CS212 : Computer Networks Lab
Assignment 4

T Satwik
190030043

1 Question 1

(a) The option required to specify the number of echo requests to send with ping command is **-c**.
eg: ping -c 5 www.iitdh.ac.in sets the number of echo request to be 5.

(b) The option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs is **-i**.
eg ping –i 5 www.iitdh.ac.in sets the time interval to be 5 seconds.

(c) The command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply is **-l**.
The limit for sending such ECHO_REQUEST packets by normal users is **3**.

(d) The command to set the ECHO_REQUEST packet size (in bytes) is **-s**
If the PacketSize is set to 64 bytes, the total packet size will be **72** (i.e 64 + 8(header))

2 Question 2

Please refer to Table 1 and Table 2, for the required output. In all the tables the RTT and latency values are mentioned in ms.

Domain Name	IP address	Geo location	Avg. RTT1	Avg.RTT2	Avg.RTT3	Total Avg RTT
www.google.com	74.125.138.106	Mountain View, US, 94043	34.441	33.477	34.537	34.152
www.amazon.in	23.62.25.28	Ashburn, US, 20149	18.466	18.432	18.117	18.338
www.instagram.com	157.240.2.174	Chicago, US, 60666	30.626	30.443	30.573	30.547
www.flipkart.com	163.53.78.110	Mumbai, IN, 400070	215.017	215.611	215.106	215.245
www.iitdh.ac.in	14.139.150.68	Hubli, IN, 580001	No RTT	No RTT	No RTT	No RTT

Table 1: Question 2 Table 1

There are cases, which shows packet loss greater than 0%. For example www.iitdh.ac.in showed a 100% packet loss when pinged on 14-feb-2020, 5:00 PM. Reasons for packet loss maybe network congestion, that is the queues for routers are full and no new packets can be enqueued. Packet loss may also occur when the firewall blocks packets from a specific source.

Average RTTs for each host are mentioned in the table.

Measured RTTs are weakly correlated with the geographical distance of the hosts. As we can see the RTT for www.flipkart.com is more when compared to www.amazon.in, though Mumbai is closer to my system compared to Chicago. RTTs are more dependent on the number of hops rather than the geographical distance, this is because the propagation delay is small in most cases as the speed of propagation is close to the speed of light which is very high.

I have picked www.amazon.in(23.62.25.28) to perform the second experiment.

	64	128	256	512	1024	1576	2048
Avg RTT1	97.471	97.563	97.515	97.639	97.514	97.542	97.914
Avg RTT2	97.455	97.518	97.481	97.512	97.472	97.526	97.550
Avg RTT3	97.543	97.555	97.495	97.480	97.520	97.632	98.015
Avg RTT	97.489	97.545	97.497	97.544	97.502	97.567	97.826

Table 2: Question 2 Table 2

The average RTT (x-axis: Packet size, y-axis: Avg RTT) graph is given in Figure 1

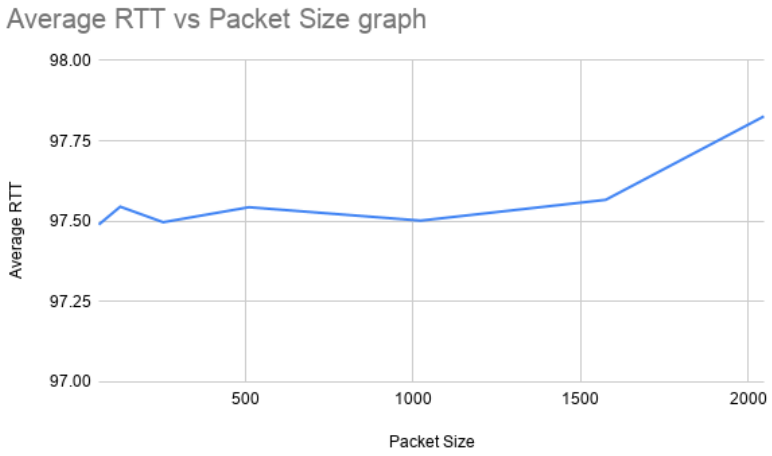

Figure 1: Average RTT vs Packet Size Graph

As we can see in Figure 1, increase in packet size increases the RTT values. The time of the day impacts the RTT, as the network traffic maybe less or more depending on the time of the day. We can say that the RTT values are more in the morning time(RTT3), hence the traffic is more at that time.

3 Question 3

I have used the IP address of www.amazon.in that is 23.62.25.28. In all the tables and graphs the RTT and latency values are mentioned in ms.

The final commands used are:

1. ping -n -c 1000 23.62.25.28 > Q3-1.txt
2. ping -p ff00 -c 1000 23.62.25.28 > Q3-2.txt

(a) The packet loss rate for command 1 is 1.4%, and for command 2 is 1%.

(b) The minimum, maximum, mean, and median latency of the pings that succeeded, for command 1 and command 2 are listed in the Table 3

Command	Packets Sent	Packets Received	Packet Loss Rate	Min Latency	Max Latency	Mean Latency	Median Latency
ping -n	1000	986	1.4%	215.443	2322.094	239.737	218
ping -p ff00	1000	990	1%	210.294	1572.190	309.761	282

Table 3: Output table for Q3

(c) The graphs of the ping latencies, obtained using command 1 is shown in Figure 2 and obtained by command 2 is shown in Figure 3

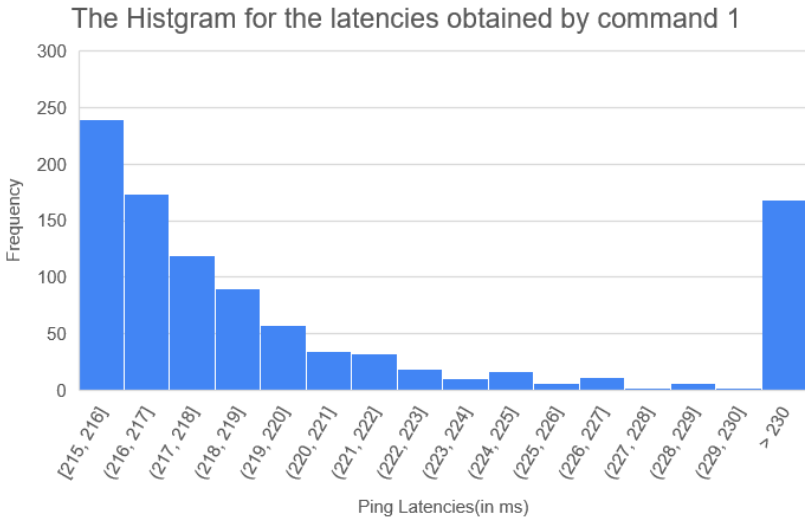

Figure 2: Histogram of ping latencies by command 1

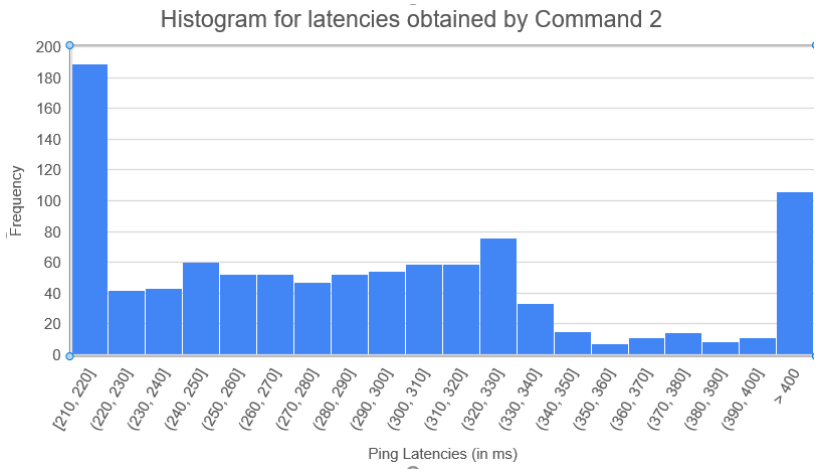

Figure 3: Histogram of ping latencies by command 2

(d) The differences in both the scenarios are:

1. In command 1 there is no particular pattern specified, hence it will be default, whereas in command 2 a pattern of ff00 is given.
2. The command 2, ensures that the packets will undergo DNS resolution, but the command 1 packets will not undergo.

4 Question 4

Figure 4 shows the output for ifconfig, since I am using wifi in my laptop, The interface that is running is wlp0s20f3.

```
talluri-satwik@Satwik-Ubuntu-PC:~/Desktop/Programming/4rth Sem Assignments/Ass4$ /sbin/ifconfig
enp7s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 98:fa:9b:d7:34:31  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 3667  bytes 406376 (406.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3667  bytes 406376 (406.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.13  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a724:bfeb:254:28c4  prefixlen 64  scopeid 0x20<link>
        ether 08:71:90:38:9b:09  txqueuelen 1000  (Ethernet)
        RX packets 237406  bytes 288882382 (288.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64533  bytes 13959888 (13.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 4: Output for ifconfig

The various values in the output of ifconfig represents the:

Flags: It shows if the particular interface is UP and running, broadcast, multicast is enabled or not. The value is calculated by using hexadecimal representation for UP, Broadcast etc.

mtu: Maximum Transmission unit, which is the largest possible size.

inet, netmask, broadcast: They represent the various addresses(IP address, Netmask address, broadcast address)

inet6: This is IPv6 address.

prefixlen: Represents the prefix length.

ether: It represents the enthernet card mac address.

txqueuelen: It represents the transaction queue length.

RX: IT represents the packets received, the size is shown in bites and is also converted into MB, it also shows the errors, packets dropped, number of packets in overruns, frames.

TX: It represents the packets transferred, the rest of the parameters are same as RX, except that they show the data for transferred packets.

carrier, collisions: When there is a problem with the modulation of signal, then carrier shows the number of packets facing the issue and collision shows the number of packets that face collisions.

Figure 5 shows the output for route,

```
talluri-satwik@Satwik-Ubuntu-PC:~/Desktop/Programming/4rth Sem Assignments/Ass4$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f3
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp0s20f3
talluri-satwik@Satwik-Ubuntu-PC:~/Desktop/Programming/4rth Sem Assignments/Ass4$
```

Figure 5: Output for route

Route command is used to view the IP routing table, the different values in the table represent:

Destination: It represents, the destination network or destination host.

Gateway: It represents, the gateway address.

Genmask: It represents, the netmask for the destination net.

Flags: It represents, if it is up(U), using Gateway(G), etc.

Metric: It represents, the hops to the target.

Ref: It represents, the number of references to this route.

Use: It represents, the count of look ups for the route.

Iface: It represents, the interface to which packets for this route will be sent.

Some Options for route command are:

-A: used to specify the address family.

-F: used to operate on the kernel's FIB (Forwarding Information Base) rout- ing table.

-C: used to operate on the kernel's routing cache.

-n: Shows numerical addresses instead of trying to determine symbolic host names.

-e: Uses netstat format for displaying the routing table.

del: used to delete a route.

add: used to add a new route.

5 Question 5

Netstat is command used to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

The parameters -t/–tcp can be used to list all the TCP connections. The output is shown in Figure 6. The various columns in the output table represent the following.

1. **Proto:** The protocol (tcp, udp, udpl, raw) used by the socket.
2. **Recv-Q:** The count of bytes not copied by the user program connected to this socket.
3. **Send-Q:** The count of bytes not acknowledged by the remote host.
4. **Local Address:** Address and port number of the local end of the socket.
5. **Foreign Address:** Address and port number of the remote end of the socket.
6. **State:** The state of the socket(eg: ESTABLISHED CLOSE_WAIT, TIME_WAIT, etc)

netstat -r shows kernel IP routing table. The output is shown in Figure 7. The various columns in the output table represent the following.

1. **Destination:** It represents, the destination network or destination host.
2. **Gateway:** It represents, the gateway address.
3. **Genmask:** It represents, the netmask for the destination net.
4. **Flags:** It represents, if it is up(U), using Gateway(G), etc.
5. **MSS:** It represents, the maximum segment size.
6. **Window:** It represents, the window size.
7. **irtt:** It represents, the initial round trip time.
8. **Iface:** It represents, the interface to which packets for this route will be sent.

```
talluri-satwik@Satwik-Ubuntu-PC:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 Satwik-Ubuntu-PC:34358  maa05s13-in-f14.1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:55242  151.101.158.137:https   ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:34054  maa05s09-in-f3.1e:https ESTABLISHED
tcp      130      0 Satwik-Ubuntu-PC:58700  maa03s34-in-f3.1e:https CLOSE_WAIT
tcp        0      0 Satwik-Ubuntu-PC:44532  252.16.213.35.bc.:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:55374  151.101.158.137:https   ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:38840  maa05s06-in-f14.1:https TIME_WAIT
tcp        0      0 Satwik-Ubuntu-PC:59930  cdn-185-199-110-1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:49740  maa05s06-in-f14.1e:http ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:40564  156.247.107.34.bc:https ESTABLISHED
tcp      130      0 Satwik-Ubuntu-PC:53980  maa05s10-in-f3.1e:https CLOSE_WAIT
tcp      130      0 Satwik-Ubuntu-PC:57772  maa03s34-in-f14.1:https CLOSE_WAIT
tcp        0      0 Satwik-Ubuntu-PC:60082  server-13-35-202-:https ESTABLISHED
tcp      130      0 Satwik-Ubuntu-PC:44862  maa03s34-in-f13.1:https CLOSE_WAIT
tcp      130      0 Satwik-Ubuntu-PC:58702  maa03s34-in-f3.1e:https CLOSE_WAIT
tcp        0      0 Satwik-Ubuntu-PC:55320  151.101.158.137:https   ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:50004  maa03s31-in-f3.1e:https TIME_WAIT
tcp       73      0 Satwik-Ubuntu-PC:47396  maa05s12-in-f14.1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:60084  server-13-35-202-:https TIME_WAIT
tcp        0      0 Satwik-Ubuntu-PC:48034  maa03s29-in-f10.1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:56206  ec2-34-210-121-31:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:44902  maa03s28-in-f16.1:https TIME_WAIT
tcp        0      0 Satwik-Ubuntu-PC:40108  125.223.231.35.bc:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:47448  maa05s12-in-f14.1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:40002  74.125.24.188:https     ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:40124  125.223.231.35.bc:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:48680  cdn-185-199-108-1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:52904  maa05s10-in-f14.1:https ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:53864  maa05s10-in-f3.1e:https TIME_WAIT
tcp        0      0 Satwik-Ubuntu-PC:57038  151.101.158.110:https   ESTABLISHED
tcp        0      0 Satwik-Ubuntu-PC:56694  maa03s35-in-f10.1:https ESTABLISHED
talluri-satwik@Satwik-Ubuntu-PC:~$
```

Figure 6: Output for netstat -t

```
talluri-satwik@Satwik-Ubuntu-PC:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp0s20f3
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 wlp0s20f3
talluri-satwik@Satwik-Ubuntu-PC:~$
```

Figure 7: Output for netstat -r

The option of netstat that can be used to display network interface status is -i and there are 4 interfaces in my machine.(as shown in Figure 8)

```
talluri-satwik@Satwik-Ubuntu-PC:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp7s0    1500        0      0      0 0             0      0      0      0 BMU
lo       65536     3294      0      0 0          3294      0      0      0 LRU
wlp0s20f  1500   112968      0      0 0         32088      0      0      0 BMRU
talluri-satwik@Satwik-Ubuntu-PC:~$
```

Figure 8: Output for netstat -i

Loop Back Interface: The Figure 9, shows the lo output. The loopback interface is a logical interface. It is used to identify the device, though we can use any interface to detect if a device is online, lo is most preferred as its address will not change and cannot be removed. It is used for troubleshooting and diagnostics and to connect to servers that run on the same machine, so that a computer can communicate with itself.

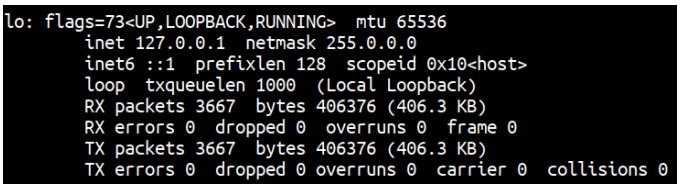

Figure 9: Loopback Interface

6 Question 6

The output table is in Table 4 **(a)** The number of hop counts for each host in each time slot is mention in Table 4 and common hops are mentioned below:

1. www.google.com: 59.144.94.165, 108.170.253.97
2. www.amazon.in: 62.115.175.230, 23.203.152.38
3. www.instagram.com: 202.56.234.81, 116.119.68.60
4. www.flipkart.com: 202.56.234.85, 116.119.35.217
5. www.iitdh.ac.in: 202.56.234.85, 10.119.73.121

(b) Yes the route changes at different times of the day, as the destination host may use multiple servers and also multiple IP addresses(as seen in Assignment 3). The shortest path may also change as the online routers may change, hence the next hop address will change. If Load Balancing is applied then the fastest route is calculated for each packet(packet switching), hence every packet may go through a different route.

(c) The traceroute www.amazon.in in the first trial does not find complete paths to the host. This maybe due to firewall blocking the packets or the server may not be online. Another possible reason is that the maximum ttl maybe exceeded, hence the packet will die before it reaches the host

(d) It is possible to find the route to certain hosts which fail to respond with ping experiment. It is because ping uses direct ICMP packets with limited TTL, whereas traceroute uses a different method which invloves increasing the TTL each time, until the destination is reached. Hence in ping the packets might be lost, but not in traceroute.

	www.google.com	www.amazon.in	www.instagram.com	www.flipkart.com	www.iitdh.ac.in
Hop Count 1	26	>64	10	11	11
Hop Count 2	26	25	10	11	11
Hop Count 3	26	42	10	33	11

Table 4: Output for Q6

7 Question 7

The full ARP table for your machine can be displayed by using arp -e.

Each column of the ARP table is explained below:

1. **Address:** The IP addresses of network machines are shown in this column
2. **Hwtype:** The hardware type of the machine is shown in this column
3. **Hwaddress:** The represents hardware address(eg:Mac Address) is shown in this column
4. **Flag:** The state of the entry(eg: C for completed M for permanent) is shown in this column.
5. **Mask:** The genmask of the entry is represented in this column
6. **Iface:** The network interface corresponding to the entry is shown in the column

When we add and static entry to the arp table, , a permanent entry is created in the ARP table, which would be helpful in case 2 machines are constantly communicating, hence the ARP caching will not take place every time a connection is established. **When we delete an entry** from the table the entries are marked as incomplete, because removing elements from cache is a hard and expensive task. The output is shown in Figure 10 and Figure 11

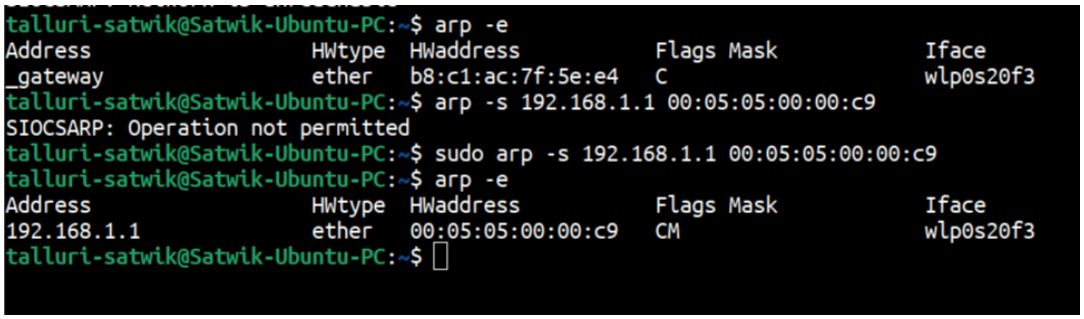

Figure 10: ARP table output after adding entry 1

Adding and Deleting entries in the ARP table.

1. **Add:** sudo arp -s IP MAC command is used.
2. **Delete:** sudo ard -d IP MAC command is used.

The output after adding the 2 entries is shown in Figure 10 and Figure 11

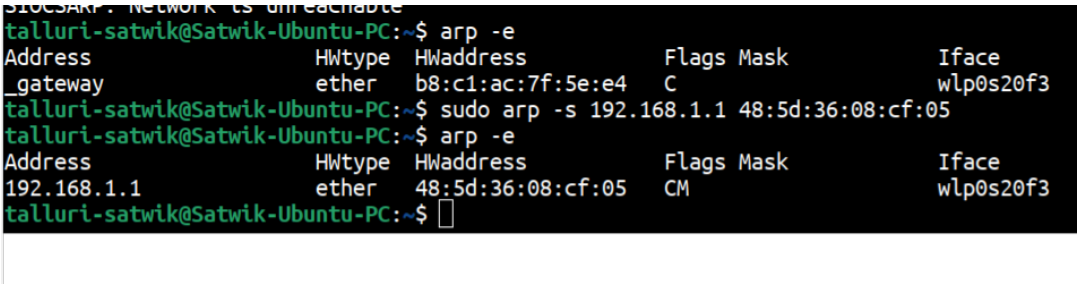

Figure 11: ARP table output after adding entry 2

The entries will stay cached in the ARP table for 4 hours for Cisco devices.

Trial-and-error method to discover the timeout value:
We first take a randomly shoose a value, then run the clock that many times faster and see if the entry still remains in the table. If it does then decrease the value, and if it doesn't increase the value. Until we get a fair idea about the time out value.

What will happen if two IP addresses map to the same Ethernet address: If 2 IP addresses map to the same MAC address on the same LAN, then neither machine can communicate properly as more number of collisions will take place, however if they are on different LANs then it is not a problem as they use a router to communicate.

How all hosts on the subnet operate. In a subnet, only the IP addresses of the machines are known. Each time ARP broadcasts are sent to get the MAC address of different machines. With the help of these MAC addresses, machines can communicate and operate with each other.