CS 349 Networks Lab Assignment 1

By: Shubham Singhal 150101072

Question 1

a) **Option required to specify the number of echo requests to send with ping**: **–c**
Example: '**ping 192.168.0.1 –c 10'** will send 10 ICMP ECHO_REQUESTS to the specified address.

b) **Option required to set time interval between two ping request(in seconds): -i**
Example: '**ping 192.168.0.1 -i 5'** will send ICMP ECHO_REQUESTS to the specified address every 5 seconds. Interval less than 0.2 seconds require 'sudo' permissions

c) **Option to send ECHO_REQUESTS packets to destination one after other without waiting for a reply**: **-f**
Example: '**sudo ping 192.168.0.1 –f'** will flood the target with ICMP ECHO_REQUESTS without waiting for reply.
Limit for sending such ECHO_REQUEST packets by normal users: Normal users can send requests with **minimum time interval of 0.2 seconds**.

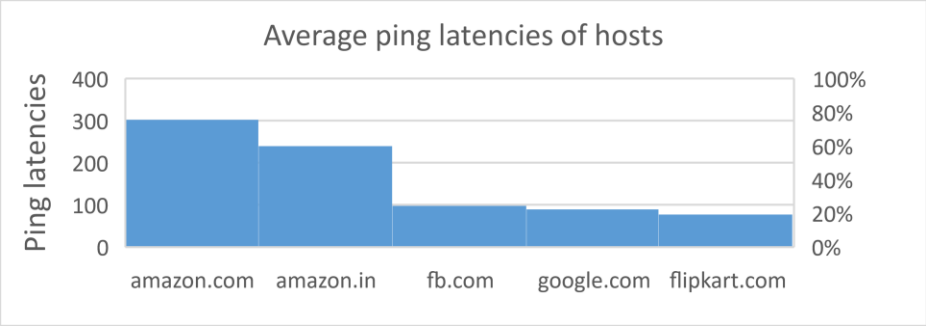
d) **Command to set the ECHO_REQUEST packet size**: -s
Example: **'ping 192.168.0.1 -s 128'** will send ICMP ECHO_REQUESTS to the specified address with 128bytes of ICMP_DATA.
When Packet Size is set to 64 bytes, then the total packet size will be **72 bytes** considering the 8 bytes of ICMP header data.

Question 2

Hosts Chosen are :

1. Google.com 2.Facebook.com 3.Flipkart.com 4. Amazon.in 5. Amazon.com

Average (data was taken at 4 different times) ping latencies of above hosts:



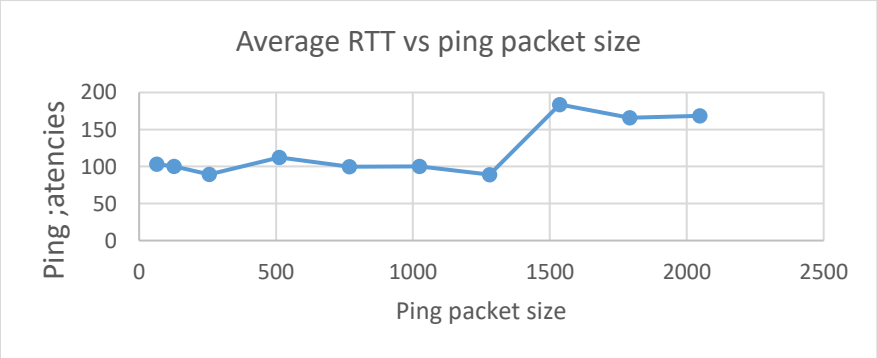
Impact of geographical distance : Ping latencies are **weakly correlated** to Geographical distance. As seen from above graph, ping latency for amazon.com is more compared to amazon.in. Since amazon.in server is likely to be in india compared to amazon.com which would be in USA.

Packet loss greater than 0% : Packet lost in above experiments were not observed except for one case where 1 packets was lost out of 20.

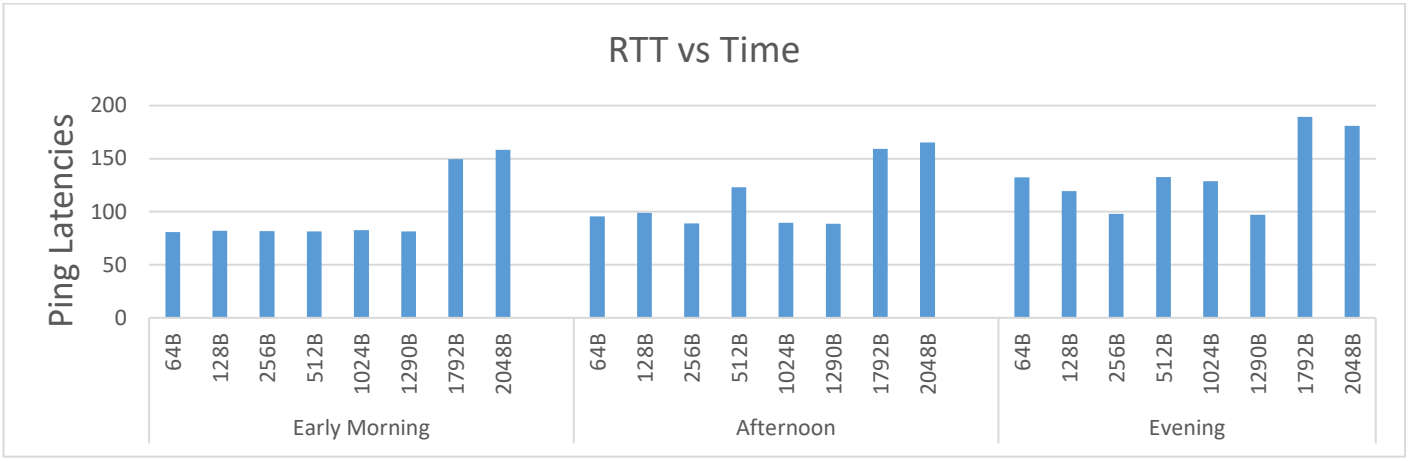
Reason for packet loss greater than 0% : 1.Packets were blocked by some firewall deployed on server. **2.** Network may be experiencing problems or may be down.

Hosts Chosen for pinging with different data size packets : Flipkart.com

Impact of ping packet size on latencies : When packet size is more than 1500(default MTU) then request is sent in multiple frame which may lead to more ping latency.



Impact of time of day on latencies



Question 3

Host: 202.141.80.14

Command : a) ping –n 202.141.80.14 –c 1000 b)ping –p ff00 –c 1000 202.141.80.14

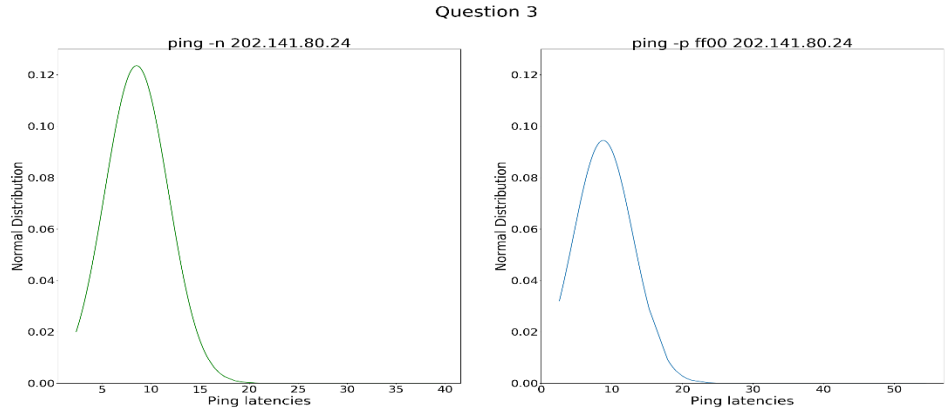
a) packet loss for each command:

command a): 1 packet out of 1000 command b): 2 packet out of 1000

b) minimum, maximum, mean, and median latency of the pings: (python scripts used to produce results: https://goo.gl/PeQzqf)

minimum latency :	a) 2.351	b) 2.599
maximum latency :	a) 39.700	b) 54.426
average latency :	a) 8.528	b) 8.816
median latency :	a) 8.440	b) 8.39

c) Normal distribution of the ping latencies: (following python scripts was used to produce the graphs : https://goo.gl/PeQzqf)



d) Difference between above two commands:

–n: No attempt will be made to lookup symbolic names for host addresses leading to **less time spent in each request**.

-p ff00: Networks in general will have problems in transmitting patterns that **doesn't have sufficient `transitions'** such as all ones or all zeros. So ff00(1111111100000000) is likely to face problem in transmission.

Hence it may occur that the command 'b' with pattern ff00 may have **more ping latency** and **higher packet loss**.

Question 4

ifconfig: A utility used to configure the kernel-resident network interfaces. It is used at boot time to set up interface as necessary. If no arguments are given. Ifconfig displays the status of the currently active interfaces.

Ifconfig explanation :

- **Link encap:Ethernet** : This represents the frame type associated with this interface. In our case it is Ethernet.
- **HWaddr** : the hardware address of the ethernet interface also known as MAC address. It is of 48 bits. First three octets represents the manufacturer id and the last three represents the serial number assigned to the device by the manufacturer.
- **inet addr** : IPv4 address assigned to the interface.

- **Bcast**: denotes the broadcast address for the current network
- **Mask** : the network mask which decides the potential size of your network
- **UP** : network interface is configured to be enabled.
- **BROADCAST** : Ethernet device supports broadcasting which is a necessary characteristic to obtain IP address via DHCP.
- **MULTICAST** : interface is configured to handle multicast packets. It allows a source to send a packet to multiple machines.
- **RUNNING** : Indicates that the network interface is operational and is ready to accept the data.
- **MTU** : Maximum Transmission Unit is a link layer characteristic which provides limit on the size of the Ethernet frame. 1500 is the default value for all Ethernet devices.
- **METRIC** : Interface metric is used to compute cost of a route. It tells the OS which interface a packet should be forwarded to, when multiple interfaces could be used to reach destination. Lower value means higher priority.
- **RX/TX packets** : the total number of packets received and transmitted respectively..
- **RX/TX bytes** : the total amount of data that has passed through the Ethernet interface.(ex. 47.2 MB download and 2.2 MB upload)
- **Interrupt** : network interface card is using the interrupt number 9. This is usually set by the system.
- **Collisions** : The number of transmitted packets that experienced Ethernet collisions. A nonzero value of this field indicates possibility of network congestion.
- **Txqueuelen**: The field provides the information about the configured length of transmission queue.

```
shubz@Dream:~$ ifconfig
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 2765  bytes 176714 (176.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2765  bytes 176714 (176.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.102  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::dece:3970:2667:ecb1  prefixlen 64  scopeid 0x20<link>
        ether 9c:b6:d0:de:45:91  txqueuelen 1000  (Ethernet)
        RX packets 35929  bytes 47295862 (47.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19050  bytes 2230580 (2.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **ifconfig –a:** display all interfaces which are currently available, even if down
- **ifconfig lo:** If a single interface argument is given, it displays the status of the given interface only. Example here it will show status of lo (loopback) adapter.
- **Ifconfig wlo1 up :**'wlo1' interface is activated.
- **Ifconfig wlo1 down :** 'wlo1' interface is deactivated.
- **Ifconfig wlo1 mtu 9000 :** set the MTU (maximum transmission unit) for 'wlo1' interface to be 9000 bytes. This setting doesn't survive after reboot.

Route: The 'route' command is used to view and make changes to the Kernel's IP routing table. Its primary use is to set up to specific hosts or networks via an interface.

```
shubz@Dream:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    20600  0        0 wlp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp2s0
192.168.0.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp2s0
```

Route explanation :

The above command shows that if the destination is within the network range 192.168.0.0 – 192.168.0.255 since the subnet mask is 255.255.255.0(last 8 bits are zero meaning 256 ip), then the gateway is *, which is 0.0.0.0. Note that this ip range is local network of router and hence packets need not go to gateway if destination is present in local network.

When packets are sent within this IP range, then the MAC address of the destination is found through ARP Protocol and the packet will be sent to the MAC address.

Destination address of 0.0.0.0 is used when no other rule is matched(subnet 0.0.0.0 means any ip will match this rule). The gateway of router which is 192.168.0.1 will be used since packets will be going out of router.

- **Destination:** address of the network that the packet is headed to.
- **Gateway:** the gateway address
- **Genmask:** The netmask for the destination net.
- **Flags:** **U** (route is up) OR **G** (use gateway) OR **M** (modified from routing daemon) OR **C**(cache entry) OR **H**(target is a host)

- **Metric:** The 'distance' to the target (usually counted in hops). It is not used by recent kernels
- **Ref:** Number of references to this route. (Not used in the Linux kernel.)
- **Use:** Count of lookups for the route.
- **Iface:** Interface to which packets for this route will be sent.

Route add -net 192.168.0.0 netmask 255.255.255.0 dev eth0 : adds a route to the local network 192.56.0.x via "eth0".

Route del default : deletes the current default route, which is labeled "default" or 0.0.0.0 in the destination field.

Question 5

Netstat: This command is capable of producing information related to network connections, routing tables, interface statistics etc. netstat is multi-platform (available on windows also). It list the network connections that currently exist between your machine and other machines, as well as sockets 'listening' for connections from other machines.

Use of Netstat :

- It helps the network administrators to keep an eye on the invalid or suspicious network connections.
- It can show you which programs are active on your network right now.
- It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

Parameters to show all the TCP connections: **Netstat –at**

```
shubz@Dream:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:hostmon         0.0.0.0:*               LISTEN
tcp        0      0 localhost:5939          0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 Dream:53766             intranet.iitg.erne:http TIME_WAIT
tcp6       0      0 [::]:hostmon            [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

Explanation

- **Proto :** tell us if the socket listed is TCP or UDP.
- **Recv-Q/Send-Q :** The count of bytes not copied by the user program connected to this socket or we can say it tell us how much data is in the queue for that socket waiting to be read (Recv-Q) or sent (Send-Q).
- **Local Address :**IP and port of local computer.
- **Foreign Address :** Address (IP and port) of foreign device(other end of socket).(**0.0.0.0:* is indicating** is that the process listening on has requested the ability to receive connections from any IP address on any port.)
- **State :** Tell about the state of listed sockets.(example : "**LISTEN**" (wait for some external computer to contact us) and "**ESTABLISHED**" (ready for communication) or **TIME_WAIT** (when waiting to be closed)).

Netstat –r output: Display the kernel routing table. (show the same output as route command) Details of routing table explained in above question. There is a irtt field in output also representing initial round trip time to that IP.

Option to display network interface status : 'netstat –i' : In my case there are **two interface : lo (loopback interface),wlp2s0 (wifi card)**

```
shubz@Dream:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
lo       65536     2889      0      0 0          2889      0      0      0 LRU
wlp2s0    1500    35963      0      0 0         19074      0      0      0 BMRU
```

Loopback interface : The loopback device is a special interface that your computer uses to **communicate with itself**. It is used mainly for diagnostics and troubleshooting, and **to connect to servers running on the local machine**. For example, if you run a web server, you have all your web documents and could examine them file by file. The loopback interface **does not represent any actual hardware**, but exists so applications running on your computer can always connect to servers on the same machine.

Question 6

Hosts Chosen are :

1. Google.com 2.Facebook.com 3.Flipkart.com 4. Amazon.in 5. Amazon.com

Hop Counts:

Host	Case 1(evening)	Case 2(afternoon)	Case 3(morning)
Google.com	20	20(18 common with case 1)	12 (6 common with case 1)
Facebook.com	13	13(same as case 1)	13 (same as case 1)
Flipkart.com	13	13(same as case 1)	13 (same as case 1)
Amazon.in	29	29 (same as case 1)	29 (same as case 1)
Amazon.com	29	28(5 common with case 1)	28 (6 common with case 1)

Explanation for different hops to same host:

- Since packets are sent via the route with less traffic due to **presence of load balancers and use of packet switching**.
- So it is possible that at different times there are different paths which **leads to the destination in lowest time** hence resulting in different no. of hops and different intermediate ip's.
- Also there are **multiple server location** for same hosts leading to different routes.

Explanation for not finding complete paths to some hosts:

- Sometimes people **block ICMP/ping packets (due to firewall rules) for security** reasons like preventing hackers from getting information about open ports and staving off denial of service attacks. When ping is blocked, the server doesn't respond at all, resulting in "request timed out" messages that prevent traceroute from ever being able to map the path to the final destination.
- May also occur due to **interrupted Internet connection or timed out request.**

Is it possible to find the route to certain hosts which fail to respond with ping experiment:

- **YES.** Some hosts have disabled / blocked ICMP packets which are sent during ping commands. We can find the route to such hosts via traceroute by **sending TCP packets instead of default packets** to find the route.
- **'traceroute –T host-ip'** will find route to host-ip via sending TCP probes.

Question 7

Full ARP table for your machine : 'arp'

arp or address resolution protocol manipulates/display the kernel's IPv4 network neighbor cache. ARP comes into play when the sending computer on network wants to know the destination MAC address (of other computer on network). Sending host will send an ARP Request and the destination host will reply with a message ARP Reply containing it's mac address and hence an entry being added.

Explanation:

```
root@vaibhav-VirtualBox:/home/vaibhav# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.108            ether   fc:f8:ae:b7:65:33   C                     enp0s3
192.168.0.105            ether   ac:2b:6e:e8:0e:db   C                     enp0s3
192.168.0.1              ether   98:de:d0:de:0b:57   C                     enp0s3
```

- **Address:** IP address for which the entry is present.
- **HW Type:** Hardware type. Here it is Ethernet.
- **HW Address:** Mac Address to which IP is assigned.
- **Flags:** Each complete entry in ARP cache marked C flag. Permanent entries are marked with M and published entries have the P flag.
- **Iface:** Interface to which this address mapping has been assigned.

Adding and Deleting entries in ARP table:

```
shubz@Dream:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.105            ether   ac:2b:6e:e8:0e:db   C                     wlp2s0
192.168.0.1              ether   98:de:d0:de:0b:57   C                     wlp2s0
shubz@Dream:~$ sudo arp -s 192.168.0.115 98:de:d0:de:0b:57
shubz@Dream:~$ sudo arp -s 192.168.0.110 98:de:d0:de:0b:57
shubz@Dream:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.110            ether   98:de:d0:de:0b:57   CM                    wlp2s0
192.168.0.115            ether   98:de:d0:de:0b:57   CM                    wlp2s0
192.168.0.105            ether   ac:2b:6e:e8:0e:db   C                     wlp2s0
192.168.0.1              ether   98:de:d0:de:0b:57   C                     wlp2s0
shubz@Dream:~$ sudo arp -d 192.168.0.115
shubz@Dream:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.110            ether   98:de:d0:de:0b:57   CM                    wlp2s0
192.168.0.105            ether   ac:2b:6e:e8:0e:db   C                     wlp2s0
192.168.0.1              ether   98:de:d0:de:0b:57   C                     wlp2s0
shubz@Dream:~$
```

Adding : **'arp –s IP mac_address' :** bind particular ip with given mac_address. **Note that entries manually added have flag M**

Deleting : **'arp –d 192.168.0.105'** : deletes the IP from arp table

What will happen if two IP addresses map to the same Ethernet address:

- **CASE 1** : On adding a rule to IP 192.168.0.110 in arp table with same mac as that of my router(now router with ip 192.168.0.1 and 192.168.0.110 have same mac address. On pinging the new ip 192.168.0.110 the reply comes from 192.168.0.1 and 192.168.0.110 i.e both the ip which was binded to the mac address.
- **CASE 2 :** if two devices with same mac are connected to router than DHCP server will assign them only 1 IP. There may be "races" where each computer (say A,B) attempts to register itself with the router and it's mac address. Any traffic coming to the machine A can get lost since packet may go to machine B because it registered itself earlier and hence the device which was registered latest in routing table of router will be UP for receiving and transmitting packets.

How long do entries stay cached in ARP table :

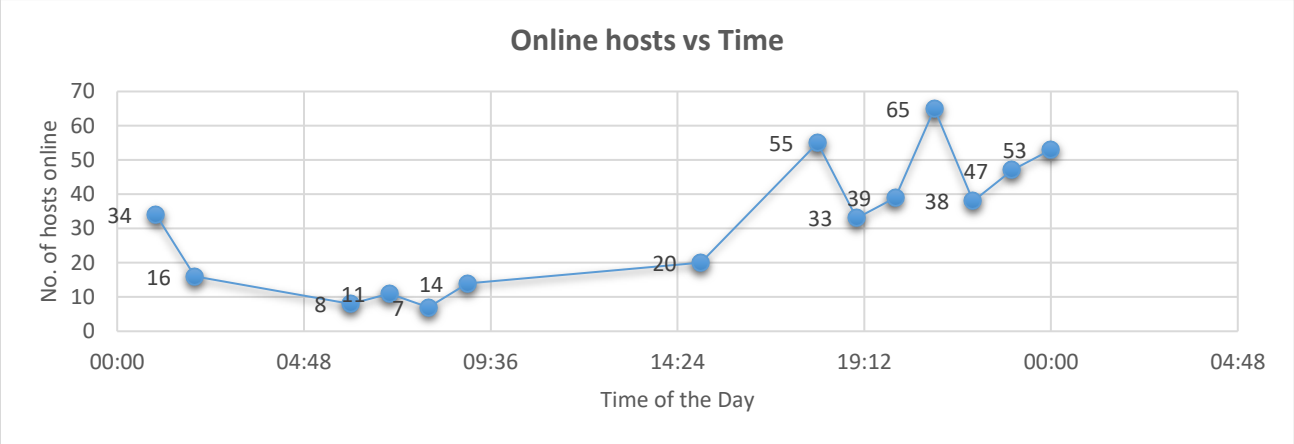
- 60 seconds is the time for which entries stay cached.
- **'Ip –s neighbor list' However Entries in arp table are not deleted from newer linux kernel**. There are subtle differences between an neighbor cache entry actually falling out of the cache entirely or just being marked as stale/invalid. When in the STALE state, if some ip is pinged it will send the packet to mac address corresponding to it right away. A second or so later it will usually send an ARP request to that ip and it's cache is updated back to a REACHABLE state. Similarly after some time REACHABLE will become STALE.

```
vaibhav@vaibhav-VirtualBox:~$ ip -s neighbor list
192.168.0.1 dev enp0s3 lladdr 98:de:d0:de:0b:57 used 189/184/140 probes 1 STALE
192.168.0.105 dev enp0s3 lladdr ac:2b:6e:e8:0e:db used 312/312/269 probes 4 STALE
192.168.0.108 dev enp0s3 lladdr fc:f8:ae:b7:65:33 used 311/311/268 probes 4 STALE
```

Question 8

LAN subnet address: 10.9.0.0/22 (B1 block of kameng hostel)

Explanation: Since last 10 bits of subnet mask is 0. It will contains ip in following range: (10.9.0.1…10.9.0.255), (10.9.1.1…10.9.1.255), (10.9.2.1…10.9.2.255), (10.9.2.1…10.9.2.255) covering the whole B1 block of Kameng Hostel.



Hourly Trends:

- Since students are at room at evening after 5PM, no of users are high around that time.
- There is a dip around 7pm-9pm since students have their SA course and most of them are fresher in B1 block where I have collected data. Dinner may also be the reason for less online hosts.
- After 9PM users are high indication most of people are at their rooms and decreases gradually after 12 in night.