CS349 Networks Lab | Name | Roll Number

Assignment 1 | Udbhav Chugh | 170101081

---

1) Ping Command and its options

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

b) The option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs is 'ping -i time".

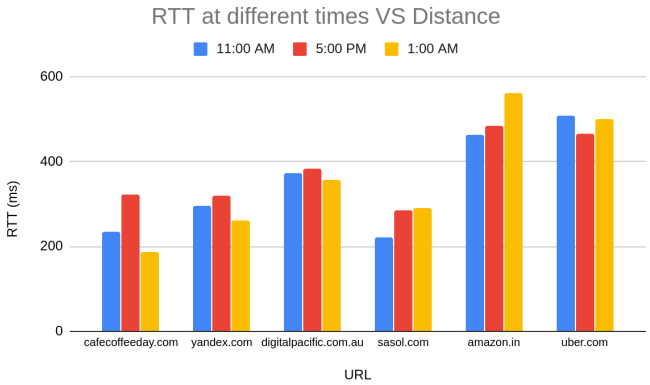
c) The command to send ECHO_REQUEST packets to the destination one after another without waiting for reply is 'ping -l preload'. The limit for sending such ECHO_REQUEST package by normal users is 3. For selecting a value more than 3, a super user is needed.

d) The command to set the ECHO_REQUEST packet size in bytes is 'ping -s packetsize'. ICMP headers (8 bytes in both IPv4 and IPv6) and IP headers (20 bytes in IPv4 and 40 bytes in IPv6) are added to the packet. Hence for a packet size of 32 bytes, the total packet size will be 32+20+8=60 bytes.

2) Ping to various hosts and analysis of RTT changes

- The time chosen to ping were 11:00 AM (RTT 1), 5:00 PM (RTT 2) and 1:00 AM (RTT 3).
- The six hosts that were pinged: cafecoffeeday.com, yandex.com, digitalpacific.com.au, sasol.com, amazon.in, reddit.com.
- The experimenting PC was in Guwahati, Assam (India) using mobile data network.

Host Domain Name	Host IP Address	Host Server Location	Avg. RTT 1 (ms)	Avg. RTT 2 (ms)	Avg. RTT 3 (ms)	Total Avg. RTT (ms)
cafecoffeeday.com	219.65.96.235	Karnataka, Bengaluru	235.329	268.842	187.671	230.614
yandex.com	213.180.204.62	Moscow, Russia	295.112	318.861	261.112	291.695
digitalpacific.com.au	202.130.44.27	Sydney, Australia	372.114	382.667	356.032	370.271
sasol.com	41.76.211.90	Johannesburg, South Africa	221.783	283.901	291.112	265.598
amazon.in	54.239.33.92	Dublin, Ireland	464.118	484.289	561.191	503.199
uber.com	34.98.127.226	San Francisco, US	509.295	465.435	499.878	491.501

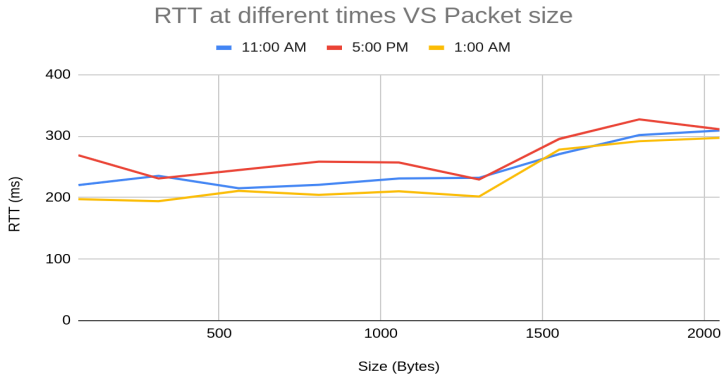


No packet loss was observed during the experiment. In a generalized scenario, packet loss may occur due to congestion in network (rate of arrival of packets is faster than the routers can process them) or a fault in the hardware (multiple routers are faulty, and packets are redirected). Sometimes large-sized packets are also rejected by certain servers.

RTT vs Distance: Measured RTTs are weakly correlated with the geographical distance. In theory, RTT should increase with distance due to an increase in the number of intermediate routers and thereby increasing the number of

hops. But practically, a lot of other factors like the performance of the host server and the amount of traffic present determine this relationship. As seen in the graph above, sasol.com's server in South Africa has less RTT compared to cafecoffeeday's server which is located in India. Similarly Amazon.in (Ireland) has larger RTT compared to uber.com (US).

Size (Bytes)	64	312	560	808	1056	1304	1552	1800	2048
Avg. RTT1 (ms)	220.329	235.442	215.226	220.836	231.225	232.198	270.768	301.755	309.123
Avg. RTT2 (ms)	268.842	231.229	244.886	258.509	257.112	229.458	295.452	327.291	311.112
Avg. RTT3 (ms)	197.605	194.112	210.98	204.451	210.195	201.727	278.11	291.735	297.109



RTT vs Time: RTT is affected by the network congestion and at different times, the users using the site vary and so does the network congestion at that time. Also, the varying propagation delay and queuing delay at different times of the day contributes to varying RTT at different times. As it is clear from the experiment, for the Indian company Café Coffee Day, at 1 am we are getting relatively less RTT as less users are active during late night hours.

- **RTT vs Packet Size**: Very slight increase in RTT is seen before 1500 bytes and a sharp increase after 1500 as MTU is set to 1500 bytes and packets with greater than 1500 bytes are sent by breaking it into smaller packets of 1500 bytes and thus have more transmission delay than the ones with less than 1500 bytes.

3) Two different ping commands and analysis

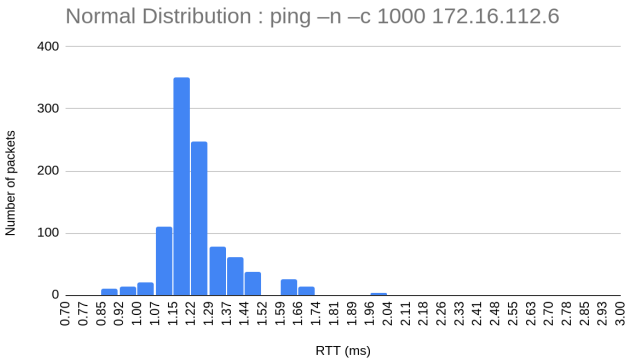
The ping was made to 172.16.112.6 (jatinga.iitg.ernet.in).

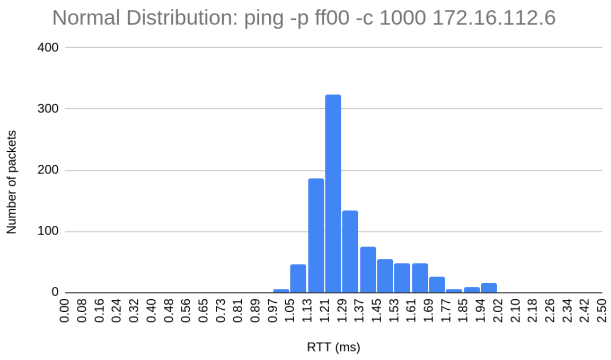
a) 996 packets out of 1000 were received in '**-n**' case. Packet Loss Rate = (4/1000) *100=0.4%.
990 packets out of 1000 were received in '**-n**' case. Packet Loss Rate = (10/1000) *100=1.0%.

b) The minimum, maximum, mean, and median latency of the pings that succeeded:

Command	Minimum Latency (ms)	Maximum Latency (ms)	Mean Latency (ms)	Median Latency (ms)
ping –n –c 1000 172.16.112.6	0.861	1.981	1.165	1.181
ping -p ff00 -c 1000 172.16.112.6	0.972	2.014	1.279	1.268

c) The below graphs depict the normal distribution of the ping latencies.





d) Lower Mean Latency in Case 1: The '**-n**' option in ping gives numeric output only and no attempt is made to lookup symbolic names for host addresses. Because of this, the mean latency in first case (01.165 ms) is less than that in second (1.279 ms).
Higher Packet Loss in Case 2: The '**-p**' option is used to specify the content of the packet we send. This is useful for diagnosing data-dependent problems in a network. The pattern sent in the second case (ff00, i.e. 1111111100000000) has only one transition (from 1 to 0 at the 9th bit) and this is likely to cause synchronization problems between sender and receiver clocks.

4) Ifconfig and route commands

```
udbhav@udbhav-G3-3579:~$ ifconfig
enp0s20f0u3c4i2 Link encap:Ethernet  HWaddr 3a:89:2c:a4:1c:9f
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

enp2s0    Link encap:Ethernet  HWaddr 54:bf:64:32:f6:a3
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:11798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11798 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1950792 (1.9 MB)  TX bytes:1950792 (1.9 MB)

wlo1      Link encap:Ethernet  HWaddr 7c:2a:31:38:63:32
          inet addr:10.150.37.208  Bcast:10.150.39.255  Mask:255.255.248.0
          inet6 addr: fe80::6612:fa88:391b:a460/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2467059 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1261483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1847280847 (1.8 GB)  TX bytes:226757498 (226.7 MB)
```

a) ifconfig stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system. If no arguments are given, ifconfig displays the status of the currently active interfaces. The output of running ifconfig is described below:
- The enp3s0 is the wired ethernet interface, wlp2s0 is the wireless ethernet interface and lo is the loopback interface which is a virtual network interface that is used by the computer to communicate to itself.
- MTU is the short form for Maximum Transmission Unit is the size of each packet received by the Ethernet card. The value of MTU for all Ethernet devices by default is set to 1500.
- The Metric indicates the associated cost of using the indicated route. Used to find efficiency of a route from two points in a network.
- RX and TX Packets are the number of packets received and transmitted through the interface respectively. The number of bytes corresponding to each are also specified.
- The number of packets dropped, overrun, collided, or had error transmitting while receiving or transmitting is also mentioned for both RX and TX packets.
- Txqueuelen denotes the transmit queue length of the device.
- Inet addr and inet6 addr are the IPV4 and IPV6 address assigned when the machine is connected to the network.
- Bcast - denotes the Broadcast Address (address at which all devices connected to the network are enabled to receive datagrams).
- Mask - is the network mask which we passed using the netmask option. This is required to extract the network address and host address from the IP address
- Flags tell about the status of the interface and its facilities. Example, the UP flag indicates an active interface. Running flag indicates that the interface is ready to accept data. Broadcast flag indicates that a broadcast address has been set. Multicast flag indicates that the interface supports multicasting, i.e., it allows a source to send a packet to multiple machines if the machines are watching out for that packet.

b) Various options about network interfaces and its flags can be specified along with ifconfig:
'-a': Display information for all network interfaces, even if they are down.
'-s': Display a short list in a format identical to the command "netstat -i".
'-v': Verbose mode; display additional information for certain error conditions.
up: This flag causes the interface to be activated.
down: This flag causes the driver for this interface to be shut down.
mtu N: sets the maximum transfer unit of an interface (limit the maximum packet size)

```
udbhav@udbhav-G3-3579:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.150.32.1     0.0.0.0         UG    600    0        0 wlo1
10.150.32.0     *               255.255.248.0   U     600    0        0 wlo1
link-local      *               255.255.0.0     U     1000   0        0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH   600    0        0 wlo1
```

c) Route command manipulates and displays the system's IP routing tables. The output of the route command is described below:

- Destination: The destination network or destination host.
- Gateway: It points to the gateway through which the network can be reached (* if none set)
- Genmask: It is the netmask for the destination net; The value is 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
- Flags: These are status indicators. Flag U indicates that the route is up, Flag G signifies that the route is to a gateway. Flag H signifies that the route is to a host which means that the destination is a complete host address.
- Metric: The Metric indicates the associated cost of using the indicated route. This is useful for determining the efficiency of a certain route from two points in a network.
- Ref: Indicates the number of references to this route.
- Use: Indicates the count of lookups for the route.
- Iface: Interface to which packets for this route will be sent.

```
udbhav@udbhav-G3-3579:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.150.32.1     0.0.0.0         UG    600    0        0 wlo1
10.150.32.0     0.0.0.0         255.255.248.0   U     600    0        0 wlo1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH   600    0        0 wlo1
udbhav@udbhav-G3-3579:~$ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.150.32.1     0.0.0.0         UG        0 0          0 wlo1
10.150.32.0     *               255.255.248.0   U         0 0          0 wlo1
link-local      *               255.255.0.0     U         0 0          0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH       0 0          0 wlo1
udbhav@udbhav-G3-3579:~$ sudo route add -net 175.56.76.0 netmask 255.255.255.0 wlo1
[sudo] password for udbhav:
udbhav@udbhav-G3-3579:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.150.32.1     0.0.0.0         UG    600    0        0 wlo1
10.150.32.0     *               255.255.248.0   U     600    0        0 wlo1
link-local      *               255.255.0.0     U     1000   0        0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH   600    0        0 wlo1
175.56.76.0     *               255.255.255.0   U     0      0        0 wlo1
udbhav@udbhav-G3-3579:~$ sudo route del -net 175.56.76.0 netmask 255.255.255.0 wlo1
udbhav@udbhav-G3-3579:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.150.32.1     0.0.0.0         UG    600    0        0 wlo1
10.150.32.0     *               255.255.248.0   U     600    0        0 wlo1
link-local      *               255.255.0.0     U     1000   0        0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH   600    0        0 wlo1
```

d) Various options along with route command are (screenshot is attached above):
-n: show numerical addresses instead of trying to determine symbolic hostnames.
-e: use netstat-format for displaying the routing table.
add: add a new route. While adding a new route, -net specifies the destination network and netmask specifies the Genmask.
del: While deleting a route, -net specifies destination network to be deleted and netmask specifies the Genmask.

5) Netstat

a) Netstat stands for network statistics. It is a command-line network utility tool that displays network connections for the Transmission Control Protocol, routing tables, and several network interface and network protocol statistics. It is one of the most basic network debugging tools and is used to find problems in the network and to determine the amount of traffic on the network as a performance measurement by telling what ports are open and whether any programs are listening on ports.

```
udbhav@udbhav-G3-3579:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 udbhav-G3-3579:domain   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 10.150.37.208:56344     13.107.6.171:https      ESTABLISHED
tcp        0      0 10.150.37.208:42234     sa-in-f189.1e100.:https ESTABLISHED
tcp        0      0 10.150.37.208:38386     maa05s02-in-f10.1:https ESTABLISHED
tcp        0      0 10.150.37.208:60070     maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 10.150.37.208:45908     sb-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 10.150.37.208:38388     maa05s02-in-f10.1:https ESTABLISHED
tcp        1      0 10.150.37.208:34408     52.114.32.24:https      CLOSE_WAIT
tcp        0      0 10.150.37.208:43046     52.109.124.38:https     ESTABLISHED
tcp        0      0 10.150.37.208:57288     13.107.6.171:https      ESTABLISHED
tcp        0      0 10.150.37.208:45724     server-13-33-142-:https ESTABLISHED
tcp        0      0 10.150.37.208:37120     maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 10.150.37.208:46076     maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 10.150.37.208:60698     maa05s04-in-f3.1e:https ESTABLISHED
tcp        0      0 10.150.37.208:42350     maa03s26-in-f14.1:https ESTABLISHED
tcp        0      0 10.150.37.208:46070     maa03s31-in-f14.1:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

b) netstat -at is used to show all TCP connections. (-a lists all connections while -t indicates TCP). We can use netstat -at | grep "ESTABLISHED" can be used to show only the ESTABLISHED TCP connections. The output of the command is explained as follows:
- Proto defines the name of the protocol (TCP or UDP).
- Recv-Q and Send-Q indicate the data in the queue to be received and sent respectively.

- Local Address is the IP addr of the local computer and the port number being used.
- Foreign Address is the IP address and port number of the remote computer to which the socket is connected.
- State indicates the state of a TCP connection. LISTEN: waiting for external host to contact. ESTABLISHED: ready to communicate. CLOSED_WAIT: remote shutdown and waiting for the socket to close.

```
udbhav@udbhav-G3-3579:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.150.32.1     0.0.0.0         UG        0 0          0 wlo1
10.150.32.0     *               255.255.248.0   U         0 0          0 wlo1
link-local      *               255.255.0.0     U         0 0          0 wlo1
172.17.1.1      10.150.32.1     255.255.255.255 UGH       0 0          0 wlo1
```

c) netstat -r shows the kernel routing table of the machine. The output of the command is explained as follows:
Destination: It indicates the pattern that the destination of a packet is compared to. While sending a packet over the network, this table is examined from top to bottom, and the first line with a matching is the destination for the packet.

- Gateway: It indicates where to send a packet that matches the destination of the same line. An asterisk means send locally as the destination is on the same network.
- Genmask: It is the netmask for the destination net. It tells how many bits from the start of the IP address are used to identify the subnet.
- Flags: This column indicates which flags apply to the current table line. Flag U indicates that the route is up, Flag G signifies that the route is to a gateway. Flag H signifies that the route is to a host which means that the destination is a complete host address.
- MSS: Maximum Segment Size is the size of the 4 largest datagram that the kernel constructs for transmission via this route. It is a TCP parameter which is used to split packets when the destination cannot handle large packets.
- Window: This column indicates the window size,i.e., how many TCP packets can be sent before at least one of them has to be acknowledged.
- irtt: Initial Round Trip Time is used by the kernel to guess about the best TCP parameters without waiting for slow replies.
- Iface: it indicates which network interface should be used for sending packets that match the destination.

```
udbhav@udbhav-G3-3579:~$ netstat -i
Kernel Interface table
Iface      MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp2s0    1500 0     226287      0      0 0         89852      0      0      0 BMU
lo       65536 0      26646      0      0 0         26646      0      0      0 LRU
wlo1      1500 0    6591230      0      0 0       2479887      0      0      0 BMRU
```

d) 'netstat -i' is used to display the status of all network interfaces. As it can be seen in the screenshot, 3 network interfaces are present on my system.

```
udbhav@udbhav-G3-3579:~$ netstat -su
IcmpMsg:
    InType0: 9820
    InType3: 381
    InType11: 768
    OutType3: 19485
    OutType8: 15790
Udp:
    200298 packets received
    19473 packets to unknown port received.
    401 packet receive errors
    93708 packets sent
    RcvbufErrors: 401
    SndbufErrors: 7
    IgnoredMulti: 316952
UdpLite:
IpExt:
    InMcastPkts: 33590
    OutMcastPkts: 7733
    InBcastPkts: 317893
    OutBcastPkts: 122
    InOctets: 7991835939
    OutOctets: 557480576
    InMcastOctets: 2173944
    OutMcastOctets: 1399678
    InBcastOctets: 42088369
    OutBcastOctets: 5884
    InNoECTPkts: 6845318
    InECT0Pkts: 107
```

e) 'netstat -su' is used to show the statistics of all UDP connections. The output is available in the screenshot.

f) The loopback device is a virtual network interface that the system uses to communicate with itself. It is not an actual hardware but helps the applications running on the machine to connect to servers on the same machine. The IPv4 address for accessing loopback interface is 127.0.0.1. It is used majorly for diagnostics and troubleshooting, and to connect to servers running on the local machine. Apart from as a diagnostic tool, it is used when a server offering a resource is running on the system itself. (like while running a web server, all the web documents can be examined file by file).

6) Traceroute

- The time chosen to ping were 11:00 AM (1), 5:00 PM (2) and 1:00 AM (3).
- The six hosts that were pinged: cafecoffeeday.com, yandex.com, digitalpacific.com.au, sasol.com, amazon.in, uber.com

	cafecoffeeday.com	yandex.com	digitalpacific.com.au	sasol.com	amazon.in	uber.com
Hop Count 1	18	11	20	21	30 (incomplete)	11
Hop Count 2	18	11	20	22	30 (incomplete)	11
Hop Count 3	18	11	22	21	30 (incomplete)	11

a) The hop counts for each host in each time slot is listed above. The common hops were 10.150.32.1 (my system) and 172.16.85.231 (this must be Jio server router).

b) While going to sasol.com server at 5pm and digitalpacific.com.au at 1::00 PM, the packets went through an additional router. The reason for this would most probably be some hardware failure on the path or network congestion. Migration of destination VM servers across data centres can also cause a change in hop count.

c) The route to amazon.in was not traced completely. Loss of ICMP/UDP reply packets from intermediate hosts or no reply from host can be a reason for this. The reason can also be from the sender's side(sender timeout or ICMP/UDP packet not sent with incremental TTL value). Sometimes routers and servers have firewall enabled which either blocks the ICMP traffic or hides the IP Addresses of the hosts to be traced by traceroute.

d) Yes, it is possible to find partial paths through traceroute in scenarios where ping fails as they use different techniques. In Ping, intermediate hosts forward the ICMP packets and the destination host replies, thus ping relies on the reply packet. Traceroute works by sending the packets of data with low survival time (Time to Live – TTL) which specifies how many steps (hops) can the packet survive before it is returned. Each intermediate host needs to respond with an ICMP/UDP packet. Hence, even if the destination host doesn't respond to ping (say to avoid DDoS attack), a partial path can always be found given source is not blocked from receiving responses (from reasons mentioned in (c)).

7) Arp command

```
udbhav@udbhav-G3-3579:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.2.1                ether   ec:44:76:74:60:42   C                     wlo1
10.19.3.110              ether   0c:80:63:16:c9:52   C                     wlo1
```

a) The command 'arp' is used to show the full arp table. Arp stands for address resolution protocol. ARP table stores the IP addresses and the corresponding MAC addresses of the hosts on the network. It can be used to find out the destination MAC address while sending packets to other hosts. The ARP table output is explained below:

- Address: the IP address of the connected host on the network.
- HWtype: indicates that host has ethernet interface
- HWaddress: is the corresponding MAC address.
- Flags: indicate if the mac address has been learned by the system by connecting to the host (C), manually set (M) (as in the screenshot below).
- Iface: denotes the interface connecting them.

b) "sudo arp –s <ip addr> <MAC_addr>" is used to add an entry. (The 4 entries with CM flag are added manually). "sudo arp -d <ip addr>" is used to delete an entry. Adding and deleting of entries is shown in the screenshot attached.

```
udbhav@udbhav-G3-3579:~$ sudo arp -s 10.19.2.2 ec:44:76:74:60:43
udbhav@udbhav-G3-3579:~$ sudo arp -s 10.19.2.3 ec:44:76:74:60:44
udbhav@udbhav-G3-3579:~$ sudo arp -s 10.19.2.4 ec:44:76:74:60:45
udbhav@udbhav-G3-3579:~$ sudo arp -s 10.19.2.5 ec:44:76:74:60:46
udbhav@udbhav-G3-3579:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.2.2                ether   ec:44:76:74:60:43   CM                    wlo1
10.19.2.1                ether   ec:44:76:74:60:42   C                     wlo1
10.19.3.110              ether   0c:80:63:16:c9:52   C                     wlo1
10.19.2.5                ether   ec:44:76:74:60:46   CM                    wlo1
10.19.2.4                ether   ec:44:76:74:60:45   CM                    wlo1
10.19.2.3                ether   ec:44:76:74:60:44   CM                    wlo1
udbhav@udbhav-G3-3579:~$ sudo arp -d 10.19.2.2
udbhav@udbhav-G3-3579:~$ sudo arp -d 10.19.2.3
udbhav@udbhav-G3-3579:~$ sudo arp -d 10.19.2.4
udbhav@udbhav-G3-3579:~$ sudo arp -d 10.19.2.5
udbhav@udbhav-G3-3579:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.2.1                ether   ec:44:76:74:60:42   C                     wlo1
10.19.3.110              ether   0c:80:63:16:c9:52   C                     wlo1
```

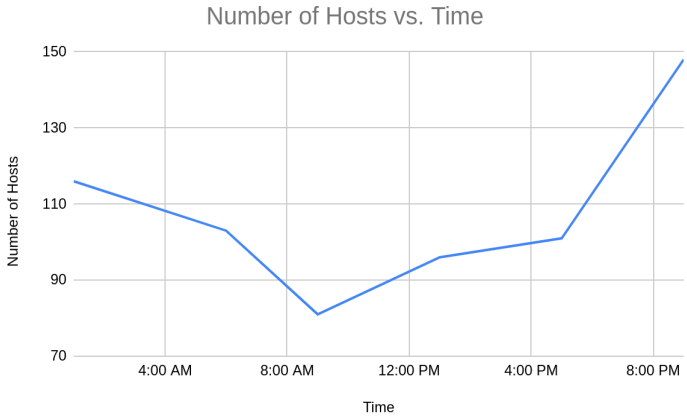
c) The command 'cat /proc/sys/net/ipv4/neigh/default/gc_stale_time' shows the ARP Timeout Value. The value is set to 60 seconds in my system.
We can find out the ARP timeout value by adding a temporary entry in the table and checking the table after fixed intervals of time (say 3-4 ms). The time when the entry is deleted is the approximate cache timeout. We can also use binary search. We can keep start=0 and end=MAX and start with a mid-value to check for deletion, if entry is deleted update end to mid-1, if not, delete entry and update start to mid+1.

d) Two IP addresses, if mapped to the same Ethernet address, belong to the same subnet which differs from the host with the ARP table. To reach the two hosts, ARP request send to both will basically return the same MAC address value for both the IP's. Hence, when either of the IP address is pinged, a 100% packet loss occurs.

8) Nmap

'nmap -n -sP 10.12.0.1/18' was used to get number of hosts active in Brahmaputra Hostel at different times of the day.

Time (in 24-hour format)	1:00 AM	6:00 AM	9:00 AM	1:00 PM	5:00 PM	9:00 PM
Number of Hosts	116	103	81	96	101	148



We can see that hostel LAN has the minimum number of active hosts (8 am - 5 pm) after which the number of active hosts increases. It is still high at around 1:00 AM and falls after that.