

# CS 342

NAME : NAMAN ANAND

BRANCH : CSE

ROLL NO : 200101070

ASSIGNMENT : 1

## NETWORK DIAGNOSTIC COMMANDS

Q1.

a)

Ans If N is no of echo requests, then : **ping -c N IP\_address**

b)

Ans **ping -i <INTERVAL> IP\_address**

c)

Ans **ping -l preload IP\_address**

Normal user ping maximum Echo request packets = 3

d)

Ans **ping -s packet\_size IP\_address**

Also if Packet\_size is 32 bytes total size of packet would be 40 bytes Due to 8 bytes of ICMP Header Data

Q2.

Ans

HOST	AVG RTT 1	AVG RTT 2	AVG RTT 3	OVERALL AVG RTT	PACKET LOSS %
takeuforward.org	157.211	153.886	277.755	196.284	0%
www.air.ircrc.co.in	NO RTT	NO RTT	NO RTT	NO RTT	100%
moz.com	126.399	106.670	165.597	132.889	0%
outlook.com	408.687	399.833	575.065	461.195	0%

<b>www.geeksforgeeks.org</b>	124.536	135.897	191.268	150.567	0%
<b>getbootstrap.com</b>	163.534	164.542	163.807	163.961	0%

Reason for packet loss greater than 0%:

- Congestion :When network become congested and hits maximum capacity, the packets will be discarded or ignored so that the network can catch up.
- Software Bugs : If rigorous testing has not been carried out or bugs have been introduced following software updates, this could result in unintended or unexpected network behaviour.
- Security threat : Packet loss can also be caused by a security breach. During an attack, a malicious user takes control of a router and sends commands that drop packets into a stream of data
- One of the reasons for 100% packet loss is restriction on host IP Address.

RTT's (Round trip time) depends on geographical distance of host. But it is weakly connected not strongly. As there are other factors such as network traffic etc , so this led to inconsistencies . RTT should increase with geographical distance as no of hops will also increase but since weakly connected so not much impact seen.

IMPACT OF PACKET SIZE :

I sent various size packets to takeuforward.org

500 , 1000 ,1500 , 2000 size packets I sent

PACKET SIZE	RTT AVG
500	128.905
1000	138.230
1500	154.472
2000	161.749



There is a increase in RTT with packet size but not much significant. It depends on the traffic and congestion and network speed also.

Q3.

**Since On Intranet we can't use ping command . So I used on my mobile data . The results are based on ping google.com**

a)

Ans 0.3% Packet Loss for ping -c 1000 -n 8.8.8.8

0.2% Packet Loss for ping -c 1000 -p ff00 8.8.8.8

b)

Ans

for ping -c 1000 -n 8.8.8.8 :

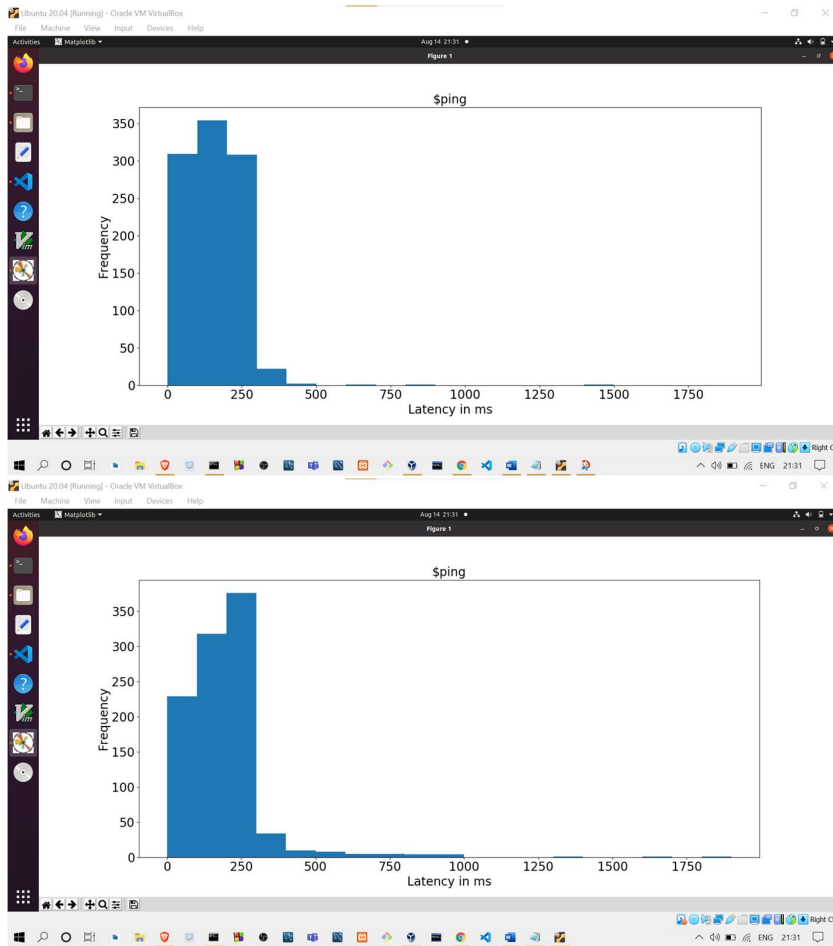
rtt min/avg/max/mdev = 71.618/200.887/1929.969/149.542 ms,

for ping -c 1000 -p ff00 8.8.8.8 :

rtt min/avg/max/mdev = 68.680/165.292/1410.988/83.382 ms

c)

Ans DISTRIBUTION OF PING LATENCY :



d)

Ans -n: It is used for Numeric Output only. No attempt will be made to lookup symbolic names for host addresses.

-p : Useful for diagnosing data-dependent problems in a network.

Q4.

Ans a)

Ans enp0s3 : en -> ethernet , p0 -> bus number of ethernet card , s3 -> slot number

RUNNING IFCONFIG WE CAN GET FOLLOWING DATA

1) Network interface: software interface to network hardware

2) IP ADDRESS , MTU , BROADCAST ETC

b)

Ans

OPTIONS THAT CAN BE PROVIDED WITH IFCONFIG COMMAND :

- 1) **-a** : Display all the interfaces available
- 2) **-v** : Run in verbose mode – log more details about execution
- 3) **-help** : Display help related to ifconfig
- 4) **-s** : Display a short list, instead of details instead of whole data

c)

Ans Route command is used for showing / update the IP/kernel Routing tables .

Output : It shows how our system is configured . If a packet come to our system and has a destination(mentioned in the routing table) in the range then it is forwarded to a corresponding gateway .In this case our system doesn't route the packets . If the destination is not in IP address range, then it is forwarded to default gateway.

Routing table has following outputs :

- 1) **DESTINATION** : IP ADDRESS OF PACKET FINAL DESTINATION
- 2) **GATEWAY** : A ROUTER THROUGH WHICH PACKETS PASS WHEN SENT TO DESTINATION
- 3) **GENMASK** : NETMASK FOR DESINATION ROUTE
- 4) **METRIC** : Assigns a cost to each available router so that most eff path can be chosen
- 5) **REF** : Number of references to the route

d)

Ans

- **-n** : display routing table in full numeric form
- **-C** : show kernel routing cache info
- **-e** : (--extend )display other/more information
- **-v** : display more verbose info

```

naman@naman-VirtualBox:~/network$ 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
192.168.122.0      0.0.0.0        255.255.255.0   U      0      0      0   virbr0

naman@naman-VirtualBox:~/network$ route -v
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
link-local         0.0.0.0        255.255.0.0     U      1000   0      0   enp0s3
192.168.122.0      0.0.0.0        255.255.255.0   U      0      0      0   virbr0

naman@naman-VirtualBox:~/network$ route -e
Kernel IP routing table
Destination        Gateway         Genmask         Flags MSS Window  irtt Iface
0.0.0.0            10.0.2.2       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
192.168.122.0      0.0.0.0        255.255.255.0   U      0      0      0   virbr0

naman@naman-VirtualBox:~/network$ route -C
Kernel IP routing cache
Source             Destination      Gateway         Flags Metric Ref    Use Iface

```

Q5.a)

Ans **NETSTAT** : It tells various network related info like network connections ,statics etc , We can configure, trouble shoot and also monitor networks connections.

b)

```

naman@naman-VirtualBox:~$ netstat -at | grep ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED
tcp        0      0 0.0.0.0:80->0.0.0.0:80  ESTABLISHED
tcp        0      0 0.0.0.0:443->0.0.0.0:443  ESTABLISHED

```

Ans

There is no direct command to get all the established TCP connections . As we know we can get all the TCP command using **netstat -at** and now we can use **netstat -at | grep ESTABLISHED** . It will give all the TCP port connections that are established

c)

Ans We can get all the kernel routing information using netstat –r command .

- **DESTINATION** : IP ADDRESS OF PACKET FINAL DESTINATION

- GATEWAY : A ROUTER THROUGH WHICH PACKETS PASS WHEN SENT TO DESTINATION
- GENMASK : NETMASK FOR DESINATION ROUTE
- FLAGS : CONTAIN VARIOUS FLAGS ( G : USE GATEWAY, U : ROUTE IS UP , H : TARGET IS HOST ETC)
- MSS : CONTAINS THE MAXIMUM SIZE SEGMENT OF TCP OF ROUTE
- WINDOW : DEFAULT WINDOW SIZE OVER THIS ROUTE
- IRTT : (Initial round trip Time) THE KERNEL USES THIS TO GUESS ABOUT THE BEST TCP PROTOCOL PARAMETERS WITHOUT WAITING ON ANSWERS
- IFACE : INTERFACE TO WHICH PACKETS WILL BE SENT FOR THIS ROUTE

d)

Ans **netstat -i** can be used to display network interface status

**netstat -i | wc -l** -> will give us 2 more than the total no of interfaces available .For me it gave 5 means I have three interfaces on my computer

e)

Ans **netstat -au**

```

naman@naman-VirtualBox:~$ netstat -i | wc -l
5
naman@naman-VirtualBox:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:mdns            0.0.0.0:*               *
udp        0      0 0.0.0.0:34731          0.0.0.0:*               *
udp        0      0 naman-VirtualBox:domain 0.0.0.0:*               *
udp        0      0 localhost:domain        0.0.0.0:*               *
udp        0      0 0.0.0.0:bootps         0.0.0.0:*               *
udp        0      0 naman-VirtualBox:bootpc  gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:631            0.0.0.0:*               *
udp        0      0 0.0.0.0:47957          0.0.0.0:*               *
udp6       0      0 :::mdns                 ::::*                   *
udp6       0      0 :::50440                ::::*                   *

```

f)

Ans The loopback interface is used to identify the device . It can be used to check the device is online . It is the best way to identify a device in a network as the loopback address never changes. It allow device to communicate with itself using virtual interface.

Q6.

HOST	HOP COUNT 1	HOP COUNT 2	HOP COUNT 3
takeuforward.org	8	8	8
www.air.ircrc.co.in	30	30	30
moz.com	18	14	21
outlook.com	20	23	23
www.geeksforgeeks.org	10	11	10
getbootstrap.com	8	10	17

a)

Ans Traceroute : It is used to show the route of packet from sender to destination . It is used as a diagnostic tool as it shows how data moves through the internet. It is used to figure out the routing hops through which data passes as well as it can used to see if there is a delay at a particular node. We can find the point of failure also using Traceroute. REQUEST TIMED OUT at any hop means maybe there is a problem.

b)

Ans Traceroute path can vary at different times of a day. This is because at different times of a day different traffic situation is there so routing algorithms works differently. Also it may be possible due to any router not functioning in some requests while functioning in others.

c)

Ans. Yes , it can be possible Traceroute for [www.air.ircrc.co.in](http://www.air.ircrc.co.in) was not able to find complete route and it exceeds max hops allowed that is 30 by default. It maybe because of restriction on site or firewall blocking or maybe due to any other reason.

d)

Ans. Yes, it is possible It is because traceroute uses UDP packets with an incrementing TTL (time to live) to the final destination whereas Ping uses ICMP . Many networks don't allow ICMP packets SO ping gets blocked whereas Traceroute can easily find the route to the host.

Q7.

a)

Ans **arp -e** command is used to show full ARP table for the machine.

- Address : IP Address of corresponding device
- HWtype : Hardware type
- HWaddress : Hardware Address
- Flags Mask : Indicates MAC address is manually set or is incomplete
- Iface : Network Interface

b)

Ans

- To add : **arp -s IPAddress MACAddress**
- To delete : **arp -d IPAddress**

c)

Ans

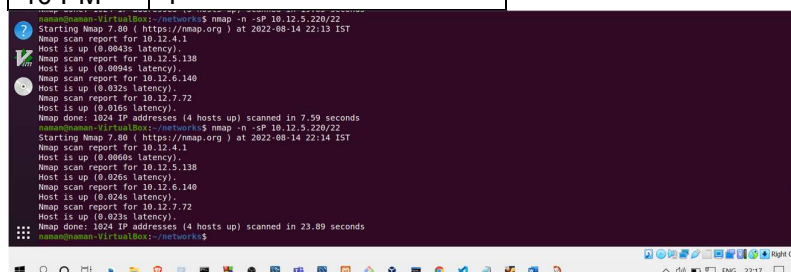
d)

Ans Because of diff MAC ADDRESS in ARP TABLE, no reply packet is received from target IP .Therefore Ping timeout occurs due to loss of packets.

Q8.

Ans Command used : **nmap -n -sP 10.12.5.220/22** for this experiment and got the following data Done on Brahmaputra Hostel

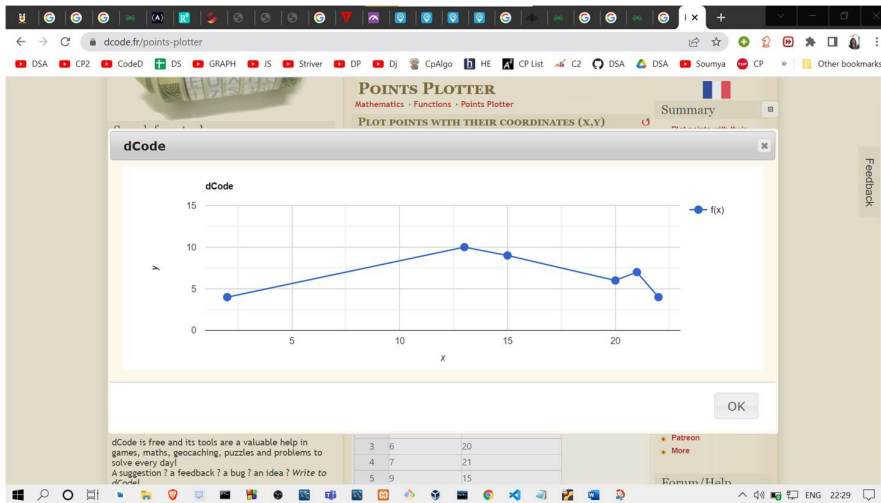
TIME	NO OF HOSTS UP
1 PM	10
3 PM	9
2 AM	4
8 PM	6
9 PM	7
10 PM	4



```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-14 22:13 IST
Nmap scan report for 10.12.4.1
Host is up (0.0043s latency).
Nmap scan report for 10.12.5.138
Host is up (0.0094s latency).
Nmap scan report for 10.12.6.140
Host is up (0.032s latency).
Nmap scan report for 10.12.7.72
Host is up (0.015s latency).
Nmap done: 1024 IP addresses (4 hosts up) scanned in 7.59 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-14 22:14 IST
Nmap scan report for 10.12.4.1
Host is up (0.0049s latency).
Nmap scan report for 10.12.5.138
Host is up (0.020s latency).
Nmap scan report for 10.12.6.140
Host is up (0.024s latency).
Nmap scan report for 10.12.7.72
Host is up (0.023s latency).
Nmap done: 1024 IP addresses (4 hosts up) scanned in 23.89 seconds
```

I was also not sure why it decreased during night at 8-10 PM maybe due to holiday.



HERE Y AXIS SHOW NO OF USERS

HERE X AXIS SHOW TIME IN HRS(24 HR FORMAT)

Q9.

Ans a) nslookup domain\_name

b) nslookup ip\_address

c) nslookup type=mx domain\_name

```

naman@naman-VirtualBox: ~/networks$ nslookup google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.238
Name:   google.com
Address: 2404:6800:4009:81f::200e

naman@naman-VirtualBox: ~/networks$ nslookup 142.250.182.238
238.182.250.142.in-addr.arpa    name = bom07s29-in-f14.1e100.net.

Authoritative answers can be found from:

naman@naman-VirtualBox: ~/networks$ nslookup -type=mx google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.com    mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:

naman@naman-VirtualBox: ~/networks$

```