CS342 Computer Networks Assignment 1

Name: Samay Varshney *Roll No: 180101097*

Answer 1:

a) The option required to specify the number of echo requests to send with ping command is **'- c'**.

b) The time interval between two successive ping requests can be set using **'- i'** option (time in seconds). However, normal users cannot set the interval to values less than 0.2 seconds.

c) We can send packets to the destination one after another without waiting for a reply by using the **'- l'** option. Normal users can only send 3 packets using this option. Also, the destination can be flooded with ping requests by using **'- f'** option.

d) The data size can be set with the '**- s'** option (in Bytes). The actual packet size will be larger than what we give due to the addition of the ICMP Header data (8 Bytes). Hence, total packet size will be 40 bytes, if data size is set as 32 bytes.

Answer 2:

- Test PC was connected to IIT Guwahati Lab PC while performing the experiment.

Destination Host Address	IP Address	Geographic Location	Avg RTT1 (ms)	Avg RTT2 (ms)	Avg RTT3 (ms)	Total Avg RTT (ms)
codeforces.com	81.27.240.126	Sankt-Peterburg	429.881	472.061	501.074	467.672
youtube.com	172.217.168.238	California	690.210	665.926	588.520	648.218
Justpakit.com	217.70.184.55	Ile-de-France	445.915	463.929	290.259	400.034
codingninjas.com	13.224.2.127	Washington	594.216	605.015	582.604	593.945
adidas.com	213.95.138.236	Bayern-Germany	485.941	492.258	423.996	467.398
vidyabharatischool.org	172.104.163.78	Singapore	252.173	238.885	178.268	223.108

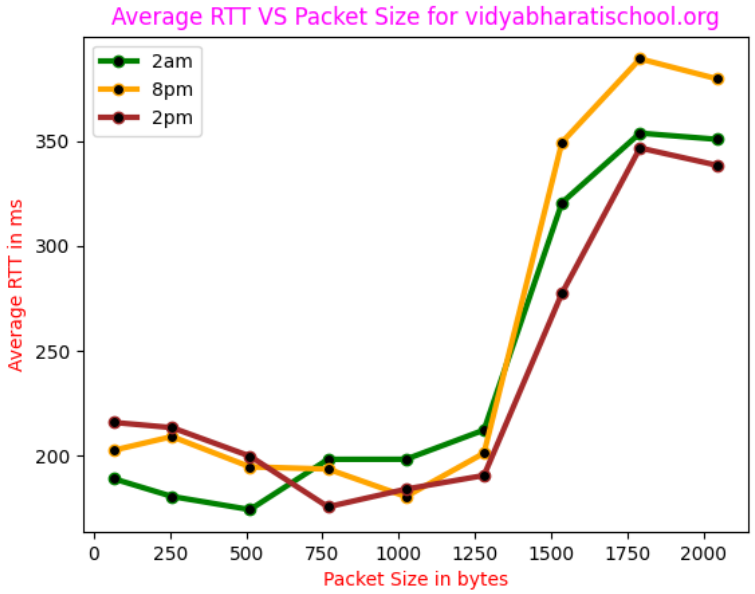
a) There exists a **weak** positive correlation between distance and Round-Trip Time (RTT) because of reasons like increased number of hops and increased propagation delay. At each router, there may be a delay, so if packets have to go through **more distance**, thus more routers, therefore **longer** the RTT. It is a weak relation because there are many other factors on which it depends like network traffic and the server capacities.

b) No cases of packet loss greater than **0%** was found. But in general, packet loss can be greater than 0% because of network congestion and traffic. There could be restrictions on source IP address that can access. Some packets may not able to reach destination within time and result in packet loss which can be because of blocking by firewall. Sometimes, there may be 100% packet loss.

c) I took *vidyabharatischool.org* for experimenting with packets of size from 64 bytes to 2048 bytes. The readings were taken at **2.00am**, **8.00pm**, **2.00pm** (IST) respectively.

Size (Bytes)	64	256	512	768	1024	1280	1536	1792	2048
Avg RTT 1 (ms)	189.173	180.710	174.433	198.399	198.420	212.349	320.631	353.784	350.795
Avg RTT 2 (ms)	202.694	209.226	194.802	193.756	180.637	211.340	349.374	389.181	379.531
Avg RTT 3 (ms)	215.989	213.496	199.902	165.759	154.200	181.697	277.521	346.711	338.367

d) DAY TIME: We observed that RTT vary with time of the day. At different times, the congestion in network is different.



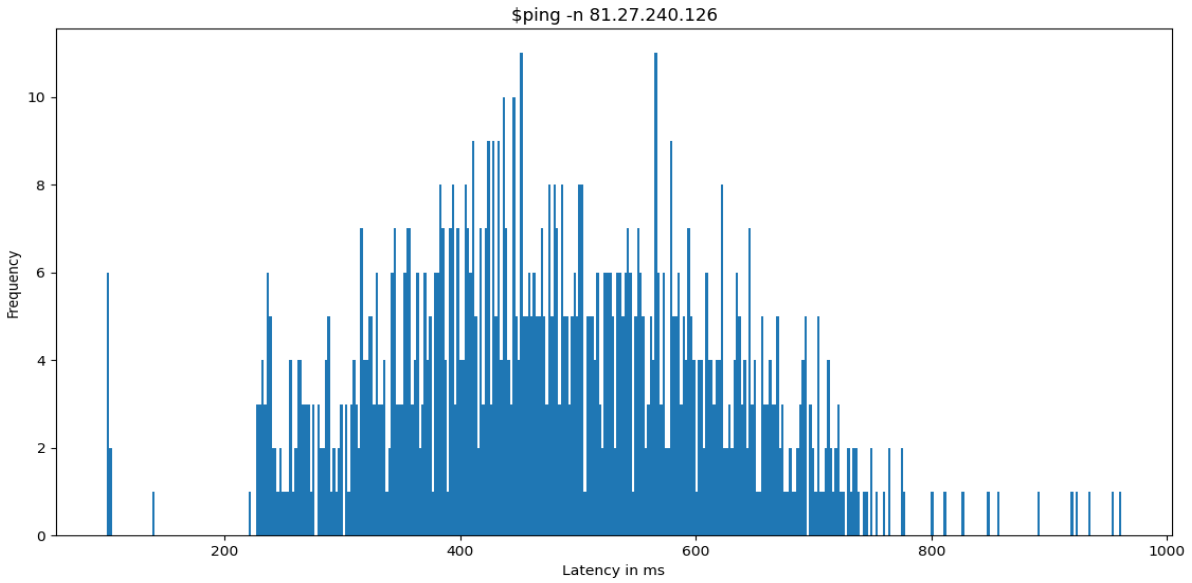
From the observations, we can say that RTT is least at 2:00 pm and maximum at 8:00pm. Around 2:00pm, RTT is little less than that at 2:00am. Hence, we can conclude that the network traffic is high around 8:00pm.

PACKET SIZE: We can clearly observe that the RTT is almost same for packets up to size 1280 Bytes. After that there is a sudden jump in the RTT. This is because the Maximum Transmission Unit (MTU) is 1500 Bytes by default. If the packet size is less than 1500 Bytes, then only one frame is sent. Hence for packets with size less than 1500 Bytes, the RTT is same. If packet size is more than 1500 Bytes, then the packet is broken into two frames of size 1500 Bytes. Hence, we observe an almost twice the RTT for packets of size 1536 bytes to 2048 bytes.

Answer 3:

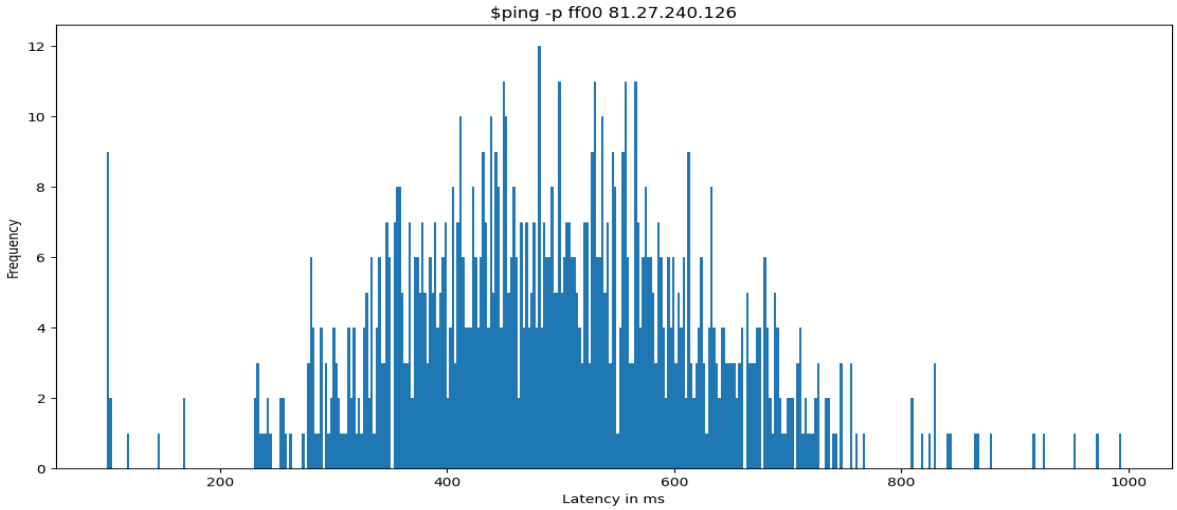
a, b, c) I choose IP Address **81.27.240.126** itself.

Command	Packets Sent	Packets Received	Packet Loss Rate	Min Latency	Max Latency	Mean Latency	Median Latency
$ ping -n 81.27.240.126	1000	1000	0%	222.781	1395.731	489.037	145.071
$ ping -p -ff00 81.27.240.126	1000	1000	0%	231.057	1693.875	509.386	150.765



d) On plotting the curves as histograms, we observe that the two cases are very similar to each other except in few aspects. Firstly, no attempt will be made to lookup symbolic names for host addresses and will go without **dns resolution** when using **'-n'**, hence it will be faster. Hence, the mean Latency is higher in second case than in the first

case. Secondly **'-p ff00'** will cause the sent packet to be filled with the pattern 11111100000000 which is useful for diagnosing data-dependent problems in a network. This will cause problems with the synchronisation of the clocks as



only one transition is present, from 1 to 0 and we observe that the packet loss is higher in the second case.

Answer 4:

```
samay@samay-Precision-Tower-3620:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.114.209  netmask 255.255.255.128  broadcast 172.16.114.255
        inet6 fe80::f7ee:5635:22d0:7d36  prefixlen 64  scopeid 0x20<link>
        ether 54:bf:64:5d:33:ed  txqueuelen 1000  (Ethernet)
        RX packets 75420540  bytes 9341359090 (9.3 GB)
        RX errors 1  dropped 30765029  overruns 0  frame 1
        TX packets 127746  bytes 9705114 (9.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef100000-ef120000

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 14116  bytes 1325280 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14116  bytes 1325280 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:af:b2:2e  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
```

a) Ifconfig displays the status of currently active interfaces. enp0s31f6, lo and virbr0 are the names of **active network interfaces** on the system.

1) **enp0s31f6** is the first ethernet interface. Others are lo, virbr0.

2) **lo** is the loopback interface. This is the special network interface which system uses to communicate with itself.

inet, inet6: IPv4 and IPv6 addresses assigned to the interface respectively.

netmask: Network mask that shows how much of the address is routable, which determines whether the computer can connect directly to a device on the LAN or whether it needs to send the packet to a router.

broadcast: Denotes the broadcast address associated with that interface.

RUNNING: Indicates that the network interface is operational and is ready to accept the data.

MULTICAST: Denotes that the Ethernet interface supports multicasting.

MTU:1500: The maximum transmission unit for which the interface is configured. It is the size of the packet received by the Ethernet card.

RX packets: Total number of received packets. Errors: Number of damaged packets received. Dropped: Number of dropped packets due to reception errors. Overruns: Number of received packets that experienced data overruns. Frame: Number of received packets that experienced frame errors.

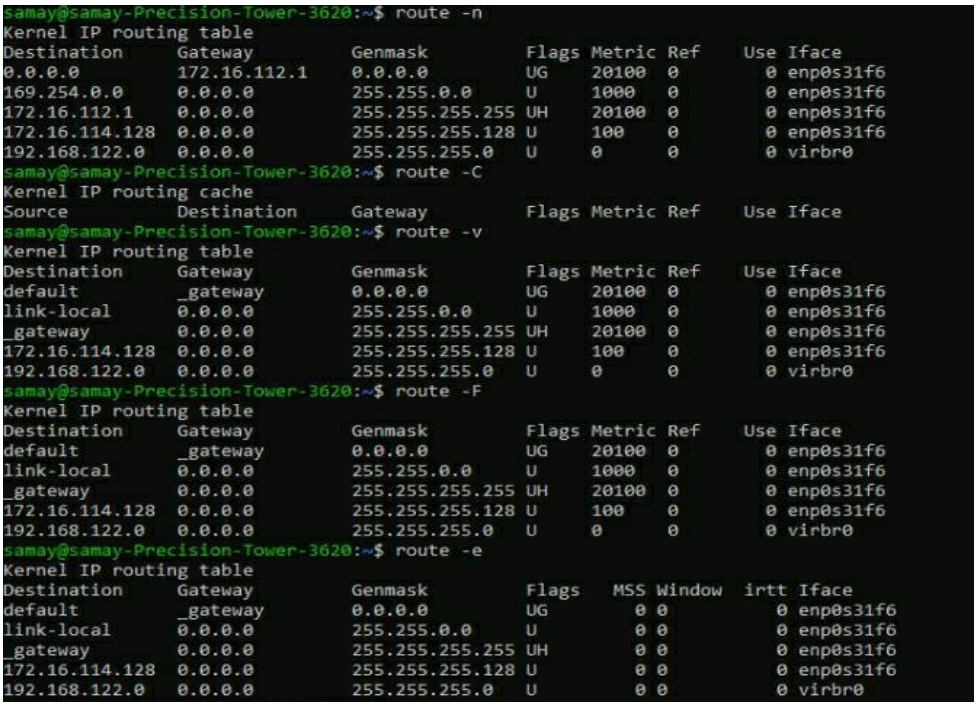
TX packets: Total number of transmitted packets. Errors: Number of packets that experienced transmission error. Dropped: Number of dropped transmitted packets due to transmission errors. Overruns: Number of transmitted packets that experienced data overruns. Carrier: Number received packets that experienced loss of carriers. Collisions: Number of packets that are colliding while traversing the network due to network congestion.

txqueuelen: Length of the transmit queue of the NIC.

RX, TX bytes: Indicates the total amount of data that has passed through the interface either way.

b) Some options for ifconfig includes

- **-a** to display information for all network interfaces, both active and inactive.
- **-v** for verbose mode, to display additional information for each network interface.
- **-s** for the shortlisting option, which shows a one-line summarized listing of data about each interface.
- **up** and **down** flag causes the activation and deactivation of interface respectively.
- **metric N** sets the interface metric, which is used by the interface to make routing decision.
- **add** and **del** <address> to add and remove an IPv6 address to an interface respectively.



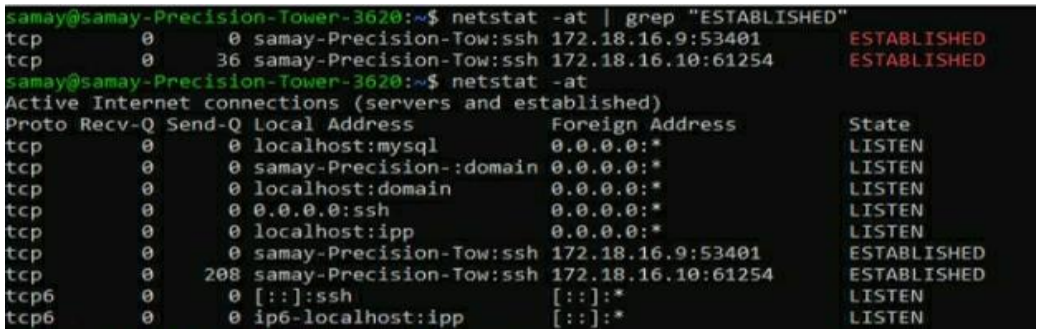
c) Route command is used to **view and manipulate the IP routing tables** in both UNIX and Windows. Its primary use is to setup static routes to specific hosts or networks.

The destination column identifies the destination host. The Gateway column identifies the defined gateway for the specified network. An * appears in this column if no forwarding gateway is needed for the network. The Genmask column shows the netmask for the network. The Iface column shows the network interface. **'enp0s31f6'** is for the Ethernet device and '**virbr0**' is for the Wireless Ethernet device.

Some of the Flags are: **U**(route is up), **G**(use gateway), **H**(target is host). Metric is the distance to the target counted in hops. Ref is the number of references to this route.

d) Route command has many options: **'-n'** is used to display the numerical IP address instead of symbolic host names. **'-C'** is used to list the kernel's routing cache information. **-F** to operate on the kernel's FIB routing table. **'-v'** to select verbose operation. **-e** to use **netstat (8)** format for displaying routing table. **'-net'** specifies that the target is a network and **'-host'** specifies that the target is a host. **'del'** to delete a route and **'add'** to add a route.

Answer 5:



a) netstat *(network statistics)* is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc. It displays active **TCP connections**, ports on which

the computer is listening, IP routing table, Ethernet, IPv4 and IPv6 statistics. It is one of the most basic network services debugging tool.

b) **-at** option is used to list all TPC connections and pipe operator with grep command is used to filter all established connections. **$ netstat -at | grep "ESTABLISHED"**.

c) The **-r** option of netstat displays the IP routing table. **Destination:** It indicates the destination of a packet. When a packet has to be sent over the network, this table is examined top to bottom, and the first line with a matching destination is then used to determine where to send the packet. **Gateway:** It tells the computer where to send a packet that matches the destination. An * here means send locally.

```
samay@samay-Precision-Tower-3620:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s31f6
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp0s31f6
_gateway        0.0.0.0         255.255.255.255 UH        0 0          0 enp0s31f6
172.16.114.128  0.0.0.0         255.255.255.128 U         0 0          0 enp0s31f6
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
samay@samay-Precision-Tower-3620:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s31f  1500 75682319      1 30891492 0       131185      0      0      0 BMRU
lo       65536    15707      0      0 0        15707      0      0      0 LRU
virbr0    1500        0      0      0 0            0      0      0      0 BMU
```

Genmask: The netmask for the destination net; 255.255.255.0 for a host destination and 0.0.0.0 for the default host.

Flags: It displays the flags that describe the route – G(uses gateway), U(interface up), H(single host), D(dynamically created), !(reject route).

MSS: Default maximum segment size for TCP connection over route. **Window:** Maximum amount of data the system will accept in a single burst from a remote host. **Irtt:** Initial round trip time. **Iface:** Tells which network interface should be used for sending packets that match the destination.

```
samay@samay-Precision-Tower-3620:~$ netstat -aus
IcmpMsg:
    InType0: 45
    InType3: 55
    InType8: 119
    OutType0: 26
    OutType3: 57
    OutType8: 82
Udp:
    18147 packets received
    7 packets to unknown port received
    0 packet receive errors
    19711 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 516881
UdpLite:
IpExt:
    InMcastPkts: 1194
    OutMcastPkts: 761
    InBcastPkts: 516974
    OutBcastPkts: 11
    InOctets: 74541314
    OutOctets: 5529088
    InMcastOctets: 110631
    OutMcastOctets: 57694
    InBcastOctets: 35176700
    OutBcastOctets: 503
    InNoECTPkts: 614639
    InECT0Pkts: 4
```

d) **netstat -i | wc -l** gives number of interfaces +2 as the output and **netstat -i** can be used to display the status of all network interfaces. My machine has 3 interfaces, which are **enp0s31f6**, **lo**, **virbr0**.

e) **'-a -u -s'** options of netstat can be used to show the statistics of all UDP connections.

f) **Loopback interface** is a special, **virtual** network interface that the computer uses to communicate with itself. It is used mainly for **diagnostics** and **troubleshooting** and to connect to servers running on the local machine. When a network interface is disconnected then no communication on that interface is possible, not even between the computer and itself. The loopback interface does not represent any actual hardware, but exists so applications running on the computer can always connect to servers on the same machine. For example, if you run a web server and have all your web documents so you could examine them file by file on the local machine.

Answer 6:

- Test PC was connected to IIT Guwahati Lab PC while performing the experiment.

Host Name	Hop Count #1 (2am)	Hop Count #2 (2pm)	Hop Count #3 (8pm)
codeforces.com	Trace aborted/Reached Firewall	Trace aborted/Reached Firewall	Trace aborted/Reached Firewall
youtube.com	26	27	26
Justpakit.com	27	28	28
codingninjas.com	27	27	27
adidas.com	24	24	24
vidyabharatischool.com	19	19	18

a) **Traceroute** is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between, allowing administrators to better resolve connectivity issues. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

b) Hops are common because of the reason that routes to these destinations pass through the same internet circles and hence overlap. The **common hops** of the six hosts are:

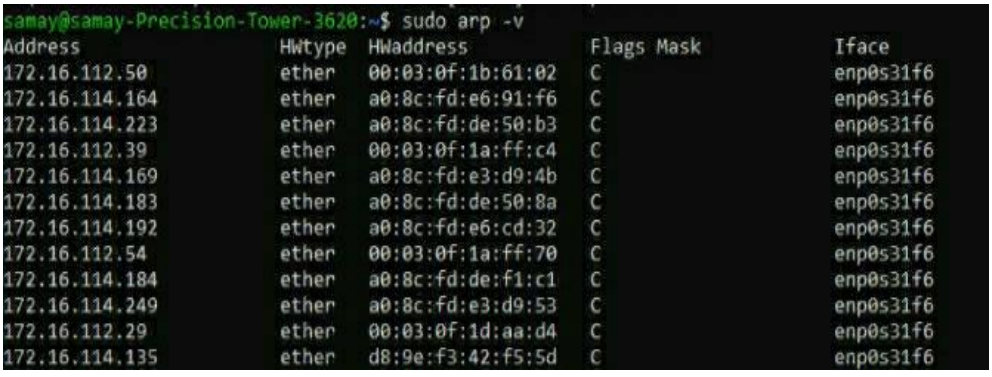
Host Name	Common Hops (IP Address)
codeforces.com	10.70.238.142, 10.71.71.2, 10.73.39.33, 103.198.140.29, 103.198.140.56, 103.198.140.75, 103.198.140.77, 172.17.115.4, 192.168.43.1, 192.168.44.54, 192.168.44.59, 81.27.240.126
youtube.com	10.71.71.2, 108.170.234.129, 108.170.241.161, 142.250.231.178, 172.17.115.4, 172.253.65.165, 192.168.43.1, 192.168.44.54, 192.168.44.58, 209.85.252.245, 72.14.216.200, 72.14.232.71
Justpakit.com	103.198.140.164, 103.198.140.56, 155.133.187.24, 172.17.115.4, 192.168.43.1, 195.66.225.161, 217.70.176.121
codingninjas.com	10.71.71.18, 172.17.115.4, 192.168.43.1, 192.168.44.53, 192.168.44.58, 192.168.44.59
adidas.com	10.71.71.2, 103.198.140.29, 130.117.0.18, 130.117.0.62, 154.54.37.217, 172.17.115.4, 192.168.43.1
vidyabharatischool.com	139.162.0.6, 172.17.115.4, 192.168.43.1, 192.168.44.54, 192.168.44.55, 27.111.228.235, 49.45.4.251

c) The route to the hosts can change at different times of the day because of network congestion. The packets are redirected to take a route having less traffic. The load balancing is done to reduce the load of the path taken.

d) **Yes**, traceroute for **codeforces.com** did not find complete paths to the hosts as it shows trace aborted at the end. It may be because **Firewall** of that host might be blocking our IP which blocks the ICMP Traffic or we **need to increase** max hops as packets might not reach destination within fixed max hops or there can be **packet loss** between routers in between the path.

e) **Yes**, it is possible to find the route to certain hosts which fail to respond with ping experiment. The ping and traceroute both use the ICMP Packets but their working is different. Ping is straight ICMP and failing ping might be because of blocked packet transmission while traceroute uses an **error message** from hop to find the route. Traceroute sends packets with TTL values that increases from packet to packet. Traceroute looks for the **ICMP Time exceeded** packet and that is why it might be possible.

Answer 7:



a) ARP stands for Address Resolution Protocol. I used for Linux **$ sudo arp -a** to show the full ARP Table for my machine. The table has six columns:

1) **Address:** Represents IP Addresses of network connections.

2) **HWtype**: Represents hardware type of the machine.

3) **HWaddress:** Represents hardware address of the machine of respective rows networks.

4) **Flags:** Complete entries are marked with C flag. Permanent entries are marked with M and published with P respectively. 5) **Mask:** Represents Genmask. 6) **Iface:** Represents network interfaces.

b) An entry for the IP address can be deleted from the ARP table using the command **$ arp –d <address>**. If you want to make a specific MAC address be used for an IP, use the command: **$ arp -s <IP_addr> <MAC_addr>**. You need to run it as a root user.

```
samay@samay-Precision-Tower-3620:~$ sudo arp -sv 172.16.114.238 ff:ff:ff:ff:ff:ff
arp: SIOCSARP()
samay@samay-Precision-Tower-3620:~$ sudo arp -sv 172.16.114.239 ff:ff:ff:ff:00:00
arp: SIOCSARP()
samay@samay-Precision-Tower-3620:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.112.50            ether   00:03:0f:1b:61:02   C                     enp0s31f6
172.16.114.164           ether   a0:8c:fd:e6:91:f6   C                     enp0s31f6
172.16.114.223           ether   a0:8c:fd:de:50:b3   C                     enp0s31f6
172.16.112.39            ether   00:03:0f:1a:ff:c4   C                     enp0s31f6
172.16.114.169           ether   a0:8c:fd:e3:d9:4b   C                     enp0s31f6
172.16.114.183           ether   a0:8c:fd:de:50:8a   C                     enp0s31f6
172.16.114.192           ether   a0:8c:fd:e6:cd:32   C                     enp0s31f6
172.16.114.238           ether   ff:ff:ff:ff:ff:ff   CM                    enp0s31f6
172.16.112.54            ether   00:03:0f:1a:ff:70   C                     enp0s31f6
172.16.114.184           ether   a0:8c:fd:de:f1:c1   C                     enp0s31f6
172.16.114.249           ether   a0:8c:fd:e3:d9:53   C                     enp0s31f6
172.16.112.29            ether   00:03:0f:1d:aa:d4   C                     enp0s31f6
172.16.114.135           ether   d8:9e:f3:42:f5:5d   C                     enp0s31f6
172.16.114.196           ether   a0:8c:fd:e6:cd:29   C                     enp0s31f6
172.16.114.226           ether   a0:8c:fd:e4:57:32   C                     enp0s31f6
172.16.112.44            ether   00:03:0f:1d:ac:0c   C                     enp0s31f6
172.16.114.150           ether   a0:8c:fd:e6:91:f1   C                     enp0s31f6
172.16.114.188           ether   a0:8c:fd:e3:d9:32   C                     enp0s31f6
172.16.114.201           ether   a0:8c:fd:e6:cd:65   C                     enp0s31f6
172.16.114.215           ether   d8:9e:f3:42:ec:7e   C                     enp0s31f6
172.16.114.155           ether   a0:8c:fd:e3:d9:b2   C                     enp0s31f6
172.16.114.161           ether   a0:8c:fd:e3:d9:6e   C                     enp0s31f6
172.16.114.216           ether   a0:8c:fd:de:f1:2d   C                     enp0s31f6
172.16.114.140                   (incomplete)                              enp0s31f6
172.16.114.170           ether   a0:8c:fd:e4:57:52   C                     enp0s31f6
172.16.114.176           ether   a0:8c:fd:e4:57:8c   C                     enp0s31f6
172.16.114.235           ether   a0:8c:fd:de:50:14   C                     enp0s31f6
172.16.114.159           ether   d8:9e:f3:43:0b:b0   C                     enp0s31f6
172.16.112.51            ether   00:03:0f:1b:60:bc   C                     enp0s31f6
172.16.114.165           ether   a0:8c:fd:e6:91:86   C                     enp0s31f6
172.16.114.220           ether   a0:8c:fd:e3:d9:1e   C                     enp0s31f6
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     enp0s31f6
172.16.112.36            ether   00:03:0f:1d:ab:26   C                     enp0s31f6
172.16.114.174           ether   a0:8c:fd:de:50:44   C                     enp0s31f6
172.16.117.213           ether   b0:7f:b9:48:5f:dc   C                     enp0s31f6
172.16.114.180                   (incomplete)                              enp0s31f6
172.16.114.193           ether   a0:8c:fd:e3:d9:64   C                     enp0s31f6
172.16.114.239           ether   ff:ff:ff:ff:00:00   CM                    enp0s31f6
```

c) No, there can't be any entry for any IP from different subnet in user's ARP table as subnets will differ between both network interfaces. If the two IP Addresses are on different subnets: it will look for a route to the destination network and then it will send its packet to the appropriate router (or to its default gateway). ARP will be used to find the hardware address of the router as the packet must be delivered to a router which can take care of it. So, the ARP request will not be sent when both communicating devices have different subnets and for both of them to be in ARP table, they both have to communicate using ARP.

d) 100% packet loss after pinging the IP with replaced address. Generally, when other nodes (e.g. my IP) will try to send data to these two nodes then since both are connected to a switch and when traffic from any of these nodes is initiated, the switch will update its Ethernet address table. When these two nodes tend to send traffic continuously, the switch will update its Ethernet address table against the port from which traffic was last received from this Ethernet address. This results in Ethernet address flapping and communication disruption occurs. It will also cause problems with DHCP. Also, the system admin would receive a message of Duplicate Address Detection (DAD) on its machine to try to resolve the situation of duplicated Ethernet addresses.

Answer 8:

a) I chose LAN subnet address 172.16.114.0-255 and used the command **$ nmap -n -sP 172.16.114.0-255** to check which PCs of my subnet are up. It will check all IPs from 172.16.114.0 – 172.16.114.255

b) $ nmap -sA <IP_Address> can be used to detect the firewall settings active on the host.

c) The graph against time to see if there are any hourly trends to when computers are switched ON/OFF in my LAN. Out of **256 hosts** below graph shows number of online hosts. **Trend is that**: Number of online/active hosts increases at night and are less during morning.