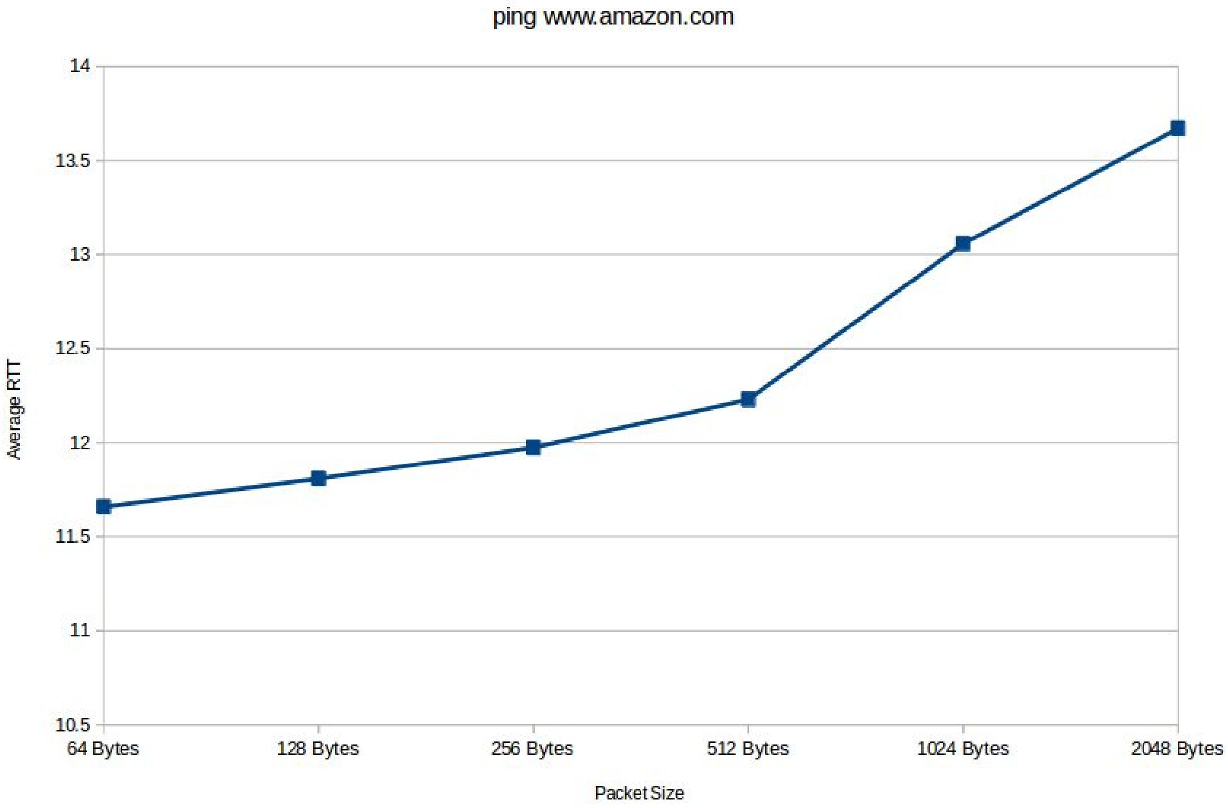
CS349 : Assignment 1 report , PIYUSH JAIN, Roll No. 150101046

1.
(a) -c *count*
(b) -i *interval*
(c) -l *preload* , 3
(d) -s *packetsize* , 64 Bytes + 8 Bytes (length of an ICMP header)= 72 Bytes

2.
Hosts : *www.amazon.com, www.google.co.in, www.amazon.co.uk, www.linkedin.com, www.nic.ru*
There was packet loss gretaer than 0% in case of *www.amazon.co.uk* for a few times.
Reasons for packet loss :

(a) Network congestion : When content arrives for a sustained period at a given router or network segment at a rate greater than it is possible to send through, there is no other option than to drop packets.
(b) Hardware : Hardware could be the issue if there are older transfer points being used, or the physical infrastructure is not optimal for the transfer.

Average RTTs :
www.amazon.com - 11.656ms *, www.google.co.in* - 5.892ms *, www.amazon.co.uk* - 6.347ms
www.linkedin.com - 11.446ms *, www.nic.ru* - 183.477ms
We can say that there is a positive weak correlation between distance and RTT. There are a number of reasons for this. For example, an increased hop count. The packets have to through more routers, at each router there may be a delay, as there are more routers, the longer the RTT.
Experiment with different packet sizes with host *www.amazon.com* :



We can see that packet size is slightly and positively correlated with the RTT. Also, RTT gets affected as the time of the experiment changes because there is difference in level of congestion in the network at different times of the day.

3. IP address : 202.141.80.14

(a) Packet loss for each command was 0%.

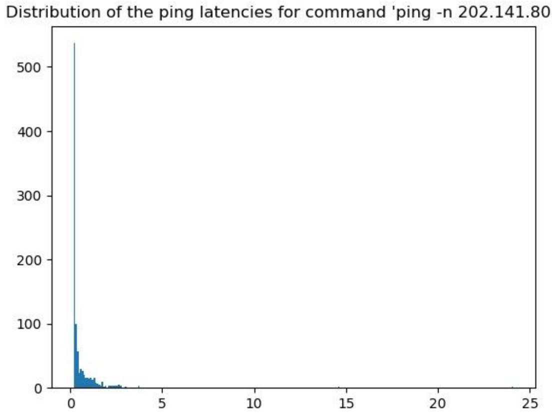
(b) For command *ping -n 202.141.80.14* :

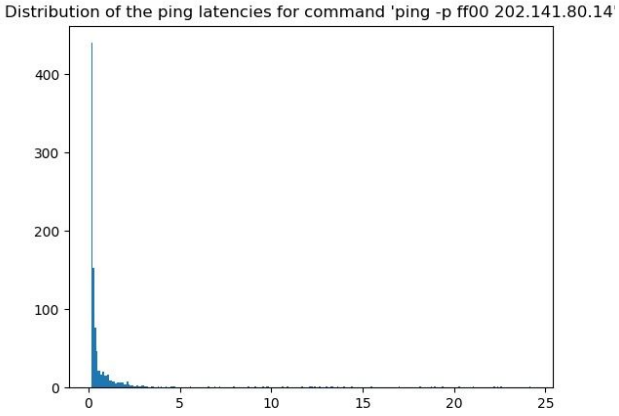
Minimum = 0.183ms, Maximum = 24.1ms, Mean = 1.040ms, Median = 0.247ms

For command *ping -p ff00 202.141.80.14* :

Minimum = 0.146ms, Maximum = 24.2s, Mean = 1.030ms, Median = 0.248ms

(c)


Distribution of the ping latencies for command 'ping -n 202.141.80.14'


Distribution of the ping latencies for command 'ping -p ff00 202.141.80.14'

(d) In cases of the particular pattern, as in our case, that doesn't have sufficient transitions, such as all ones or all zeros,there is problem in correctly identifying packets. There are good chances of error. So, Packet loss should be higher in case of our pattern. Another point to note is that ping -n doesn’t look up dns server which makes it faster from the usual ping command.

4. ***Ifconfig***

ifconfig **-** It shows all the information of all the network interfaces. Information like : Link encap, Hardware Address, RX and TX Packets, etc. It also helps in configuring an interface, enabling and disabling an interface.

sudo ifconfig eno1 10.1.2.67 netmask 255.255.252.0 broadcast 10.1.3.255

- **Link encap:Ethernet** - This denotes that the interface is an Ethernet related device.
- **HWaddr -** This is the hardware address or MAC address which is unique to each Ethernet card which is manufactured.
- **inet addr** - It indicates the machine IP address.
- **Bcast** - It denotes the broadcast address.
- **Mask** - It is the network mask which we have set in the netmask option.
- **UP** - This flag indicates that the kernel modules related to the Ethernet interface has been loaded.
- **BROADCAST** - Denotes that the Ethernet device supports broadcasting.
- **RUNNING** - The interface is ready to accept data.
- **MULTICAST** - This indicates that the Ethernet interface supports multicasting.
- **MTU** - MTU stands for Maximum Transmission Unit. It is the size of each packet received by the Ethernet card.
- **Metric -** The value of this property decides the priority of the device, lower the better.

- **RX Packets, TX Packets** - These show the total number of packets received and transmitted respectively.
- **collisions** - Greater than zero value means collision, sign of network congestion.
- **txqueuelen** - This denotes the length of the transmit queue of the device.
- **RX Bytes, TX Bytes** - These indicate the total amount of data that has passed through the Ethernet interface either way.

route

route command displays routing table resides in kernel and also used to modify the routing table.The tables which specifies how packets are routed to a host is called routing table.
It displays the table containing following colums :
Destination -Indicates the IP address of desination host/network.
Gateway - Indicates gateway from which desination host/network could be reached
Genmask - Indicates the subnetmask destination
Flags - Indicates the current status of route (U-Route is up, H-Target is a host, G-Use gateway)
Iface - Indicates the interface

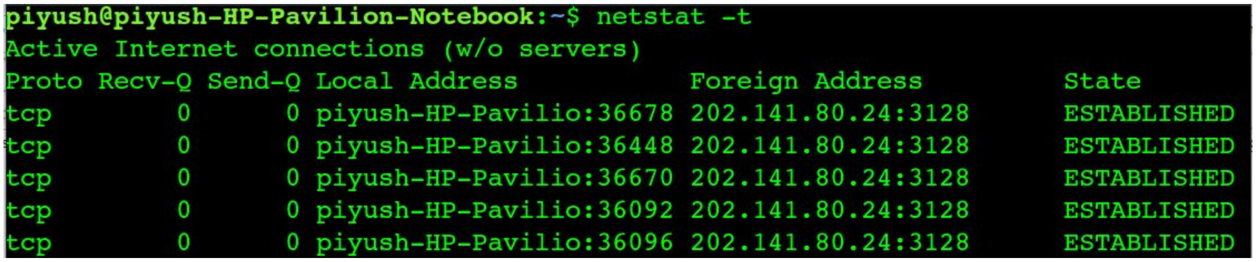
Options :
-n : dispalys routing table in numerical[IP Address] format
-e : dispalys routing table in Hostname format
add : Adds a new route to the routing table
del : Deletes a route from the routing table
Options used with add and del :
-net : Indicate the target is network
-host : Indicate the target is host
gw : Specifies the gateway of target host/network
netmask : Used to specifiy the subnet-mask of destination network/host
dev : Specify the device or interface where the packets will be sent
reject : rejects the packets sent to particular route/host

5.

netstat

netstat ("network statistics") is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.
It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement. It prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Output of ***netstat -t*** :



```
piyush@piyush-HP-Pavilion-Notebook:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 piyush-HP-Pavilio:36678 202.141.80.24:3128      ESTABLISHED
tcp        0      0 piyush-HP-Pavilio:36448 202.141.80.24:3128      ESTABLISHED
tcp        0      0 piyush-HP-Pavilio:36670 202.141.80.24:3128      ESTABLISHED
tcp        0      0 piyush-HP-Pavilio:36092 202.141.80.24:3128      ESTABLISHED
tcp        0      0 piyush-HP-Pavilio:36096 202.141.80.24:3128      ESTABLISHED
```

Proto The protocol (**tcp**, **udp**, **raw**) used by the socket.
Recv-Q The count of bytes not copied by the user program connected to this socket.
Send-Q The count of bytes not acknowledged by the remote host.
Local Address Address and port number of the local end of the socket.
Foreign Address Address and port number of the remote end of the socket.
State The state of the socket. Since there are no states in raw mode and usually no states used in UDP, this column may be left blank.

netstat -r : Display the kernel routing tables.
Output fields :

- **Destination** : The destination network or destination host.
- **Gateway** : It shows the gateway the routing entry points to.
- **Genmask** : The netmask for the destination network; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
- **Flags** : Possible flags includeU (route is up), H (target is a host), G (use gateway), etc.
- **Metric** : The distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
- **Ref** : Number of references to this route. (Not used in the Linux kernel.)
- **Use** : Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
- **Iface** : Interface to which packets for this route will be sent.
- **MSS** : Default maximum segment size for TCP connections over this route.
- **Window** : Default window size for TCP connections over this route.
- **irtt** : Initial RTT (Round Trip Time). The kernel uses this to guess about the best TCP protocol parameters without waiting on (possibly slow) answers.

Display network interface : ***netstat -i***

Netstat command to display **number of interfaces on your machine.**

Loopback Interface : The loopback device is a special, virtual network interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine.
It can perform the following functions:

- Device identification—The loopback interface is used to identify the device.
- Routing information—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as ping mpls require a loopback address to function correctly.
- Packet filtering—Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

The Internet Protocol (IP) specifies a loopback network with the (IPv4) address 127.0.0.0/8. Most IP implementations support a loopback interface (lo0) to represent the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6. The standard domain name for the address is localhost.

6.
(1.) Number of hops :

@1AM
www.amazon.com - 7, *www.google.com* - 7, *www.amazon.co.uk* : 6 and incomplete path, *www.linkedin.com* - 8, *www.nic.ru* - 11
@9AM
www.amazon.com - 7, *www.google.com* - 7, *www.amazon.co.uk* : 9, *www.linkedin.com* - 8, *www.nic.ru* - 11
@7PM
www.amazon.com - 7, *www.google.com* - 7, *www.amazon.co.uk* : 6 and incomplete path, *www.linkedin.com* - 8, *www.nic.ru* - 11
Common hops : Hops 77.93.199.253 and 83.167.254.142 were common among all of the five sites. Other than that, *www.nic.ru* and *www.linkedin.in* had 62.115.147.38 and 62.115.137.40 in common. 62.115.147.38 was common in *www.amazon.co.uk* and *www.amazon.com* .

(2.) Yes, route to same host changes at different times of the day. Because there are different servers at different locations for some hosts. Also There are different paths (series of hops) for the same server. The packet chooses the next hop considering the network congestion in the path. So, route changes as per traffic which may vary at different times of the day.

(3.) Traceroute does not find complete path for *www.amazon.co.uk* . There could be number of reasons for this, like :

- The network connection between the server on those hops is broken.
- The server on the those hops is down.
- There is some problem with the way in which the server on those hops has been setup.

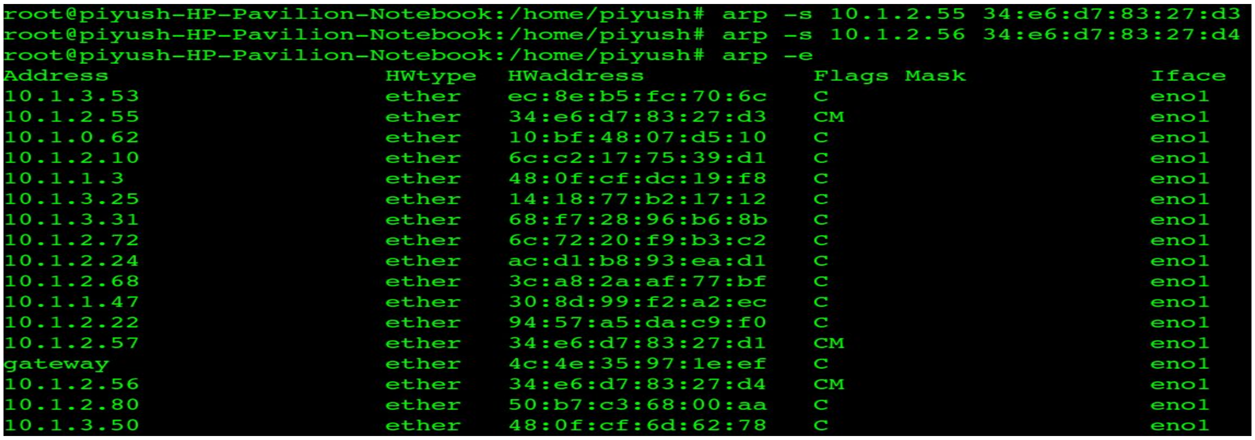
(4.) Yes, it is possible to find the route to certain hosts which fail to respond with ping experiment. Ping is straight ICMP from point A to point B, that traverses networks via routing rules. Traceroute works very different, even though it uses ICMP. Traceroute works by targeting the final hop, but limiting the TTL and waiting for a time exceeded message, and then increasing it by one for the next iteration.

7. The ***arp -e*** command would display full ARP table for your machine in Linux style and ***arp -a*** in BSD style.

- Address : The protocol address (IPv4 Address) of the intended receiver.
- HWtype : It specifies the type of hardware used for the local network transmitting the Address Resolution Protocol (ARP) message.
- HWaddress : Layer 2 (MAC Address) of the intended receiver.
- Flags : It can be **- C** (complete), **M** (permanent), and **P** (publish).
- Iface : Network Interface.

Add entry in arp table : An entry is added after the ***arp -s ip-address 10.0.0.1 XX:XX:XX:XX:XX:XX*** command. So the arp table has been manually updated here.
Delete entry from arp table *:* The entry would not be removed from the arp table after the ***arp -d 10.0.0.1*** command. This changes its hardware address to a sign of **<incompelete>** instead.

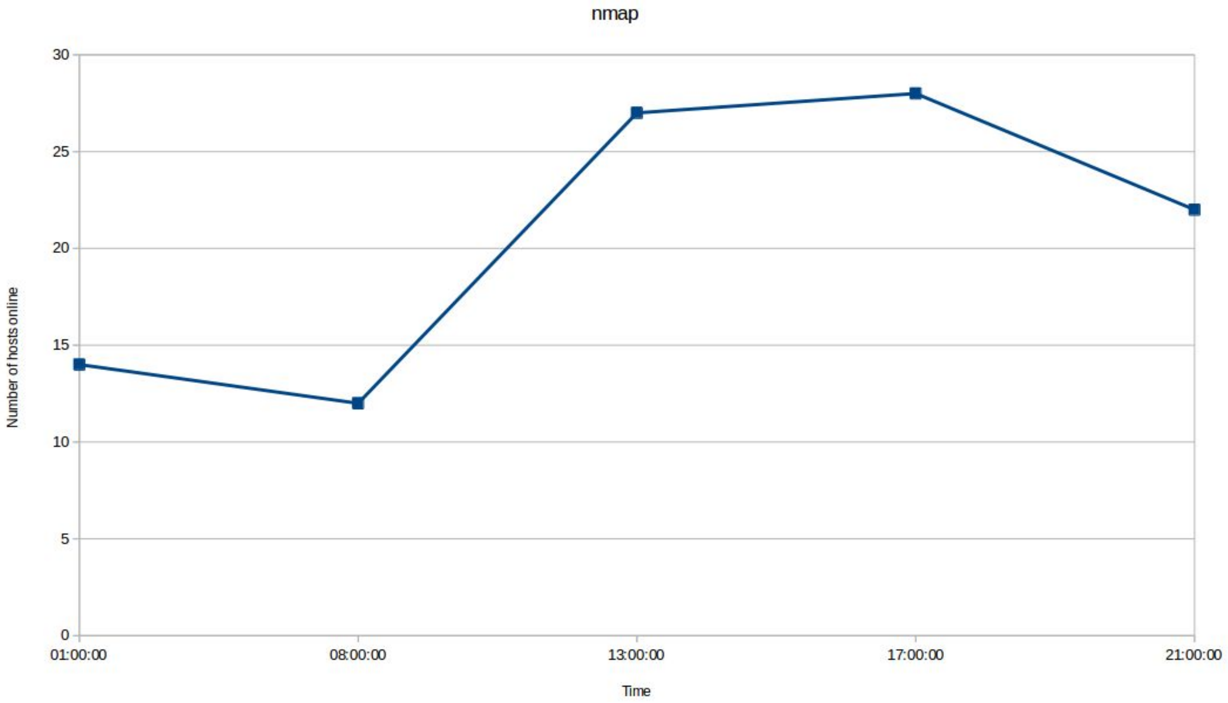
Add two entries :



```
root@piyush-HP-Pavilion-Notebook:/home/piyush# arp -s 10.1.2.55 34:e6:d7:83:27:d3
root@piyush-HP-Pavilion-Notebook:/home/piyush# arp -s 10.1.2.56 34:e6:d7:83:27:d4
root@piyush-HP-Pavilion-Notebook:/home/piyush# arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.3.53                ether   ec:8e:b5:fc:70:6c   C                     eno1
10.1.2.55                ether   34:e6:d7:83:27:d3   CM                    eno1
10.1.0.62                ether   10:bf:48:07:d5:10   C                     eno1
10.1.2.10                ether   6c:c2:17:75:39:d1   C                     eno1
10.1.1.3                 ether   48:0f:cf:dc:19:f8   C                     eno1
10.1.3.25                ether   14:18:77:b2:17:12   C                     eno1
10.1.3.31                ether   68:f7:28:96:b6:8b   C                     eno1
10.1.2.72                ether   6c:72:20:f9:b3:c2   C                     eno1
10.1.2.24                ether   ac:d1:b8:93:ea:d1   C                     eno1
10.1.2.68                ether   3c:a8:2a:af:77:bf   C                     eno1
10.1.1.47                ether   30:8d:99:f2:a2:ec   C                     eno1
10.1.2.22                ether   94:57:a5:da:c9:f0   C                     eno1
10.1.2.57                ether   34:e6:d7:83:27:d1   CM                    eno1
gateway                  ether   4c:4e:35:97:1e:ef   C                     eno1
10.1.2.56                ether   34:e6:d7:83:27:d4   CM                    eno1
10.1.2.80                ether   50:b7:c3:68:00:aa   C                     eno1
10.1.3.50                ether   48:0f:cf:6d:62:78   C                     eno1
```

By default, entries stay cached in the ARP table for 60 seconds.
Trial-and-error method : We may use a bisection method and try by error. For example, we guess the timeout value of 60 mins and then make the system clock 60 mins faster and see what happens. Try 30 mins if the arp cache has been cleared or some value bigger if it hasn’t.
I use the “arp -s” command to set a new entry and bind another Intranet IP address 10.1.2.12 with the hardware address of 10.1.2.10 (originally in the table). So, they both share the same hardware address. On pinging 10.1.2.12 (added IP), I see that the response is received from the original IP address (10.1.2.10) as well with same sequence number.

8. *nmap -n -sP 172.16.114.001-050*


nmap
Number of hosts online
01:00:00
08:00:00
13:00:00
17:00:00
21:00:00
Time