Lab 3

Dhruv Patel (B18CSE012)

Q1) *ifconfig*

a. Ifconfig is used to show the all the network configuration info of the system, enable or disable network interfaces and changing them (eg. setting ip address or netmask to a network interface, like for a docker0 network; or setting up hardware address)
b. My PC has 13 network interfaces out of which 11 ar active

```
//Active Interfaces [ ifconfig ]
br-2049ad9528b1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
br-b83b9f551781: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
vethb2c25aa: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
vethd788504: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
virbr0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
virbr1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
vnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
vnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
wlp59s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500

//Inactive Interfaces [ diff <(ifconfig) <(ifconfig -a) ]
virbr1-nic: flags=4098<BROADCAST,MULTICAST>  mtu 1500
virbr0-nic: flags=4098<BROADCAST,MULTICAST>  mtu 1500
```

c. The WiFi interface has an interface name `wlp59s0`. We can change the ip address using *ifconfig* using sudo `ifconfig wlp59s0 <ip address>`.
d. A Virtual IP address (VIP/VIPA) is an IP address that doesn't have any physical network interface. It eliminates hosts dependency upon individual network interfaces, when they fail or the interface connection was lost.
To add a Virtual IP run : `ifconfig <interface>:<n> <VIPA>` .

```
dell@dell-XPS-15-9570: ~
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp59s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.107  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::c142:1d55:d81a:9f15  prefixlen 64  scopeid 0x20<link>
        ether 9c:b6:d0:be:2e:fb  txqueuelen 1000  (Ethernet)
        RX packets 4229161  bytes 3721960225 (3.7 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1956030  bytes 520598832 (520.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp59s0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.10  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 9c:b6:d0:be:2e:fb  txqueuelen 1000  (Ethernet)

wlp59s0:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.11  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 9c:b6:d0:be:2e:fb  txqueuelen 1000  (Ethernet)

wlp59s0:3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.12  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 9c:b6:d0:be:2e:fb  txqueuelen 1000  (Ethernet)

dell@dell-XPS-15-9570:~$
```

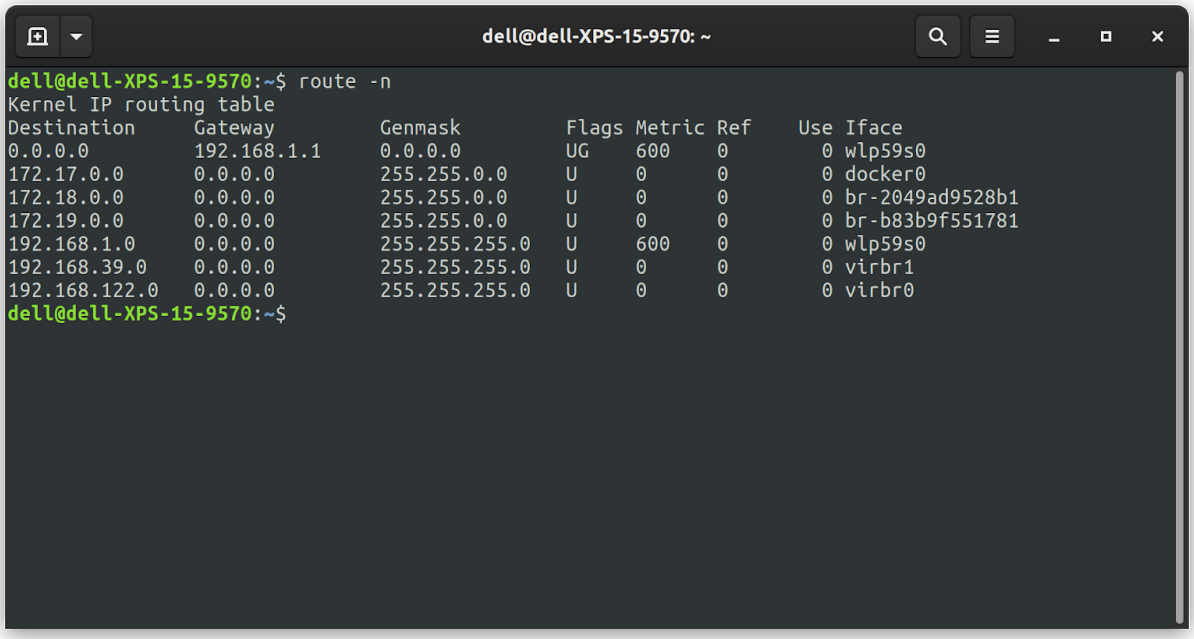
2) Route command

a. *route* command is used to view and manipulate the IP routing table.
b. It displays the IP routing table.

```
dell@dell-XPS-15-9570: ~
dell@dell-XPS-15-9570:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp59s0
10.0.0.0        0.0.0.0         255.0.0.0       U     0      0        0 wlp59s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 virbr1
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-2049ad9528b1
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-b83b9f551781
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp59s0
192.168.39.0    0.0.0.0         255.255.255.0   U     0      0        0 virbr1
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
dell@dell-XPS-15-9570:~$
```

Destination specifies the address of the network that the packet goes to.
Gnemask defines the subnet mask, to determine the destination subnet
Interface defines the which network interface (wifi card, LAN etc) it uses
Gateway defines the IP address through which the packets will be send to destination
Metric tells the cost to send the package in integer to calculate the fastest, most reliable route.
The flags define the state of the route (like if its up, down, modified, is leading to a gateway)

c. `Route -n` give us the gateway address for wlp59s : **192.168.1.1**

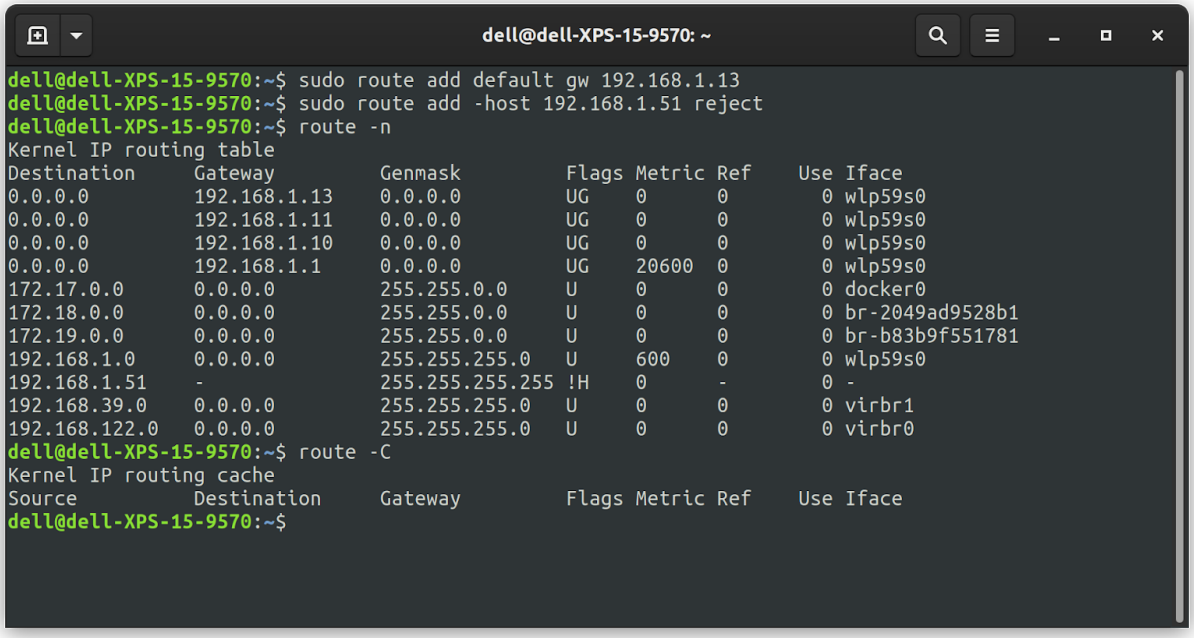


d.

Route add default gw <address>: Reassign the default gateway to use when packets don't belong to a network

Route -Cn : Get the cache of the routing table saved by the kernel

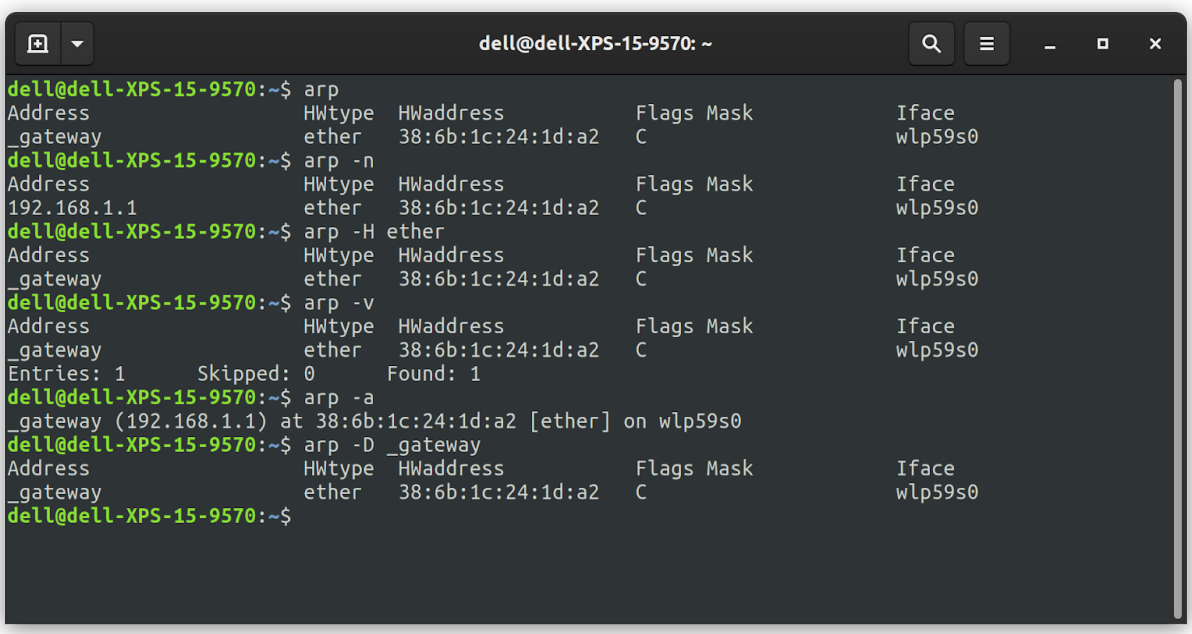
Route add -host <address> reject: Rejecting routing to a particular network



```
dell@dell-XPS-15-9570: ~
dell@dell-XPS-15-9570:~$ sudo route add default gw 192.168.1.13
dell@dell-XPS-15-9570:~$ sudo route add -host 192.168.1.51 reject
dell@dell-XPS-15-9570:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.13    0.0.0.0         UG    0      0        0 wlp59s0
0.0.0.0         192.168.1.11    0.0.0.0         UG    0      0        0 wlp59s0
0.0.0.0         192.168.1.10    0.0.0.0         UG    0      0        0 wlp59s0
0.0.0.0         192.168.1.1     0.0.0.0         UG    20600  0        0 wlp59s0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-2049ad9528b1
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-b83b9f551781
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp59s0
192.168.1.51    -               255.255.255.255 !H    0      -        0 -
192.168.39.0    0.0.0.0         255.255.255.0   U     0      0        0 virbr1
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
dell@dell-XPS-15-9570:~$ route -C
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
dell@dell-XPS-15-9570:~$
```

Q3) Address Resolution Protocol

a.



```
dell@dell-XPS-15-9570: ~
dell@dell-XPS-15-9570:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   38:6b:1c:24:1d:a2   C                     wlp59s0
dell@dell-XPS-15-9570:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   38:6b:1c:24:1d:a2   C                     wlp59s0
dell@dell-XPS-15-9570:~$ arp -H ether
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   38:6b:1c:24:1d:a2   C                     wlp59s0
dell@dell-XPS-15-9570:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   38:6b:1c:24:1d:a2   C                     wlp59s0
Entries: 1      Skipped: 0      Found: 1
dell@dell-XPS-15-9570:~$ arp -a
_gateway (192.168.1.1) at 38:6b:1c:24:1d:a2 [ether] on wlp59s0
dell@dell-XPS-15-9570:~$ arp -D _gateway
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   38:6b:1c:24:1d:a2   C                     wlp59s0
dell@dell-XPS-15-9570:~$
```

b. arp only shows the local MAC address, i.e. only within the small group of computers on a LAN and not the internet. So no, it wont be able to tell the MAC

address of www.google.com.

4) *arping* (ARP Ping)

1. Arping is used to send a ARP request to a neighbouring host/local hosts.
2. Ping sends ICMP requests to network hosts while arping sends ARP requests to local hosts.

5) netstat (Network Statistics)

a. Think of netstat as a swiss knife to view/print anything about your networks, like routing tables, network connections, interface stats, masquerade connections, and multicast memberships
b. Tcp: `netstat -at > netstat_tcp.txt` netstat_tcp.txt
   Udp: `netstat -au > netstat_udp.txt` netstat_udp.txt

6) nslookup

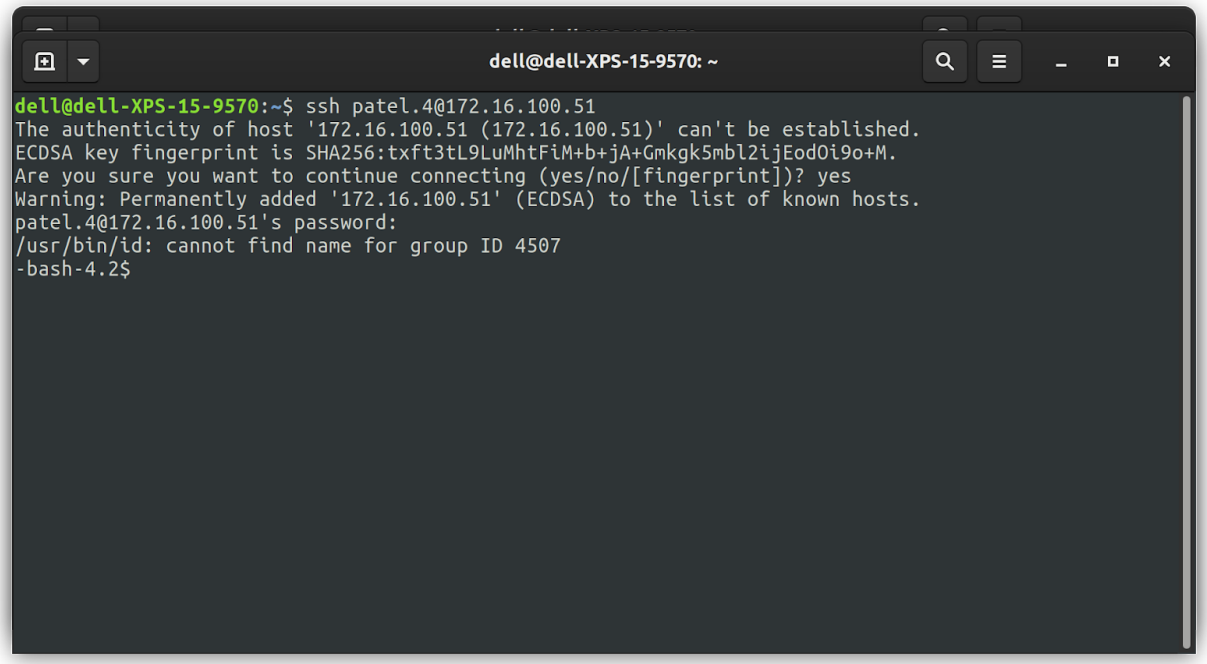
nslookup is a cmd to query Internet domain name servers in interactive (info of various hosts in a domain) and non-interactive way (just the requested info for the host or domain).

It gives the list of hosts in each domain. IITJ has one host with address `14.139.37.5` , while google has 2 hosts with address `172.217.160.206` and `2404:6800:4009:80b::200e` , while yahoo.com has 12 different host addresses you can reach.

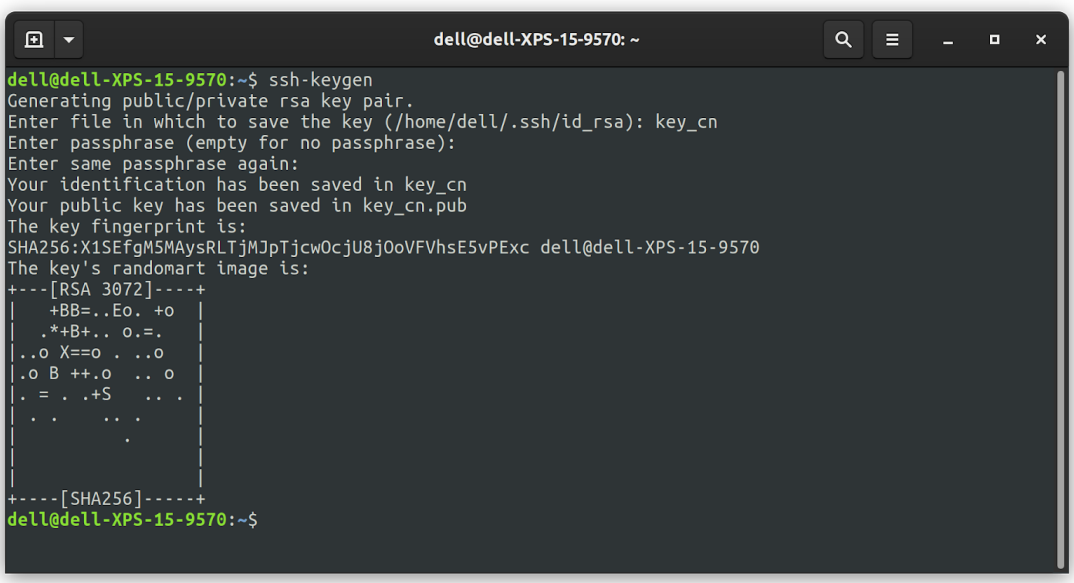
```
dell@dell-XPS-15-9570: ~
dell@dell-XPS-15-9570:~$ nslookup iitj.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   iitj.ac.in
Address: 14.139.37.5

dell@dell-XPS-15-9570:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.160.206
Name:   google.com
Address: 2404:6800:4009:80b::200e

dell@dell-XPS-15-9570:~$ nslookup yahoo.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   yahoo.com
Address: 74.6.143.26
Name:   yahoo.com
Address: 74.6.143.25
Name:   yahoo.com
Address: 98.137.11.164
Name:   yahoo.com
Address: 74.6.231.20
Name:   yahoo.com
Address: 74.6.231.21
Name:   yahoo.com
Address: 98.137.11.163
Name:   yahoo.com
Address: 2001:4998:24:120d::1:1
Name:   yahoo.com
Address: 2001:4998:24:120d::1:0
Name:   yahoo.com
Address: 2001:4998:44:3507::8000
Name:   yahoo.com
Address: 2001:4998:44:3507::8001
Name:   yahoo.com
Address: 2001:4998:124:1507::f001
Name:   yahoo.com
Address: 2001:4998:124:1507::f000

dell@dell-XPS-15-9570:~$
```

7) ssh and scp

a. Use `ssh patel.4@172.16.100.51` to login to home.iitj.ac.in account.

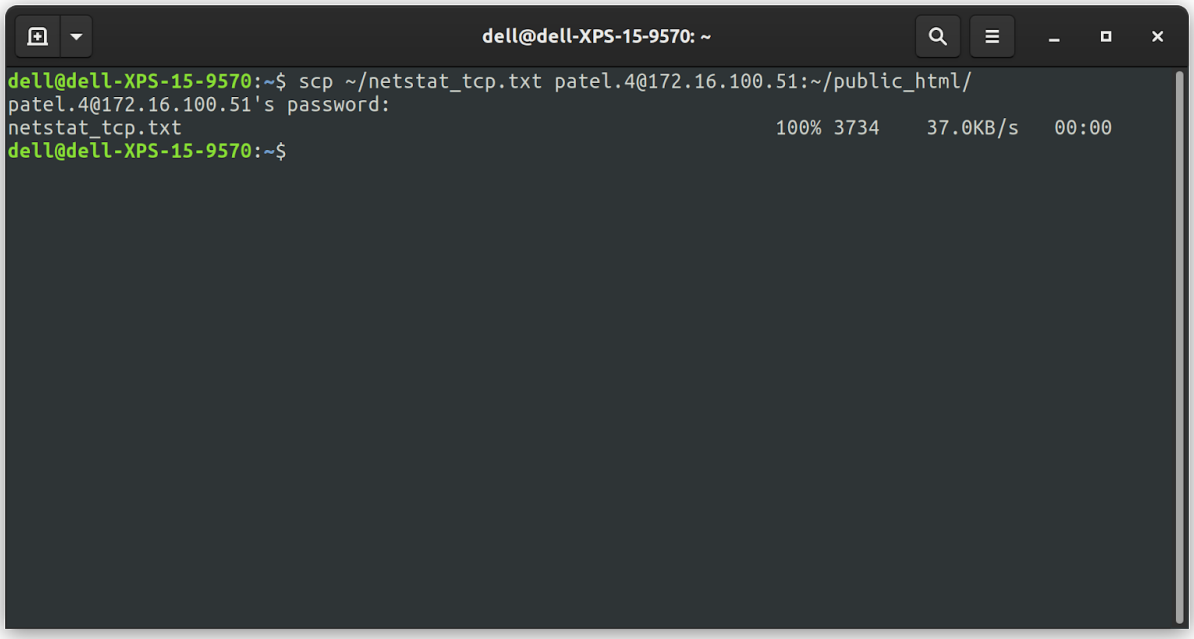


b. Use `ssh-keygen` to create a RSA key pair

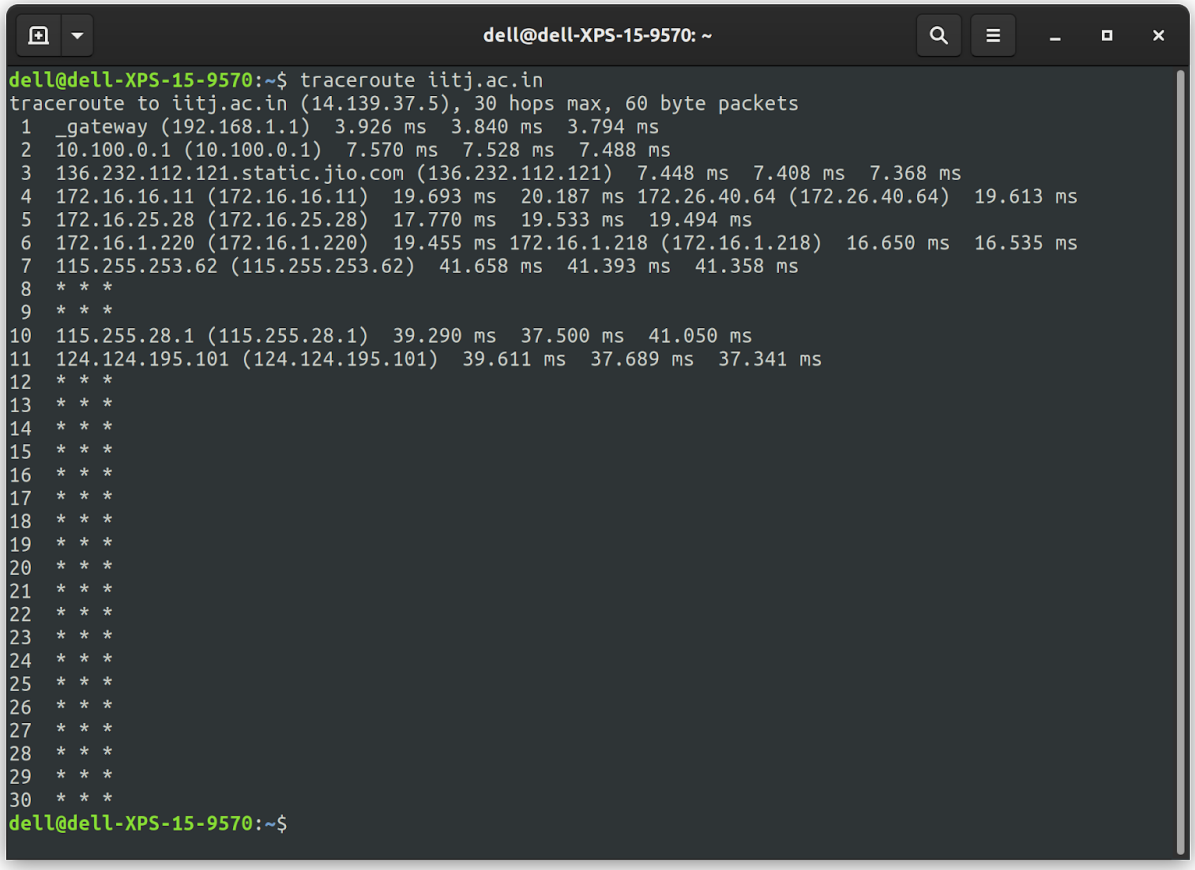


c. Use `scp netstat_tcp.txt patel.4@172.16.100.51:~/public_html/` to transfer a

file from your local machine to the IITJ server.



d. Use `scp patel.4@172.16.100.51:~/public_html/index.html ~/Documents` to transfer a file from IITJ server to your local machine.



8) *traceroute*

a. Traceroute is used to keep track of the route packets take to reach the network host.
b. Yes.
c. Yes. The average of the last three values in the last hop is the average RTT of that packet.
d. Traceroute uses IP protocols time-to-live(TTL) field and tries to obtain an ICMP “time exceeded” reply from each gateway along the path. If no response is generate it returns ***.