CS 558: Computer Systems Lab

Assignment – 1: Network Diagnostic Commands & Socket Programming

Q1. The Internet Ping command bounces a small packet(s) to test network communications, and then shows how long this packet(s) took to make the round trip. The Internet Ping program works much like a sonar echo location, sending a small packet of information containing an ICMP ECHO_REQUEST to a specified computer, which then sends an ECHO_REPLY packet in return. Explore more about the ping command and answer the following questions (Unix or GNU/Linux version only):

1.a) What is the option required to specify the number of echo requests to send with ping command?

-c <count>   stop after <count> replies

For Linux: ping -c 10 google.com

1.b) What is the option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs?

-i <interval>   seconds between sending each packet

ping -i 2 amazon.in

1.c) What is the command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply? What is the limit for sending such ECHO_REQUEST packets by normal users (not super user)?

-l preload

If preload is specified, ping sends many packets not waiting for reply. Only the super-user may select preload more than 3.

Command: ping –l 3 google.com

Limit For normal user: 3

For super user: 65536

1.d) What is the command to set the ECHO_REQUEST packet size (in bytes)? If the Packet size is set to 32 bytes, what will be the total packet size?

ping -s 32 google.in

Total packet size: 40 bytes

ICMP Header: 8 Bytes

2) Select six hosts of your choice on the Internet (mention the list in your report) and experiment with pinging each host 25 times at three different hours of the day. Check if there exist cases which show packet loss greater than 0% and provide reasoning. Find out average RTT for each host and explain whether measured RTTs are strongly or weakly correlated with the geographical distance of the hosts.

	11:00 AM		**1:00 PM**		**2:30 PM**	
Hosts	**Avg RTT (ms)**	**Packet Loss %**	**Avg RTT (ms)**	**Packet Loss %**	**Avg RTT (ms)**	**Packet Loss %**
amazon.in	**343.750**	**0**	**332.473**	**0**	**327.279**	**4**
flipkart.com	**440.104**	**12**	**430.842**	**0**	**104.595**	**0**
instagram.com	**336.065**	**0**	**138.667**	**0**	**94.893**	**0**
amazon.com	**446.616**	**0**	**490.024**	**0**	**416.970**	**0**
axisbank.com	**145.735**	**0**	**293.955**	**0**	**71.241**	**0**
liveindia.com	**215.092**	**0**	**414.675**	**0**	**180.465**	**0**

Yes, there exist some cases which show packet loss greater than 0%. I faced it two times, once for amazon.in at 2:30 PM and flipkart.com at 11:00.

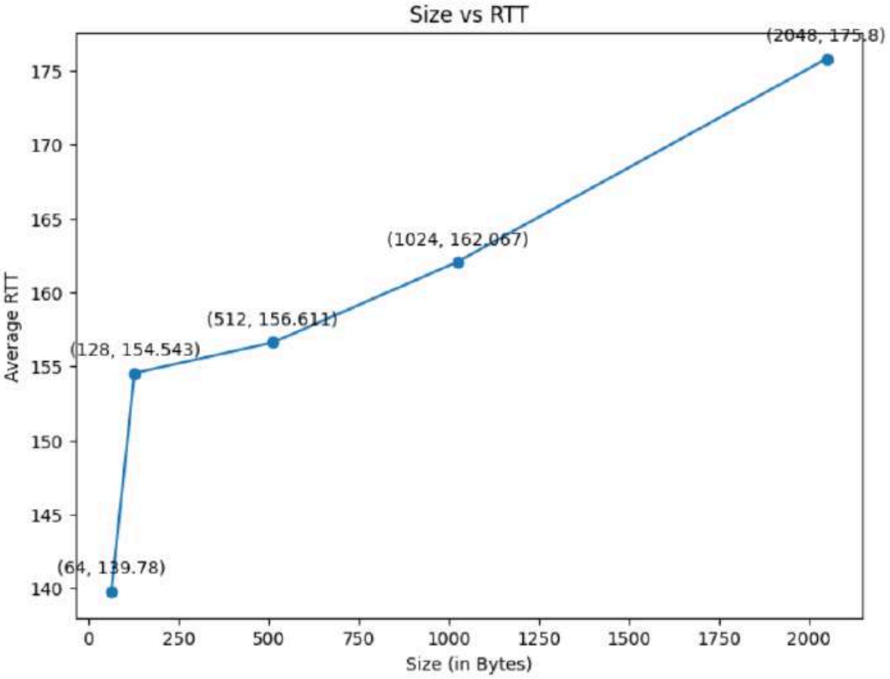
There can be several reasons for packet loss, and few might be these:

- **Network Congestion:** High network traffic or congestion can lead to packet loss. If there's a significant load on the network infrastructure between your device and Amazon's servers, some packets may be dropped.
- **Router Issues:** The router in your local network might be experiencing problems, leading to packet loss. Check for any issues with your router, such as overheating, outdated firmware, or hardware malfunctions.
- **Firewall or Security Software:** Security software, firewalls, or antivirus programs on your device may be configured to block certain types of traffic, causing packet loss during the ping.
- **Wireless Interference:** If you're using a wireless connection, interference from other devices or neighboring networks can lead to packet loss. Try using a wired connection to see if the issue persists

Measured Round-Trip Times (RTTs) are generally strongly correlated with geographical distance. In most cases, the farther the hosts are from each other, the longer the RTT due to increased signal propagation time. However, other factors like network congestion and routing inefficiencies can influence RTT, potentially leading to variations in the correlation strength.

2.1) Pick one of the above used hosts and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot the average RTT and explain how changes in packet size and time of the day impact RTT.

I used Axisbank.com for the experiment with different packet sizes i.e. 64 bytes, 128 bytes, 512 bytes, 1024 bytes, 2048 bytes.



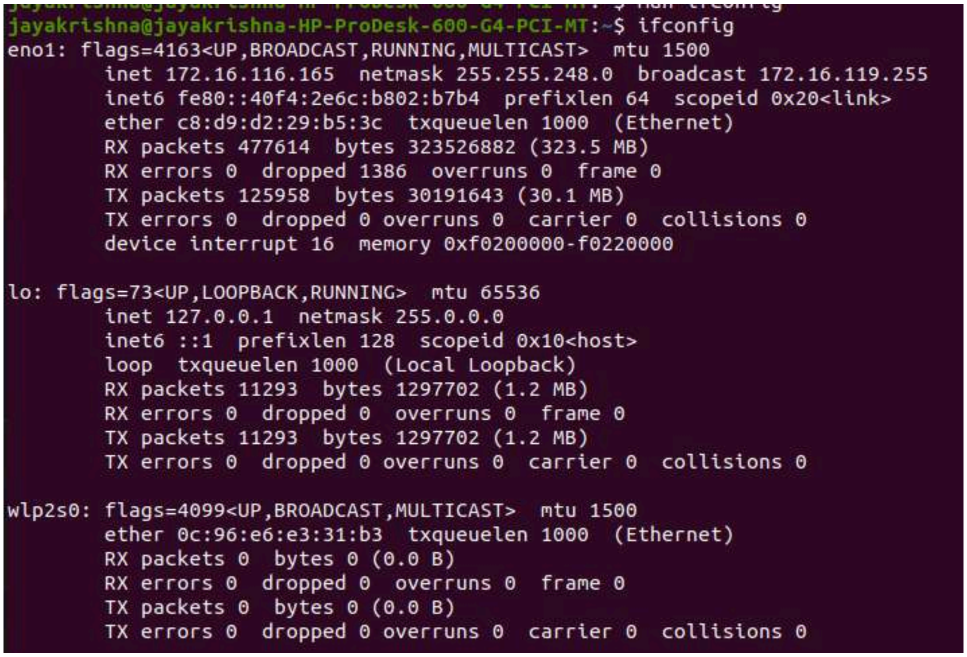
The initial ping with a packet size of 64 bytes exhibited a longer duration, and subsequently, as the packet size increased, the average Round-Trip Time (RTT) showed a slight increment during the first attempt for each packet size.

The first ping, using a packet size of 64 bytes, had a longer duration. If I repeat the ping with the same size, the time decreases. However, as the packet size increases, the average Round-Trip Time (RTT) shows a slight increment.

Q3. With regard to ifconfig and route commands, answer the following questions:

3.a) Run ifconfig command and describe its output (identify and explain as much of what is printed on the screen as you can).

ifconfig stands for “interface configuration.” It allows us to view and configure network interface settings.



```
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ man ifconfig
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.116.165  netmask 255.255.248.0  broadcast 172.16.119.255
        inet6 fe80::40f4:2e6c:b802:b7b4  prefixlen 64  scopeid 0x20<link>
        ether c8:d9:d2:29:b5:3c  txqueuelen 1000  (Ethernet)
        RX packets 477614  bytes 323526882 (323.5 MB)
        RX errors 0  dropped 1386  overruns 0  frame 0
        TX packets 125958  bytes 30191643 (30.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf0200000-f0220000

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 11293  bytes 1297702 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11293  bytes 1297702 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 0c:96:e6:e3:31:b3  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
```

1. Interface Listing:

- Interface names: The names of the network interfaces present on your system, such as en01, wlp2s0, or lo (loopback).

2. Interface Status:

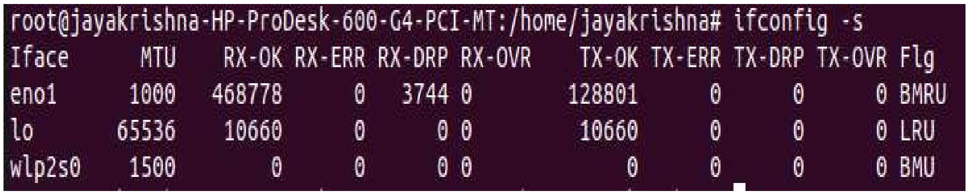
- Link encap: The type of encapsulation used by the interface (e.g., Ethernet, Wi-Fi, Local loop back).
- Hardware address: The hardware address (MAC address) of the interface.
- inet address: The IPv4 address assigned to the interface, if any.
- Broadcast: The broadcast address for the network the interface is on.
- Netmask: The subnet mask for the network.
- UP BROADCAST RUNNING MULTICAST: Flags indicating the interface's status (up or down, capable of broadcasting, multicasting, etc.).

3. Additional Information:

- inet6 addr: The IPv6 address assigned to the interface, if any.
- MTU: Maximum Transmission Unit, the largest packet size that can be transmitted over the interface.
- RX packets/bytes: The number of packets/bytes received by the interface.
- TX packets/bytes: The number of packets/bytes transmitted by the interface.
- Dropped: The number of packets dropped by the interface.
- Interrupt: The interrupt number used by the interface.
- TX errors: The number of transmission errors.
- RX errors: The number of reception errors.
- TX dropped: The number of packets dropped during transmission.
- RX dropped: The number of packets dropped during reception.

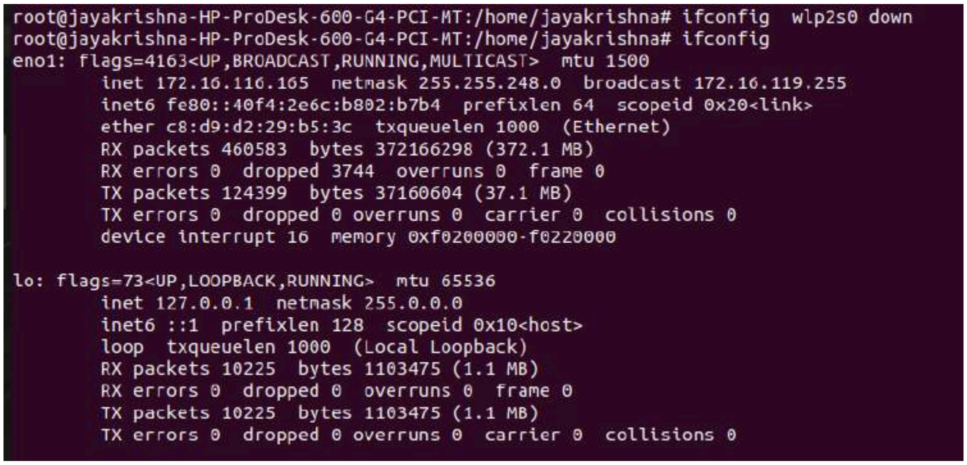
3.b) What options can be provided with the ifconfig command? Mention and explain at least four options.

-s display a short list (like netstat -i)



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig -s
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno1      1000   468778      0   3744 0        128801      0      0      0 BMRU
lo       65536    10660      0      0 0         10660      0      0      0 LRU
wlp2s0    1500        0      0      0 0             0      0      0      0 BMU
```

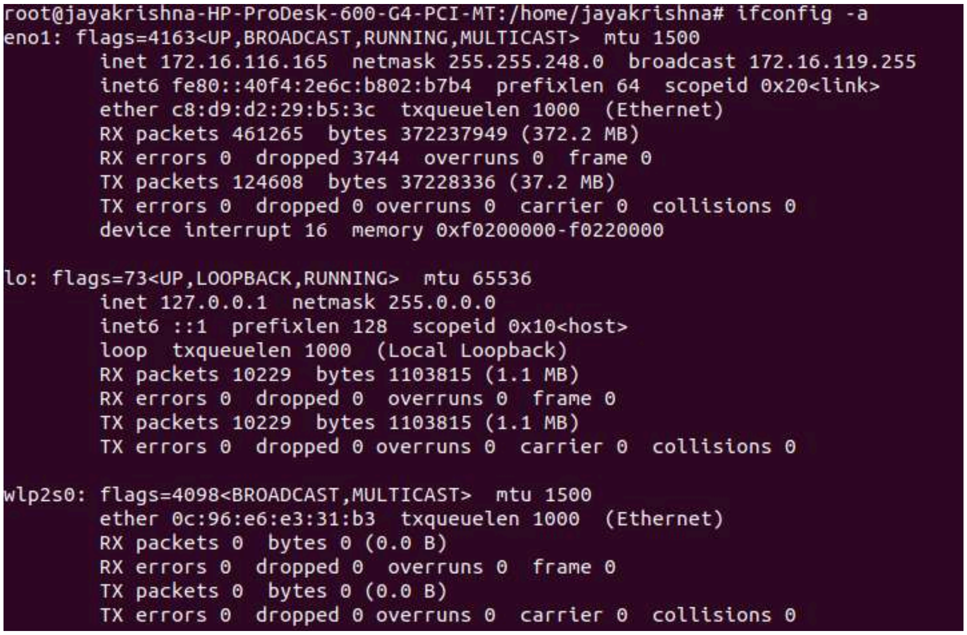
down This flag causes the driver for this interface to be shut down.



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig  wlp2s0 down
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.116.165  netmask 255.255.248.0  broadcast 172.16.119.255
        inet6 fe80::40f4:2e6c:b802:b7b4  prefixlen 64  scopeid 0x20<link>
        ether c8:d9:d2:29:b5:3c  txqueuelen 1000  (Ethernet)
        RX packets 460583  bytes 372166298 (372.1 MB)
        RX errors 0  dropped 3744  overruns 0  frame 0
        TX packets 124399  bytes 37160604 (37.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf0200000-f0220000

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 10225  bytes 1103475 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10225  bytes 1103475 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-a   display all interfaces which are currently available, even if down

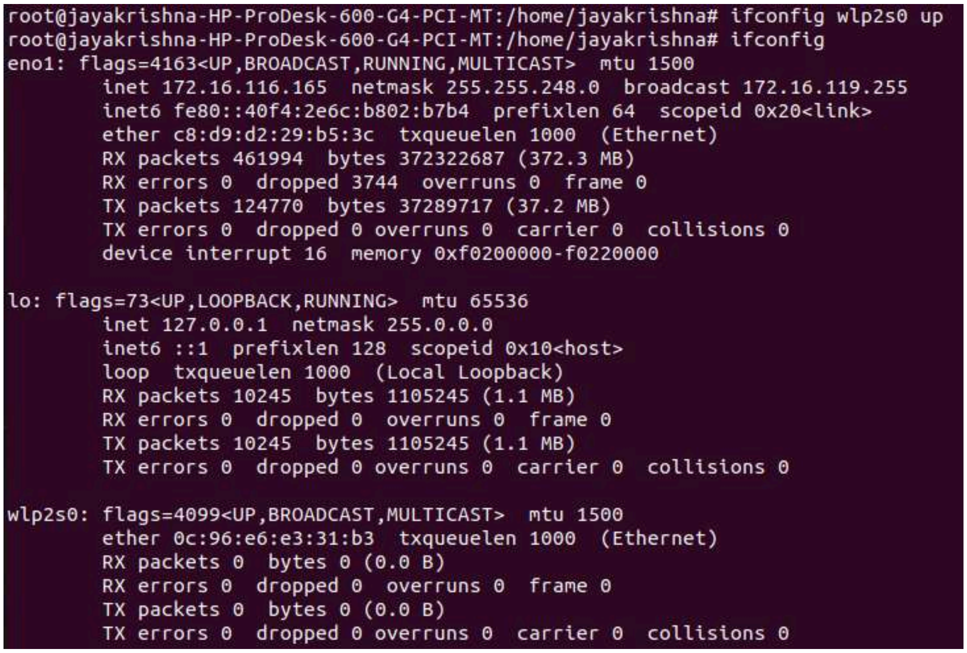


```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig -a
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.116.165  netmask 255.255.248.0  broadcast 172.16.119.255
        inet6 fe80::40f4:2e6c:b802:b7b4  prefixlen 64  scopeid 0x20<link>
        ether c8:d9:d2:29:b5:3c  txqueuelen 1000  (Ethernet)
        RX packets 461265  bytes 372237949 (372.2 MB)
        RX errors 0  dropped 3744  overruns 0  frame 0
        TX packets 124608  bytes 37228336 (37.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf0200000-f0220000

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 10229  bytes 1103815 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10229  bytes 1103815 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 0c:96:e6:e3:31:b3  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
```

up   This flag causes the interface to be activated.

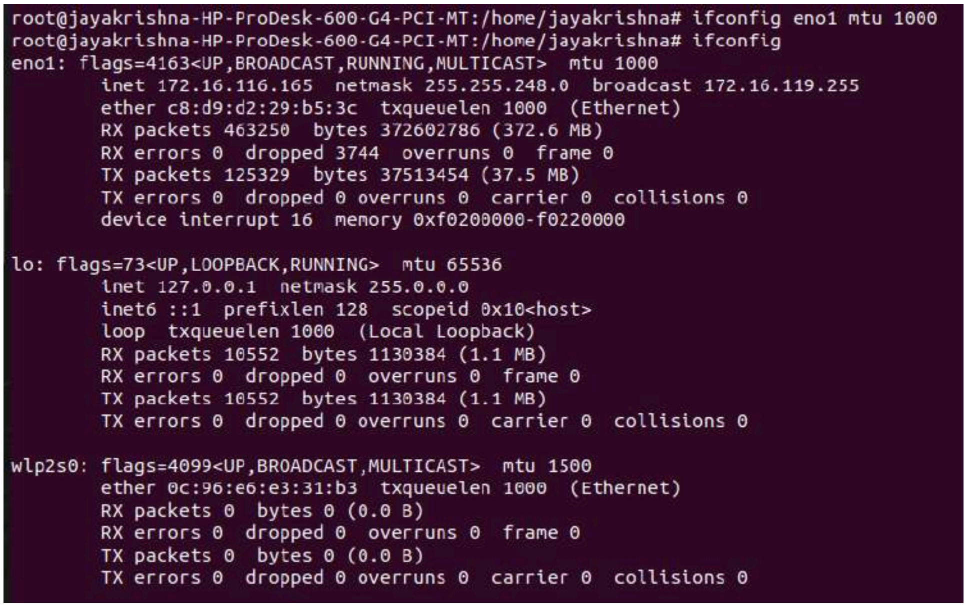


```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig wlp2s0 up
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.116.165  netmask 255.255.248.0  broadcast 172.16.119.255
        inet6 fe80::40f4:2e6c:b802:b7b4  prefixlen 64  scopeid 0x20<link>
        ether c8:d9:d2:29:b5:3c  txqueuelen 1000  (Ethernet)
        RX packets 461994  bytes 372322687 (372.3 MB)
        RX errors 0  dropped 3744  overruns 0  frame 0
        TX packets 124770  bytes 37289717 (37.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf0200000-f0220000

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 10245  bytes 1105245 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10245  bytes 1105245 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 0c:96:e6:e3:31:b3  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
```

mtu N This parameter sets the Maximum Transfer Unit (MTU) of an interface.



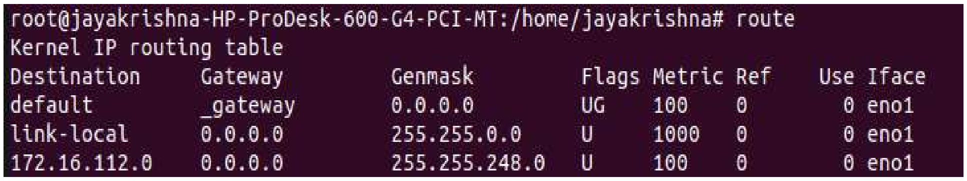
```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig eno1 mtu 1000
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1000
        inet 172.16.116.165  netmask 255.255.248.0  broadcast 172.16.119.255
        ether c8:d9:d2:29:b5:3c  txqueuelen 1000  (Ethernet)
        RX packets 463250  bytes 372602786 (372.6 MB)
        RX errors 0  dropped 3744  overruns 0  frame 0
        TX packets 125329  bytes 37513454 (37.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf0200000-f0220000

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 10552  bytes 1130384 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10552  bytes 1130384 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 0c:96:e6:e3:31:b3  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
```

3.c) Explain the output of route command.

Route manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig program.



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 eno1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U     100    0        0 eno1
```

1. Routing Table:

- Each row represents a route, indicating how to reach a specific network destination.
- Key columns include:
    - o Destination: The network or host that the route applies to (e.g., 0.0.0.0 for the default route, or a specific IP address or network range).
    - o Gateway: The IP address of the router to use when forwarding packets to that destination (if a gateway is needed).
    - o Gen mask: The network mask associated with the destination, determining which IP addresses belong to that network.
    - o Flags: Special flags indicating route properties, such as:

    - U: Up (the route is active)
    - G: Gateway (the route uses a gateway)
    - H: Host (the route is for a specific host, not a network)
    - D: Dynamic (the route was learned dynamically, not manually configured)
    - M: Modified (the route has been modified manually)
    - !: Reject (packets for this destination are discarded)
  - Metric: A numerical value representing the "cost" of the route, used for determining the best path when multiple routes exist. Lower metrics are preferred.
  - Ref: Number of references to this route.
  - Iface: The network interface through which packets for this destination should be sent.

2. Default Route:

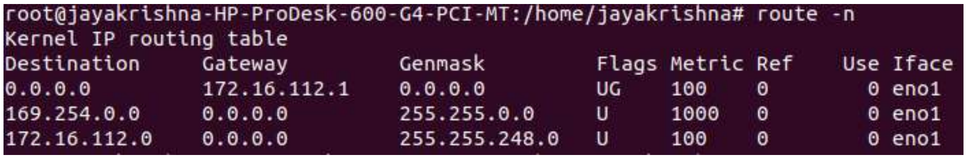
- The route with 0.0.0.0 as the destination and a gateway is the default route. It is used for any traffic that does not match a more specific route in the table.

3. Directly Connected Networks:

- Routes with 0.0.0.0 in the Gateway column are directly connected networks, meaning they are reachable directly without a gateway.

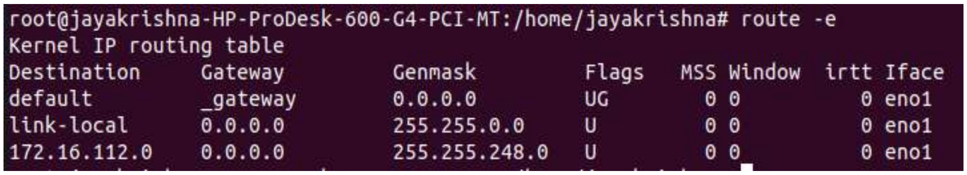
3.d) Mention and explain at least four options of the route command. Execute the route command with these four options and show the output.

-n show numerical addresses instead of trying to determine symbolic host names. This is useful if you are trying to determine why the route to your nameserver has vanished.



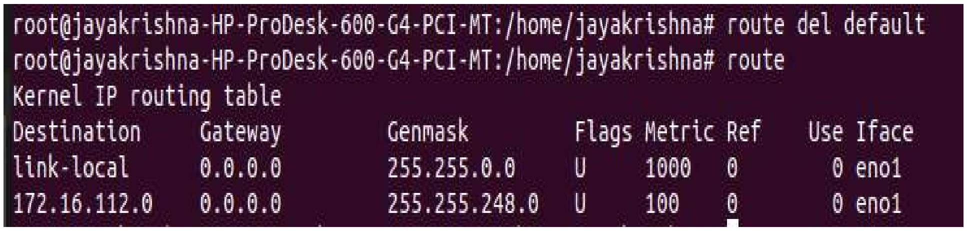
```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.112.1    0.0.0.0         UG    100    0        0 eno1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U     100    0        0 eno1
```

-e use netstat (8)-format for displaying the routing table. -ee will generate a very long line with all parameters from the routing table.



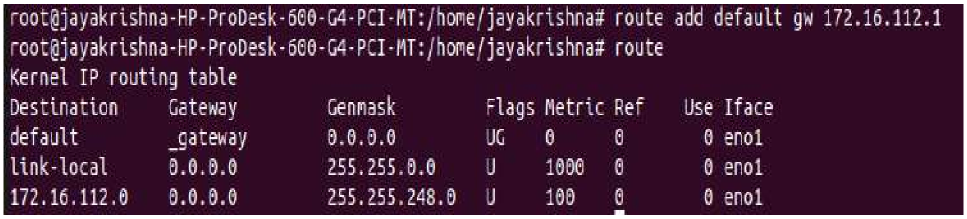
```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 eno1
link-local      0.0.0.0         255.255.0.0     U         0 0          0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U         0 0          0 eno1
```

del   delete a route.



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route del default
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U     100    0        0 eno1
```

add   add a new route.



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route add default gw 172.16.112.1
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    0      0        0 eno1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U     100    0        0 eno1
```

Q4. Answer the following questions related to netstat command.

4.a) What is the command netstat used for?

The netstat command is a valuable tool for displaying network-related information and diagnosing various networking issues in Unix-like operating systems.

Here's a breakdown of its common uses:

1. Displaying Active Connections:

- netstat without any options typically shows a list of active TCP connections, including:
  - Protocol (TCP or UDP)
  - Local address and port
  - Foreign address and port
  - Connection state (e.g., ESTABLISHED, LISTENING, TIME_WAIT)
  - PID (process ID) of the program using the connection

2. Troubleshooting Connectivity Problems:

- Identify open ports and listening services.
- Check for established connections to specific hosts or ports.
- Inspect connection states to diagnose issues like connection failures or timeouts.

3. Monitoring Network Activity:

- View active connections and their states in real time.
- Track network traffic patterns and identify potential bottlenecks.
- Investigate suspicious connections for security purposes.

4. Viewing Routing Information:

- Display the system's routing table with netstat -r.
- See how network packets are routed to different destinations.
- Identify potential routing problems.

5. Checking Interface Statistics:

- View statistics for each network interface with netstat -i.
- Monitor packet transmission and reception rates, errors, and other metrics.
- Identify potential interface issues.

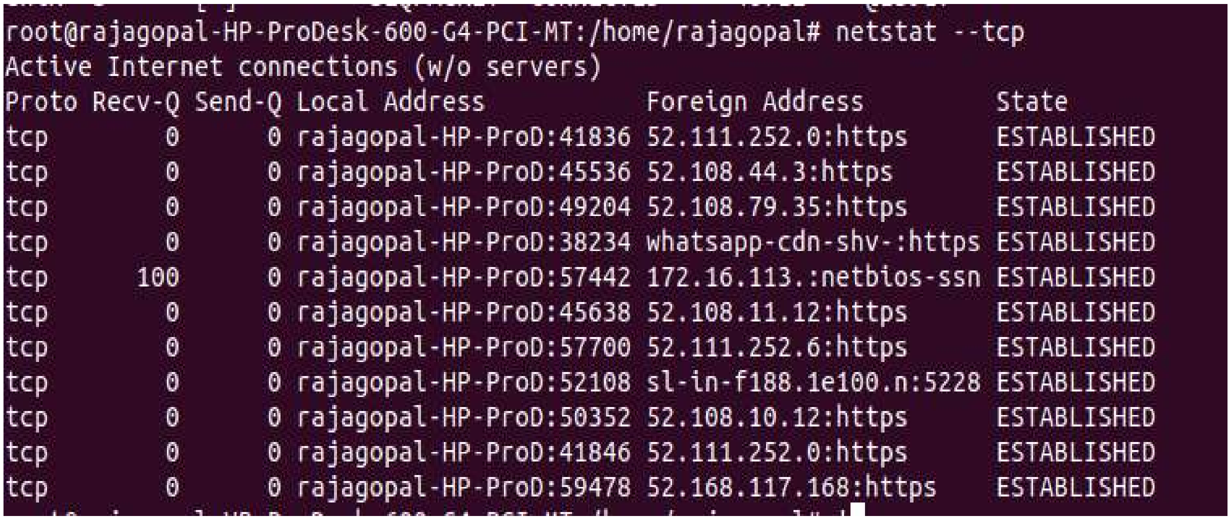
6. Displaying Protocol Statistics:

- View statistics for TCP, UDP, ICMP, and other protocols with netstat -s.
- Analyze network traffic patterns and identify potential issues.

7. Filtering Output:

- Use options to filter output based on protocol, state, port, address, etc.
- Narrow down the information to focus on specific areas of interest.

4.b) What parameters for netstat should you use to show all the established TCP connections? Include a screenshot of this list for your computer and explain all the fields of the table in the output?



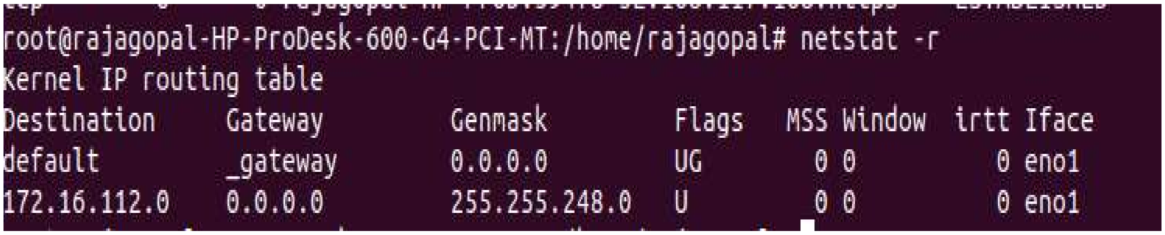
```
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal# netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 rajagopal-HP-ProD:41836 52.111.252.0:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:45536 52.108.44.3:https       ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:49204 52.108.79.35:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:38234 whatsapp-cdn-shv-:https ESTABLISHED
tcp      100      0 rajagopal-HP-ProD:57442 172.16.113.:netbios-ssn ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:45638 52.108.11.12:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:57700 52.111.252.6:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:52108 sl-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:50352 52.108.10.12:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:41846 52.111.252.0:https      ESTABLISHED
tcp        0      0 rajagopal-HP-ProD:59478 52.168.117.168:https    ESTABLISHED
```

The fields of the table in the output are:

- Proto: This column shows the protocol used for the connection, which is TCP in all cases here.
- Recv-Q: This column shows the size of the receive queue for the connection. This is the buffer where data received from the remote host is stored before being processed by the application.
- Send-Q: This column shows the size of the send queue for the connection. This is the buffer where data to be sent to the remote host is stored before being transmitted.
- Local Address: This column shows the local IP address and port number of the connection. The format is IP_address:port_number.
- Foreign Address: This column shows the remote IP address and port number of the connection. The format is the same as for the local address.
- State: This column shows the state of the connection. Some common states are:
  - ESTABLISHED: The connection is active and data can be exchanged between the two hosts.
  - LISTEN: The local application is listening on the specified port for incoming connections.
  - CLOSE_WAIT: The local application has closed the connection, but is still waiting for the remote host to close its end.
  - TIME_WAIT: The local host has closed the connection and is in a waiting state before the connection can be finally removed.

4.c) What does “netstat –r” show? Explain all the fields of the output?

netstat –r displays the kernel IP routing table.

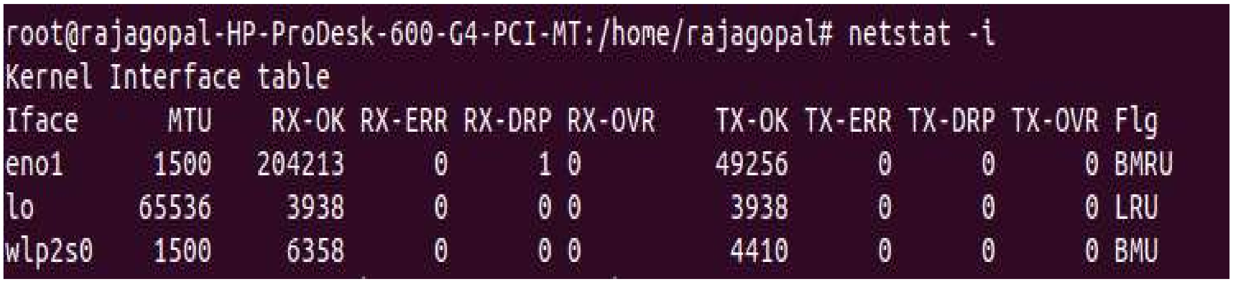


```
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 eno1
172.16.112.0    0.0.0.0         255.255.248.0   U         0 0          0 eno1
```

The fields in the routing table are explained in question 3.c.

4.d) What option of netstat can be used to display the status of all network interfaces? By using netstat, figure out the number of interfaces on your computer.

netstat -i can be used to display the status of all network interfaces.

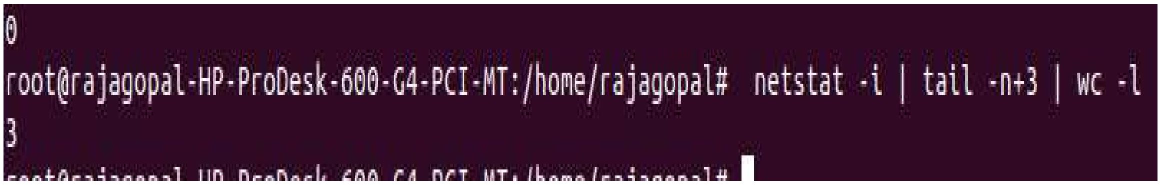


```
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal# netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno1      1500   204213      0      1 0         49256      0      0      0 BMRU
lo       65536     3938      0      0 0          3938      0      0      0 LRU
wlp2s0    1500     6358      0      0 0          4410      0      0      0 BMU
```

netstat -i: Displays interface statistics.

tail -n +3: Skips the first two lines of the output, which are headers, and starts from the third line.

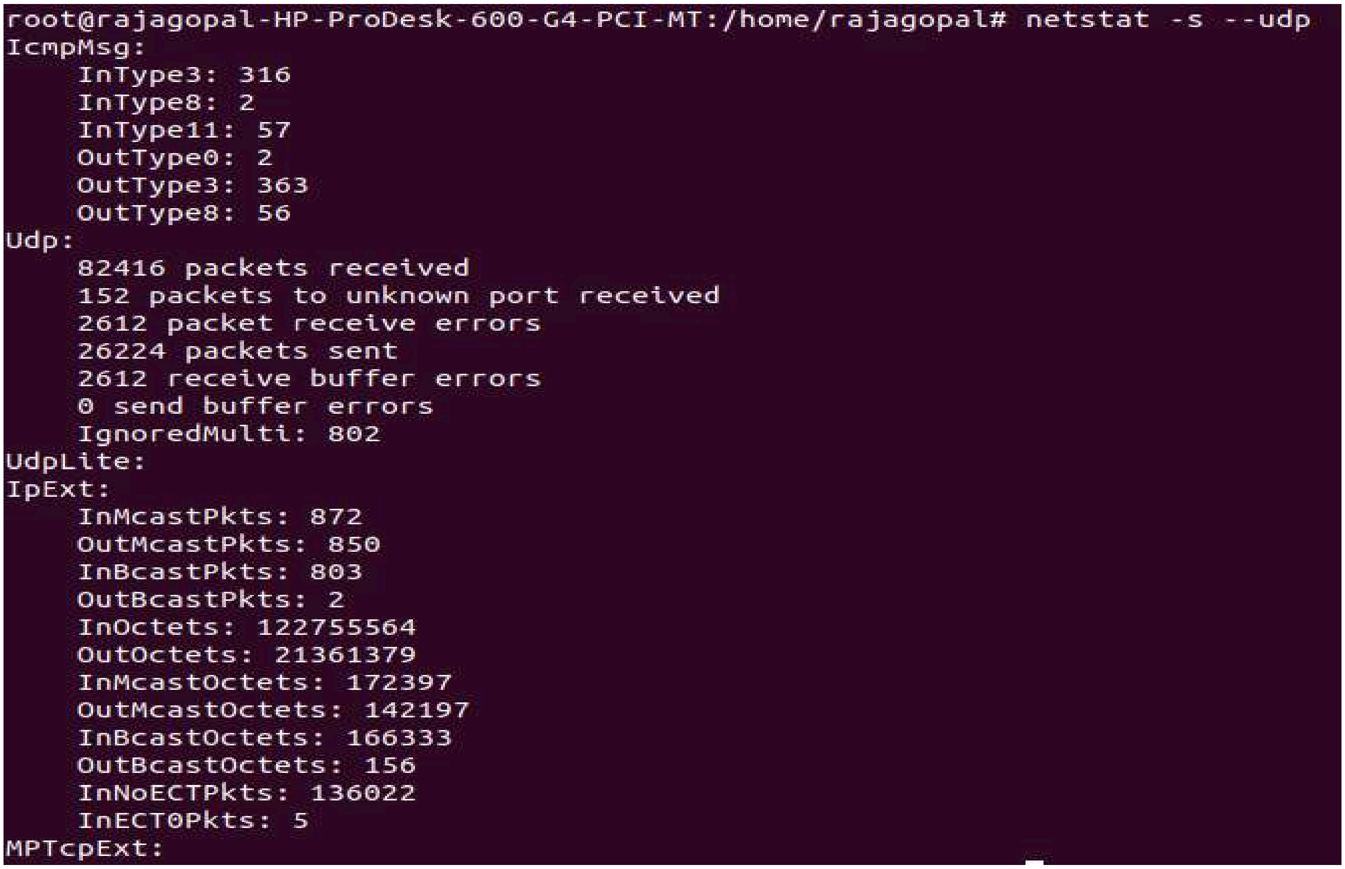
wc -l: Counts the number of lines in the remaining output, which corresponds to the number of interfaces.



```
0
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal#  netstat -i | tail -n+3 | wc -l
3
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal#
```

4.e) What option of netstat can be used to show the statistics of all UDP connections? Run the command for this purpose on your computer and show the output.

netstat –s –udp can be used to show the statistics of all UDP connections.



```
root@rajagopal-HP-ProDesk-600-G4-PCI-MT:/home/rajagopal# netstat -s --udp
IcmpMsg:
    InType3: 316
    InType8: 2
    InType11: 57
    OutType0: 2
    OutType3: 363
    OutType8: 56
Udp:
    82416 packets received
    152 packets to unknown port received
    2612 packet receive errors
    26224 packets sent
    2612 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 802
UdpLite:
IpExt:
    InMcastPkts: 872
    OutMcastPkts: 850
    InBcastPkts: 803
    OutBcastPkts: 2
    InOctets: 122755564
    OutOctets: 21361379
    InMcastOctets: 172397
    OutMcastOctets: 142197
    InBcastOctets: 166333
    OutBcastOctets: 156
    InNoECTPkts: 136022
    InECT0Pkts: 5
MPTcpExt:
```

4.f) Show and explain the function of loopback interface.

Loopback Interface: A Virtual Network Within Your Computer

What it is:

- It's a virtual network interface that's always present and active on your computer.
- It's usually assigned the IP address 127.0.0.1.
- It's commonly referred to as "lo" or "localhost."
- It doesn't connect to any external network; it's entirely internal.

Key Functions:

1. Local Communication:
   - Enables applications and services on your computer to communicate with each other directly without going through a physical network interface.
   - It's often used for testing network applications and services before deploying them on a real network.
2. Always-Reachable Interface:
   - It's always considered "up" and reachable, even if other network interfaces are down.
   - This makes it useful for services that need to be always accessible, even if there's no network connectivity.
3. Routing Purposes:
   - It's often used in routing protocols to represent the local system itself.
   - It can be used as a stable identifier for the device on the network.

Q5. What is a traceroute tool used for? Perform a traceroute experiment (with same hosts used in Q2) at three different hours of the day, and then answer the questions below.

A traceroute tool is a network diagnostic tool used to map the path taken by packets of data from your computer to a destination on the internet. It works like a map for your data, revealing the hops, or routers, it jumps through before reaching its final point.

5.a) List out the hop counts for each host in each time slot. Determine the common hops between two routes if they exist.

Hop counts for each host:

	3:30 PM	**4:30 PM**	**5:30 PM**
amazon.in	11	11	11
flipkart.com	7	8	8
instagram.com	8	8	8
amazon.com	8	8	8
axisbank.com	5	9	6
liveindia.com	10	10	10

Common Hops:

	Common Hops
amazon.in	192.168.25.231, 125.22.222.221, 99.83.67.152
flipkart.com	192.168.25.231, 125.22.222.217
instagram.com	2404:a800::88, 2620:0:1cff:dead:beee::160c, 2a03:2880:f26b:e6:face:b00c:0:4420
amazon.com	192.168.25.231, 116.119.119.1,
axisbank.com	2404:a800:4a00:202::19
liveindia.com	192.168.25.231, 116.119.50.142, 125.19.53.94, 180.179.193.100, 103.25.130.37

5.b) Check and explain the reason if route to same host changes at different times of the day.
Ex: axisbank.com

At 3:30 PM, the journey to the destination involved 5 hops. By 4:30 PM, the route expanded to 9 hops, taking a completely different path. At 5:30 PM, the journey comprised 6 hops, with some of these hops overlapping with the initial route.

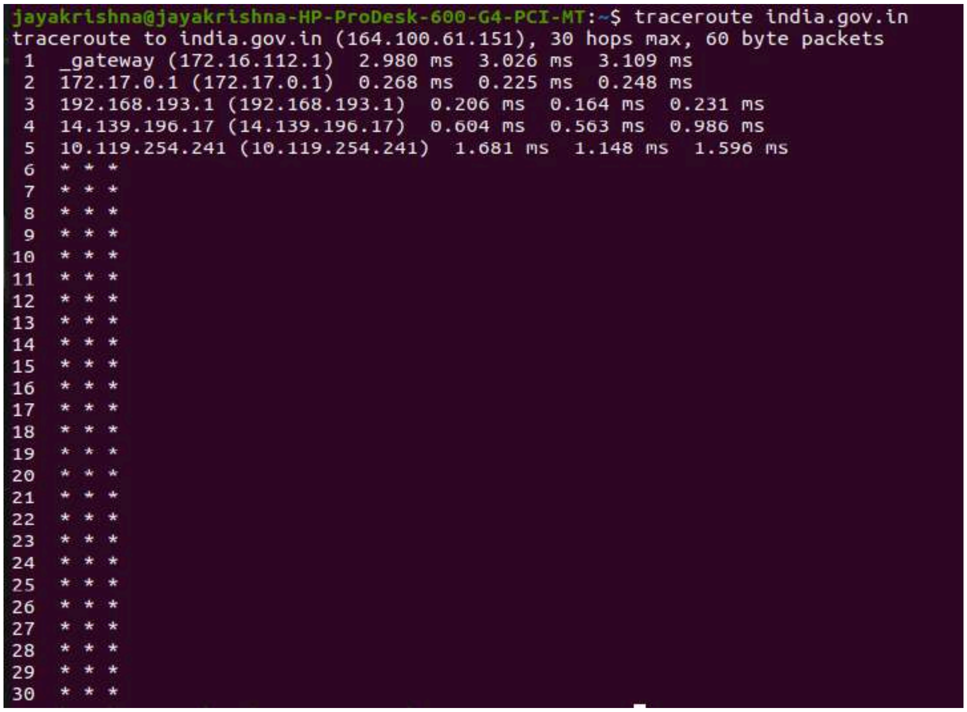
The route to the same host changing at different times of the day can be attributed to several factors in the dynamic and complex nature of the Internet's routing infrastructure.

- **Network Traffic and Load Balancing:** During peak hours, network traffic can be higher, leading to congestion on certain routes. To optimize performance and distribute traffic, network administrators may implement load balancing algorithms that dynamically alter the routing paths.
- **Dynamic Routing Protocols:** Internet routers use dynamic routing protocols to exchange information about network paths. Changes in network conditions or the availability of routes may cause routers to choose different paths to reach the same destination.

5.c) Inspect the cases when traceroute does not find complete paths to some hosts and provide reasoning.

Ex 1: india.gov.in

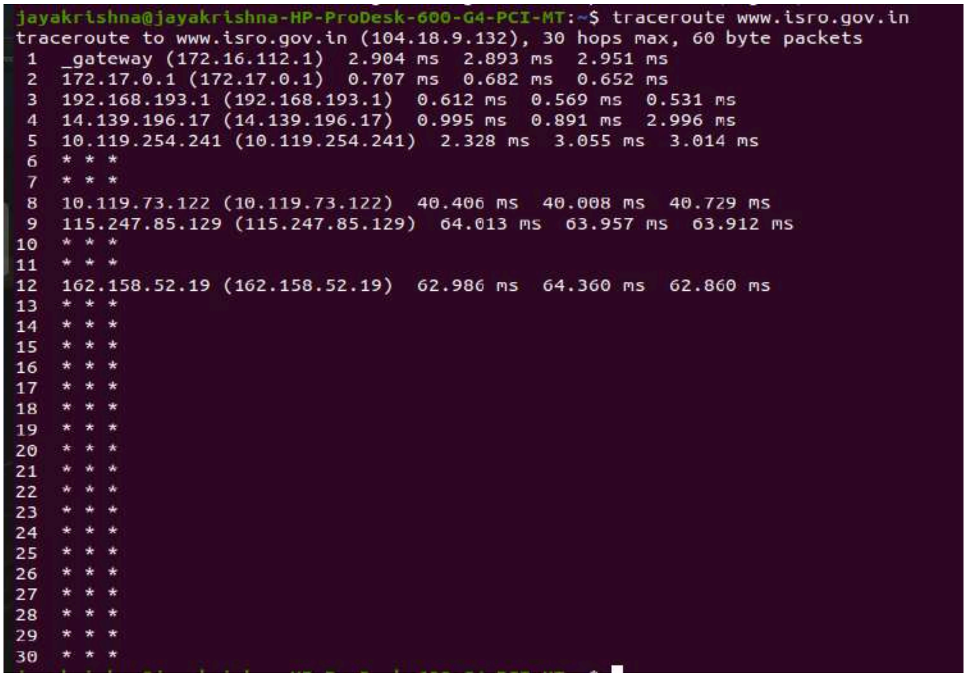
we Inspected the website india.gov.in using traceroute and we did not find the complete path to the host.



```
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ traceroute india.gov.in
traceroute to india.gov.in (164.100.61.151), 30 hops max, 60 byte packets
 1  _gateway (172.16.112.1)  2.980 ms  3.026 ms  3.109 ms
 2  172.17.0.1 (172.17.0.1)  0.268 ms  0.225 ms  0.248 ms
 3  192.168.193.1 (192.168.193.1)  0.206 ms  0.164 ms  0.231 ms
 4  14.139.196.17 (14.139.196.17)  0.604 ms  0.563 ms  0.986 ms
 5  10.119.254.241 (10.119.254.241)  1.681 ms  1.148 ms  1.596 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Ex 2: www.isro.gov.in

we Inspected the website www.isro.gov.in using traceroute and we did not find the complete path to the host.



```
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ traceroute www.isro.gov.in
traceroute to www.isro.gov.in (104.18.9.132), 30 hops max, 60 byte packets
 1  _gateway (172.16.112.1)  2.904 ms  2.893 ms  2.951 ms
 2  172.17.0.1 (172.17.0.1)  0.707 ms  0.682 ms  0.652 ms
 3  192.168.193.1 (192.168.193.1)  0.612 ms  0.569 ms  0.531 ms
 4  14.139.196.17 (14.139.196.17)  0.995 ms  0.891 ms  2.996 ms
 5  10.119.254.241 (10.119.254.241)  2.328 ms  3.055 ms  3.014 ms
 6  * * *
 7  * * *
 8  10.119.73.122 (10.119.73.122)  40.406 ms  40.008 ms  40.729 ms
 9  115.247.85.129 (115.247.85.129)  64.013 ms  63.957 ms  63.912 ms
10  * * *
11  * * *
12  162.158.52.19 (162.158.52.19)  62.986 ms  64.360 ms  62.860 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

There are several reasons why traceroute may not find complete paths to some hosts.

- **Firewall Blocking ICMP:** Many hosts and routers are configured to block ICMP (Internet Control Message Protocol) packets, which traceroute relies on. If a firewall is configured to block ICMP, the router or host will not respond to the traceroute requests, and the path will appear incomplete and that too we tried government websites maybe they are blocking to prevent DOS attack.
- **Network Filtering Policies:** Some network administrators may implement filtering policies that restrict or prioritize certain types of traffic. If traceroute packets are filtered out, the tool may not receive responses from specific routers, causing gaps in the path.

5.d) Is it possible to find the route to certain hosts which fail to respond with ping experiment? Give reasoning.

Yes, it is possible to attempt to find the route to certain hosts even if they fail to respond to ping requests. Ping uses the Internet Control Message Protocol (ICMP) to send Echo Request messages to a destination IP address, and it expects an Echo Reply in response. However, not all hosts or routers are configured to respond to ping requests, either for security reasons or as a deliberate configuration choice.

If a host does not respond to ping, you can use the "traceroute" command. Traceroute works by sending a series of UDP or ICMP packets with increasing Time-to-Live (TTL) values, and as each packet reaches a router along the path to the destination, the router decrements the TTL. When the TTL reaches zero, the router sends an ICMP Time Exceeded message back to the source, allowing the source to identify the router's IP address.

There will be some cases in which some networks and devices are configured to block or limit responses to traceroute requests as well. In such cases, we might not get a complete picture of the entire route. Additionally, firewalls, security policies, or deliberate filtering can affect the success of traceroute.

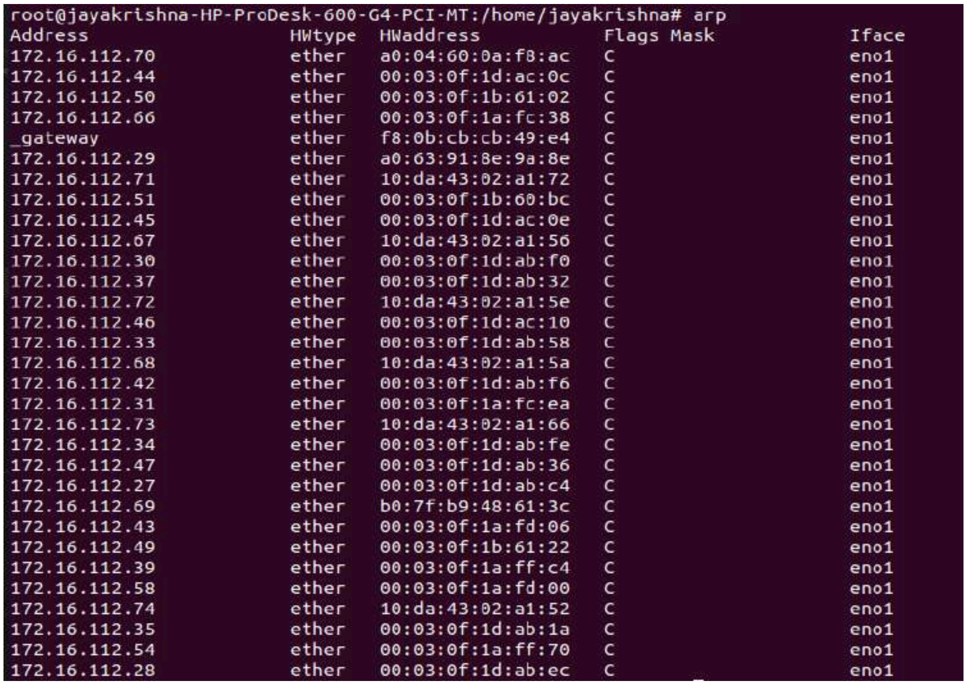
Q6. Answer the following questions with regard to network addresses.

a) How do you show the full ARP table for your machine? Explain each column of the ARP table.

You can use the command arp or arp –e to view the full ARP table for our machine.

By using arp –a also you can view but with no fixed columns.

The ARP table maps IP addresses to MAC addresses, enabling efficient communication on a local network.



```
root@jayakrishna-HP-ProDesk-600-G4-PCI-MT:/home/jayakrishna# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.112.70            ether   a0:04:60:0a:f8:ac   C                     eno1
172.16.112.44            ether   00:03:0f:1d:ac:0c   C                     eno1
172.16.112.50            ether   00:03:0f:1b:61:02   C                     eno1
172.16.112.66            ether   00:03:0f:1a:fc:38   C                     eno1
_gateway                 ether   f8:0b:cb:cb:49:e4   C                     eno1
172.16.112.29            ether   a0:63:91:8e:9a:8e   C                     eno1
172.16.112.71            ether   10:da:43:02:a1:72   C                     eno1
172.16.112.51            ether   00:03:0f:1b:60:bc   C                     eno1
172.16.112.45            ether   00:03:0f:1d:ac:0e   C                     eno1
172.16.112.67            ether   10:da:43:02:a1:56   C                     eno1
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     eno1
172.16.112.37            ether   00:03:0f:1d:ab:32   C                     eno1
172.16.112.72            ether   10:da:43:02:a1:5e   C                     eno1
172.16.112.46            ether   00:03:0f:1d:ac:10   C                     eno1
172.16.112.33            ether   00:03:0f:1d:ab:58   C                     eno1
172.16.112.68            ether   10:da:43:02:a1:5a   C                     eno1
172.16.112.42            ether   00:03:0f:1d:ab:f6   C                     eno1
172.16.112.31            ether   00:03:0f:1a:fc:ea   C                     eno1
172.16.112.73            ether   10:da:43:02:a1:66   C                     eno1
172.16.112.34            ether   00:03:0f:1d:ab:fe   C                     eno1
172.16.112.47            ether   00:03:0f:1d:ab:36   C                     eno1
172.16.112.27            ether   00:03:0f:1d:ab:c4   C                     eno1
172.16.112.69            ether   b0:7f:b9:48:61:3c   C                     eno1
172.16.112.43            ether   00:03:0f:1a:fd:06   C                     eno1
172.16.112.49            ether   00:03:0f:1b:61:22   C                     eno1
172.16.112.39            ether   00:03:0f:1a:ff:c4   C                     eno1
172.16.112.58            ether   00:03:0f:1a:fd:00   C                     eno1
172.16.112.74            ether   10:da:43:02:a1:52   C                     eno1
172.16.112.35            ether   00:03:0f:1d:ab:1a   C                     eno1
172.16.112.54            ether   00:03:0f:1a:ff:70   C                     eno1
172.16.112.28            ether   00:03:0f:1d:ab:ec   C                     eno1
```

Column Explanations:

- Interface: The network interface on which the ARP entry is found (e.g., eth0, wlan0).
- Internet Address: The IP address of the device on the network.
- Physical Address: The MAC address (Media Access Control) of the device, which uniquely identifies it on the network.
- Type: The type of ARP entry (e.g., dynamic, static, incomplete).
- HW Type: The type of hardware the device is using (e.g., Ethernet).
- Flags: Information about the ARP entry's status (e.g., permanent, published).
- Mask: The subnet mask associated with the IP address.

b) Check and explain what happens if you try and use the arp command to add or delete an entry to the ARP table. Find out how to add, delete or change entries in the ARP table. Use this mechanism to add at least four new hosts to the ARP table and include a printout.

Adding Entries:

arp -s <IP_address> <MAC_address>

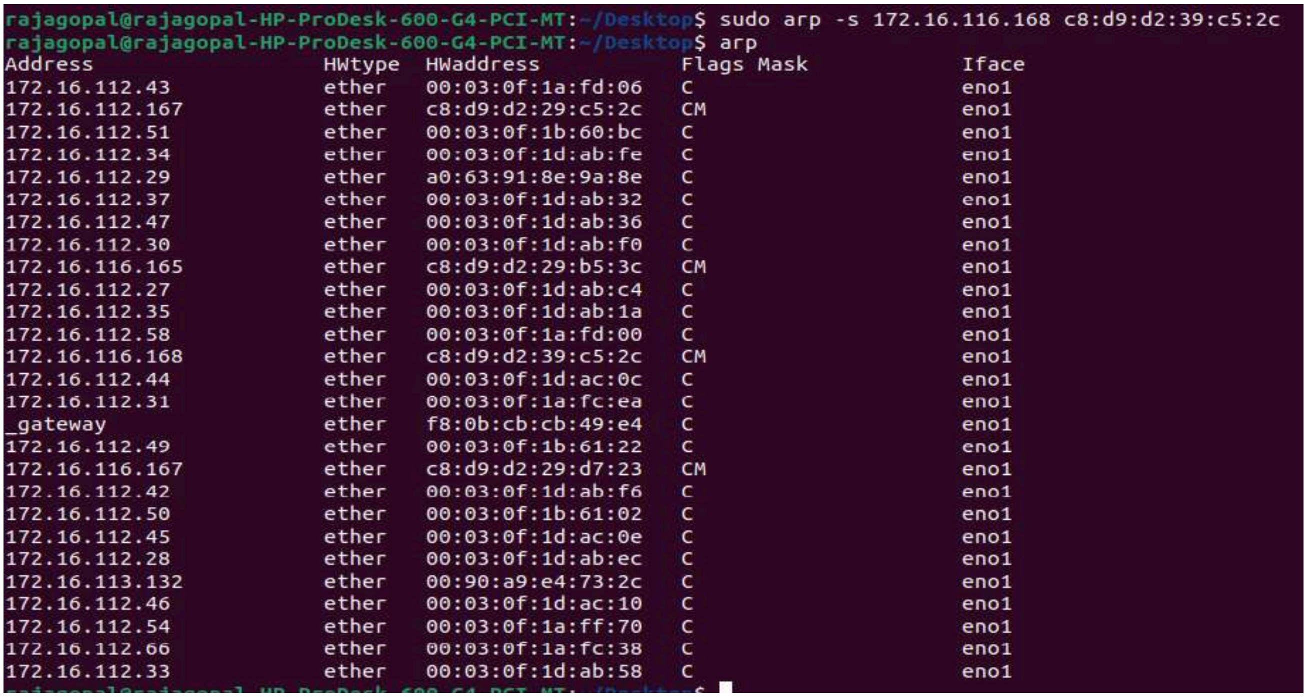
- The system verifies the validity of the provided IP address and MAC address.
- If valid, it creates a new ARP entry with the specified information.
- The entry is marked as "static" or "manual," indicating it was added manually, not learned dynamically.
- The entry is typically added to the ARP cache for the specific network interface associated with the IP address.

sudo arp -s 172.16.116.167 c8:d9:d2:29:d7:23

sudo arp -s 172.16.116.165 c8:d9:d2:29:b5:3c

sudo arp -s 192.168.1.4 c8:d9:d2:29:c5:2c

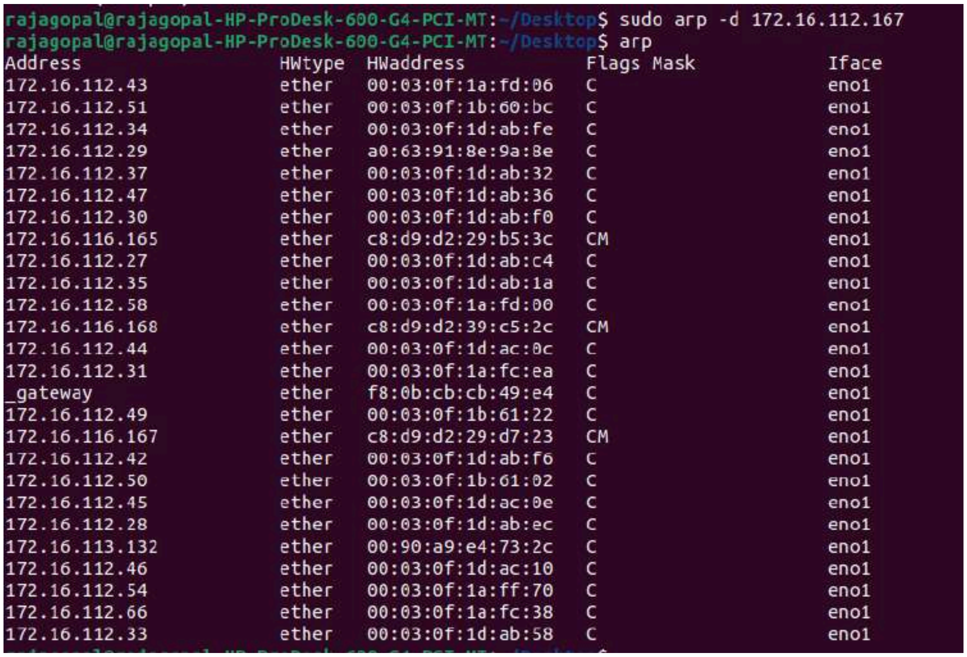
sudo arp -s 172.16.112.167 c8:d9:d2:29:c5:2c



```
rajagopal@rajagopal-HP-ProDesk-600-G4-PCI-MT:~/Desktop$ sudo arp -s 172.16.116.168 c8:d9:d2:39:c5:2c
rajagopal@rajagopal-HP-ProDesk-600-G4-PCI-MT:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.112.43            ether   00:03:0f:1a:fd:06   C                     eno1
172.16.112.167           ether   c8:d9:d2:29:c5:2c   CM                    eno1
172.16.112.51            ether   00:03:0f:1b:60:bc   C                     eno1
172.16.112.34            ether   00:03:0f:1d:ab:fe   C                     eno1
172.16.112.29            ether   a0:63:91:8e:9a:8e   C                     eno1
172.16.112.37            ether   00:03:0f:1d:ab:32   C                     eno1
172.16.112.47            ether   00:03:0f:1d:ab:36   C                     eno1
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     eno1
172.16.116.165           ether   c8:d9:d2:29:b5:3c   CM                    eno1
172.16.112.27            ether   00:03:0f:1d:ab:c4   C                     eno1
172.16.112.35            ether   00:03:0f:1d:ab:1a   C                     eno1
172.16.112.58            ether   00:03:0f:1a:fd:00   C                     eno1
172.16.116.168           ether   c8:d9:d2:39:c5:2c   CM                    eno1
172.16.112.44            ether   00:03:0f:1d:ac:0c   C                     eno1
172.16.112.31            ether   00:03:0f:1a:fc:ea   C                     eno1
_gateway                 ether   f8:0b:cb:cb:49:e4   C                     eno1
172.16.112.49            ether   00:03:0f:1b:61:22   C                     eno1
172.16.116.167           ether   c8:d9:d2:29:d7:23   CM                    eno1
172.16.112.42            ether   00:03:0f:1d:ab:f6   C                     eno1
172.16.112.50            ether   00:03:0f:1b:61:02   C                     eno1
172.16.112.45            ether   00:03:0f:1d:ac:0e   C                     eno1
172.16.112.28            ether   00:03:0f:1d:ab:ec   C                     eno1
172.16.113.132           ether   00:90:a9:e4:73:2c   C                     eno1
172.16.112.46            ether   00:03:0f:1d:ac:10   C                     eno1
172.16.112.54            ether   00:03:0f:1a:ff:70   C                     eno1
172.16.112.66            ether   00:03:0f:1a:fc:38   C                     eno1
172.16.112.33            ether   00:03:0f:1d:ab:58   C                     eno1
rajagopal@rajagopal-HP-ProDesk-600-G4-PCI-MT:~/Desktop$
```

Deleting entry: arp –d <host address>

- If the entry is found, it's removed from the ARP table.
- This means the system no longer has a cached association between the IP address and its corresponding MAC address.



```
rajagopal@rajagopal-HP-ProDesk-600-G4-PCI-MT:~/Desktop$ sudo arp -d 172.16.112.167
rajagopal@rajagopal-HP-ProDesk-600-G4-PCI-MT:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.112.43            ether   00:03:0f:1a:fd:06   C                     eno1
172.16.112.51            ether   00:03:0f:1b:60:bc   C                     eno1
172.16.112.34            ether   00:03:0f:1d:ab:fe   C                     eno1
172.16.112.29            ether   a0:63:91:8e:9a:8e   C                     eno1
172.16.112.37            ether   00:03:0f:1d:ab:32   C                     eno1
172.16.112.47            ether   00:03:0f:1d:ab:36   C                     eno1
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     eno1
172.16.116.165           ether   c8:d9:d2:29:b5:3c   CM                    eno1
172.16.112.27            ether   00:03:0f:1d:ab:c4   C                     eno1
172.16.112.35            ether   00:03:0f:1d:ab:1a   C                     eno1
172.16.112.58            ether   00:03:0f:1a:fd:00   C                     eno1
172.16.116.168           ether   c8:d9:d2:39:c5:2c   CM                    eno1
172.16.112.44            ether   00:03:0f:1d:ac:0c   C                     eno1
172.16.112.31            ether   00:03:0f:1a:fc:ea   C                     eno1
_gateway                 ether   f8:0b:cb:cb:49:e4   C                     eno1
172.16.112.49            ether   00:03:0f:1b:61:22   C                     eno1
172.16.116.167           ether   c8:d9:d2:29:d7:23   CM                    eno1
172.16.112.42            ether   00:03:0f:1d:ab:f6   C                     eno1
172.16.112.50            ether   00:03:0f:1b:61:02   C                     eno1
172.16.112.45            ether   00:03:0f:1d:ac:0e   C                     eno1
172.16.112.28            ether   00:03:0f:1d:ab:ec   C                     eno1
172.16.113.132           ether   00:90:a9:e4:73:2c   C                     eno1
172.16.112.46            ether   00:03:0f:1d:ac:10   C                     eno1
172.16.112.54            ether   00:03:0f:1a:ff:70   C                     eno1
172.16.112.66            ether   00:03:0f:1a:fc:38   C                     eno1
172.16.112.33            ether   00:03:0f:1d:ab:58   C                     eno1
```

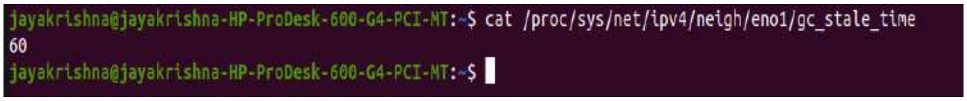
6.c) What are the parameters that determine how long the entries in the cache of the ARP module of the kernel remain valid and when they get deleted from the cache? Describe a trial-and-error method to discover the timeout value for the ARP cache entries.

base_reachable_time_ms:

It controls how long an ARP cache entry is valid, and it defaults to 30000 milliseconds (about 30 seconds).

gc_stale_time:

The **gc_stale_time** parameter is related to the ARP cache and is used to set the timeout for stale entries in the Neighbor Table. The Neighbor Table is part of the ARP module and is used to maintain a mapping between IP addresses and hardware (MAC) addresses. Stale entries in this context refer to ARP cache entries that haven't been used for a certain period.



```
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ cat /proc/sys/net/ipv4/neigh/eno1/gc_stale_time
60
jayakrishna@jayakrishna-HP-ProDesk-600-G4-PCI-MT:~$ 
```

This parameter helps manage the size of the ARP cache by removing entries that have not been actively used, preventing the cache from growing indefinitely.

Trial-and-Error Method to Discover Timeout Value:

- Clear the ARP Cache:
  - Use the arp -d command (or a similar command for your operating system) to clear existing entries.
- Generate ARP Traffic:
  - Initiate communication with a specific IP address on your network to trigger ARP resolution and cache entry creation.
  - Use tools like ping or arp to send ARP requests.
- Record Initial Timestamp:
  - Note the exact time you generated the ARP traffic.
- Cease ARP Traffic:
  - Stop communicating with the IP address.
- Monitor ARP Cache:
  - Use the arp command to periodically check the ARP cache.
- Observe Entry Removal:
  - Keep checking until the entry for the IP address disappears from the cache.
- Calculate Timeout Value:
  - Subtract the initial timestamp from the time of entry removal to estimate the timeout value.
- Repeat for Accuracy:
  - Perform multiple trials to obtain a more accurate average timeout value.

As the stale time is set to 60 seconds the entry will be deleted if it is stale or not communicated for 60 seconds.

6.d) What will happen if two IP addresses map to the same Ethernet address? Be specific on how all hosts on the subnet operate.

- When two IP addresses map to the same Ethernet address, devices on the subnet get confused about which device to send data to.
- Broadcasts and multicasts reach both devices, potentially causing unintended behavior.

ARP (Address Resolution Protocol) Confusion:

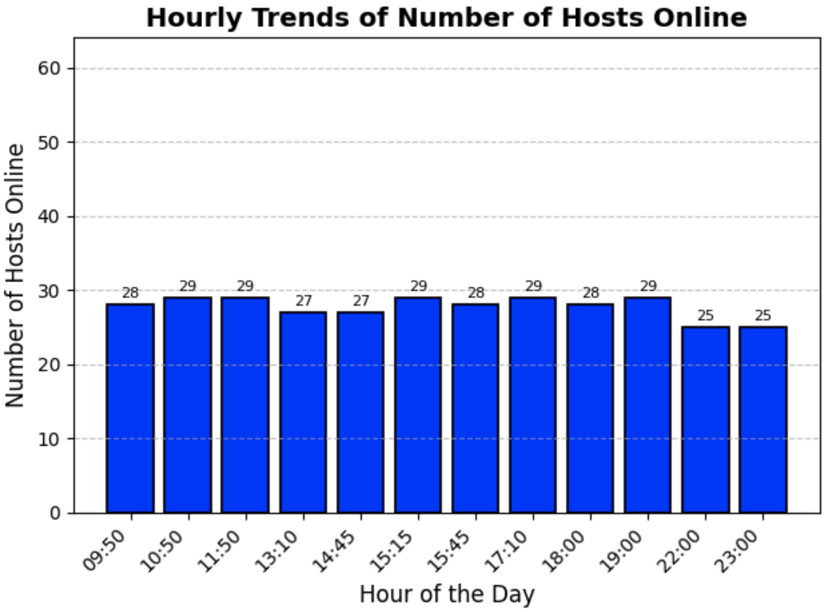
  - ARP is used to map IP addresses to MAC addresses in a local network.
  - When a device needs to communicate with another device in the same subnet, it uses ARP to discover the MAC address associated with the destination IP address.
  - If two IP addresses are mapped to the same MAC address, ARP responses can become ambiguous, leading to confusion about which IP address corresponds to the requested MAC address.

Packet Forwarding Issues:

- When a device sends a packet to a destination IP address, it encapsulates the packet with the MAC address of the destination device.
- If multiple IP addresses share the same MAC address, the device receiving the packet may not be the intended destination, causing incorrect packet forwarding.

Q7. Local network analysis: Query your LAN using the nmap command to discover which hosts are online. Use a command such as: nmap –n –sP (e.g., 172.16.112.0/26) You can choose a different LAN subnet address as well (make sure you report the same in your report explicitly). Now run the command repeatedly at different times of the day and find the number of hosts online. Do it at least 6 times with sufficient time gap. Plot a graph against time to see if there are any hourly trends for when computers are switched ON or OFF in your LAN.

The LAN subnet address we are using for the local network analysis is: **172.16.116.128/25.**


Hourly Trends of Number of Hosts Online
Number of Hosts Online
09:50
10:50
11:50
13:10
14:45
15:15
15:45
17:10
18:00
19:00
22:00
23:00
Hour of the Day