CS349 NETWORKS LAB – ASSIGNMENT 1

Saurabh Bazari - 160101061

Q1.

A. ping -c [number] www.google.com
B. ping -i [time interval in sec] www.google.com
C. ping -l [no. of packet] www.google.com Normal user : 3 packets
D. ping -s [size in B] www.google.com
   92 B, slightly larger than what we enter due to the addition of the ICMP header(8 Bytes) and IP Headers(20 Bytes).

Q2.

Reading RTT1 at 06:00 PM, RTT2 at 01:00 AM, RTT3 at 11:00 AM.

DESTINATION HOST ADDRESS	IP ADDRESS	GEOGRAPHIC LOCATION	Avg. RTT1	Avg. RTT2	Avg. RTT3	Total Avg. RTT
google.com	216.58.197.36	California, US	70.251	81.744	104.162	85.385
alibaba.com	47.89.75.243	San Mateo, US	102.137	364.020	122.802	196.319
flipkart.com	163.53.78.128	karnataka, India	77.204	72.058	105.324	84.862
airtel.com	115.111.96.64	Bengaluru, India	66.258	162.195	85.130	104.527
youtube.com	216.58.196.174	California, US	74.604	84.163	92.114	83.627

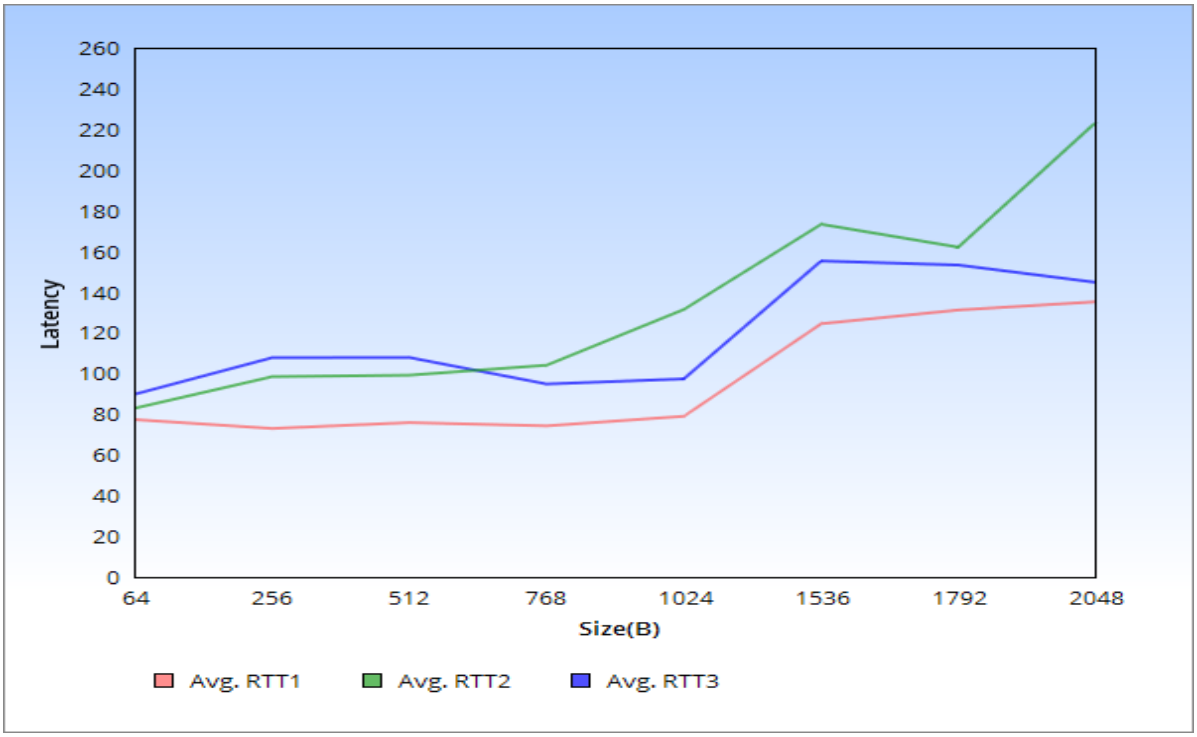
No one show **packet loss** greater than 0%. If we increase count or any specific pattern filled then there may be any packet loss. Packet loss is either caused by errors in data transmission, typically across wireless networks or network congestion. The ICMP Packets have lower priority. So they might take longer time to process in some destination server's queue. Sometimes packet loss is 100% because the destination server is not reachable.
RTT is strongly correlated with a **geographical distance** of the hosts. Like Larger the distance, like Alibaba server in the USA takes more time than India's server like Flipkart. The number of nodes(hops) increases and then network traffic also increases, so RTT is more.

flipkart.com - (163.53.78.128) with range from 64B to 2048B packet size.

Size(B)	64	256	512	768	1024	1536	1792	2048
Avg. RTT 1	77.312	72.951	75.843	74.235	78.961	124.408	131.153	135.189
Avg. RTT 2	82.922	98.420	99.138	104.052	131.449	173.286	162.009	223.244
Avg. RTT 3	89.806	107.744	107.812	94.797	97.318	155.254	153.241	144.742

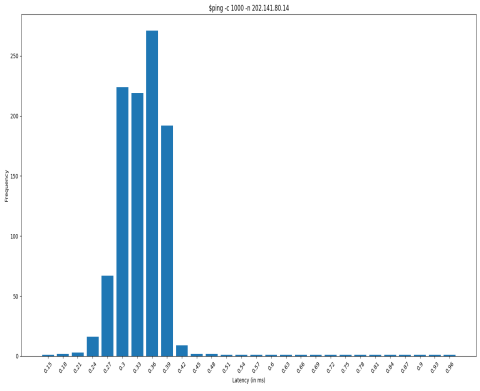
RTT vary with **time of the day**, the different time the network traffic also be different. Like in morning 11 AM, RTT is maximum and around late night for India's server, RTT is less maybe be network traffic is less comparison morning 11 AM. Average network traffic around 6 PM in the evening.
We observed that **packet size** until 1024 almost the same, but after 1024 it increases rapidly almost twice. Ethernet Maximum Transmission Unit was chosen to be 1500 bytes for one packet. If we transmit more then 1500 Bytes then it breaks packet of 1500 B and then transmits so between 1536

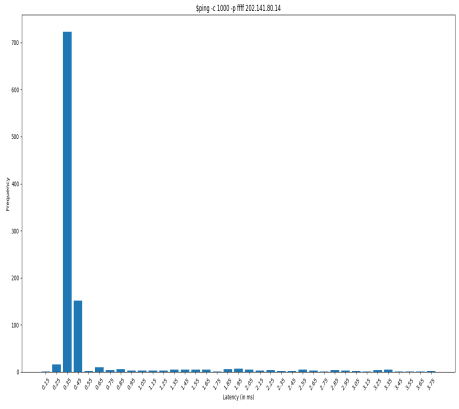
to 2048 it break the packet into two and then transmit so we observed twice RTT then small size packet.



Q3.

Command	Packet Sent	Packet Received	Packet Loss%	Min Latency	Max Latency	Mean Latency	Median Latency
ping -n -c 1000 202.141.80.14	1000	997	0.3%	0.178	0.970	0.323	0.326
ping -p ffff -c 1000 202.141.80.14	1000	973	2.7%	0.217	3.777	0.442	0.318





Mean Latency will be less in **‘-n’** option then another one because option ‘-n’ is used for no attempt will be made to lookup Symbolic name for the host address. So, the first one is faster.
Packet loss will be more in **‘-p ffff’** option then first one, because ‘-p ffff’ option send packet with specific pattern 1111111111111111 which is useful for identifying the nature of the data-dependent

problem in networks. Only one transition is present in the padding, from 1 to 0, so it will cause problems with the synchronization of the clocks. Hence, the clocks are more likely to go out of synchronization in the second case and we observe that the packet loss is higher in the second case.

Q4 **Command: ifconfig -a -v**

Wired ethernet interface (enp4s0f1), a loopback interface (lo) and a wireless ethernet interface (wlp3s0).

```
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.178  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::9f6c:c189:f7d8:3484  prefixlen 64  scopeid 0x20<link>
        ether 80:a5:89:35:ff:17  txqueuelen 1000  (Ethernet)
        RX packets 50694  bytes 35358048 (35.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 51344  bytes 11743628 (11.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

MTU :If IP has a datagram to send and the size of the datagram is larger than the link layer MTU then IP layer breaks the datagram into smaller pieces (fragments), so that each is smaller than the MTU.**UP** indicates that kernel modules related to the interface have been loaded and interface is activated.**BROADCAST** indicates that interface is configured to handle broadcast packets, which is required for obtaining IP address via DHCP.**RUNNING** indicates that interface is ready to accept data.**MULTICAST** indicates that interface supports multicasting.**inet** addr is IPv4 address assigned to the interface.**netmask** is network mask for the interface.**inet6** addr is IPv6 address assigned to the interface.**Scope** is scope of IPv6 address. It can be link-local or global. Link-local address is used in local area network and is not routable. Global address is routable.**ether** is the Hardware Address or the MAC address.**Txqueuelen :** The field provides the information about the configured length of transmission queue.**RX/TX Packets** : The number of packets received/transmitted via the interface. **RX/TX bytes:** The total bytes received/transmitted over this interface. **RX/TX overruns :** The number of received/transmitted packets that experienced data overruns.**RX errors** : The number of damaged packets received. **TX errors :** The number of packets that experienced transmission error. **RX/TX dropped** : The number of dropped packets due to reception/transmission errors. **RX frame :** The number received packets that experienced frame errors. **TX overruns :** The number of packets that experienced data overruns.**TX carriers:** The number received packets that experienced loss of carriers.**TX collisions:** The number of transmitted packets that experienced Ethernet collisions. A nonzero value of this field indicates possibility of network congestion.

Command : route -n

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags  Metric Ref    Use Iface
0.0.0.0         192.168.31.1    0.0.0.0         UG     20600  0        0 wlp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U      1000   0        0 wlp3s0
192.168.31.0    0.0.0.0         255.255.255.0   U      600    0        0 wlp3s0
```

Destination : The destination network or destination host.**Gateway** : The gateway address or â€™*â€™ if none set.**Genmask** : The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route. **Flags** : Possible flags include [**U** (route is up) , **H** (target is a host) , **G** (use gateway) , **R** (reinstate route for dynamic routing) , **D** (dynamically installed by daemon or redirect) , **M** (modified from routing daemon or redirect)]. **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 M : sets MTU of the route to M bytes. **Window W** set the TCP window size for connections over this route to W bytes. **Irtt I** set the initial round trip time (irtt) for TCP connections over this route to I milliseconds (1-12000).
Options: *'-F'* operate on the kernel's FIB (Forwarding Information Base) routing table. This is the default. '*-C*' operate on the kernel's routing cache. '*-v*' select verbose operation. '*-n*' show numerical addresses instead of trying to determine symbolic host names. *'del'* delete a route. '*add'* add a new route. *'-net'* the target is a network. *'-host'* the target is a host.

Q5.

Netstat (network statistics) is a command-line network utility tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of a 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.

```
saurabh@saurabh-X550JX:~/Downloads$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 saurabh-X550JX:38640    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38196    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38642    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38544    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38546    bichitra.iitg.erne:3128 TIME_WAIT
tcp        0      0 saurabh-X550JX:38638    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38542    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38562    bichitra.iitg.erne:3128 ESTABLISHED
tcp        0      0 saurabh-X550JX:38636    bichitra.iitg.erne:3128 ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

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. Unless the --numeric (-n) option is specified, the socket address is resolved to its canonical hostname (FQDN), and the port number is translated into the corresponding service name. **Foreign Address :** Address and port number of the remote end of the socket. Analogous to "Local Address."
State: ***ESTABLISHED*** The socket has an established connection.***LISTEN*** The socket is listening for incoming connections. Such sockets are not included in the output unless you specify the --listening (-l) or --all (-a) option. ***TIME_WAIT*** The socket is waiting after close to handle packets still in the network.

Command : netstat -r . This command for showing routing table which is similar to a **Command** - **route** and all its parameter and field are explained in Q4 route command.

Command: netstat - i **---** display network interface status

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp4s0f1  1500     1801      0      0 0           252      0      0      0 BMU
lo       65536    26948      0      0 0         26948      0      0      0 LRU
wlp3s0    1500   116689      0      0 0        102402      0      0      0 BMRU
```

3 interfaces, which are enp4s0f1 (Wired Ethernet), lo (loopback device), wlp3s0 (Wireless Ethernet).

Loopback: A loopback address is primarily used as a means to validate that the locally connected physical network card is working properly and the TCP/IP stack installed. Typically, a data packet

sent on a loopback address, never leaves the host system and is sent back to the source application. When testing network/IP based applications, it is implemented on a virtual network interface card, which acts an addition to the physical network card. This enables users to test an application with an instance of a server and client on the same machine, with the ability to transmit network data between, even without access to a physical network. In IPv4, 127.0.0.1 is the most commonly used loopback address, however, this can range be extended to 127.255.255.255.

Q6.
Reading Hop Count #1 at 06:00 PM, Hop Count #2 at 01:00 AM, Hop Count #3 at 11:00 AM.

	google.com	alibaba.com	flipkart.com	airtel.com	youtube.com
Hop Count #1	12	22	12	6	12
Hop Count #2	12	22	12	6	13
Hop Count #3	12	22	11	6	12

Common hops found: 10.8.0.1 (My machine) and 206.189.128.253/254 (VPN Service Provider's IP) one of them is same in all experiment. 138.197.249.18, common in google.com, alibaba.com, and youtube.com. 219.65.110.189 common in google.com, airtel.com, and youtube.com. 14.140.100.6, 115.112.71.65, 121.240.1.50 are common in google and youtube. Maybe google and youtube server at same places or in same internet circle, so no. of common hops are more than others.

At a different time of day, network traffic and congestion will be different. According to the load-balancing route always chosen which has less traffic.

Sometimes, traceroute might not find a complete path to some host. Some routers do not provide the information like IP address to a client or may have set up firewalls which block the ICMP Traffic. However, they still send the data to the next router till destination IP or max hop limit is reached.

Yes, it is possible. Ping is straight ICMP from point A to point B, that traverses networks via routing rules and expects an ICMP Reply from the host. Traceroute sends packets with TTL values that gradually increase from packet to packet. Routers decrement TTL values of packets by one and discard packets whose TTL value has reached zero, returning the ICMP error (ICMP Time Exceeded). Traceroute looks for the ICMP Time Exceeded packet and not the ICMP Reply Packet, and that is why it might be possible.

Q7. **Command : arp –a** shows the complete ARP Table

```
saurabh@saurabh-X550JX:~$ arp -v -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.0.1                ether   ec:44:76:74:60:41   C                     enp4s0f1
Entries: 1      Skipped: 0      Found: 1
saurabh@saurabh-X550JX:~$ sudo arp -sv 10.19.1.3 ff:ff:ff:ff:00:00
arp: SIOCSARP()
saurabh@saurabh-X550JX:~$ sudo arp -sv 10.19.1.2 ff:ff:ff:ff:ff:00
arp: SIOCSARP()
saurabh@saurabh-X550JX:~$ arp -v -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.1.2                ether   ff:ff:ff:ff:ff:00   CM                    enp4s0f1
10.19.1.3                ether   ff:ff:ff:ff:00:00   CM                    enp4s0f1
10.19.0.1                ether   ec:44:76:74:60:41   C                     enp4s0f1
Entries: 3      Skipped: 0      Found: 3
saurabh@saurabh-X550JX:~$ sudo arp -d 10.19.1.3
saurabh@saurabh-X550JX:~$ sudo arp -d 10.19.1.2
saurabh@saurabh-X550JX:~$ arp -v -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.0.1                ether   ec:44:76:74:60:41   C                     enp4s0f1
Entries: 1      Skipped: 0      Found: 1
```

It shows the **Address** is the IP address. **HWtype** is the type of the connection of the host.
HWaddress is the MAC address.
Flag: Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag.
Iface: It is the network interface used by the IP host.

Commands : Add entry **: sudo arp -sv <ip> <mac address>** Delete entry **: sudo arp -d <ip>**
IP is mapped to specific MAC addr and involve using arp table to resolve it.

Entries stay cached in the ARP table for **60 seconds**.

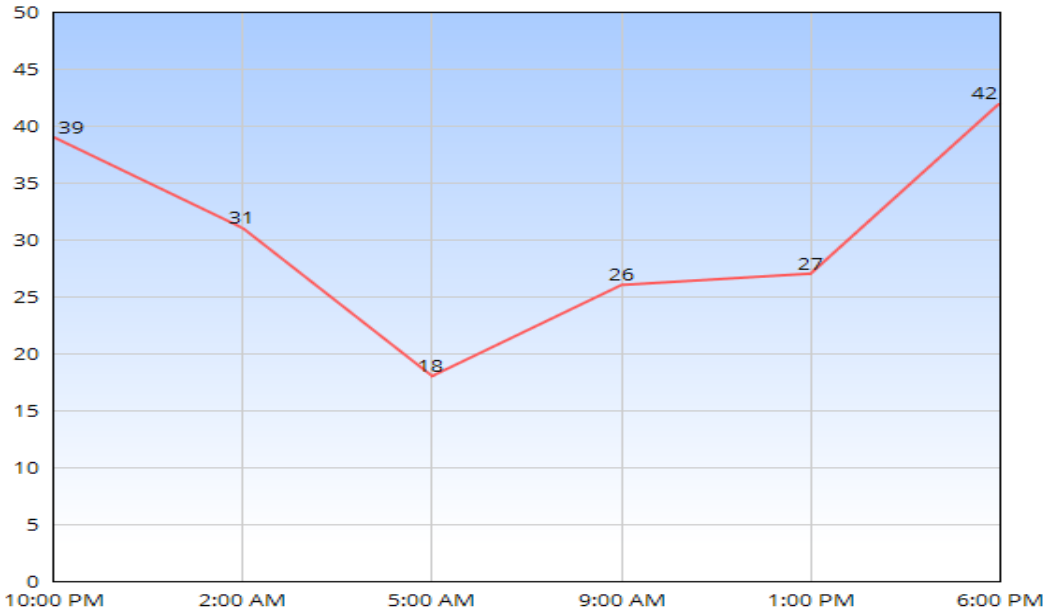
Trial and Error method to discover take enter a dummy entry in arp table and check for random values of time check entry will disappeared or not, for optimizing we use binary search.

When a gateway connects to a range of subnet ranges , same Ethernet address can be assigned to multiple IP. ARP table consists of all IP connected to other subnet range that have ethernet address/MAC address of Gateway. ARP table translates IP address to MAC address and packet are transmitted to Gateway which further directs it to the appropriate device.

Q8.

This IP address range of Kapili Hostel.
Command : nmap –n –sP 10.1.0-3.0-255

Time	10:00 PM	2:00 AM	5:00 AM	9:00 AM	1:00 PM	6:00 PM
No. of hosts Online	39	31	18	26	27	42



From the above graph, we conclude that more host up at evening and decrease at late night and then increase at morning, then almost constant at afternoon because academic after 5 PM again no of host online increases.