CS 349 Assignment 1

Chirag Gupta (170101019)

---

1) Ping Command

a) Option '-c' command is used to specify the number of echo requests to send with 'ping' command. *Example: ping -c8 intranet.iitg.ernet.in*

b) Option '-i' command is required to set time interval (in seconds) between two consecutive ping requests. *Example: ping -i5 intranet.iitg.ernet.in*

c) Option '-l' command is required to send ECHO_REQUEST packets to the destination one after another without waiting for a reply. The limit for sending such packets by a normal user is 3. *Example: ping -l3 intranet.iitg.ernet.in.*
Also, option '-f' command can be used to flood the requests one after the other without waiting for a reply. However normal users have to set a minimum time limit of 200ms using -i command.

d) Option '-s' command is used to set the ECHO_REQUEST packet size (in bytes). The actual packet size is larger than what we specify, due to the addition of ICMP header(8 bytes) and IP headers(20 bytes). Hence if the packet size is set to 32 bytes, the total packet size sent would be 32+8+20 = 60 bytes.
Example: ping -s 32 cricbuzz.com

2) Round-Trip_Time (RTT) changes due to various factors

- Six hosts were used for the experiment amazon.in, reddit.com, cricbuzz.com,
- Readings were taken at 10 am 2 pm and 8 pm for all the six hosts respectively.
- Test PC was connected to SetUp Vpn(New Delhi, India) while performing the experiment.
- Packet Loss: It is shown in parenthesis alongside with RTT in the table.

Host Address	IP Address	Location	Avg. RTT 1 (ms) at 10 am	Avg. RTT 2 (ms) at 2 pm	Avg. RTT 3 (ms) at 8 pm	Total Avg, RTT (ms)
amazon.in	54.239.33.92	Dublin	23.85 (0%)	39.52 (0%)	42.85 (0%)	35.40
reddit.com	151.101.193.140	California	8.59 (0%)	7.69(0%)	11.63 (0%)	9.23
cricbuzz.com	35.200.167.142	California	279.15(0%)	368.11(0%)	354.26(0%)	333.84
codeforces.com	81.27.240.126	Russia	64.23(8%)	47.13(4%)	59.67(0%)	57.01
bet365.com	5.226.176.16	England	35.14(0%)	22.98(0%)	25.30(0%)	27.8
yahoo.com	98.138.219.231	New York	240.81(0%)	160.56(0%)	149.69(0%)	183.64

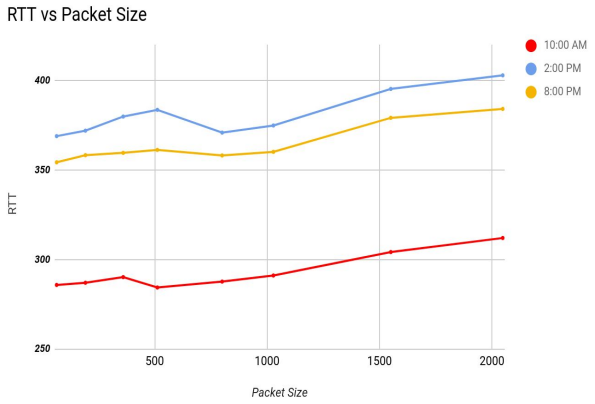
- **Packet Loss:** Yes there exists a packet loss of more than 0% in the case of *codeforces.com*. One of the major reasons for packet loss is because of Link Congestion. It occurs when one or more packets of data travelling across a computer fail to reach their destination IP. There might be some fault in hardware which can cause some packets to be lost. Also if packets are sent at a faster rate than the nodes can process, then packet loss is inevitable.

- **Geographical Location:** In general, if someone is using a server closer to the client device, the latency would be less rather in the case where the server would be a larger distance. However, it is seen that the amount of packet switching and network hardware between the two computers/devices is often more significant. Hence RTTs measured are weakly correlated with the geographical distance of the hosts. Also in our data, it can be seen that in general, the locations closer to India(Dublin/England/Russia) have lower latency than those that are far away(California/New York).

- **Time of the day:** The Internet Service Provider(ISP) gateway can handle only a constant number of requests per second. So during some hours of the day(generally during afternoon/evening), it can be seen that ping time has increased, which is mainly because the number of users trying to access that website has substantially increased during that time. Also, it can be seen that yahoo.com(USA server) has higher latency(240.81ms) during the night local time in the USA while having lower latency(149.69) during the morning local time.

Size(Bytes)	64	192	360	512	800	1028	1550	2048
Avg. RTT 1	285.75	286.98	290.12	284.32	289.23	291.03	295.31	302.21
Avg. RTT 2	368.90	371.96	379.85	383.58	370.87	374.85	397.52	400.51
Avg. RTT 3	354.28	358.26	359.56	361.21	358.12	360.12	380.26	385.15

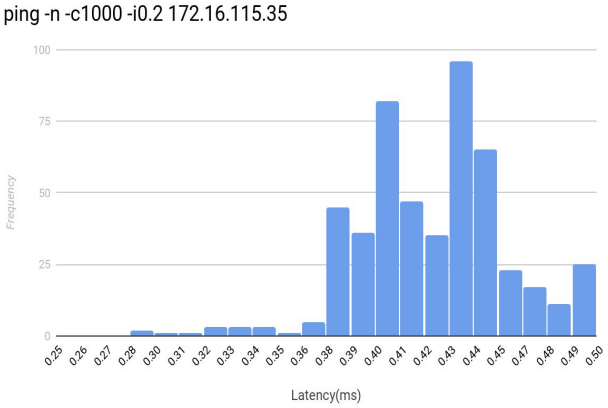
- **Packet Size:** In general, as the packet size increases the latency also increases. Also over a certain size, the latency rapidly increases. This is because of the concept of the *Maximum Transmission Unit(MTU).* The most common MTU size is 1500 bytes, which means that if the size of the packet is less than 1500 bytes, they will be sent as one frame and hence have smaller latencies. However, for a packet with a size greater than 1500 bytes, packets are broken into multiple frames leading to an increase in latency time.

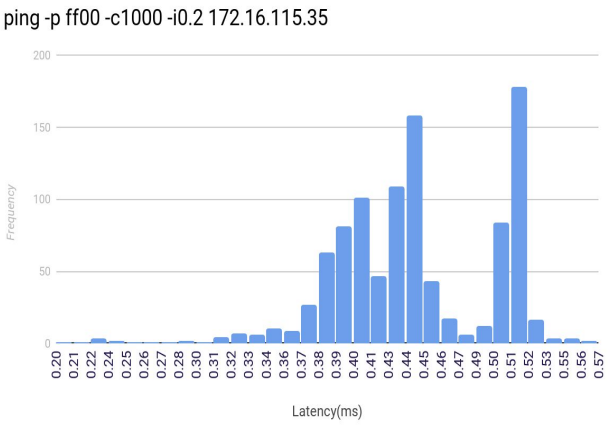


3) 2 Different Scenarios of Ping

Linux Terminal Command	Packets sent	Packets received	Packet Loss	Minimum latency	Maximum latency	Average latency
ping -n -c1000 -i0.2 172.16.115.35	1000	1000	0%	0.246ms	0.552ms	0.469ms
ping -p ff00 -c1000 -i0.2 172.16.115.35	1000	994	0.6%	0.190ms	0.561ms	0.483ms

- The two cases are very similar to each other except in two aspects. '-n' specifies that no attempt will be made to lookup symbolic names for host addresses and hence, it is faster than normal ping. So, the average latency is higher in the second case than the average latency in the first case. '-p' is used to pad bytes to fill out the packets that are sent which is useful for diagnosing data-dependent problems in a network. '-p ff00' will cause the packet to be padded with the pattern *1111111100000000.* This will cause problems with the synchronisation of the clocks because only one transition is present in the padding, from 1 to 0. Hence, the clocks are more likely to go out of synchronisation in the second case and we observe that the packet loss is higher in the second case.

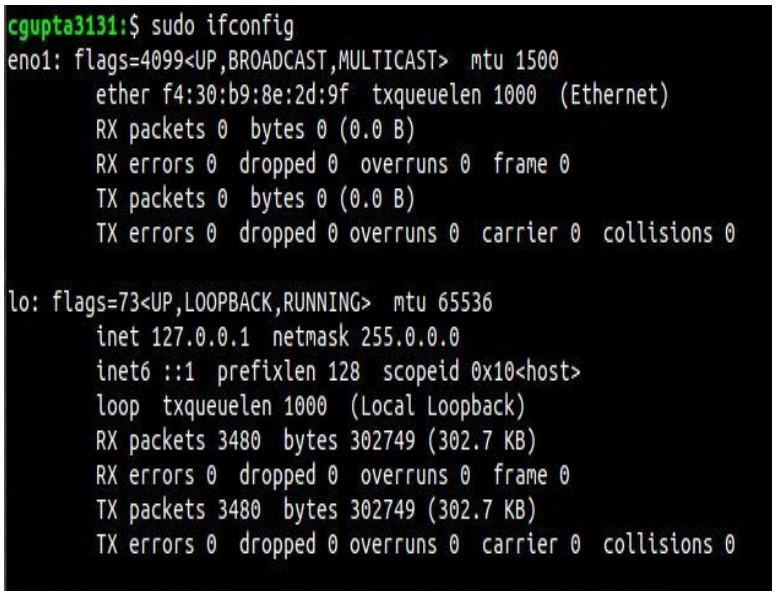




4) Ifconfig and Route

The command ***'ifconfig'*** shows details of the network interfaces that are up and running in the computer. My machine has a wired ethernet interface (eno1) and a loopback interface (lo).

a) The output of ifconfig command explained:



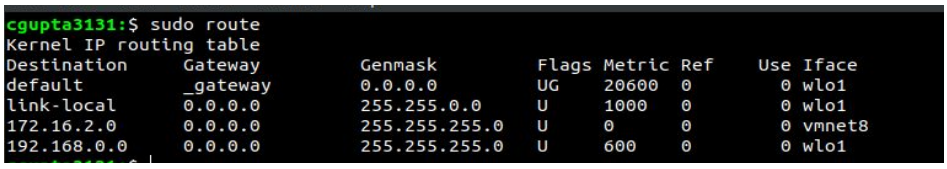
- **Inet Addr**: It indicates the IPv4 and IPv66 addresses
- **Bcast**: Denotes the Broadcast address at which all devices connected to the network are enabled to receive datagrams.
- **Mask**: Network Mask and is required to extract the network and host address from the IP address.
- **UP**: This flag indicates that the kernel modules related to the Ethernet interface have been loaded.
- **BROADCAST**: Denotes that the Ethernet device supports broadcasting
- **NOTRAILERS**: indicate that trailer encapsulation is disabled. Linux usually ignores trailer encapsulation so this value has no effect at all.
- **RUNNING**: The interface is ready to accept data.
- **MULTICAST**: This indicates that the Ethernet interface supports multicasting.
- **MTU**: 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.
- **RX/TX PACKETS**: show the total number of packets received and transmitted respectively.
- **COLLISIONS**: Shows the number of packets that are colliding due to network congestion.
- **TXQUEUELEN**: Denotes the length of the transmit queue of the device.
- **RX/TX BYTES**: indicate the total amount of data that has passed through the Ethernet interface either way.

b) Options provided with ifconfig command:

- **-a**: Displays all interfaces which are currently available, even if down
- **Up**: This flag causes the interface to be activated.
- **Down**: This flag causes the driver for this interface to be shut down.
- **Mtu n**: This parament sets the Maximum Transmission Unit of an interface.
- **Address:** The IP address to be assigned to this interface.

The ***'route'*** command shows the routing table of the device. My computer has a total of 4 route entries out of which 3 are wireless and one is a virtual network.

c) The output of the route command explained:



- **DESTINATION**: The destination network or destination host.
- **GATEWAY**: The gateway address or '*' if none set.
- **GENMASK**: The netmask for the destination net.
- **FLAGS**: U: route is up and G: use gateway.
- **METRIC**: The 'distance' to the target(counted in hops).
- **REF**: Number of references to this route.
- **USE**: count of lookups for the route.
- **IFACE**: Interface to which packets for this route will be sent.

d) Options provided with route command:

```
dishaislove@cgupta3131: route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.112.1    0.0.0.0         UG    20100  0        0 enp0s31f6
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s31f6
172.16.112.1    0.0.0.0         255.255.255.255 UH    20100  0        0 enp0s31f6
172.16.115.0    0.0.0.0         255.255.255.128 U     100    0        0 enp0s31f6
```

- **DEL**: Delete a route
- **ADD**: Add a route
- **TARGET**: The destination network or host
- **-net**: Target is a network
- **-host**: Target is a host
- **-n:** Show numerical addresses instead of symbolic hostnames.

5) Netstat Command

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 is one of the most basic network service debugging tools, which tells us which ports are open and whether any programs are listening on ports.

```
cgupta3131:$ netstat -at | grep "ESTABLISHED"
tcp        0      0 cgupta3131-HP-Pav:43886 maa03s26-in-f10.1:https ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:57850 edge-star-shv-02-:https ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:44772 maa05s05-in-f1.1e:https ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:39122 xx-fbcdn-shv-02-b:https ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:56864 104.27.158.78:https     ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:46008 maa05s02-in-f3.1e:https ESTABLISHED
tcp        0      0 cgupta3131-HP-Pav:48430 ec2-35-161-43-202.:http ESTABLISHED
```

b) **Netstat -at** command is used to show all the TCP established connections.

Explanation:

Proto: Tells socket is TCP or UDP(Protocol). TCP makes reliable connections but slows down dramatically if the network quality is bad. UDP stays fast but may lose a few packets or deliver them in the wrong order.

Local and Foreign Address: Tells to which hosts and ports the listed sockets are connected. The local end is always on the computer on which you're running netstat, and the foreign end is about the other computer.

Recv-Q and Send-Q: Tells how much data is in the queue for that socket waiting to be read(Recv-Q) or sent(Send-Q). In short: if this is 0, everything's ok, if there are non-zero values anywhere, there may be trouble.

State: Tells in which state the listed sockets are. The TCP protocol defines states, including "LISTEN" (wait for some external computer to contact us) and "ESTABLISHED" (ready for communication).

c) **Netstat -r** command is used to display the kernel routing table i.e it nearly shows the same output as route command does.

```
cgupta3131:$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlo1
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlo1
172.16.2.0      0.0.0.0         255.255.255.0   U         0 0          0 vmnet8
172.16.170.0    0.0.0.0         255.255.255.0   U         0 0          0 vmnet1
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 wlo1
```

An explanation for extra columns:

MSS: It lists the value of the Maximum Segment Size. It is a TCP parameter and is used to split packets when the destination has indicated that it can't handle larger ones.

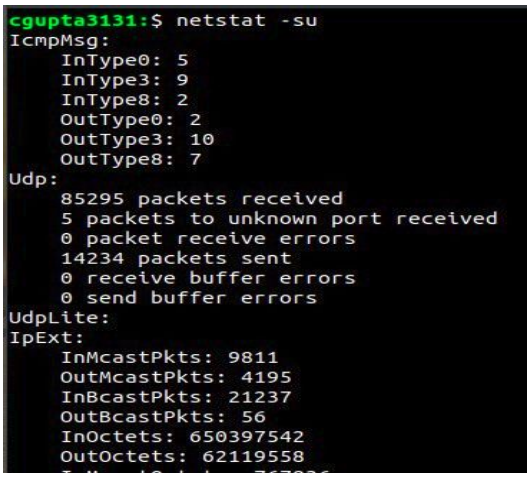
WINDOW: It shows the window size, which indicates how many TCP packets can be sent before atleast one of them has to be Acknowledged.

IRTT: Initial Round Trip Time and used to guess about the best TCP parameters.

d) Netstat -i command is used to display the status of all network interfaces. As we can see, the total number of interfaces on my computer is 5(eno1, lo, vmnet1,vmnet8 and wlo1).

```
cgupta3131:$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno1      1500        0      0      0 0             0      0      0      0 BMU
lo       65536     7558      0      0 0          7558      0      0      0 LRU
vmnet1    1500        0      0      0 0          1489      0      0      0 BMRU
vmnet8    1500        0      0      0 0          1489      0      0      0 BMRU
wlo1      1500   876889      0      0 0        277156      0      0      0 BMRU
```

e) Netstat -su is used to showing the statistics of all UDP connections.



f) ***Loopback Interface:*** It is a virtual interface. The only purpose of the loopback interface is to return the packets sent to it, i.e whatever you send to it is received on the interface. It makes little sense to put a default route on the loopback interface because the only place it can send packets to is the imaginary piece of wire that is looped from the output of the interface to the input. It mainly performs the following functions:

Device identification: The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method.

Routing information: The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as ping mpls require a loopback address to function correctly.

6) Traceroute Experiment

- The six hosts used for the experiment were amazon.in, reddit.com, cricbuzz.com, codeforces.com, bet365.com, and yahoo.com.
- Readings were taken at three times of a day: **10 am, 2 pm and 8 pm;**
- Uptrends utility (*https://www.uptrends.com/tools/traceroute*) was used to take the observations with New Delhi as the host server.

Time of the Day	amazon.in	reddit.com	cricbuzz.com	codeforces.com	bet365.com	yahoo.com
10 AM	10	6	26	20	13	17
2 PM	10	5	25	20	14	17
8 PM	11	5	27	4(Incomplete)	14`	19

a) The most common hops found are the IP addresses: ***164.52.192.1 and 180.179.194.122.*** These would be most probably be the IP address of “uptrends” website through which traceroute and hops are being calculated. Hops are common because of the reason that routes to these destinations pass through the same internet circles and hence overlap.

b) The same company host doesn’t mean that they are on the same network, so route and ping might be different if they are connected to a different network element. The packets are redirected by the nodes to take a route having less traffic. The load balancing is done to reduce the load of a congested path. For example, at 2 PM(54.239.33.92) amazon.in have a different destination server address, while at 8 PM (54.239.100.236)it has a different address.

c) As we can see the traceroute was unable to reach the codeforces.com destination server at 2 PM. because many people block ICMP/ping for security reasons, like preventing hackers from getting information about open ports and starving off denial of service attacks. However, they still send the data to the next hop as there are results that follow. Many network providers disable ICMP traffic if their network is under heavy load.

d) Yes, it is possible. This is because **ping** sends an ICMP segment from source to destination, that traverses networks via routing rules and expects an ICMP reply from the host. Most probably the server is blocking the reply. On the other hand, Traceroute works by targeting the final hop, but limiting the TTL and waiting for a time exceeded message, and then increasing it by one for the next iteration. Therefore, the response it gets is not an ICMP echo reply to the ICMP echo request from the host along the way, but a time exceeded message from that host - so even though it is using ICMP, it is using it in a very different way.

7) ARP Table

a) ARP is the **Address Resolution Protocol** and its job is to match MAC address to IP address and vice versa. Command to show full ARP table: ***arp.***

Address: IP address of the device to which communication was established.
Flags: Each permanent entries are marked with M and published entries have the P flag. Complete entry in the ARP cache will be marked with the C flag;
HWtype: MAC address. It specifies the type of hardware used for the local network transmission. Ethernet Is the most common Hardware type and its value is 1.
Iface: Interface to which address mapping is assigned.

```
cgupta3131:$ sudo arp -s 172.16.170.86 00:50:59:e1:1b:ad
cgupta3131:$ sudo arp -s 172.16.170.98 04:50:59:e1:1b:ad
cgupta3131:$ sudo arp -s 172.16.170.109 04:50:d9:a1:9b:ad
cgupta3131:$ sudo arp -s 172.16.170.31 14:50:d9:a1:9b:ad
cgupta3131:$ sudo arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.170.254           ether   00:50:56:e1:1b:ac   C                     vmnet1
172.16.170.109           ether   04:50:d9:a1:9b:ad   CM                    vmnet1
_gateway                 ether   30:b5:c2:b4:d2:d5   C                     wlo1
172.16.170.31            ether   14:50:d9:a1:9b:ad   CM                    vmnet1
172.16.170.86            ether   00:50:59:e1:1b:ad   CM                    vmnet1
172.16.170.98            ether   04:50:59:e1:1b:ad   CM                    vmnet1
```

```
dishaislove@cgupta3131: arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     enp0s31f6
172.16.112.66            ether   00:03:0f:1a:fc:38   C                     enp0s31f6
172.16.112.49            ether   00:03:0f:1b:61:22   C                     enp0s31f6
172.16.112.34            ether   00:03:0f:1d:ab:fe   C                     enp0s31f6
```

b) **Add entry:** sudo arp -s ip_address HWadress (Note the entries manually added have flag M)
Delete entry: sudo arp -d ip_address

c) By default, entries in the ARP table stay cached for ***60 seconds*** which is stored in the file ***/proc/sys/net/ipv4/neigh/default/gc_stale_time***. A trial and error method to discover the timeout value is to add a temporary entry in the table and keep checking the table after fixed intervals of time. The time after which it is deleted from the cache is the required cache timeout. Alternatively, one can use binary search also for finding the cache time, for e.g.– Add a temporary entry in ARP and check after 5000ms. If then entry has been deleted, then add the entry again and check after 2500ms

d) The scenario where two IP's can map to same Ethernet Address is when a router or a gateway connects two or more subnet ranges. When communicating with machines on the same subnet range, *the MAC address is used for directing the packages*. In the ARP Table, the IP's of the devices which are connected in the other subnet range have the ethernet address/MAC address as that of the Router or Gateway which connects the two subnet ranges. ARP table is referred to convert these IP addresses to the MAC address and packets are sent to it(router/gateway). The router then uses it's routing table and sends the packet further to the correct device

`

8) Local Network Analysis

- Nmap ("Network Mapper") is an open-source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts.
- The command used for the analysis is **nmap -n -sP 10.1.2.53/22** scanning 1024 IP addresses in the Kapili hostel.
- The trend observed is that there is an increase in the number of hosts during hostel hours. The number of users increases at around 12 Noon and there is a slight dip at around 6 PM as students have their SA/NSO course during that time. Also, there is a high boost at around 8 PM and 10 PM as students come back to their room and work on their laptops.