Computer Networks Lab, Assignment 1

Suyash Gaurav

210010054

1 Task 1. Background

(i) $ ping www.google.com :

Ping command is used to know whether two networks are reachable. It is going to send ICMP(Internet Control Message Protocol) request packets to *www.google.com* and in return *www.google.com* will respond with ICMP response. Also, RTT(Round Trip Time) will be printed for each trip in ms.

Output of 1 packet looks like: $64 bytes from maa03s46-in-f14.1e100.net (142.250.196.78) : icmp_seq = 1 ttl = 56 time = 30.8 ms$

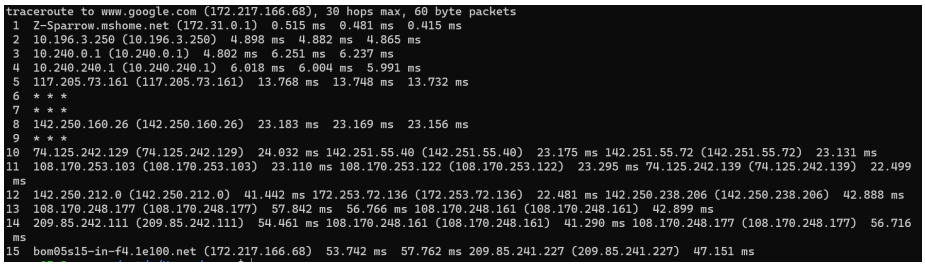
Here, 142.250.196.78 is IP address of *www.google.com* and RTT is 30.8ms

```
PING www.google.com (142.250.70.68) 56(84) bytes of data.
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=1 ttl=56 time=48.1 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=2 ttl=56 time=51.9 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=3 ttl=56 time=53.5 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=4 ttl=56 time=48.9 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=5 ttl=56 time=51.6 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=6 ttl=56 time=72.8 ms
64 bytes from pnbomb-ab-in-f4.1e100.net (142.250.70.68): icmp_seq=7 ttl=56 time=97.6 ms
```

(ii) $ traceroute www.google.com :

The traceroute command is used to trace the path that packets take from a computer to a destination host (i.e., *www.google.com*) on a network. It is going to print the IP

of each route between a computer and www.google.com. It will stop if it will reaches the IP of the destination host (i.e. *www.google.com*)



(iii) $ arp :

The Address Resolution Protocol (ARP) is used for mapping an IP address to a physical machine address(i.e., MAC Address) that is recognized in the local network.

Address	**HWtype**	**HWaddress**	**Flags Mask**	**Iface**
suyash.mshome.net	ether	00:15:5d:13:7b:d9	C	eth0

Here, HWaddress is the MAC address of my computer and it is mapped to resolve hostname (or IP).

(iv) $ ifconfig :

The ifconfig command provides information about the network interfaces on the system that includes a detailed view of the current network configuration, including IP addresses, MAC addresses, etc.

(v) $ hostname :

It displays the name of the host of the system and it is used to identify the device within the network. Output: user@suyash:/mnt/c/Users/suyas$ hostname

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.2.22  netmask 255.255.240.0  broadcast 172.31.15.255
        inet6 fe80::215:5dff:fe0d:f05b  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:0d:f0:5b  txqueuelen 1000  (Ethernet)
        RX packets 226  bytes 22204 (22.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 135  bytes 11995 (11.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

suyash

(vi) /etc/hostname, /etc/hosts, /etc/resolv.conf, /etc/protocols, /etc/services :

The **/etc/hostname** file contains the hostname of the system.

The **/etc/hosts** file is used to map IP addresses to hostnames.

IP Address	**Hostname**
127.0.0.1	localhost
127.0.1.1	suyash.localdomain

Here 127.0.0.1 address corresponds to localhost of the system. 127.0.1.1 is another address, for associating the machine's hostname with an IP address. suyash.localdomain is a hostname associated with the machine.

The **/etc/resolv.conf** file specifies the domain name and IP addresses of DNS (Domain Name System) servers and is used for domain name resolution. Output: nameserver 172.18.0.1

The **/etc/protocols** file contains a list of protocol names and their corresponding protocol numbers.

icmp	**1**	**ICMP**
igmp	**2**	**IGMP**

The **/etc/services** provides a mapping between port numbers and the services that use those ports.

2 Task 2. Warm-up Questions

(i) Hostname: suyash and IP address corresponding to eth0: 172.31.2.22 and localhost: 127.0.0.1
One can get this info by *hostname* and ifconfig commands.

(ii) The hop refers to a point where data transfers from one network segment to another. The IP address is used to route the data between different networks. The MAC address is used for communication on the local network to forward the data to the next hop. IP of the next hop will be determined by the "*ip route*" command and check the mapping of "*arp -n*" to get the MAC address.
IP Address: 172.31.2.22
MAC Address: 00:15:5d:13:7b:d9

(iii) This **/etc/resolv.conf** contains information about the DNS servers used by the system. Run the command:
nano /etc/resolv.conf
Output: nameserver 172.18.0.1

(iv) The **/etc/protocols** file is used to map protocol names to their corresponding protocol number. Each line in the file typically represents a protocol and provides information about its name, number, and aliases.

(v) SSH (Secure Shell) Port Number: 22

NFS (Network File System): Port Number: 2049 (TCP and UDP)
FTP (File Transfer Protocol) Port Numbers:
FTP Control: 21 (TCP)
FTP Data: 20 (TCP)
SMTP (Simple Mail Transfer Protocol - Email) Port Number: 25 (TCP)
One can get the port number of these protocols by finding in **/etc/services** file. Command: **nano /etc/services**

(vi) Probably, we can find IP addresses for android phones. All other info will not be possible to find.

3 Task 3. Questions

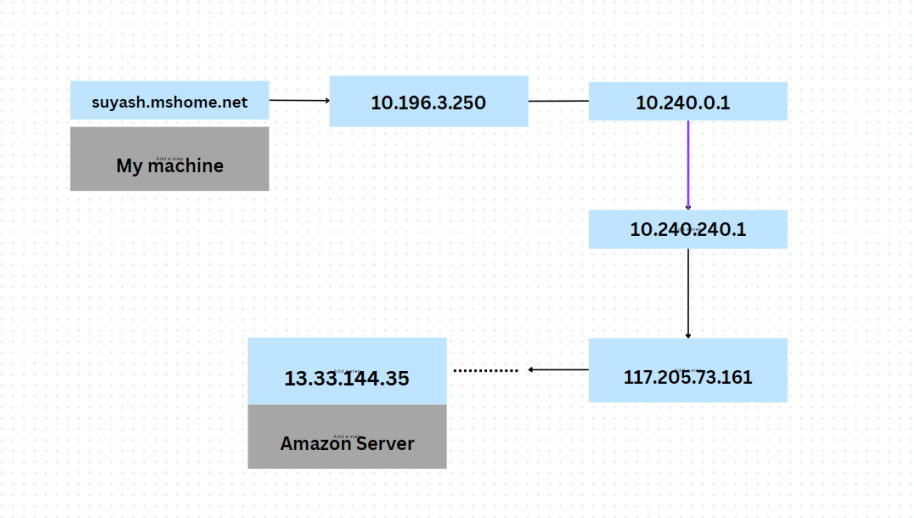
(i.a) Successful ping means we got replies back from the target, like in **ping www.amazon.com**. But a failure occurs if there's no reply within a certain time or if the host is unreachable and blocking ICMP packets, as happened with **ping www.iitb.ac.in**. In failure, we are going to face 100% packet loss.

```
PING d3ag4hukkh62yn.cloudfront.net (13.33.144.35) 56(84) bytes of data.
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=1 ttl=244 time=25.4 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=2 ttl=244 time=30.7 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=3 ttl=244 time=31.0 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=4 ttl=244 time=25.1 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=5 ttl=244 time=22.9 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=6 ttl=244 time=26.3 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=7 ttl=244 time=34.5 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=8 ttl=244 time=25.3 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=9 ttl=244 time=28.4 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=10 ttl=244 time=27.1 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=11 ttl=244 time=25.7 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=12 ttl=244 time=26.3 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=13 ttl=244 time=25.4 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=14 ttl=244 time=25.9 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=15 ttl=244 time=28.4 ms
64 bytes from server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35): icmp_seq=16 ttl=244 time=33.6 ms
```

```
PING www.iitb.ac.in (103.21.124.10) 56(84) bytes of data.
^C
--- www.iitb.ac.in ping statistics ---
18 packets transmitted, 0 received, 100% packet loss, time 17699ms
```

(i.b) RTT(Round Trip Time) is the travel time from source to destination and coming back. If the distance is larger or traffic is more between source and destination, RTT will also be higher. In **www.amazon.com** I am getting RTT as 71ms. But IITB does not giving any response, so RTT is not defined for it.

(ii.a) Traceroute displays the path with the IP of the router in between source and destination. For the output **traceroute www.amazon.com**:
suyash.mshome.net (172.18.0.1) 0.192 ms 0.208 ms 0.127



ms
10.196.3.250 (10.196.3.250) 6.133 ms 9.943 ms 22.331 ms
10.240.0.1 (10.240.0.1) 22.341 ms 22.336 ms 22.334 ms
10.240.240.1 (10.240.240.1) 10.005 ms 10.002 ms 9.999

ms
117.205.73.161 (117.205.73.161) 60.851 ms 60.847 ms 60.844
ms .....
.... server-13-33-144-35.maa50.r.cloudfront.net (13.33.144.35)
23.247 ms 23.159 ms 21.759 ms
map: suyash.mshome.net (My Machine) → Router1(10.196.3.250)
→ Router2(10.240.0.1) → Router3(10.240.240.1) → Router4(117.205.73.161)
→ . . . → → Amazon Server (13.33.144.35)

(ii.b) Hop is used to find the number of intermediary devices a packet found on its way to the destination. We can change it by following command:
traceroute -m 20 www.amazon.com

(ii.c) First timestamp: RTT of the first packet sent to that hop.
Second timestamp: RTT of the second packet sent to that hop.
Third timestamp: the third packet sent to that hop. in ms.

(ii.d) The **Time To Live (TTL)** field in a packet represents the maximum number of hops (routers) the packet can traverse. Each router along the route decrements the TTL by one. When the TTL reaches zero, the packet is discarded, and an ICMP Time Exceeded message is sent back to the source. It is used to prevent packets from circulating endlessly.