_bus_socket
unix 3      [ ]          STREAM     CONNECTED   17359
unix 3      [ ]          STREAM     CONNECTED   23861      /mnt/wslg/PulseAudioRDPSSink
unix 2      [ ]          DGRAM       CONNECTED   25766
unix 3      [ ]          DGRAM       CONNECTED   19542
unix 3      [ ]          STREAM     CONNECTED   31
unix 3      [ ]          STREAM     CONNECTED   17363      /run/systemd/journal/stdout
unix 3      [ ]          STREAM     CONNECTED   27650
unix 3      [ ]          STREAM     CONNECTED   23860      /run/systemd/journal/stdout
unix 3      [ ]          STREAM     CONNECTED   20652

```

The routing table shows Protocol, Reference Count, Flags, Type of Service, State (in this case, all **CONNECTED**), I-Node and Path.

2. Using `netstat -a` to display all connections:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -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
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 (servers and established)
Proto RefCnt Flags   Type       State       I-Node      Path
unix  2      [ ACC ] STREAM    LISTENING   22551       /run/WSL/2_interop
unix  2      [ ACC ] STREAM    LISTENING   19495       /run/WSL/1_interop
unix  2      [ ACC ] STREAM    LISTENING    28          /var/run/dbus/system_bus_socket
unix  2      [ ACC ] SEQPACKET LISTENING   21518       /mnt/wslg/weston-notify.sock
unix  2      [ ACC ] STREAM    LISTENING   20655       /run/systemd/resolve/io.systemd.Resolve
unix  2      [ ACC ] STREAM    LISTENING   20494       /mnt/wslg/runtime-dir/wayland-0
unix  2      [ ACC ] STREAM    LISTENING   20495       /tmp/.X11-unix/X0
unix  2      [ ]      DGRAM     LISTENING   17790       /var/run/chrony/chronyd.sock
unix  2      [ ACC ] STREAM    LISTENING   20530       /mnt/wslg/runtime-dir/pulse/native
unix  2      [ ACC ] STREAM    LISTENING   22678       /mnt/wslg/PulseAudioRDPSSource
unix  2      [ ACC ] STREAM    LISTENING   26749       /mnt/wslg/PulseAudioRDPSSink
unix  2      [ ]      DGRAM     LISTENING   20705       /run/user/1000/systemd/notify
unix  2      [ ACC ] STREAM    LISTENING   20708       /run/user/1000/systemd/private
unix  2      [ ACC ] STREAM    LISTENING   17807       /tmp/dbus-XC920eap3G
unix  2      [ ACC ] STREAM    LISTENING   20714       /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ] STREAM    LISTENING   20716       /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ] STREAM    LISTENING   20718       /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ] STREAM    LISTENING   20720       /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ] STREAM    LISTENING   20722       /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ] STREAM    LISTENING   20724       /run/user/1000/pk-debconf-socket

```

unix	9	[]	DGRAM	CONNECTED	23601	/run/systemd/journal/dev-log
unix	7	[]	DGRAM	CONNECTED	23603	/run/systemd/journal/socket
unix	2	[ACC]	STREAM	LISTENING	23605	/run/systemd/journal/stdout
unix	2	[ACC]	SEQPACKET	LISTENING	23607	/run/udev/control
unix	2	[ACC]	STREAM	LISTENING	27733	/mnt/wslg/PulseServer
unix	2	[ACC]	STREAM	LISTENING	18656	/run/subiquity/socket
unix	2	[ACC]	STREAM	LISTENING	17830	/run/systemd/journal/io.systemd.journal
unix	2	[ACC]	STREAM	LISTENING	23708	/run/apport.socket
unix	2	[ACC]	STREAM	LISTENING	23710	/run/dbus/system_bus_socket
unix	2	[ACC]	STREAM	LISTENING	23712	/run/snapd.socket
unix	2	[ACC]	STREAM	LISTENING	23714	/run/snapd-snap.socket
unix	2	[ACC]	STREAM	LISTENING	23716	/run/uuid/request
unix	3	[]	STREAM	CONNECTED	22545	
unix	3	[]	STREAM	CONNECTED	20536	
unix	3	[]	STREAM	CONNECTED	26752	
unix	3	[]	STREAM	CONNECTED	18013	/tmp/.X11-unix/X0
unix	3	[]	STREAM	CONNECTED	21605	
unix	2	[]	DGRAM	CONNECTED	23642	
unix	2	[]	DGRAM	CONNECTED	17834	
unix	3	[]	STREAM	CONNECTED	17896	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	18652	
unix	2	[]	DGRAM	CONNECTED	25789	
unix	3	[]	DGRAM	CONNECTED	19541	
unix	3	[]	STREAM	CONNECTED	32	
unix	3	[]	STREAM	CONNECTED	17941	
unix	3	[]	STREAM	CONNECTED	66004	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	23777	
unix	3	[]	STREAM	CONNECTED	20710	
unix	3	[]	STREAM	CONNECTED	21650	
unix	3	[]	STREAM	CONNECTED	17362	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	23780	
unix	3	[]	DGRAM	CONNECTED	20707	
unix	3	[]	STREAM	CONNECTED	48117	/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	66016	
unix	3	[]	STREAM	CONNECTED	19644	/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	17811	
unix	3	[]	STREAM	CONNECTED	22667	/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22544	
unix	3	[]	STREAM	CONNECTED	17930	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	22659	/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	17246	

`netstat -a` displays all connections and **LISTENING** ports.

3. Using `netstat -t` to display TCP connections:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -t
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
```

Notice how there are no active connections in the TCP table but listening ports are available.

4. Using `netstat -u` to display UDP connections:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -u
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:*               LISTEN
udp      0      0 10.255.255.254:domain   0.0.0.0:*               LISTEN
udp      0      0 localhost:323            0.0.0.0:*               LISTEN
udp6     0      0 ip6-localhost:323       [::]:*                  LISTEN
```

Similar to the TCP table, there are no active connections in the UDP table but listening ports are available.

5. Using `netstat -p` to display the process ID of the connections:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node  PID/Program name  Path
unix  2      [ ]     DGRAM      -             17790    -                 /var/run/chrony/chronyd.sock
unix  2      [ ]     DGRAM      -             20705    386/systemd       /run/user/1000/systemd/notify
unix  3      [ ]     DGRAM      CONNECTED     23584    -                 /run/systemd/notify
unix  2      [ ]     DGRAM      -             23593    -                 /run/systemd/journal/syslog
unix  9      [ ]     DGRAM      CONNECTED     23601    -                 /run/systemd/journal/dev-log
unix  7      [ ]     DGRAM      CONNECTED     23603    -                 /run/systemd/journal/socket
unix  3      [ ]     STREAM     CONNECTED     22545    -
unix  3      [ ]     STREAM     CONNECTED     20536    -
unix  3      [ ]     STREAM     CONNECTED     26752    -
unix  3      [ ]     STREAM     CONNECTED     18013    -                 /tmp/.X11-unix/X0
unix  3      [ ]     STREAM     CONNECTED     21605    -
unix  2      [ ]     DGRAM      CONNECTED     23642    -
unix  2      [ ]     DGRAM      CONNECTED     17834    -
unix  3      [ ]     STREAM     CONNECTED     17896    -                 /run/systemd/journal/stdout
unix  3      [ ]     STREAM     CONNECTED     18652    -
unix  2      [ ]     DGRAM      CONNECTED     25789    -
unix  3      [ ]     DGRAM      CONNECTED     19541    -
unix  3      [ ]     STREAM     CONNECTED     32        -
unix  3      [ ]     STREAM     CONNECTED     17941    -
unix  3      [ ]     STREAM     CONNECTED     66004    -                 /run/systemd/journal/stdout
unix  3      [ ]     STREAM     CONNECTED     23777    -
unix  3      [ ]     STREAM     CONNECTED     20710    386/systemd
unix  3      [ ]     STREAM     CONNECTED     21650    -
unix  3      [ ]     STREAM     CONNECTED     17362    -                 /run/systemd/journal/stdout
unix  3      [ ]     STREAM     CONNECTED     23780    -
unix  3      [ ]     DGRAM      CONNECTED     20707    386/systemd
unix  3      [ ]     STREAM     CONNECTED     48117    -                 /run/dbus/system_bus_socket
unix  3      [ ]     STREAM     CONNECTED     66016    -
unix  3      [ ]     STREAM     CONNECTED     19644    -                 /run/dbus/system_bus_socket
unix  3      [ ]     STREAM     CONNECTED     17811    -
unix  3      [ ]     STREAM     CONNECTED     22667    -                 /run/dbus/system_bus_socket
unix  3      [ ]     STREAM     CONNECTED     22544    -
unix  3      [ ]     STREAM     CONNECTED     17930    -                 /run/systemd/journal/stdout
unix  3      [ ]     STREAM     CONNECTED     22659    -                 /run/dbus/system_bus_socket

```

```

unix 3 [ ] STREAM CONNECTED 20583 -
unix 3 [ ] DGRAM CONNECTED 20706 386/systemd
unix 2 [ ] DGRAM CONNECTED 19683 386/systemd
unix 2 [ ] STREAM CONNECTED 19507 -
unix 3 [ ] STREAM CONNECTED 66014 -
unix 3 [ ] STREAM CONNECTED 27671 -
unix 3 [ ] STREAM CONNECTED 23727 -
unix 3 [ ] STREAM CONNECTED 150 -
unix 2 [ ] DGRAM CONNECTED 18003 -
unix 2 [ ] DGRAM CONNECTED 19675 -
unix 3 [ ] STREAM CONNECTED 24693 - /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 17810 -
unix 3 [ ] STREAM CONNECTED 20538 -
unix 3 [ ] STREAM CONNECTED 23779 -
unix 3 [ ] STREAM CONNECTED 27723 386/systemd
unix 3 [ ] STREAM CONNECTED 20632 - /run/systemd/journal/stdout
unix 3 [ ] DGRAM CONNECTED 23585 -
unix 3 [ ] STREAM CONNECTED 21647 -
unix 3 [ ] STREAM CONNECTED 74167 -
unix 3 [ ] STREAM CONNECTED 18016 - /tmp/dbus-XC920eap3G
unix 3 [ ] STREAM CONNECTED 24712 - /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 22647 -
unix 2 [ ] DGRAM CONNECTED 74170 -
unix 3 [ ] STREAM CONNECTED 17955 -
unix 3 [ ] STREAM CONNECTED 17348 - /run/systemd/journal/stdout
unix 2 [ ] DGRAM CONNECTED 139 -
unix 2 [ ] DGRAM CONNECTED 17944 -
unix 3 [ ] STREAM CONNECTED 20537 -
unix 2 [ ] DGRAM CONNECTED 19645 -
unix 3 [ ] STREAM CONNECTED 18591 -
unix 3 [ ] STREAM CONNECTED 19689 - /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 19649 - /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 19530 -
unix 3 [ ] STREAM CONNECTED 19648 - /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 17359 -
unix 3 [ ] STREAM CONNECTED 23861 - /mnt/wslg/PulseAudioRDPSSink
unix 2 [ ] DGRAM CONNECTED 25766 -
unix 3 [ ] DGRAM CONNECTED 19542 -
unix 3 [ ] STREAM CONNECTED 31 -
unix 3 [ ] STREAM CONNECTED 17363 - /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 27650 -

```

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -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 (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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 (servers and established)
Proto RefCnt Flags       Type       State      I-Node   PID/Program name  Path
unix   2      [ ACC ] STREAM    LISTENING  22551     -                 /run/WSL/2_interop
unix   2      [ ACC ] STREAM    LISTENING  19495     -                 /run/WSL/1_interop
unix   2      [ ACC ] STREAM    LISTENING  28        -                 /var/run/dbus/system_bus_socket
unix   2      [ ACC ] SEQPACKET LISTENING  21518     -                 /mnt/wslg/weston-notify.sock
unix   2      [ ACC ] STREAM    LISTENING  20655     -                 /run/systemd/resolve/io.systemd.Resolve
unix   2      [ ACC ] STREAM    LISTENING  20494     -                 /mnt/wslg/runtime-dir/wayland-0
unix   2      [ ACC ] STREAM    LISTENING  20495     -                 /tmp/.X11-unix/X0
unix   2      [ ]        DGRAM     17790     -                 /var/run/chrony/chronyd.sock
unix   2      [ ACC ] STREAM    LISTENING  20530     -                 /mnt/wslg/runtime-dir/pulse/native
unix   2      [ ACC ] STREAM    LISTENING  22678     -                 /mnt/wslg/PulseAudioRDPSource
unix   2      [ ACC ] STREAM    LISTENING  26749     -                 /mnt/wslg/PulseAudioRDPSSink
unix   2      [ ]        DGRAM     20705     386/systemd        /run/user/1000/systemd/notify
unix   2      [ ACC ] STREAM    LISTENING  20708     386/systemd        /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM    LISTENING  17807     -                 /tmp/dbus-XC920eap3G
unix   2      [ ACC ] STREAM    LISTENING  20714     386/systemd        /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ] STREAM    LISTENING  20716     386/systemd        /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ] STREAM    LISTENING  20718     386/systemd        /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ] STREAM    LISTENING  20720     386/systemd        /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ] STREAM    LISTENING  20722     386/systemd        /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ] STREAM    LISTENING  20724     386/systemd        /run/user/1000/pk-debconf-socket
unix   2      [ ACC ] STREAM    LISTENING  20726     386/systemd        /run/user/1000/snapd-session-agent.socket
unix   3      [ ]        DGRAM     23584     -                 /run/systemd/notify
unix   2      [ ACC ] STREAM    LISTENING  23587     -                 /run/systemd/private
unix   2      [ ACC ] STREAM    LISTENING  23589     -                 /run/systemd/userdb/io.systemd.DynamicUser
unix   2      [ ACC ] STREAM    LISTENING  25781     -                 /run/WSL/350_interop
unix   2      [ ACC ] STREAM    LISTENING  23590     -                 /run/systemd/io.system.ManagedOOM

```

6. Using `netstat -r` to display the kernel routing table:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags       MSS  Window  irtt  Iface
default          DESKTOP-V520N37 0.0.0.0         UG          0 0        0     eth0
172.30.144.0     0.0.0.0         255.255.240.0   U           0 0        0     eth0
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags       MSS  Window  irtt  Iface
default          DESKTOP-V520N37 0.0.0.0         UG          0 0        0     eth0
172.30.144.0     0.0.0.0         255.255.240.0   U           0 0        0     eth0
```

The routing table shows Destination, Gateway, Genmask, Flags, MSS, Window, IRTT and Interface.

7. Using `netstat -i` to display the network interfaces:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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     1500    3415   0      0 0      2278   0      0      0 BMRU
lo       65536   272    0      0 0      272    0      0      0 LRU
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -i
Kernel Interface table
Iface    MTU     RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0     1500    3415   0      0 0      2278   0      0      0 BMRU
lo       65536   272    0      0 0      272    0      0      0 LRU
```

The network interfaces table shows Kernel Interface, MTU, Met, RX-OK, RX-ERR, RX-DRP, RX-OVR, TX-OK, TX-ERR, TX-DRP, TX-OVR and Flags. What this means:

- **RX-OK** is the number of packets received without errors.
- **RX-ERR** is the number of packets received with errors.
- **RX-DRP** is the number of packets dropped.
- **RX-OVR** is the number of packets received but the buffer was full.
- **TX-OK** is the number of packets transmitted without errors.
- **TX-ERR** is the number of packets transmitted with errors.
- **TX-DRP** is the number of packets dropped.
- **TX-OVR** is the number of packets transmitted but the buffer was full.

8. Using `netstat -l` to display only listening ports:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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        22551  /run/WSL/2_interop
unix   2      [ ACC ] STREAM            LISTENING        19495  /run/WSL/1_interop
unix   2      [ ACC ] STREAM            LISTENING        28     /var/run/dbus/system_bus_socket
unix   2      [ ACC ] SEQPACKET         LISTENING        21518  /mnt/wslg/weston-notify.sock
unix   2      [ ACC ] STREAM            LISTENING        20655  /run/systemd/resolve/io.systemd.Resolve
unix   2      [ ACC ] STREAM            LISTENING        20494  /mnt/wslg/runtime-dir/wayland-0
unix   2      [ ACC ] STREAM            LISTENING        20495  /tmp/.X11-unix/X0
unix   2      [ ACC ] STREAM            LISTENING        20530  /mnt/wslg/runtime-dir/pulse/native
unix   2      [ ACC ] STREAM            LISTENING        22678  /mnt/wslg/PulseAudioRDPSource
unix   2      [ ACC ] STREAM            LISTENING        26749  /mnt/wslg/PulseAudioRDPSink
unix   2      [ ACC ] STREAM            LISTENING        20708  /run/user/1000/systemd/private
unix   2      [ ACC ] STREAM            LISTENING        17807  /tmp/dbus-XC920eap3G
unix   2      [ ACC ] STREAM            LISTENING        20714  /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ] STREAM            LISTENING        20716  /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ] STREAM            LISTENING        20718  /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ] STREAM            LISTENING        20720  /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ] STREAM            LISTENING        20722  /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ] STREAM            LISTENING        20724  /run/user/1000/pk-debconf-socket
unix   2      [ ACC ] STREAM            LISTENING        20726  /run/user/1000/snapd-session-agent.socket
unix   2      [ ACC ] STREAM            LISTENING        23587  /run/systemd/private
unix   2      [ ACC ] STREAM            LISTENING        23589  /run/systemd/userdb/io.systemd.DynamicUser
unix   2      [ ACC ] STREAM            LISTENING        25781  /run/WSL/350_interop
unix   2      [ ACC ] STREAM            LISTENING        23590  /run/systemd/io.system.ManagedOOM
unix   2      [ ACC ] STREAM            LISTENING        23605  /run/systemd/journal/stdout
unix   2      [ ACC ] SEQPACKET         LISTENING        23607  /run/udev/control
unix   2      [ ACC ] STREAM            LISTENING        27733  /mnt/wslg/PulseServer
unix   2      [ ACC ] STREAM            LISTENING        18656  /run/subiquity/socket
unix   2      [ ACC ] STREAM            LISTENING        17830  /run/systemd/journal/io.systemd.journal

```

However, using `netstat -a -l` displays all connections and listening ports.

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ netstat -a -l
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
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 (servers and established)
Proto RefCnt Flags               Type               State         I-Node  Path
unix   2      [ ACC ]                STREAM            LISTENING      22551    /run/WSL/2_interop
unix   2      [ ACC ]                STREAM            LISTENING      19495    /run/WSL/1_interop
unix   2      [ ACC ]                STREAM            LISTENING       28       /var/run/dbus/system_bus_socket
unix   2      [ ACC ]                SEQPACKET         LISTENING     21518    /mnt/wslg/weston-notify.sock
unix   2      [ ACC ]                STREAM            LISTENING     20655    /run/systemd/resolve/io.systemd.Resolve
unix   2      [ ACC ]                STREAM            LISTENING     20494    /mnt/wslg/runtime-dir/wayland-0
unix   2      [ ACC ]                STREAM            LISTENING     20495    /tmp/.X11-unix/X0
unix   2      [ ]                DGRAM             17790    /var/run/chrony/chronyd.sock
unix   2      [ ACC ]                STREAM            LISTENING     20530    /mnt/wslg/runtime-dir/pulse/native
unix   2      [ ACC ]                STREAM            LISTENING     22678    /mnt/wslg/PulseAudioRDPSource
unix   2      [ ACC ]                STREAM            LISTENING     26749    /mnt/wslg/PulseAudioRDPSSink
unix   2      [ ]                DGRAM             20705    /run/user/1000/systemd/notify
unix   2      [ ACC ]                STREAM            LISTENING     20708    /run/user/1000/systemd/private
unix   2      [ ACC ]                STREAM            LISTENING     17807    /tmp/dbus-XC920eap3G
unix   2      [ ACC ]                STREAM            LISTENING     20714    /run/user/1000/gnupg/S.dirmngr
unix   2      [ ACC ]                STREAM            LISTENING     20716    /run/user/1000/gnupg/S.gpg-agent.browser
unix   2      [ ACC ]                STREAM            LISTENING     20718    /run/user/1000/gnupg/S.gpg-agent.extra
unix   2      [ ACC ]                STREAM            LISTENING     20720    /run/user/1000/gnupg/S.gpg-agent.ssh
unix   2      [ ACC ]                STREAM            LISTENING     20722    /run/user/1000/gnupg/S.gpg-agent
unix   2      [ ACC ]                STREAM            LISTENING     20724    /run/user/1000/pk-debconf-socket
unix   2      [ ACC ]                STREAM            LISTENING     20726    /run/user/1000/snapd-session-agent.socket
unix   3      [ ]                DGRAM             23584    /run/systemd/notify
unix   2      [ ACC ]                STREAM            LISTENING     23587    /run/systemd/private
unix   2      [ ACC ]                STREAM            LISTENING     23589    /run/systemd/userdb/io.systemd.DynamicUser
unix   2      [ ACC ]                STREAM            LISTENING     25781    /run/WSL/350_interop
unix   2      [ ACC ]                STREAM            LISTENING     23590    /run/systemd/io.system.ManagedOOM
unix   2      [ ]                DGRAM             23593    /run/systemd/journal/syslog
unix   9      [ ]                DGRAM             23601    /run/systemd/journal/dev-log
unix   7      [ ]                DGRAM             23603    /run/systemd/journal/socket

unix   2      [ ACC ]                STREAM            LISTENING     25781    /run/WSL/350_interop
unix   2      [ ACC ]                STREAM            LISTENING     23590    /run/systemd/io.system.ManagedOOM
unix   2      [ ]                DGRAM             23593    /run/systemd/journal/syslog
unix   9      [ ]                DGRAM             23601    /run/systemd/journal/dev-log
unix   7      [ ]                DGRAM             23603    /run/systemd/journal/socket
unix   2      [ ACC ]                STREAM            LISTENING     23605    /run/systemd/journal/stdout
unix   2      [ ACC ]                SEQPACKET         LISTENING     23607    /run/udev/control
unix   2      [ ACC ]                STREAM            LISTENING     27733    /mnt/wslg/PulseServer
unix   2      [ ACC ]                STREAM            LISTENING     18656    /run/subiquity/socket
unix   2      [ ACC ]                STREAM            LISTENING     17830    /run/systemd/journal/io.systemd.journal
unix   2      [ ACC ]                STREAM            LISTENING     23708    /run/apport.socket
unix   2      [ ACC ]                STREAM            LISTENING     23710    /run/dbus/system_bus_socket
unix   2      [ ACC ]                STREAM            LISTENING     23712    /run/snapd.socket
unix   2      [ ACC ]                STREAM            LISTENING     23714    /run/snapd-snap.socket
unix   2      [ ACC ]                STREAM            LISTENING     23716    /run/uuid/request
unix   3      [ ]                STREAM            CONNECTED     22545
unix   3      [ ]                STREAM            CONNECTED     20536
unix   3      [ ]                STREAM            CONNECTED     26752
unix   3      [ ]                STREAM            CONNECTED     18013    /tmp/.X11-unix/X0
unix   3      [ ]                STREAM            CONNECTED     21605
unix   2      [ ]                DGRAM             23642
unix   2      [ ]                DGRAM             17834
unix   3      [ ]                STREAM            CONNECTED     17896    /run/systemd/journal/stdout
unix   3      [ ]                STREAM            CONNECTED     18652
unix   2      [ ]                DGRAM             25789
unix   3      [ ]                DGRAM             19541
unix   3      [ ]                STREAM            CONNECTED     32
unix   3      [ ]                STREAM            CONNECTED     17941
unix   3      [ ]                STREAM            CONNECTED     66004    /run/systemd/journal/stdout
unix   3      [ ]                STREAM            CONNECTED     23777
unix   3      [ ]                STREAM            CONNECTED     20710
unix   3      [ ]                STREAM            CONNECTED     21650
unix   3      [ ]                STREAM            CONNECTED     17362    /run/systemd/journal/stdout
unix   3      [ ]                STREAM            CONNECTED     23780
unix   3      [ ]                DGRAM             20707
unix   3      [ ]                STREAM            CONNECTED     48117    /run/dbus/system_bus_socket
unix   3      [ ]                STREAM            CONNECTED     66016
unix   3      [ ]                STREAM            CONNECTED     19644    /run/dbus/system_bus_socket
unix   3      [ ]                STREAM            CONNECTED     17811
unix   3      [ ]                STREAM            CONNECTED     22667    /run/dbus/system_bus_socket
unix   3      [ ]                STREAM            CONNECTED     22544

```

5. nslookup command:

nslookup or Name Server Lookup is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping or other DNS records.

1. Using **nslookup** to query the IP address of www.google.com:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup google.com
Server:          10.255.255.254
Address:         10.255.255.254#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.206.174
Name:   google.com
Address: 2404:6800:4002:82d::200e
```

The address changes when we query **nslookup** for www.google.in.

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup google.in
Server:          10.255.255.254
Address:         10.255.255.254#53

Non-authoritative answer:
Name:   google.in
Address: 142.250.192.228
Name:   google.in
Address: 2404:6800:4002:818::2004
```

2. Using **nslookup** to query the domain name of www.github.com:

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup github.com
Server:          10.255.255.254
Address:         10.255.255.254#53

Non-authoritative answer:
Name:   github.com
Address: 20.207.73.82

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup 20.207.73.82
** server can't find 82.73.207.20.in-addr.arpa: NXDOMAIN
```

However, doing reverse lookup using the IP address of www.github.com does not give the domain name. So, we try to get an authoritative answer using the command

```
nslookup -type=ns <host>
```

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup -type=ns github.com
Server:          10.255.255.254
Address:         10.255.255.254#53

Non-authoritative answer:
github.com       nameserver = ns-520.awsdns-01.net.
github.com       nameserver = ns-421.awsdns-52.com.
github.com       nameserver = ns-1707.awsdns-21.co.uk.
github.com       nameserver = ns-1283.awsdns-32.org.
github.com       nameserver = dns1.p08.nsone.net.
github.com       nameserver = dns2.p08.nsone.net.
github.com       nameserver = dns3.p08.nsone.net.
github.com       nameserver = dns4.p08.nsone.net.

Authoritative answers can be found from:
ns-421.awsdns-52.com    internet address = 205.251.193.165

```

Now, doing reverse lookup directly on the address still gives no answer. But doing the same using the address name successfully gives the domain name.

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup 205.251.193.165
165.193.251.205.in-addr.arpa    name = ns-421.awsdns-52.com.

Authoritative answers can be found from:

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup github.com ns-421.awsdns-52.com
Server:          ns-421.awsdns-52.com
Address:         205.251.193.165#53

Name:   github.com
Address: 20.207.73.82

```

3. We can also query a specific DNS server using the command

```
nslookup <host> <dns_server>
```

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup www.meta.com 8.8.8.8
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
www.meta.com     canonical name = star.c10r.facebook.com.
Name:   star.c10r.facebook.com
Address: 163.70.144.8
Name:   star.c10r.facebook.com
Address: 2a03:2880:f0a4:109:face:b00c:0:2

```

Here we try to query www.meta.com using 8.8.8.8 as the DNS server.

Trying to perform a similar query using 1.1.1.1 as the DNS server gives an error because the DNS server is not reachable.

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup github.com 8.8.8.8
Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
Name:   github.com
Address: 20.207.73.82

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nslookup github.com 1.1.1.1
;; communications error to 1.1.1.1#53: timed out
;; communications error to 1.1.1.1#53: timed out
;; communications error to 1.1.1.1#53: timed out
;; no servers could be reached

```

6. **dig** command:

dig or Domain Information Groper is a network administration command-line tool for querying Domain Name System (DNS) name servers, mostly for troubleshooting DNS problems.

1. Using **dig** to query the IP address of www.google.com:

```

ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ dig www.google.com

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30880
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;; udp: 4000
;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                126     IN      A      142.250.182.164

;; Query time: 9 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Wed Aug 21 22:59:40 IST 2024
;; MSG SIZE rcvd: 59

```

. In the output, we can see the IP address of www.google.com and the time taken to query the DNS server, as well as date, message size, flags, query time, server, when the query was received, the answer section, authority section and additional section. Answer section gives the IP address of www.google.com. Authority section gives the name servers for google.com. Additional section gives the IP address of the name servers.

2. Using MX record to query the mail servers of [google.com](https://www.google.com):

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ dig www.google.com MX
; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> www.google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17266
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.google.com.                IN      MX
;; AUTHORITY SECTION:
google.com.                     26      IN      SOA     ns1.google.com. dns-admin.google.com. 665267952 900 900 1800 60
;; Query time: 29 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Wed Aug 21 23:00:24 IST 2024
;; MSG SIZE rcvd: 93
```

Mail servers are basically the servers that receive and send emails.

3. We can also query a specific DNS server using the command

```
dig @<dns_server> <host>
```

```
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ dig @8.8.8.8 twitter.com
; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @8.8.8.8 twitter.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13282
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;twitter.com.                IN      A
;; ANSWER SECTION:
twitter.com.                 1543    IN      A       104.244.42.129
;; Query time: 59 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Aug 21 23:03:11 IST 2024
;; MSG SIZE rcvd: 56
```

This command was used to query www.twitter.com using 8.8.8.8 as the DNS server.

7. **netcat** command:

netcat is a simple Unix utility that reads and writes data across network connections using the TCP or UDP protocol. It is also known as the TCP/IP swiss army knife. It is like WhatsApp for the command line. Here is a simple example of me establishing a connection between two terminals on my device using **netcat** in a way

that whatever is typed in the first terminal is displayed in the second terminal.

```

ritika@DESKTOP-V520N37: /n  X  +  v
* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/pro

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/ritika/.hushlogin file.
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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=52 time=7.96 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=11.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=7.14 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.144/8.824/11.374/1.832 ms
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nc -lv 8080
Listening on 0.0.0.0 8080
Connection received on localhost 60340
Hello
World
^C
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$

ritika@DESKTOP-V520N37: /n  X  +  v
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.153.1-microsoft-standard-W
SL2 x86_64)

* Documentation: https://help.ubuntu.com
* Management:   https://landscape.canonical.com
* Support:      https://ubuntu.com/pro

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/ritika/.hushlogin file.
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ 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=52 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=8.19 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 8.185/9.381/10.577/1.196 ms
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$ nc -v 0.0.0.0 8080
Connection to 0.0.0.0 8080 port [tcp/http-alt] succeeded!
Hello
World
^C
ritika@DESKTOP-V520N37:/mnt/c/Users/Ritika$

```

Overall,

we were able to learn about the basic Linux command line utilities and their usage. We also learned how to change the IP address, subnet mask, broadcast address and MTU of a network interface using **ifconfig**. We learned how to check the connectivity between two devices using **ping**, trace the path to a network system using **traceroute**, display network connections, routing tables, interface statistics and masquerade connections using **netstat**, query the Domain Name System (DNS) to obtain domain name or IP address mapping or other DNS records using **nslookup** and **dig** and establish a connection between two terminals using **netcat**.