CS349- Assignment 1

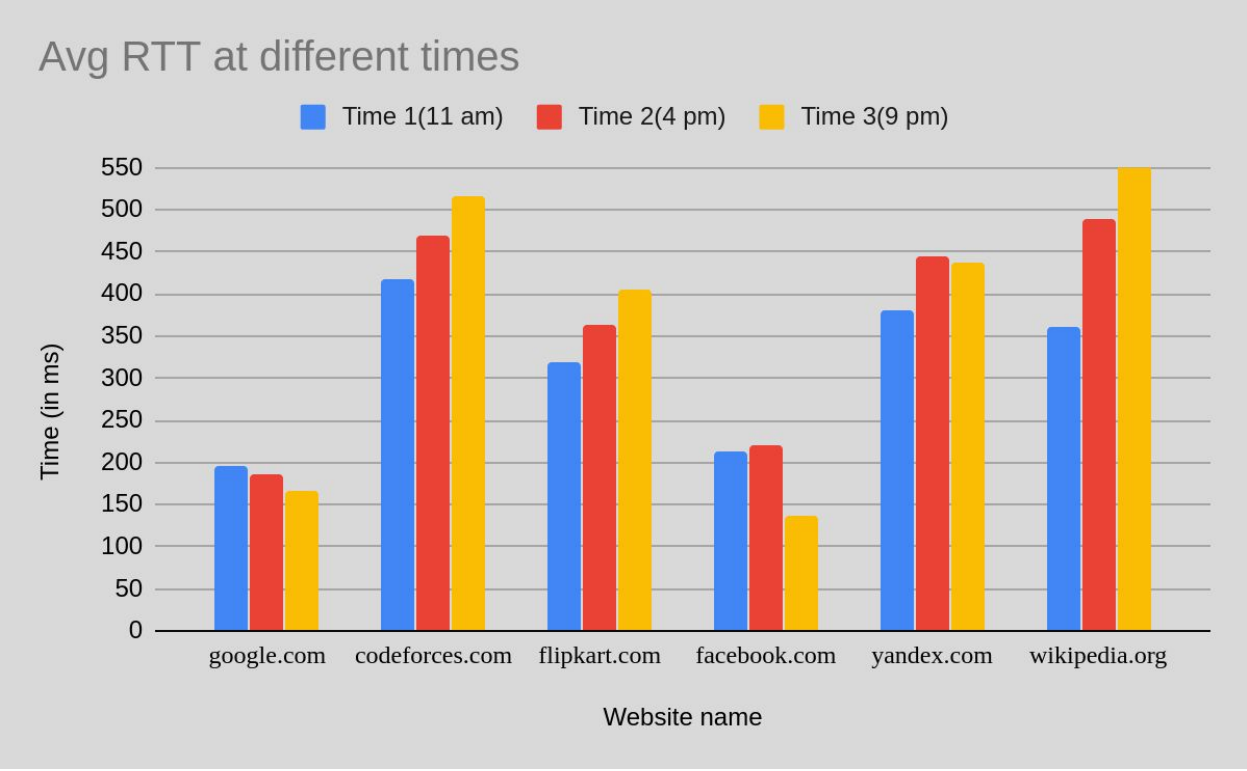
Tushar Bhutada- 170101073

Answer 1

A) ping –c count- the value of count specifies the number of requests to be sent.
B) ping -i interval- the value of interval specifies the duration between the packets.
C) ping –l preload- the value of preload determines the number of packets to send without waiting for a reply. the limit for sending such ECHO_REQUEST packets by normal users is 3.
D) ping –s packetsize- the packetsize denoting the size of packet to be sent. The packet is added with 20 bytes IP header and 8 bytes ICMP header. Thus, the total packet size is 20+8+32=60 bytes.

Answer 2

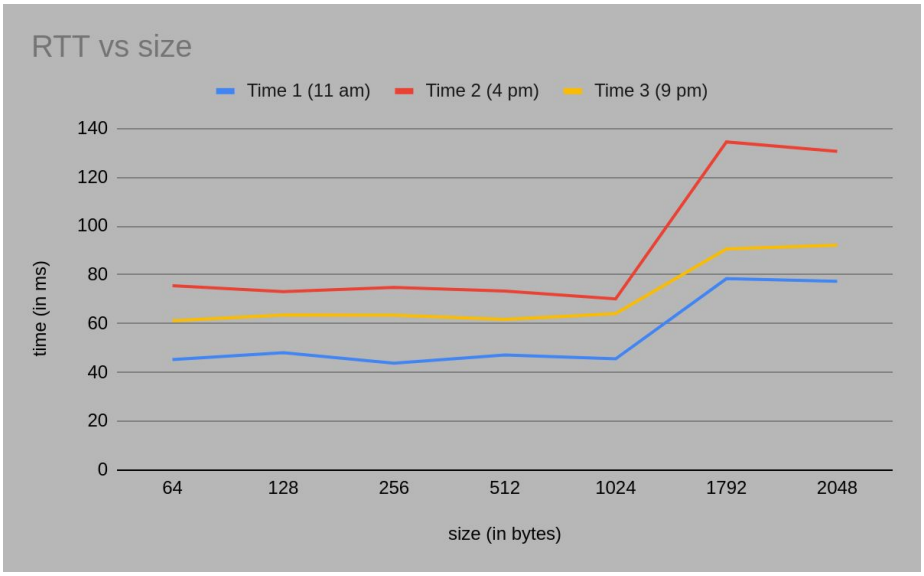
Host	IP address	Location	RTT1(11 am)	RTT2(4 pm)	RTT3(9 pm)	Avg. RTT
google.com	172.217.163.46	California, USA	194.9	186.447	166.957	182.768
codeforces.com	81.27.240.126	Moscow, Russia	417.678	469.523	515.503	467.568
flipkart.com	163.53.78.128	Bangalore,India	318.794	364.398	404.96	362.717
facebook.com	157.240.23.35	Chennai,India	214.097	220.472	135.847	190.139
yandex.com	231.180.204.62	Russia	380.848	445.196	438.096	421.38
wikipedia.org	103.102.166.224	New York,USA	360.918	488.357	594.221	481.165



Avg RTT vs Location: From the graph, it can be inferred that there exists weakly positive correlation between the Geographic distance and Round Trip Time (RTT). Numerous reasons like number of hops, propagation delay and

others can affect this correlation. With increasing distance, it takes packets generally more time to reach the target host. With increasing distance, node count increases which results in further processing delay. It is a weak relation because distance isn't the sole factor which determines the RTT. Some servers gave a packet loss in range from 4-10 % at 4pm slot but other slots had 0% packet loss.

Avg RTT vs time: There is no strong relation with time that i could infer because all servers have different locations but for most of the observations, the RTT was higher for the latter two times compared to 11 am which indicates that network congestion is higher in the other two time slots. Alos, it depends on the individual host audience too. For Eg: Codeforces had a contest from 8-10 pm which increased traffic to the host.

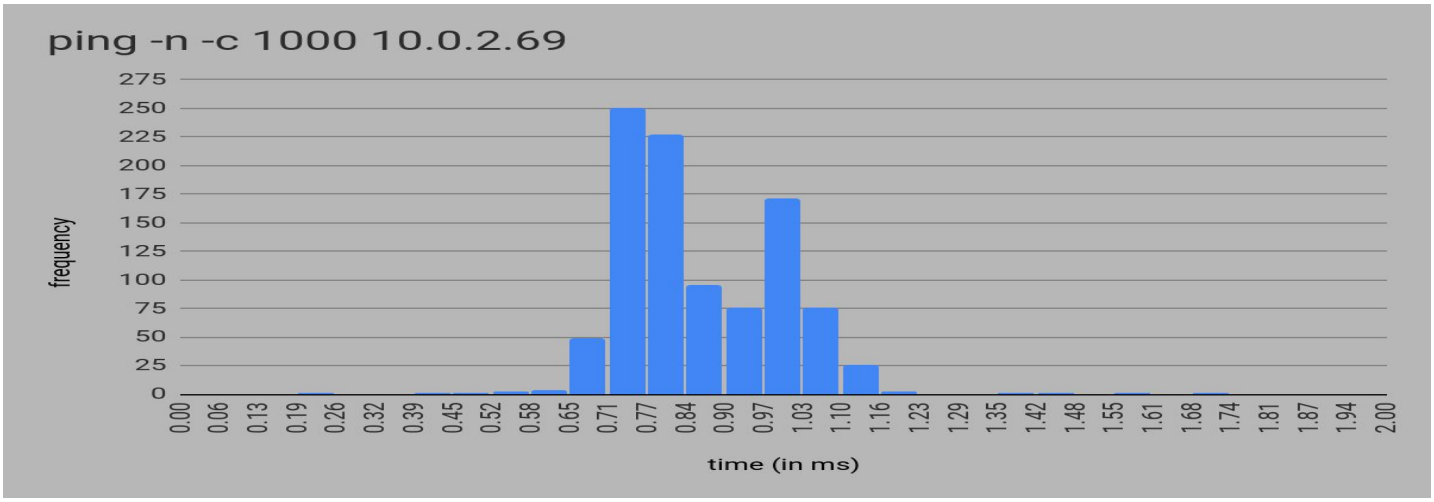


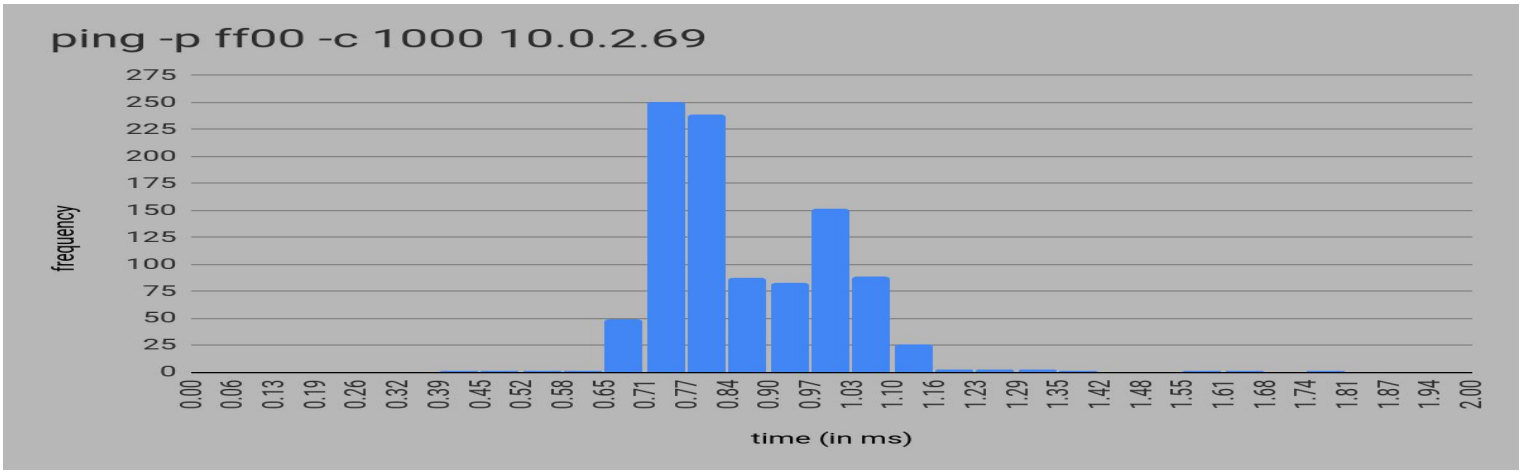
Avg RTT vs packet size: From the graph it comes to notice that RTT is similar for almost similar for sizes till 1028 bytes. Then it almost doubles up for 2048 bytes. The reason for this is that Maximum Transmission Unit is 1500 bytes. So for sizes less than that the packet is stuffed to 1500 bytes. But for sizes bigger, the packet is broken down to two frames of size 1500 bytes, as a result of which time increases.

Answer 3

A) and B) The selected IP was 10.0.2.69. The table below shows the answers for the two parts

Command	Packets sent	Packets received	Packet loss rate	Min. latency	Max latency	Mean latency	Median latency
Ping -n -c 1000 10.0.2.69	1000	1000	0%	0.205	5.024	0.894	0.322
Ping -p ff00 -c 1000 10.0.2.69	1000	999	0.1%	0.405	3.215	0.881	0.199





D) ping -n displays numeric output only. No attempt is made to lookup symbolic names for host addresses.ping -p ff00 stuffs the packet with the pattern 1111111100000000 which is useful for diagnosing data-dependent problems in a network. Thus due to non stuffing -n option has lower mean latency. Also due to stuffing, synchronisation problem arises for the clocks because only one transition is present in the padding which is from 1 to 0. Hence, packet loss is observed is observed in second case as clocks are likely to go out of synchronisation.

Answer 4

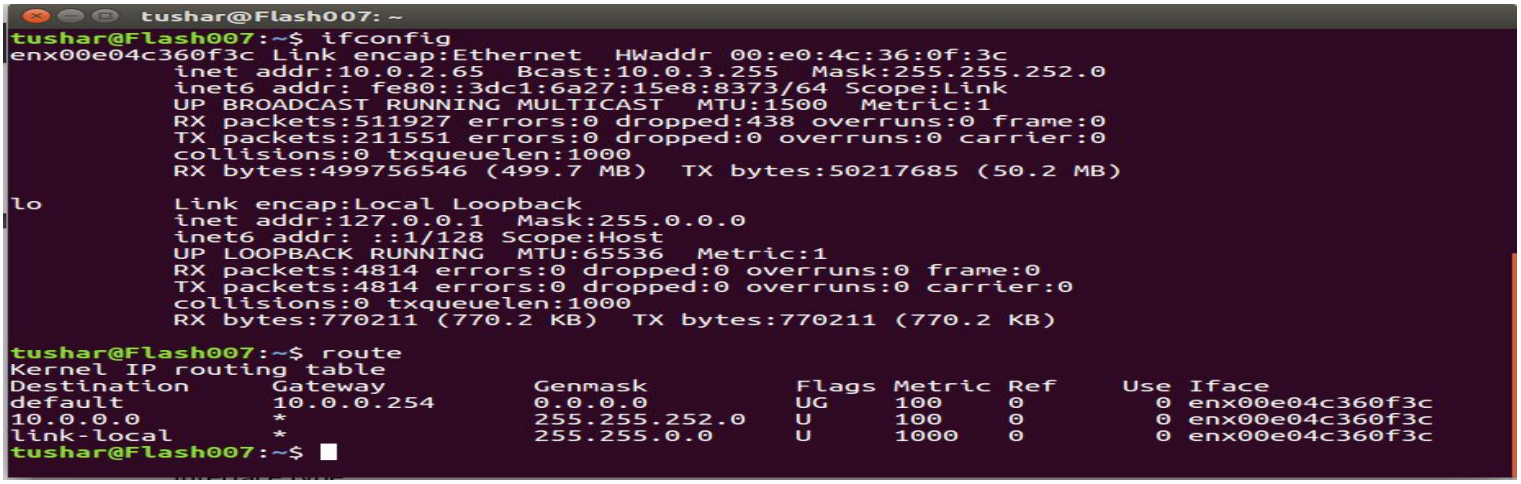
Note: All commands have been shown in one screenshot for efficiency.

A) **ifconfig** stands for "interface configuration." It is used to view and change the configuration of the network interfaces on your system. **Link encap** refers to the interface type. **HWaddr** refers to unique MAC address of the ethernet card. **inet and Bcast** refer to IP and broadcast addresses respectively. **Up** indicates ethernet modules are loaded. **Broadcast** denotes Broadcasting is supported. Running means ready acceptance for data. **Multicast** refers to source able to send packets to multiple machines. **RX** and **TX** packets refers to received and transmitted packets respectively. **RX bytes** and **TX bytes** refer to the total data passed through ethernet in both directions. **Collisions** refer to the degree of network congestion. **txqueuele** denotes length of transmit queue. **Metric** denotes the priority of device. **MTU (Max. Transmission Unit)** is the size of each packet received by ethernet card.

B) Use **mtu N** to set packet size for transmission. **Multicast** to set this flag to the interface to allow multiple transmissions. **-a** to display all interfaces which are currently available, even if down. **add addr** to add an IPv6 address to an interface.

C) **Destination** column identifies the destination network. The **Gateway** column identifies the gateway for the specified network. The **Genmask** column shows the netmask for the network. The **Flags** may be U (Up route) and G (Gateway route). **Metric** refers to the number of hops to the destination. **Ref** is the number of references to this route. **Iface** column shows the network interface (Ethernet or wireless ethernet).

D) **-net** option is used to denote target is network. **del/add** can be used to delete/add routes. **-n** to show numeric addresses instead of symbolic names. **metric M** to set the metric field value in routing table to M.



Answer 5

Note: All commands have been shown in one screenshot for efficiency.

A) Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

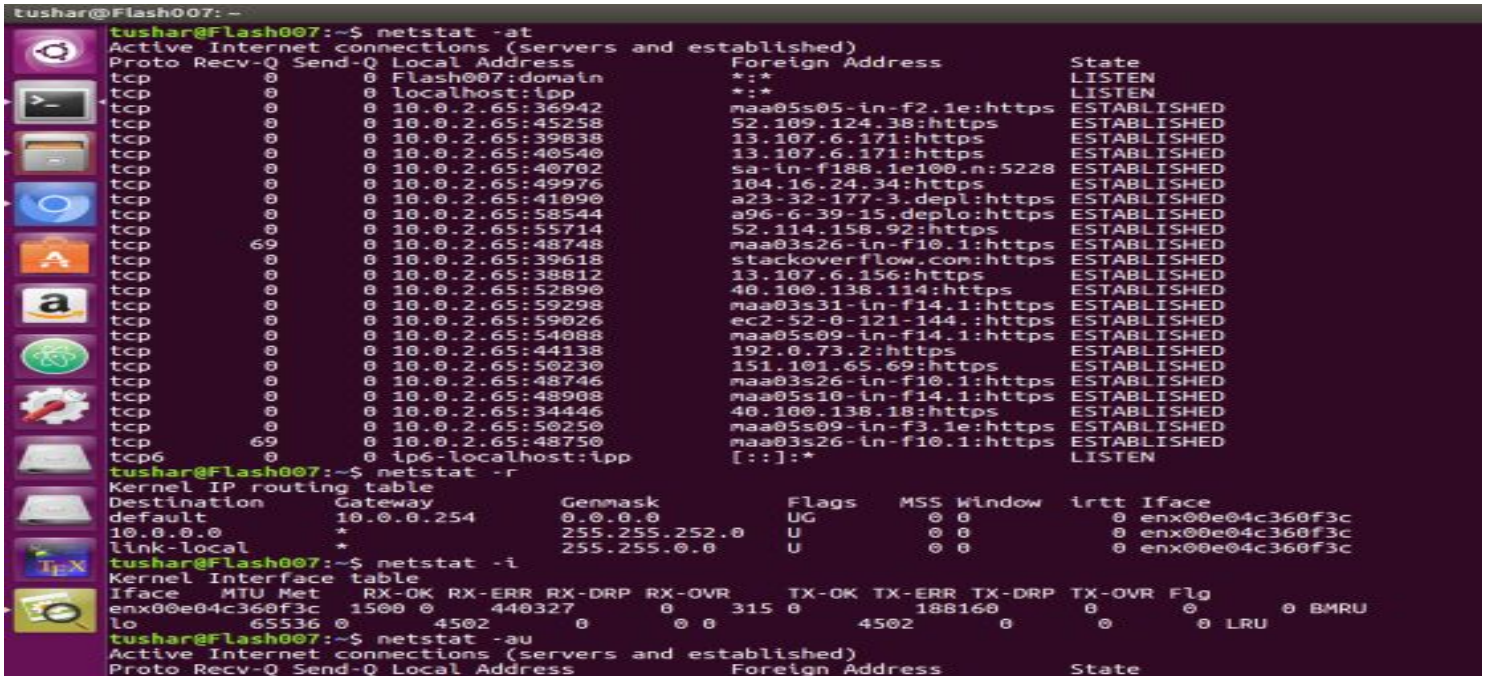
B) **netstat –at** is the required command. **Proto** indicates the protocol used. **Recv-Q** and **Send-Q** refers to the data queued to be received and sent respectively. **Local address** specifies Address and port number of the local end of the socket. **Foreign address** specifies Address and port number of the remote end of the socket. **State** refers to the state of the socket out of predefined values set.

C) It shows the Kernel Routing Table of the Machine. **Destination** column indicates the pattern that the destination of a packet is compared to. The **Gateway** column refers to the location where a packet is to be sent on the matching destination. The **Genmask** column identifies the subnet by indicating the bit count from the start of IP address. The **Flags** column describe the route - G(gateway), U(up), H (Single host), D(dynamic), M (set if entry was modified by an ICMP redirect message). The **MSS (Maximum Segment Size)** is the size of the largest datagram that will be used for the transmission by the kernel. The **Window** refers to the maximum amount of data accepted in single out from remote host. **IRTT** refers to initial round trip time. The **Iface** column refers to the network interface type.

D) **netstat -i** is the required command. Looking at the output, my device has 3 interfaces, namely enx00e04c360f3c and lo

E) **netstat –au** is the required command.

F) The loopback device 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.



Answer 6

Note: All commands have been shown in one screenshot for efficiency.
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. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

Time slot	google.com	codeforces.com	flipkart.com	facebook.com	yandex.com	wikipedia.com
11 pm	10	12	7	9	14	9
4 pm	10	12	8	9	13	9
9 pm	10	12	7	8	13	9

A) The common IP I found in all the hops was the starting one, which obviously being my laptop's Ip. Apart from these, same hosts in nearby geographical locations seemed to have some intermediary IP same because of the fact that they might have the same internet circles for longer transmission distance.
B) Yes. The route changed at different times because of the fact that network congestion is variable at all times during a day. Generally, packets are preferred to sent through lower congestion node to increase efficiency and speed as a result of which route changes.
C) In my observation, I had to change the tool once for getting a route because the server displayed the message "Couldn't reach destination because of firewall blocking". Firewall can block ICMP packets or in some cases hosts may not provide complete path is network congestion exceeds a specified limit.
D) Yes the route might be possible. This is due to the fact that ping and traceroute differ in their fundamental working. Ping sends ICMP packets to the host and expects the reply. If the server blocks the reply, ping fails. But in the case of traceroute, packets are sent with TTL values that decrement with each passing router and when the value turns zero, is shows ICMP error (ICMP Time Exceeded). Thus if TTL value stays greater than zero after reaching host, we can find a route.

Answer 7

Note: All commands have been shown in one screenshot for efficiency.
A) arp is the required command. Address refers to the IP address. HWtype signifies the network link protocol type. **HWaddress** refers to unique MAC address of the ethernet card.The flags indicate if the mac address has been learned, manually set, published (announced by another node than the requested) or is incomplete. Mask refers to the subnet mask. Iface refers to the specific type of interface.
B) arp -s ipaddr mac_addr is used to add new table entry. Arp -d address is used to delete a specific entry.
C) The time limit for cache entries is about 60 seconds. The trial and error method could be to add a new entry and check at regular intervals, say 4 seconds, if the entry is still in the arp table. Efficiency and performance of

this method can be made better by increasing/decreasing the time intervals. We can also use binary search to get closer approximation.
D) Two IP's map to same Ethernet Address when a router/gateway connects multiple subnet ranges.ARP table does the job of converting these IP addresses to the MAC address and packets are sent to it. The router then uses its routing table to find the correct destination to which the packet has to be sent.

```
tushar@Flash007: ~/Desktop
tushar@Flash007:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.1.10                ether   50:3e:aa:db:d9:ea   C                     enx00e04c360f3c
10.0.2.48                ether   d0:bf:9c:0f:7f:18   C                     enx00e04c360f3c
172.17.1.1               ether   4c:4e:35:97:1e:ef   C                     enx00e04c360f3c
10.0.1.9                 ether   e4:be:ed:1f:b2:b1   C                     enx00e04c360f3c
10.0.2.31                ether   d0:bf:9c:21:00:27   C                     enx00e04c360f3c
10.0.0.254               ether   4c:4e:35:97:1e:ef   C                     enx00e04c360f3c
tushar@Flash007:~/Desktop$ arp -s 10.0.2.32 ff:ff:ff:ff:ff:ff
SIOCSARP: Operation not permitted
tushar@Flash007:~/Desktop$ sudo arp -s 10.0.2.32 ff:ff:ff:ff:ff:ff
[sudo] password for tushar:
tushar@Flash007:~/Desktop$ sudo arp -s 10.0.2.33 ff:ff:ff:ff:ff:ff
tushar@Flash007:~/Desktop$ sudo arp -s 10.0.2.34 ff:ff:ff:ff:ff:00
tushar@Flash007:~/Desktop$ sudo arp -s 10.0.2.35 ff:ff:ff:ff:00:00
tushar@Flash007:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.35                ether   ff:ff:ff:ff:00:00   CM                    enx00e04c360f3c
10.0.1.10                ether   50:3e:aa:db:d9:ea   C                     enx00e04c360f3c
10.0.2.48                ether   d0:bf:9c:0f:7f:18   C                     enx00e04c360f3c
10.0.2.34                ether   ff:ff:ff:ff:ff:00   CM                    enx00e04c360f3c
172.17.1.1               ether   4c:4e:35:97:1e:ef   C                     enx00e04c360f3c
10.0.1.9                 ether   e4:be:ed:1f:b2:b1   C                     enx00e04c360f3c
10.0.2.31                ether   d0:bf:9c:21:00:27   C                     enx00e04c360f3c
10.0.2.33                ether   ff:ff:ff:ff:ff:ff   CM                    enx00e04c360f3c
10.0.2.32                ether   ff:ff:ff:ff:ff:ff   CM                    enx00e04c360f3c
10.0.0.254               ether   4c:4e:35:97:1e:ef   C                     enx00e04c360f3c
tushar@Flash007:~/Desktop$
```

Answer 8

The command used is nmap -n -sP 10.0.0.0/26 which concern with the Ip's of Dihing hostel. From the graph, it is inferred that the number of hosts increases till 5 in the evening (when classes get over). Then from 5-12 am increase slightly and decreases thereafter.