CS349 ASSIGNMENT 01

ANIKET RAJPUT (170101007)

01. PING COMMAND

(a) To specify the number of ECHO_REQUESTS to send with ping command '**-c**' option is used.
"**ping -c 25 iitg.ac.in**" 25 ECHO_REQUESTS will be sent.

(b) To specify the time interval (in seconds) between successive ECHO_REQUESTS '**-i**' option is used.
"**ping -i 5 iitg.ac.in**" 5 seconds delay between consecutive requests.

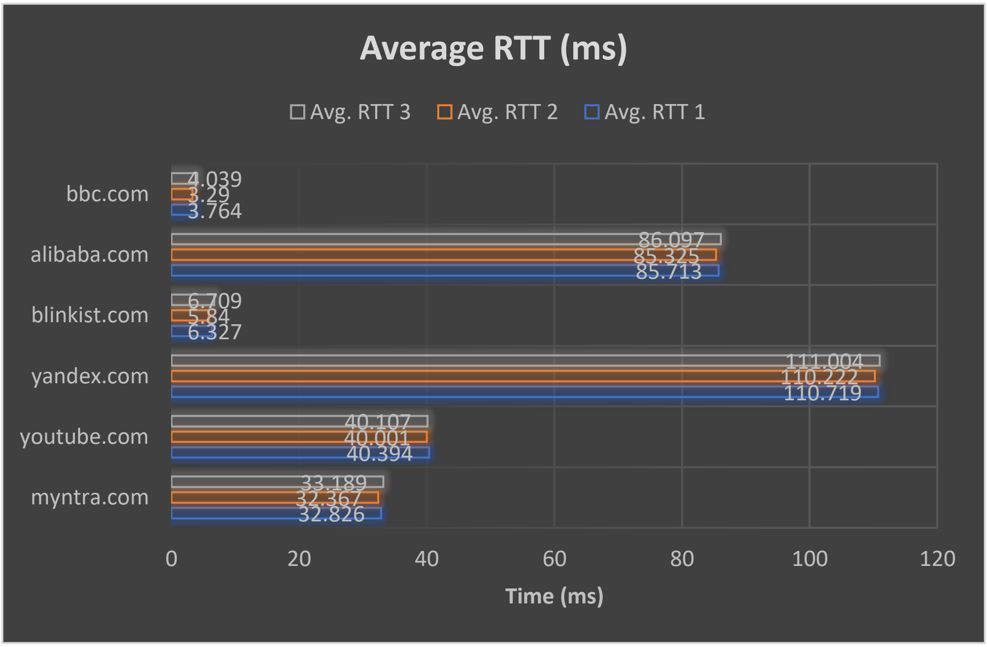
(c) To send packets one after another without waiting for reply '**-l**' option is used.
"**ping -l 2 iitg.ac.in**" Normal users can send at most **3** packets using this option.
Super user can use '**-f**' option to send packets without waiting for reply continuously.

(d) To set the packet size of ECHO_REQUESTS in bytes '**-s**' option is used.
"**ping -s 64 iitg.ac.in**" 64 bytes packets will be sent.
A packet is added with IP header of 20 bytes and ICMP header of 8 bytes hence, for a packet of 32 bytes, total packet size will be 60 bytes.

02. PING EXPERIMENT

- The online tool used for this experiment was 'http://www.spfld.com/ping.html'.
- Hosts were pinged at **12:00 P.M.**, **6:00 P.M.** and **12:00 A.M.** respectively.

Destination Hostname	IP Address	Geographical Location	Avg. RTT 1 (ms)	Avg. RTT 2 (ms)	Avg. RTT 3 (ms)
myntra.com	72.247.169.36	Bengaluru, India	32.826	32.367	33.189
youtube.com	64.233.177.93	California, US	40.394	40.001	40.107
yandex.com	213.180.204.62	Moscow, Russia	110.719	110.222	111.004
blinkist.com	104.26.15.130	Berlin, Germany	6.327	5.84	6.709
alibaba.com	205.204.101.142	Hangzhou, China	85.713	85.325	86.097
bbc.com	151.101.128.81	London, UK	3.764	3.29	4.039



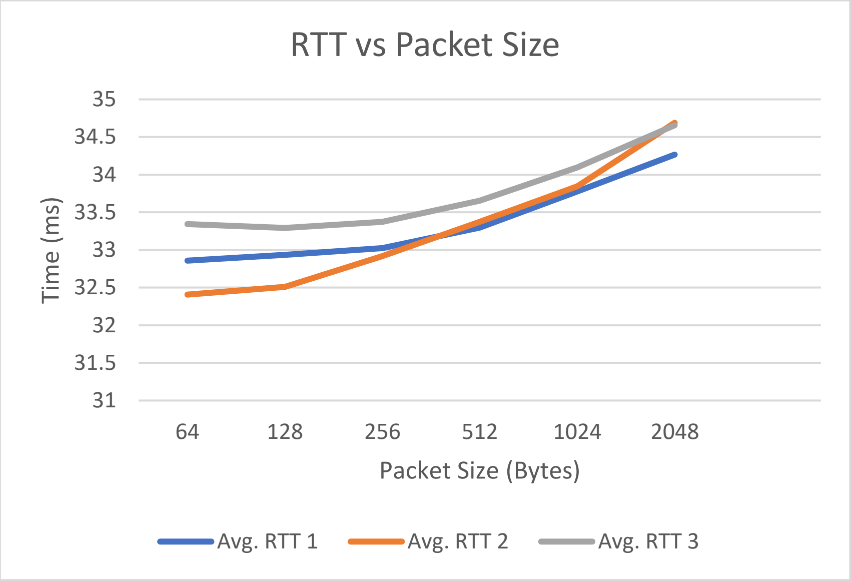
- In the above experiment there was **no case of packet loss greater than 0%**. Packet loss can occur due to link congestion i.e. more packets arriving than the link can handle. Glitches in the medium can also lead to loss of packets. Wireless networks are more susceptible to packet losses. Some routers drop ICMP packets at high load.
- There exists a **weakly positive correlation** between geographical distance and RTT. A greater geographical distance incurs a greater propagation delay and also may have a greater number of switches and routers to increase the delay. But the signals travel at very high speeds resulting in less difference, also RTT depends greatly on link congestion, network traffic and number of routers. In the experiment Moscow is fairly nearer to source than Hangzhou but still yandex.com has the greatest RTT.

- For next experiment ‘**myntra.com**’ is chosen for pinging with packets of different sizes.

- Host was pinged at **12:00 P.M.**, **6:00 P.M.** and **12:00 A.M.** respectively.

Size (Bytes)	64	128	256	512	1024	2048
Avg. RTT 1 (ms)	32.858	32.933	33.023	33.297	33.775	34.266
Avg. RTT 2 (ms)	32.407	32.508	32.916	33.372	33.846	34.689
Avg. RTT 3 (ms)	33.342	33.292	33.373	33.654	34.095	34.656

- In the above table it is evident that RTT does not differ very much for smaller packet sizes but slightly greater values are observed for packet size of 2048 bytes. This can be due to the fact that Maximum Transmission Unit (MTU) is 1500 bytes, hence packets bigger than this are fragmented before transmission resulting in higher RTT and packets smaller than MTU are zero padded before transmission resulting in almost same RTT for smaller packets.

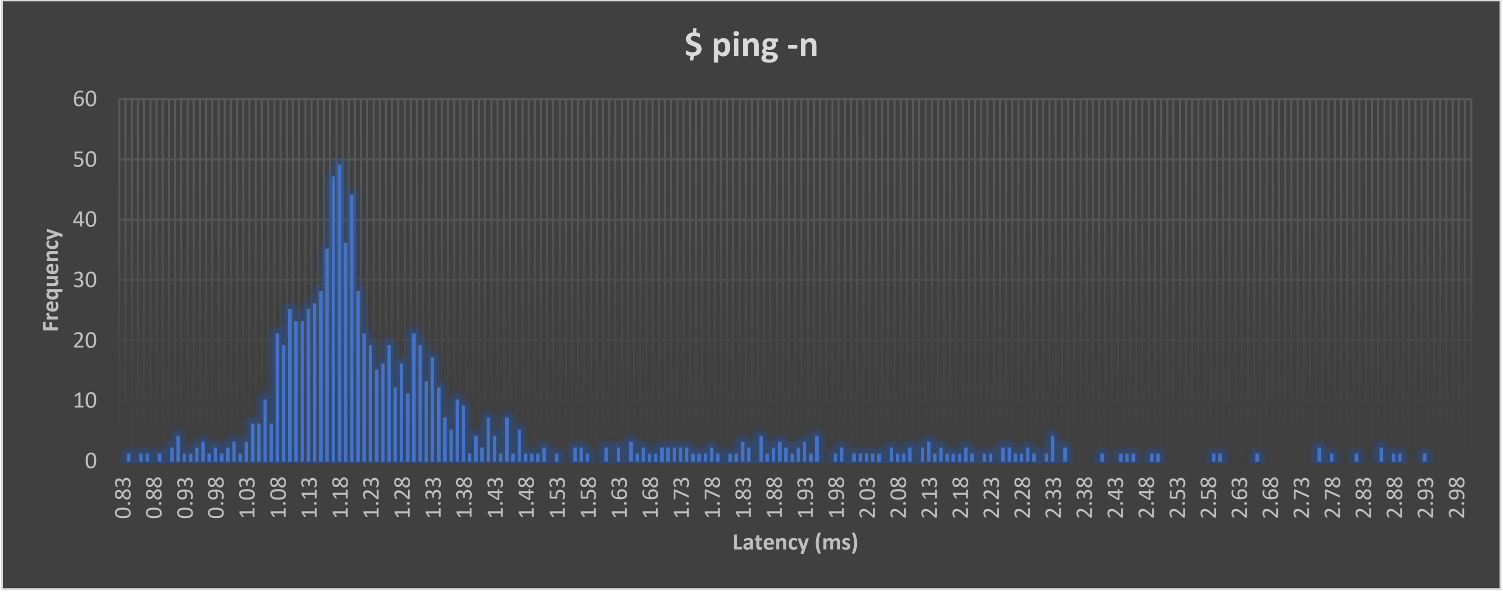


- From the above data it is observed that RTT is fairly high at 12:00 A.M. for all hosts which means there was a higher network congestion at 12:00 A.M. The values of RTT are slightly greater for host at 12:00 P.M. than at 6:00 P.M. Hence, we can say that network congestion was highest at 12:00 A.M.

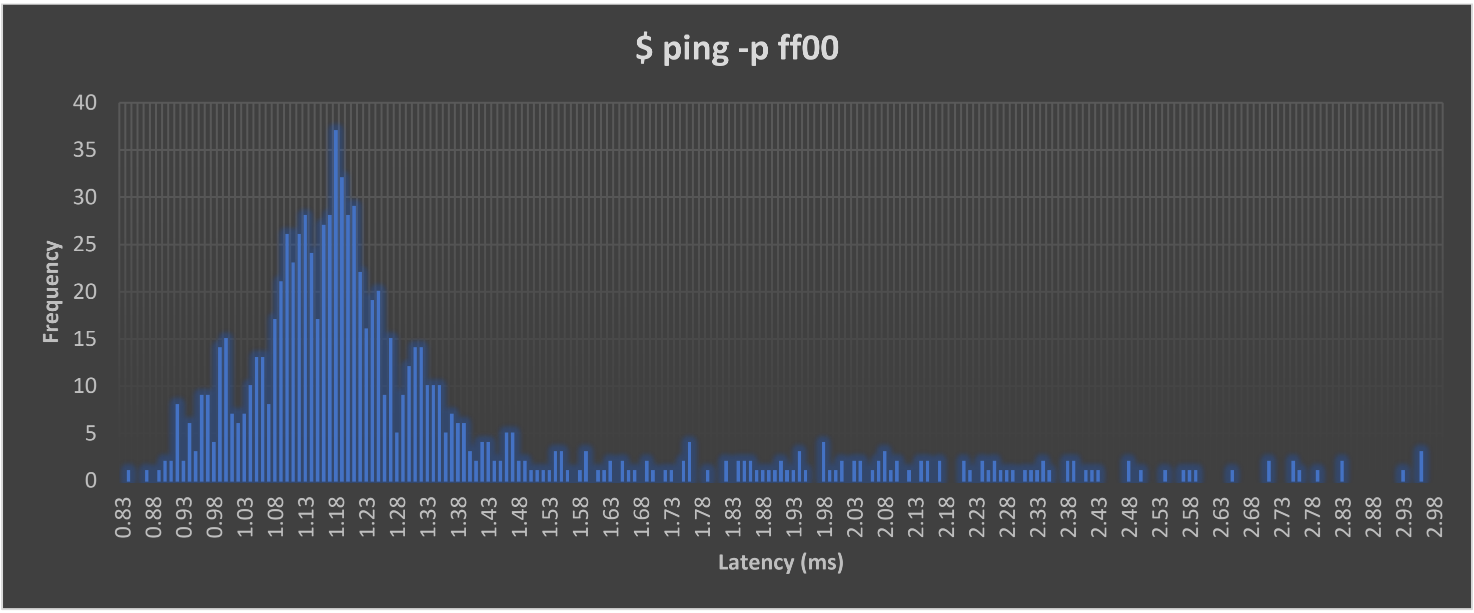
03. PING COMMAND IN 2 DIFFERENT SCENARIOS

The IP address selected for this experiment is “**172.16.112.36**”.

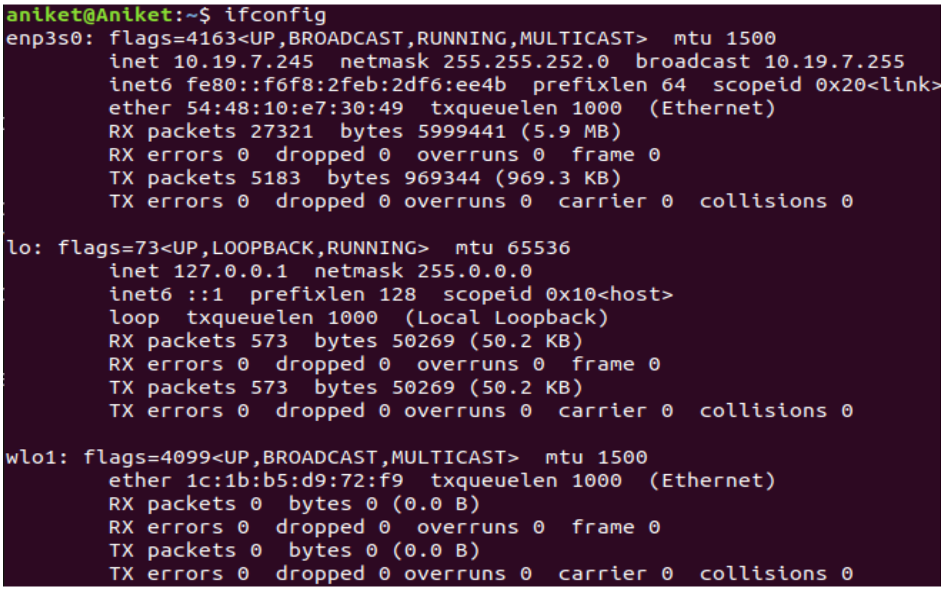
Command	Packets Sent	Packets Received	Packets Loss Rate	Minimum Latency	Maximum Latency	Mean Latency	Median Latency
$ ping -n -c 1000 172.16.112.36	1000	987	1.3%	0.836 ms	31.926 ms	1.873 ms	1.22 ms
$ ping -p ff00 -c 1000 172.16.112.36	1000	955	4.5%	0.834 ms	37.825 ms	1.854 ms	1.21 ms



- The plot of ‘**Frequency vs Latency**’ in both the cases resembles the graph of a normal distribution.
- In the first case, ‘-n’ option with ping command is used to display the network addresses as numbers rather than as hostnames. Hence, no attempt is made to look up for symbolic names of network addresses. While ‘-p’ option is used to pad the packets with the pattern ‘ff00’ in the second case. The second case exhibited a higher packet loss rate. This may be due to the presence of less number of transitions in the packets causing desynchronization among requests packets.



04. IFCONFIG AND ROUTE COMMANDS



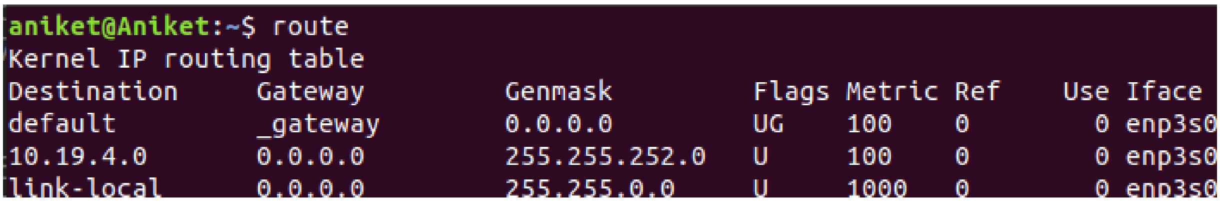
```
aniket@Aniket:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.19.7.245  netmask 255.255.252.0  broadcast 10.19.7.255
        inet6 fe80::f6f8:2feb:2df6:ee4b  prefixlen 64  scopeid 0x20<link>
        ether 54:48:10:e7:30:49  txqueuelen 1000  (Ethernet)
        RX packets 27321  bytes 5999441 (5.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5183  bytes 969344 (969.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 573  bytes 50269 (50.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 573  bytes 50269 (50.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 1c:1b:b5:d9:72:f9  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* (interface configuration) is used to view the configuration of the network interfaces of the system. The above system has three network interfaces. ‘**enp3s0**’ is the wired ethernet interface. ‘**lo**’ is the loopback interface and ‘**wlo1**’ is the wireless network interface. UP, BROADCAST, RUNNING, LOOPBACK & MULTICAST are flags. ‘UP’ means the interface is up. ‘BROADCAST’ means interface can transmit a packet that can be received by every device on the network. ‘RUNNING’ means the interface is ready to transmit and receive packets. ‘LOOPBACK’ means interface is in loopback mode. ‘MULTICAST’ means interface can broadcast packets to specific devices. ‘MTU’ is the maximum transmission unit for the interface. ‘**inet**’ and ‘**inet6**’ are IPV4 and IPV6 addresses respectively assigned to the interface. ‘**Netmask**’ is used to divide IP address into subnets and specify the network’s available hosts. ‘**Broadcast address**’ is used to target all devices on network. ‘**Scope**’ of an IP address tells how far from the local host the IP address is known. Scope type ‘**link**’ means address can be used within the LAN only while scope type ‘**host**’ means address can be used to communicate to itself only. ‘**prefix**’ determines the number of IP addresses within a particular host section of IP addresses. ‘**ether**’ is the MAC address of the device. ‘**txqueuelen**’ limits the number of packets in the transmission queue of interface device. ‘**RX**’ and ‘**TX**’ are received and transmitted packets respectively.

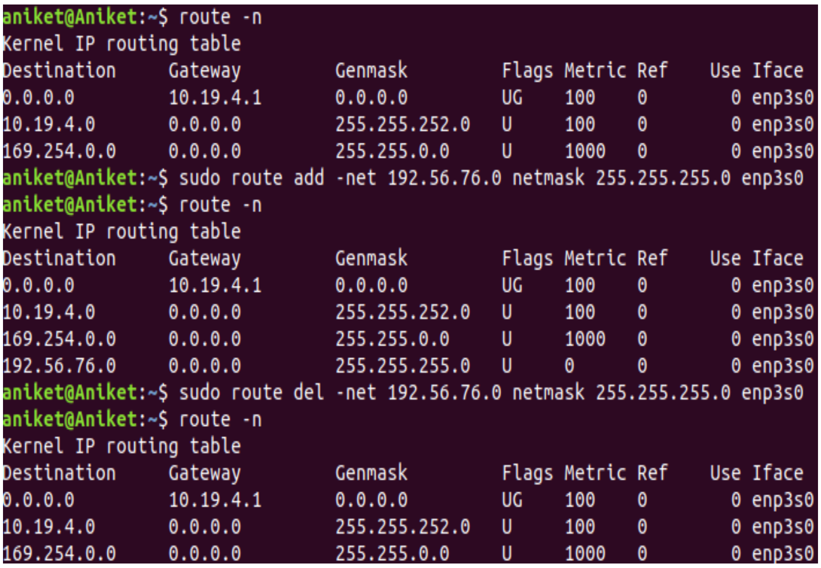
(b) “**ifconfig -a**” option is used to display all the interfaces present in the device whether down or up. “**ifconfig <interface> up**” is used to enable the interface. “**ifconfig <interface> mtu <N>**” is used to set MTU of the interface to N bytes. “**ifconfig <interface> broadcast <address>**” is used to set the broadcast address for the given interface.



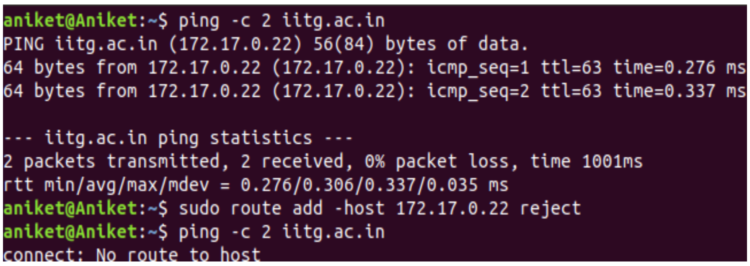
```
aniket@Aniket:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp3s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp3s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp3s0
```

(c) ‘**route**’ command displays the routing table of the system. It is used to setup static routes to specific hosts. The ‘**Destination**’ column has the addresses of destination hosts. ‘**Default**’ route is used when no specific route can be determined for a destination. ‘**link-local**’ address is used for communication within local network. ‘**Gateway**’ is the hardware device between two networks. ‘0.0.0.0’ means **unspecified** gateway. ‘**Genmask**’ column has the netmask for destination. ’0.0.0.0’ is for the **default** route. In the **flag** column ‘**U**’ represents that the route is up, ‘**H**’ represents host, ‘**G**’ represents to use gateway and ‘**!**’ represents to reject a route. ‘**Metric**’ is the distance in hops to the target. ‘**Ref**’ represents the number of references to the route. ‘**Use**’ is count of lookups i.e. routes for which router must look up the connected route to next hop. ‘**Iface**’ is the interface to which packets for the route will be sent.

(d) ‘**route -n**’ command is used to represent the routing table with numerical entries. ‘**route add**’ and ‘**route del**’ are used as super user to add and delete an entry in the routing table.
‘**sudo route add -host <address> reject**’ is used to add a host with rejected route.



```
aniket@Aniket:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.4.1       0.0.0.0         UG    100    0        0 enp3s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp3s0
aniket@Aniket:~$ sudo route add -net 192.56.76.0 netmask 255.255.255.0 enp3s0
aniket@Aniket:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.4.1       0.0.0.0         UG    100    0        0 enp3s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp3s0
192.56.76.0     0.0.0.0         255.255.255.0   U     0      0        0 enp3s0
aniket@Aniket:~$ sudo route del -net 192.56.76.0 netmask 255.255.255.0 enp3s0
aniket@Aniket:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.4.1       0.0.0.0         UG    100    0        0 enp3s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp3s0
```



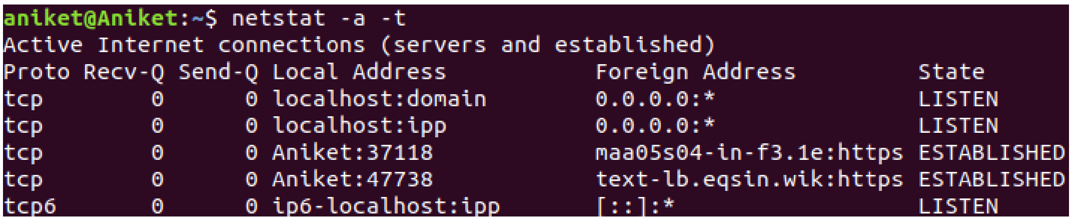
```
aniket@Aniket:~$ ping -c 2 iitg.ac.in
PING iitg.ac.in (172.17.0.22) 56(84) bytes of data.
64 bytes from 172.17.0.22 (172.17.0.22): icmp_seq=1 ttl=63 time=0.276 ms
64 bytes from 172.17.0.22 (172.17.0.22): icmp_seq=2 ttl=63 time=0.337 ms

--- iitg.ac.in ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.276/0.306/0.337/0.035 ms
aniket@Aniket:~$ sudo route add -host 172.17.0.22 reject
aniket@Aniket:~$ ping -c 2 iitg.ac.in
connect: No route to host
```

05. NETSTAT COMMAND

(a) ‘netstat’ tool displays the network connections, routing tables, network interfaces 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.

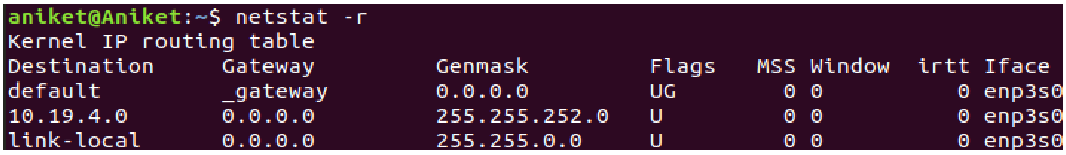
(b) ‘**netstat -a -t**’ command is used to show all the established TCP connections.



```
aniket@Aniket:~$ netstat -a -t
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 Aniket:37118            maa05s04-in-f3.1e:https ESTABLISHED
tcp        0      0 Aniket:47738            text-lb.eqsin.wik:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

‘**Proto**’ column gives the protocol used by the socket. ‘**Recv-Q**’ is the count of bytes not copied by the user program connected to socket. ‘**Send-Q**’ is the count of bytes not acknowledged by the remote host. ‘**Local Address**’ column has the address and port number of the local end of socket. ‘**Foreign Address**’ column has the address and port number of the remote end of the socket. **'LISTEN' state** means the socket is listening for incoming connections. **'ESTABLISHED' state** means socket has an established connection.

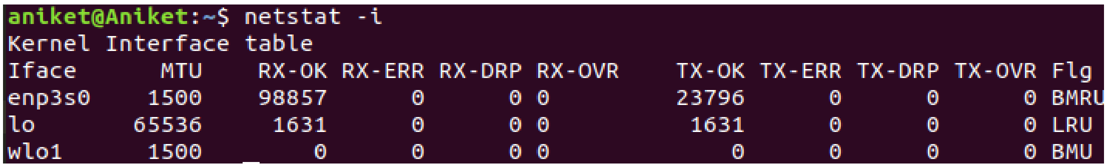
(c) '**netstat -r**' command gives the routing table of the device.



```
aniket@Aniket:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp3s0
10.19.4.0       0.0.0.0         255.255.252.0   U         0 0          0 enp3s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp3s0
```

'**Destination**', '**Gateway**', '**Genmask**', '**Flags**' and '**Iface**' columns are explained in ans **04. (c)**. '**MSS**' is the maximum segment size for TCP connections over the route. '**Window**' is the maximum amount of data system will accept in a single burst of remote host. '**irtt**' is initial round trip time.

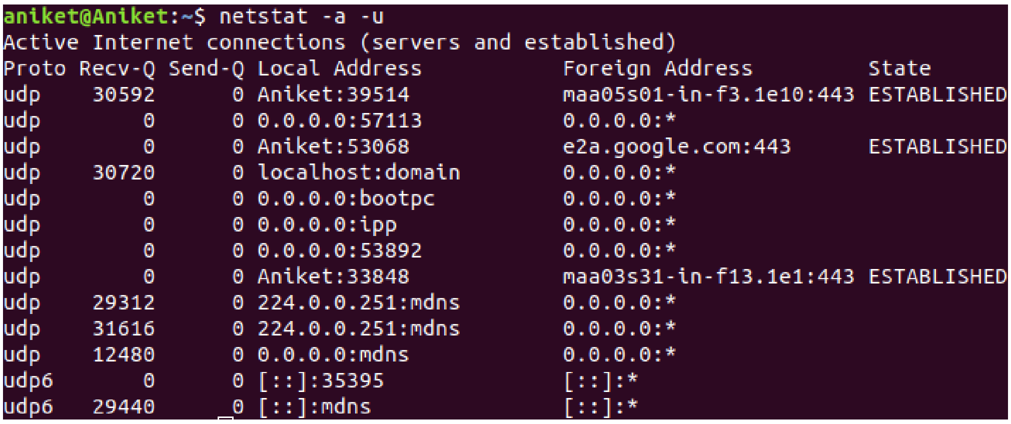
(d) '**netstat -i**' command is used to display the status of all network interfaces.



```
aniket@Aniket:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp3s0    1500    98857      0      0 0         23796      0      0      0 BMRU
lo       65536     1631      0      0 0          1631      0      0      0 LRU
wlo1      1500        0      0      0 0             0      0      0      0 BMU
```

From the table we can see there are '**three**' interfaces on my system.

(e) '**netstat -a -u**' command is used to show the statistics of all UDP connections.



```
aniket@Aniket:~$ netstat -a -u
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp    30592      0 Aniket:39514            maa05s01-in-f3.1e10:443 ESTABLISHED
udp        0      0 0.0.0.0:57113           0.0.0.0:*
udp        0      0 Aniket:53068            e2a.google.com:443      ESTABLISHED
udp    30720      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 0.0.0.0:53892           0.0.0.0:*
udp        0      0 Aniket:33848            maa03s31-in-f13.1e1:443 ESTABLISHED
udp    29312      0 224.0.0.251:mdns        0.0.0.0:*
udp    31616      0 224.0.0.251:mdns        0.0.0.0:*
udp    12480      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:35395              [::]:*
udp6   29440      0 [::]:mdns               [::]:*
```

(f) Loopback interface is a network interface that a system uses to communicate with itself. It does not represent any real hardware. It exists so applications running on the computer can always connect to servers on the same computer because when ethernet or Wi-Fi is disconnected, communication of computer with itself is also ceased. It is used as a diagnostic and troubleshooting tool and is helpful when a server offering a resource in need in running on the same machine.

06. TRACEROUTE

Traceroute is used to show the route taken by packets across an IP network. It helps to determine the problems in the connection with a server. It helps to see how the ISP connects to the internet and how the systems are interconnected.

(a) This experiment was conducted at **12:00 P.M.**, **6:00 P.M.** and **12:00 A.M.** respectively.
The online tool used for this experiment was 'http://ping.eu'.

	myntra.com	**youtube.com**	**yandex.com**	**blinkist.com**	**alibaba.com**	**bbc.com**
Hop count #1	18	8	8	5	16	11
Hop count #2	18	8	8	5	16	11
Hop count #3	18	8	8	5	16	11

There was existence of common hops among the hosts. **213.239.245.237** was a common first hop among all hosts except yandex.com. **213.239.245.18** was common hop of **myntra.com** and **yandex.com**. **213.239.245.241** was common hop of **alibaba.com** and **bbc.com**. **213.239.252.237** & **213.239.252.241** were common hops of **blinkist.com** and **bbc.com**. **213.239.252.33** was a common hop of **youtube.com** and **alibaba.com**. Existence of common hops is because routes of more than one destination can exist through the same routers.

(b) Change in route for same host at different times of day was observed with some of the above hosts. This happens because some of the network routes might be congested, so the router routes them to the less congested routes.

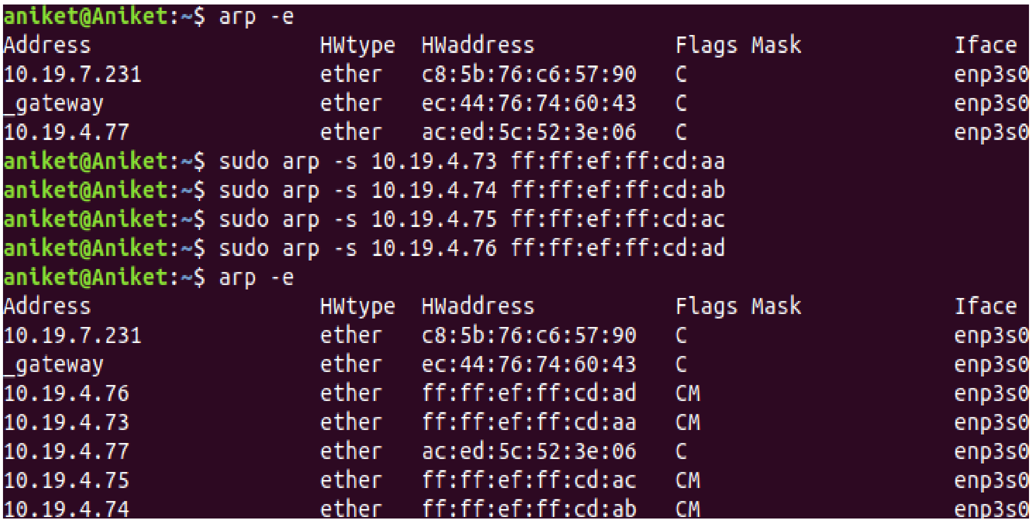
(c) In the above experiment, complete path was found **only** for **yandex.com**. Some websites setup firewall which blocks ICMP traffic while some networks blocks ICMP under heavy load. Under such conditions complete path cannot be found for some hosts.

(d) ‘Ping’ and ‘traceroute’ used ICMP packets in a different working from each other. Ping traverses the network and waits for an ICMP reply from the host. But traceroute sends these packets along with TTL (Time To Live) values. Routers on receiving these packets decrement the TTL value and discards the one with zero. Hence, traceroute do not look for ICMP reply but it targets the final hop, waits for a time exceeding message and increase the TTL for the next iteration so every time packet hops one step further. Hence, a route can be found without the ICMP reply.

07. ARP TABLE

(a) ‘**arp -e**’ command is used to display the full ARP table of machine. ‘**Address**’ column of the table displays the IP addresses of the devices. ‘**HWaddress**’ column displays the MAC address associated with the IP addresses. ‘**HWtype**’ column gives the type of hardware for network transmission. ‘**Iface**’ gives the interface on machine on which corresponding host is connected. ‘**Flag Masks**’ indicate if the MAC address has been learned, manually set or is incomplete.

(b) We can add or delete an entry in the ARP table as **super user**. ‘**sudo arp -s <IP address> <MAC address>**’ command is used to add an entry and ‘**sudo arp -d <IP address>**’ is used to delete an entry. The new entries are added with flag ‘**CM**’ indicating **manually set**.



```
aniket@Aniket:~$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.7.231              ether   c8:5b:76:c6:57:90   C                     enp3s0
_gateway                 ether   ec:44:76:74:60:43   C                     enp3s0
10.19.4.77               ether   ac:ed:5c:52:3e:06   C                     enp3s0
aniket@Aniket:~$ sudo arp -s 10.19.4.73 ff:ff:ef:ff:cd:aa
aniket@Aniket:~$ sudo arp -s 10.19.4.74 ff:ff:ef:ff:cd:ab
aniket@Aniket:~$ sudo arp -s 10.19.4.75 ff:ff:ef:ff:cd:ac
aniket@Aniket:~$ sudo arp -s 10.19.4.76 ff:ff:ef:ff:cd:ad
aniket@Aniket:~$ arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.7.231              ether   c8:5b:76:c6:57:90   C                     enp3s0
_gateway                 ether   ec:44:76:74:60:43   C                     enp3s0
10.19.4.76               ether   ff:ff:ef:ff:cd:ad   CM                    enp3s0
10.19.4.73               ether   ff:ff:ef:ff:cd:aa   CM                    enp3s0
10.19.4.77               ether   ac:ed:5c:52:3e:06   C                     enp3s0
10.19.4.75               ether   ff:ff:ef:ff:cd:ac   CM                    enp3s0
10.19.4.74               ether   ff:ff:ef:ff:cd:ab   CM                    enp3s0
```

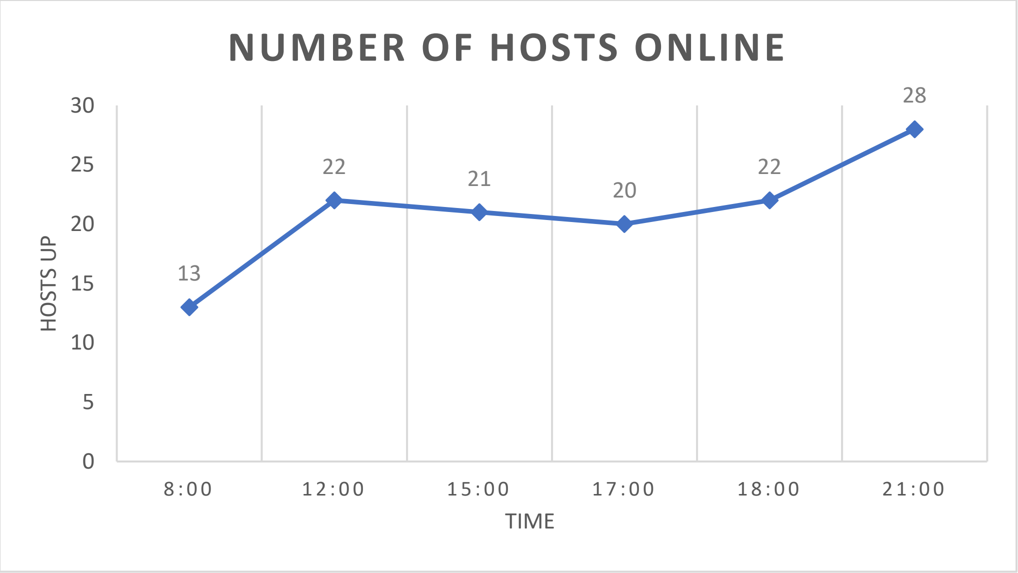
(c) The static entries of ARP table i.e. manually created entries stay forever in the table while dynamic entries created automatically by the normal operation of the protocol in the cache of ARP module gets removed after 60 seconds. The cache is manipulated by use of ioctls and sysctls. The parameters in sysctls interface affecting cache period are gc_interval, gc_thresh2, gc_thresh3 and locktime. These parameters control how frequently the cache values should be updated and the number of entries to be kept in cache. A **trial and error** method to check timeout would be to add a temporary entry and wait for a fixed interval of time and repeatedly check the entry in cache. Decrease the interval successively for precision.

(d) Two IP addresses can map to same Ethernet address when a router connects two or more subnet ranges. MAC address is used for communication with machines on same subnet range. The ARP table has the IP address of devices from other subnet range has the MAC address of that of the connecting router. To send the packets to correct device ARP table is used for the MAC address and routing table of router for further.

08. NMAP

The “Subnet Range” used for this experiment is ’**10.0.0.254/22**’.

The command used is ‘$ nmap -n -sP **10.0.0.254/22**’.



It is observed that at the beginning of the day a smaller number of hosts are online and increases as the day progresses. There is a slight change in the number of hosts throughout the day and but there is a greater increase observed from evening to night.