

# 1

## 1.1 What is the option required to specify the number of echo requests to send with ping command?

To make the ping command automatically to send a certain number of packets, we can use COUNT (*-c*) option of the ping command.

Command :-

```
ping -c [number of packets] [hostname-IP]
```

## 1.2 What is the option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO\_REQUESTs?

We can use the INTERVAL (*-i*) option of the ping command to set the wait interval seconds between sending each packet. The default is to wait for one second between each packet normally, or not to wait in flood mode.

Command :-

```
ping -i [time interval (in seconds) ] [hostname-IP]
```

## 1.3 What is the command to send ECHO\_REQUEST packets to the destination one after another without waiting for a reply? What is the limit for sending such ECHO\_REQUEST packets by normal users (not superuser)?

PRELOAD (*-l*) option of the ping command is used to send packets without waiting for reply.

Command :-

```
ping -l [number of packets to send without waiting for a reply] [hostname-IP]
```

Command to use preload in superuser mode :-

```
sudo ping -l [number of packets to send without waiting for a reply] [hostname-IP]
```

The limit on the number of such packets sent by a normal user (without superuser permissions) is 3 i.e. without superuser permissions one can not send more than 3 such packets.

## 1.4 What is the command to set the ECHO\_REQUEST payload/data size (in bytes)? If the payload size is set to 32 bytes, what will be the total packet size?

PACKETSIZE (*-s*) option of the ping command is used to set the data size of the packet. The default packet size is 56 (84) bytes.

Command :-

```
ping -s [number of data bytes to send] [hostname-IP]
```

If a packet with payload size of 32 bytes is sent the total packet size is 40 bytes when the ICMP header is considered, and 60 bytes including IPv4 header.

## 2

### 2.1 List out the average RTT for each host in tabular form, and explain whether RTT has a correlation with the geographical distance of the destinations from source.

Host	RTT			Avg. RTT
	@10:00 PM	@1:00 AM	@11:00 AM	
cloudflare.com	38.912	27.506	27.717	31.378
flipkart.com	47.314	44.256	42.754	44.775
google.com	58.846	48.26	44.207	50.438
google.co.in	27.82	45.358	27.968	33.715
mega.nz	156.464	154.888	157.062	156.138
in.yahoo.com	227.212	278.619	238.129	247.987

There is a very weak relation that can be observed in our experiment. The relation is there because as the distance increases propagation delay is increased also the packets have to go through more number of nodes and at each nodes there may be a delay i.e processing delay.

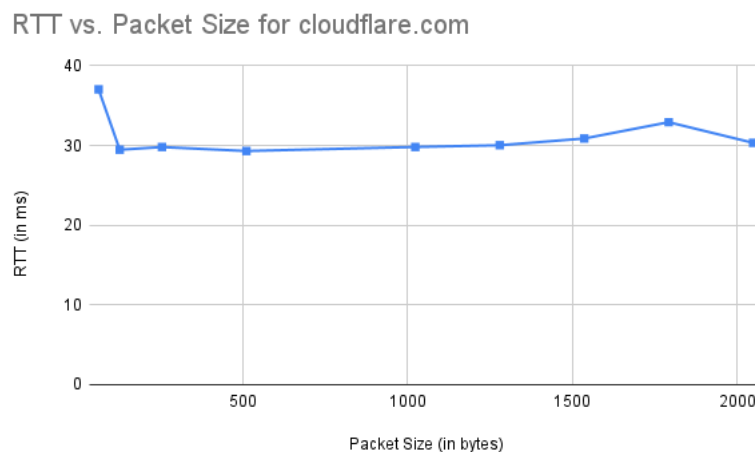
### 2.2 Check if in any case, packet loss is greater than 0% and provide reason for the same.

In my experiment there is 0% packet loss in case of all of the hosts.

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination.

Reason behind packet loss are errors in data transmission, collision between packets, or network congestion.

### 2.3 Pick one of the above used hosts, and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot average RTT vs packet size.



### 2.4 Explain how change in packet size, and time of the day impact RTT.

When packet size is increased the RTT also increases because of increase in transmission delay. It is the amount of time required to push (transmit) all of the packet's bits into the link.

We see change in RTT with respect to the time of day because at different time there is different amount of traffic on the network. Queuing delay increases when the traffic is heavy, as many other packets are also waiting to be transmitted onto the link.

### 3

#### 3.1 What was the packet loss rate for each command?

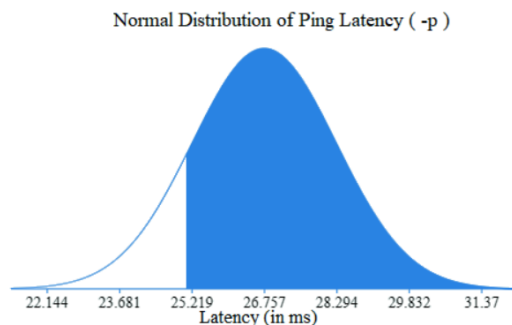
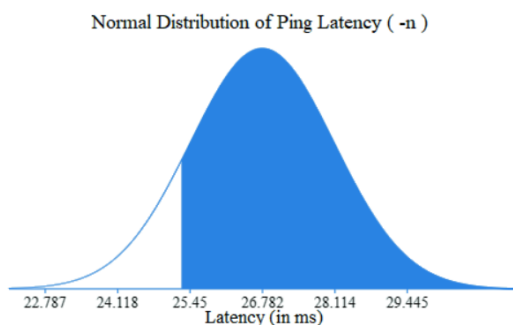
Packet loss while executing the ping command for 1.1.1.1 with the option  $-n$  was 0% and for  $-p$  it was 0.1%

#### 3.2 What was the minimum, maximum, mean, and median latency of the pings that succeeded? Ignore pings that failed in the calculation.

$-n$	
Min.	25.269
Max.	42.330
Mean	26.782
Median	26.7

$-p$	
Min.	25.067
Max.	47.913
Mean	26.757
Median	26.6

#### 3.3 Give plot to show the normal distribution of the ping latency.



#### 3.4 The two experiments are almost similar except in few aspects. Describe the significant network behavior difference (if any) you observed between the two experiments.

The two commands are different in the following aspect:-

1. While using the  $-p$  `ff00` command we are specifying the packet to be filled by `ff00` i.e. 8 1s and then 8 0s ( 1111111100000000 ) in binary. This specific data might have caused problem while padding because of which we can observe higher packet loss rate.
2. In case of  $-n$  option we are not trying to get symbolic names for host address hence mean latency in this case is slightly lower.

### 4

#### 4.1 Run `ifconfig` command and briefly describe its output (important attributes).

```
shrey@shrey:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::87af:e9a2:fc10:347c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:16:aa:00 txqueuelen 1000 (Ethernet)
    RX packets 9024 bytes 7204737 (7.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5699 bytes 626715 (626.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 783 bytes 77595 (77.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 783 bytes 77595 (77.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

*enp0s3* - Interface name. In the first part **en** stands for ethernet, **wl** is for wireless lan, **lo** for loopback device. The remaining part describes physical location of device in the PC. **p0** is for PCI bus and **s0** stands for slot number.

*inet* - IP address of the machine, *netmask* - IPv4 netmask of particular interface, *ether* - MAC address, *RX* - This Section indicates details such as number, total size of the **Received Packets**, *TX* - This section contains information about the **Transmitted Packets**.

#### 4.2 What are the different uses of ifconfig command? Mention and explain at least four functions.

ifconfig(interface configuration) command is used to configure the kernel-resident network interfaces.

1. **View configuration of all interfaces:** With the *-a* option of this command we view list of all the network devices even if they are turned off.
2. **For debugging a network interface:** We can get the information about different interfaces in detail which can be used to figure out the problem.
3. **Enabling/Disabling interface:** We can use to keep only necessary network interfaces turned on and turn off the remaining ones.
4. **Configuring an interface:** This command can be used to assign the IP address and netmask to an interface.

#### 4.3 Mention and explain at least four options of the ifconfig command. Execute the ifconfig command with these four options and explain the output.

1. *up*  
This flag causes the interface to be activated.
2. *down*  
This flag causes the driver for this interface to be shut down.
3. *-a*  
Displays all interfaces which are currently available, even if they're down.
4. *-s*  
It displays details of the network interfaces in a short list with details in tabular form.

## 5

### 5.1 What is the command netstat used for?

netstat ( **network statistics** ) is used for displaying network related information such as network connections, routing tables, interface statistics etc.

### 5.2 What parameters for netstat should you use to show the established TCP connections?

```
netstat -at j grep -n "ESTABLISHED"
```

```

shrey@shrey:~$ netstat -at | grep -n "ESTABLISHED"
13:tcp      0      0 shrey:54812      117.18.237.29:http      ESTABLISHED
15:tcp      0      0 shrey:33966      ec2-34-216-180-35:https  ESTABLISHED
16:tcp      0      0 shrey:33456      ec2-54-149-149-16:https  ESTABLISHED
17:tcp      0      0 shrey:51748      server-13-227-191:https  ESTABLISHED
18:tcp      0      0 shrey:44112      ec2-54-184-190-18:https  ESTABLISHED
19:tcp      0      0 shrey:50376      maa05s25-in-f3.1e1:http  ESTABLISHED
21:tcp      0      0 shrey:41778      36.75.98.34.bc.g:https  ESTABLISHED
22:tcp      0      0 shrey:57438      a23-46-187-9.deplo:http  ESTABLISHED
24:tcp      0      0 shrey:58664      ec2-54-213-37-69.:https  ESTABLISHED
25:tcp      0      0 shrey:59834      82.221.107.34.bc.g:http  ESTABLISHED
26:tcp      0      0 shrey:40832      server-13-227-191:https  ESTABLISHED
28:tcp      0      0 shrey:54822      117.18.237.29:http      ESTABLISHED
29:tcp      0      0 shrey:59836      82.221.107.34.bc.g:http  ESTABLISHED
30:tcp      0      0 shrey:44100      ec2-54-184-190-18:https  ESTABLISHED
31:tcp      0      0 shrey:54826      117.18.237.29:http      ESTABLISHED
32:tcp      0      0 shrey:51754      server-13-227-191:https  ESTABLISHED
34:tcp      0      0 shrey:55298      140.227.186.35.bc:https  ESTABLISHED
35:tcp      0      0 shrey:57436      a23-46-187-9.deplo:http  ESTABLISHED
36:tcp      0      0 shrey:44094      ec2-54-184-190-18:https  ESTABLISHED
37:tcp      0      0 shrey:54844      117.18.237.29:http      ESTABLISHED
39:tcp      0      0 shrey:54412      239.237.117.34.bc:https  ESTABLISHED
40:tcp      0      0 shrey:43818      ec2-54-200-38-59.:https  ESTABLISHED
41:tcp      0      0 shrey:54818      117.18.237.29:http      ESTABLISHED
42:tcp      0      0 shrey:53712      201.181.244.35.bc:https  ESTABLISHED
43:tcp      0      0 shrey:48494      102.115.120.34.bc:https  ESTABLISHED
44:tcp      0      0 shrey:44098      ec2-54-184-190-18:https  ESTABLISHED
45:tcp      0      0 shrey:54816      117.18.237.29:http      ESTABLISHED
47:tcp      0      0 shrey:51350      76.237.120.34.bc.:https  ESTABLISHED
49:tcp      0      0 shrey:56816      221.5.120.34.bc.g:https  ESTABLISHED
50:tcp      0      0 shrey:39298      server-13-227-214:https  ESTABLISHED
shrey@shrey:~$

```

### 5.3 What does “netstat -r” show? Explain all the fields of the output.

netstat -r shows the kernel routing information in a tabular form with the following columns:-

1. Destination: IP address of the destination network.
2. Gateway: IP address of the gateway router ( \* is displayed when none is set )
3. Genmask: The netmask for the destination net. For a host destination 255.255.255.255 and for the default route it shows 0.0.0.0.
4. Flags: Different flag related to a route. For example U : route is up, D : dynamically installed by daemon or redirect, G : use gateway.
5. MSS: Default maximum segment size for TCP connections over this route.
6. irtt: Initial round trip time.
7. Iface: Interface to which the packets for this route will be sent.

### 5.4 What option of netstat can be used to display the status of all network interfaces? By using netstat, figure out the number of interfaces on your computer.

The option `-ai` is a combination of two options `-a` : all and `-i` : interface thus it displays status of all network interfaces.

This command lists the interfaces in tabular form in the same way as `$ ifconfig -s`. The following command subtracts 2 from the line count of the output of the command `netstat -ai`. Hence, it returns the number of interfaces:

```
echo $[(netstat -ai | wc -l)-2]
```

### 5.5 What option of netstat can be used to show the statistics of all UDP connections?

We can use `-a` ( All ), `-s` ( Statistics ) and `-u` ( UDP ) option combined together for showing statistics of all the UDP connections

```
netstat -asu
```

```
shrey@shrey:~$ netstat -asu
IcmpMsg:
  InType0: 2860
  InType3: 180
  InType11: 30
  OutType3: 40
  OutType8: 5720
Udp:
  1659 packets received
  40 packets to unknown port received
  0 packet receive errors
  1710 packets sent
  0 receive buffer errors
  0 send buffer errors
  IgnoredMulti: 4
UdpLite:
IpExt:
  InMcastPkts: 60
  OutMcastPkts: 62
  InBcastPkts: 4
  OutBcastPkts: 4
  InOctets: 7037148
  OutOctets: 613886
  InMcastOctets: 6032
  OutMcastOctets: 6112
  InBcastOctets: 310
  OutBcastOctets: 310
  InNoECTPkts: 9819
```

## 5.6 Show and explain the function of loop-back interface.

A loopback interface is a virtual interface that is used by machine to communicate with itself. It is first interface that get activated during start up . This interface is used for network diagnosis and debugging. When a network interface in a machine is not established, the interface is unable to communicate with the servers in the same machine as well this problem is solved by loopback interface.

# 6

## 6.1 What is the use of traceroute tool?

- Traceroute tracks the route packets taken from an IP network on their way to a given host.
- It also returns the time taken during each hop the packet makes during its route to the destination. It uses TTL to elicit an timed out response from each gateway along the path.

## 6.2 List out the hop counts for each host in each time slot. Determine the common hops between two routes if they exist.

Host	Hops		
	@9:00 PM	@11:00 PM	@7:00 PM
cloudflare.com	6	6	6
flipkart.com	9	9	10
google.com	11	11	11
google.co.in	11	8	11
mega.nz	10	10	10
in.yahoo.com	10	10	11

## 6.3 Check and explain the reason, if route to same host changes at different times of the day.

In my experiment the route and the number hops changes at different times of the day because of load balancing that is done to reduce the the latency. The packets are redirected such that they take the route with

less traffic.

#### 6.4 Inspect the cases when traceroute does not find complete paths to some hosts, and explain the reasons.

I tried to traceroute amazon.com at 11:00PM and after 13 hops it started returning request timed out for almost all the remaining hops.

The reason behind this might be some servers not being configured to respond to ICMP Traffic by using firewall. These servers still forward the data to next hop as there are results following them. Some servers are even configured to disable ICMP traffic when they run under heavy load.

#### 6.5 Is it possible to find the route to certain hosts which fail to respond with ping experiment? Give reasoning.

It is possible to

find the route to certain hosts which fail to respond with ping experiment. Both ping and traceroute use the ICMP Packets but their working is different. Each IP packet sent on the Internet has a field known as Time-To-Live (TTL). But this field is not explicitly related to the time measured by the number of hops. It is instead, the maximum number of hops that a packet can travel across the Internet before it gets discarded. Ping is straight ICMP from point A to point B and has a default TTL value between 1 to 255 which decrements by 1 at every router between the source to destination and expects a ICMP Reply Packet from the host. Most probably the server is blocking the reply. On the other hand, In a traceroute, the source re-defines the TTL value every time it gets a response and sends the packet with  $TTL = TTL + 1$  until it reaches its destination. When a packet reaches its maximum TTL, the last hop in line will send back an ICMP TTL Exceeded packet back to the source.

## 7

#### 7.1 Do you see the full ARP table on your machine? Explain each column of the ARP table.

arp is used to display the complete ARP table on our machine. The output of the above command is organised in the form of a table with following columns: (i) Hostname: It is the hostname if the hostname cannot be resolved then you get a ?. (ii) IP address: It is the IP address of the host. (iii) MAC address: It is a six part hexadecimal number. In practice also known as hardware address or ethernet address. (iv) HWtype: It is the Hardware type it could be ether i.e ethernet. (v) Flags: (1) C : Complete Entry (2) M : Permanent Entry (3) P : Published Entry (vi) Iface: Network interface.

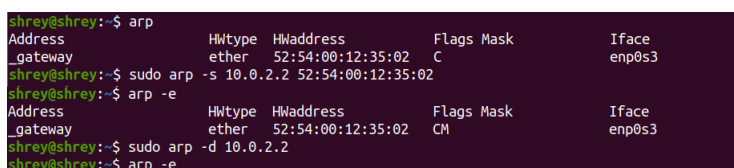
#### 7.2 What command is used to add or delete an entry into the ARP table. Use this mechanism to add at least two new hosts to the ARP table and include a screenshot.

Delete an entry:

```
sudo arp -d [IP address]
```

Add an entry:

```
sudo arp -s [IP address] [MAC address]
```



```
shrey@shrey:~$ arp
Address HWtype HWaddress Flags Mask Iface
_gateway ether 52:54:00:12:35:02 C enp0s3
shrey@shrey:~$ sudo arp -s 10.0.2.2 52:54:00:12:35:02
shrey@shrey:~$ arp -e
Address HWtype HWaddress Flags Mask Iface
_gateway ether 52:54:00:12:35:02 CM enp0s3
shrey@shrey:~$ sudo arp -d 10.0.2.2
shrey@shrey:~$ arp -e
```

**7.3** Can there be an entry for any IP from different subnet in the ARP table of your PC? Explain your answer.