

NAME : RITIK MANDLOI

ROLL NO : 180101066

CS342 NETWORKS LAB ASSIGNMENT 1

Q1)

a) ping -c [count] [IP Address/ Hostname]

count : no of echo requests,

Example : ping -c 10 www.google.com

b) ping -i [time_interval] [IP Address/ Hostname]

Time_interval : time interval between two successive ping ECHO_REQUESTS

Example: ping -i 2 www.google.com

c) ping -l [count] [IP Address/ Hostname]

count : no of ECHO_REQUEST packets

Example: ping -l 2 www.google.com

Limit for sending ECHO_REQUEST packets by normal users is 3.

d) ping -s [size] [IP Address/ Hostname]

size: size of the packet

Example: ping -s 32 www.google.com

If the payload size is set to 32 bytes, what will be the total packet size ?

Ans: Size of the packet = ICMP payload + ICMP header + header payload size.

The size of the header depends on whether the request is IPV4 or IPV6.

If we consider a general IPV4 32 bytes payload with 8 byte ICMP header and 20 bytes header, the total packet size becomes $32+8+20 = 60$ bytes.

Q2)

HOST	IP	LOCATION	First	Second	Third	Avg. rtt
www.google.com	172.217.174.228	US	59.924	111.000	111.605	94.176
www.amazon.co.uk	184.29.25.14	UK	60.621	124.534	91.149	92.101
en.wikipedia.org	103.102.166.224	Netherland	134.702	149.524	182.667	155.631
web.whatsapp.com	31.13.79.53	Ireland	55.366	108.901	94.336	86.201
www.twitter.com	104.244.42.193	US	197.849	153.368	141.109	164.108
www.australia.gov.au	13.227.234.6	Australia	60.510	124.466	119.152	101.376

a) There is positive correlation between RTT and geographic distance . As the distance increases hop count increases ,and the packet has to go through more routers. But this dependency is not that strong hence from only the above data relation between them cannot be inferred that correctly.

b) Yes, I experience packet loss for some domains

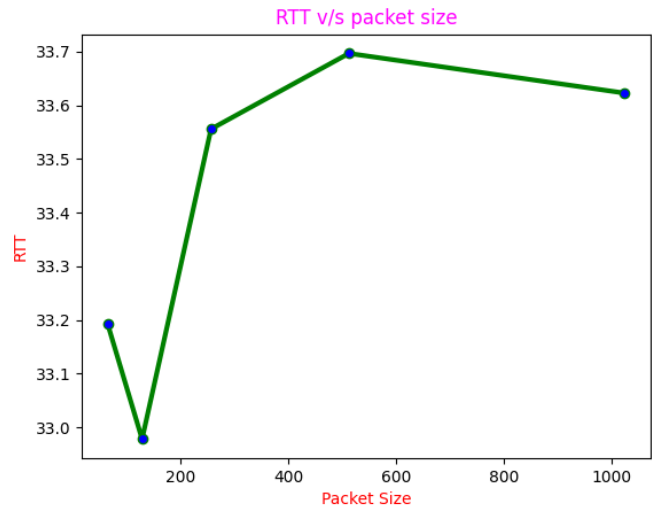
Possible reasons :

Network becomes congested with traffic and hits maximum capacity.

Faulty or outdated network hardware such as firewalls, network switches and routers can slow down network traffic. Also, increasing packet size above MTU gave 100% packet loss.(when I tried 2048 bytes)

c) Host : www.google.com

Packet Size (in Bytes)	Avg. RTT (in ms)
64	33.193
128	32.978
256	33.556
512	33.697
1024	33.623
2048	100% packet loss



d)

Time of Day: The number of active users of the host change according to different times of the day and this leads to change in network congestion. The more the network congestion the more the RTT.

Packet Size: Increasing the packet size or payload size lead to an increase in RTT

Q3)

IP address : (www.google.com)172.217.166.36

a) Both the commands had 0% packet loss rate.

b)

i) ping -n www.google.com

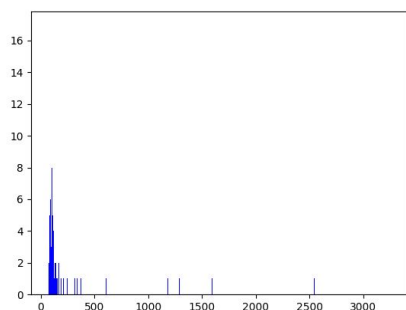
median: 90.4, mean: 135.829, max: 2940.0, min: 70.3, variance: 49610.844

ii) ping -p ff00 www.google.com

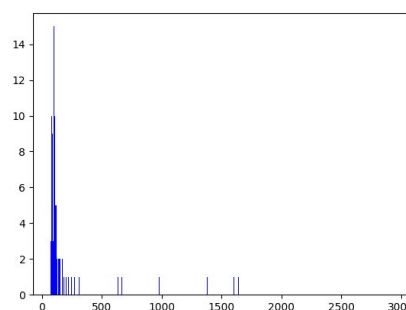
median: 91.7, mean: 146.884, max: 3267.0, min: 69.3, variance: 67484.018

c) i) : Normal distribution with $\mu = 135.829$ and $\sigma^2 = 49610.844$

ii): Normal distribution with $\mu = 146.884$ and $\sigma^2 = 67484.018$



i)



ii)

d)

ping -p ff00 actually attaches a hexadecimal string of ones and zeros at the end of packet and it helps to find the data dependent problems in the network whereas ping -n just simply ping the host without a reverse DNS lookup due to which

a) mean and median of i) is slightly less.

b) packet loss in ii) is slightly more.

Q4)

a)

ifconfig stands for interface configuration and it displays network settings of all network interfaces on the system

Output Explanation:

i) **Link encap** : Type of interface like eth0 for ethernet.

ii) **Internet address** : The IPv4 address assigned to the interface.

iii) **broadcast** : The broadcast address of the network associated with the interface.

iv) **mask** : Network mask associated with the interface

v) **MTU** : The maximum transmission unit for which the interface is configured

vi) **Flags** : UP: This flag indicates that the network interface is configured to be enabled.

BROADCAST: Indicates that the interface is configured to handle broadcast packets.

This is important for obtaining the IP address via DHCP server.

RUNNING: Indicates that the network interface is operational and is ready to accept the data.

MULTICAST: Indicates that the interface is configured to handle multicast packets.

vii) Output interfaces:-

1.enp3s0 (Ethernet) 2.lo (loopback interface)

Interface Stats: RX packets – received dropped picked override, TX packets – received dropped picked override

b)

i) ifconfig -a : To Display Information of All Network Interfaces

ii) sudo ifconfig [interface_name] up: activating a particular network interface.

iii) sudo ifconfig [interface_name] down: deactivating a particular network interface.

iv) sudo ifconfig [interface_name] mtu [mtu_value] : To Change MTU for an Network Interface

v) ifconfig [interface_name] : View the network settings on the interface specified.

c)

The route command is used to view and make changes to the kernel routing table.

Important output attributes of route command are:

Columns in the table :

Destination : The destination network or destination host.

Gateway : The gateway address or '*' if none set.

Genmask : The netmask for the destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.

Flags : Possible flags include

U (route is up), H (target is a host), G (use gateway), R (reinstate route for dynamic routing), D

(dynamically installed by daemon or redirect), M (modified from routing daemon or redirect), A (installed by addrconf), C (cache entry), ! (reject route)

Metric : The distance to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.

Ref : Number of references to this route. (Not used in the Linux kernel.)

Use : Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).

Iface : Interface to which packets for this route will be sent.

d)

```
mandloi@mandloi-VirtualBox: ~
File Edit View Search Terminal Help
mandloi@mandloi-VirtualBox:~$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
mandloi@mandloi-VirtualBox:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.0.2.2 0.0.0.0 UG 100 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
mandloi@mandloi-VirtualBox:~$ route -e
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default _gateway 0.0.0.0 UG 0 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 0 0 0 enp0s3
mandloi@mandloi-VirtualBox:~$ route -C
Kernel IP routing cache
Source Destination Gateway Flags Metric Ref Use Iface
mandloi@mandloi-VirtualBox:~$ route -v
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 enp0s3
10.0.2.0 0.0.0.0 255.255.255.0 U 100 0 0 enp0s3
link-local 0.0.0.0 255.255.0.0 U 1000 0 0 enp0s3
mandloi@mandloi-VirtualBox:~$
```

-n : Displays host and network names numerically, rather than symbolically, when reporting results of a flush or of any action in verbose mode.

-e : It used to display additional information.

-C: It is used to display routing cache instead of FIB(Forwarding Information Base).

-v : Specifies verbose mode and prints additional details

Q5)

a)The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in a table format, routing table information, and interface information.

b)

I was trying through virtual machine but the netstat command isn't working fine in it *

but it worked fine on windows command prompt, so please consider it

Command: netstat -t | FINDSTR "ESTABLISHED"

(findstr is similar to grep in Linux)

```
C:\Users\RITIK MANDLOI>netstat -t | FINDSTR "ESTABLISHED"
TCP 127.0.0.1:49670 LAPTOP-F3FN1956:49671 ESTABLISHED InHost
TCP 127.0.0.1:49671 LAPTOP-F3FN1956:49670 ESTABLISHED InHost
TCP 192.168.43.134:49960 52.108.44.4:https ESTABLISHED InHost
TCP 192.168.43.134:50244 13.107.21.200:https ESTABLISHED InHost
TCP 192.168.43.134:50245 13.107.21.200:https ESTABLISHED InHost
TCP 192.168.43.134:50247 13.107.246.10:https ESTABLISHED InHost
TCP 192.168.43.134:50248 13.107.6.254:https ESTABLISHED InHost
TCP 192.168.43.134:50249 204.79.197.254:https ESTABLISHED InHost
TCP 192.168.43.134:50250 204.79.197.222:https ESTABLISHED InHost
TCP 192.168.43.134:50256 whatsapp-cdn-shv-02-bom1:https ESTABLISHED InHost
TCP 192.168.43.134:50262 13.107.6.171:https ESTABLISHED InHost
TCP 192.168.43.134:50263 13.107.6.171:https ESTABLISHED InHost
TCP 192.168.43.134:50264 13.83.65.43:https ESTABLISHED InHost
TCP 192.168.43.134:50267 13.83.65.43:https ESTABLISHED InHost
TCP 192.168.43.134:50925 13.94.40.40:https ESTABLISHED InHost
TCP 192.168.43.134:50991 172.217.194.188:5228 ESTABLISHED InHost
TCP 192.168.43.134:59292 52.139.250.253:https ESTABLISHED InHost
TCP 192.168.43.134:59293 52.139.250.253:https ESTABLISHED InHost
TCP 192.168.43.134:61162 a23-210-76-11:https ESTABLISHED InHost
C:\Users\RITIK MANDLOI>
```

c)

It displays the kernel IP routing table.

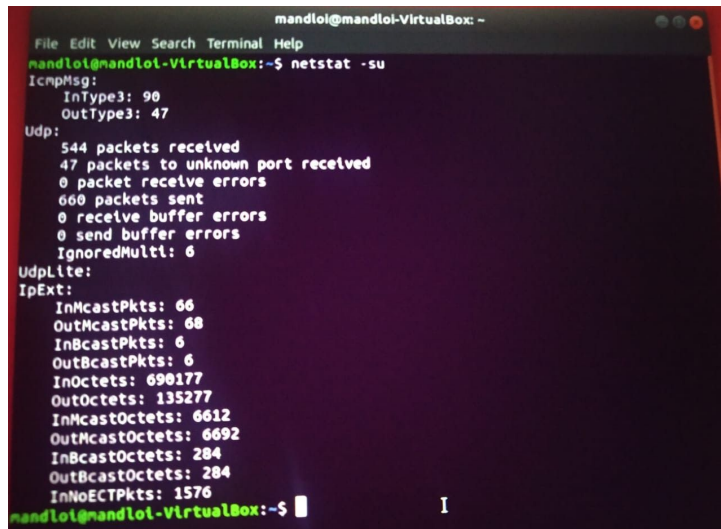
The columns are : 1)**Destination**: Identifies the destination network. 2)**Gateway**: Specifies the gateway to use for forwarding packets. 3)**Genmask**: Represents the subnet mask . 4)**Flags**: Indicates the current status of the route. The U flag indicates that the route is up. The G flag indicates that the route is to a

gateway. 5) **iface**: Indicates the particular interface on the local host that is the source endpoint of the transmission.

d) `netstat -i` :

The output is the network interface table which displayed inly two network interfaces(enp0s3, lo)

e) `netstat -su`



```
mandloi@mandloi-VirtualBox: ~  
File Edit View Search Terminal Help  
mandloi@mandloi-VirtualBox:~$ netstat -su  
IcmpMsg:  
  InType3: 90  
  OutType3: 47  
Udp:  
  544 packets received  
  47 packets to unknown port received  
  0 packet receive errors  
  660 packets sent  
  0 receive buffer errors  
  0 send buffer errors  
  IgnoredMulti: 6  
UdpLite:  
IpExt:  
  InMcastPkts: 66  
  OutMcastPkts: 68  
  InBcastPkts: 6  
  OutBcastPkts: 6  
  InOctets: 690177  
  OutOctets: 135277  
  InMcastOctets: 6612  
  OutMcastOctets: 6692  
  InBcastOctets: 284  
  OutBcastOctets: 284  
  InNoECTPkts: 1576  
mandloi@mandloi-VirtualBox:~$
```

f)

The interface lo is the loopback interface, also known as localhost.(127.0.0.1)

The loopback device is a special, virtual network 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.

Q6)

a) 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.

b)

Host	4 PM	7PM	9PM
www.google.com	8	8	8
www.amazon.co.uk	8	11	13
en.wikipedia.org	9	9	9
web.whatsapp.com	9	9	9
www.twitter.com	5	5	5
www.australia.gov.au	8	9	8

Yes, there exist common hops between two routes from the above hosts as all the packets initially pass through our default gateway within the home network.

Some of the common hops observed:

core1.fra.hetzner.com	213.239.229.77	de	5.035 ms
core4.fra.hetzner.com	213.239.229.73	de	12.003 ms
core0.fra.hetzner.com	213.239.252.41	de	8.241 ms

c) The reason is the fast switching technique which changes the routing table of the router accordingly when packets pass through to access the route faster through the cache. The route to the same host changes as the routing table changes.

d) Some of the reasons are: 1) Firewall blocking either ICMP or UDP packets. 2) If a router is busy routing packets and does not have the resources to send out ICMP packets. 3) Some devices do not decrement the TTL of packets passing through them, so they will not show up in traceroutes at all.

e) Yes.

The most significant difference between ping and traceroute is ping uses ICMP packets to get a response which can be generally blocked by the firewall because of which it fails but traceroute uses UDP packets (as in Linux) with a decrement of the TTL field which may not be blocked by the firewall hence it works.

Q7)

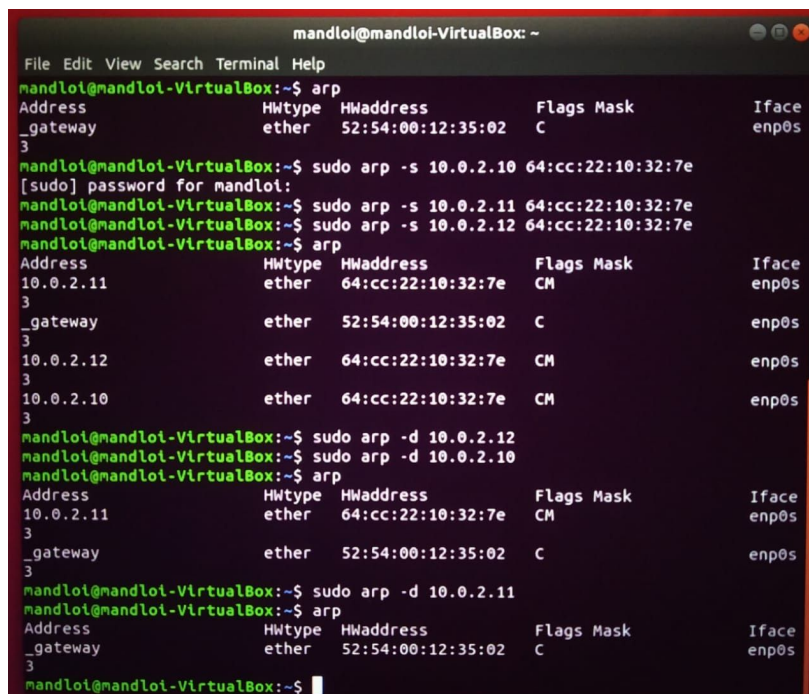
a) arp

Columns of the arp table:

i) **Internet address**: The IP address of the network. ii) **Physical address**: The MAC address of the hardware. iii) **HWType**: The type of hardware address. iv) **Interface**: Indicates the particular interface on the local host that is the source endpoint of the transmission.

b) `sudo arp -s [IP_ADDRESS] [MAC_ADDRESS]` is used to add the entry in the ARP table.

`sudo arp -d [IP_ADDRESS]` is used to delete the entry in the ARP table.



```
mandloi@mandloi-VirtualBox: ~  
File Edit View Search Terminal Help  
mandloi@mandloi-VirtualBox:~$ arp  
Address      HWtype  HWaddress    Flags Mask    Iface  
_gateway     ether   52:54:00:12:35:02  C             enp0s  
3  
mandloi@mandloi-VirtualBox:~$ sudo arp -s 10.0.2.10 64:cc:22:10:32:7e  
[sudo] password for mandloi:  
mandloi@mandloi-VirtualBox:~$ sudo arp -s 10.0.2.11 64:cc:22:10:32:7e  
mandloi@mandloi-VirtualBox:~$ sudo arp -s 10.0.2.12 64:cc:22:10:32:7e  
mandloi@mandloi-VirtualBox:~$ arp  
Address      HWtype  HWaddress    Flags Mask    Iface  
10.0.2.11     ether   64:cc:22:10:32:7e  CM             enp0s  
3  
_gateway     ether   52:54:00:12:35:02  C             enp0s  
3  
10.0.2.12     ether   64:cc:22:10:32:7e  CM             enp0s  
3  
10.0.2.10     ether   64:cc:22:10:32:7e  CM             enp0s  
3  
mandloi@mandloi-VirtualBox:~$ sudo arp -d 10.0.2.12  
mandloi@mandloi-VirtualBox:~$ sudo arp -d 10.0.2.10  
mandloi@mandloi-VirtualBox:~$ arp  
Address      HWtype  HWaddress    Flags Mask    Iface  
10.0.2.11     ether   64:cc:22:10:32:7e  CM             enp0s  
3  
_gateway     ether   52:54:00:12:35:02  C             enp0s  
3  
mandloi@mandloi-VirtualBox:~$ sudo arp -d 10.0.2.11  
mandloi@mandloi-VirtualBox:~$ arp  
Address      HWtype  HWaddress    Flags Mask    Iface  
_gateway     ether   52:54:00:12:35:02  C             enp0s  
3  
mandloi@mandloi-VirtualBox:~$
```

c) ARP only works between devices in the same IP subnet.

When a device with IP address A needs to send a packet to a device with IP address B, the first thing it does is consulting its routing table to determine if IP address B belongs to a subnet it can directly reach through its network interface(s) and if it does, then device A uses ARP to map IP address B to a physical Ethernet address. But if the two IP addresses are on different subnets it will look in its routing table for a route to the destination network, and then it will send its packet to the appropriate router.

d) If we ping the IP after forcefully replacing their ARP entry, it leads to 100% packet loss. When you ping an IP address the layer 3 header is built first and passed to layer 2. At layer 2 the PC checks the corresponding ARP table and MAC address. The device sends an ARP request to the destination MAC address and if the reply ARP packet does not have the particular IP then the requesting device does not get a reply.

Q8)

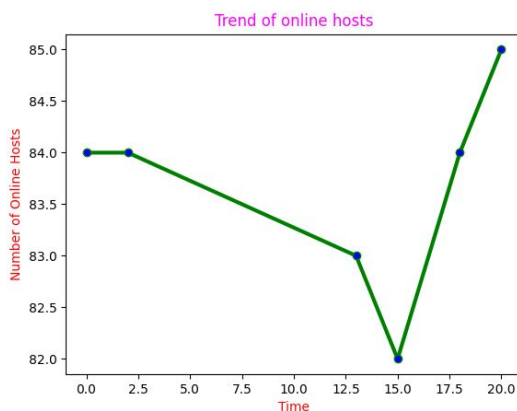
a)

IP address of the PC : 172.16.114.160/25

Command: nmap -sn 172.16.114.160/25

b) sudo nmap -sA 172.16.114.160

c)



```
ritik@ritik-Precision-Tower-3620: ~  
File Edit View Search Terminal Help  
Nmap scan report for 172.16.114.233  
Host is up (0.00065s latency).  
Nmap scan report for 172.16.114.235  
Host is up (0.00041s latency).  
Nmap scan report for 172.16.114.240  
Host is up (0.00034s latency).  
Nmap scan report for 172.16.114.243  
Host is up (0.00032s latency).  
Nmap scan report for 172.16.114.245  
Host is up (0.00052s latency).  
Nmap scan report for 172.16.114.246  
Host is up (0.0046s latency).  
Nmap scan report for 172.16.114.248  
Host is up (0.00068s latency).  
Nmap scan report for 172.16.114.249  
Host is up (0.00050s latency).  
Nmap done: 128 IP addresses (83 hosts up) scanned in 118.33 seconds  
ritik@ritik-Precision-Tower-3620:~$
```

The above graph represents the hourly trends of ON/OFF in computers.

From the graph. It is clearly evident that more hosts are online in the evening-night period than the day period.