CS349 NETWORKS LAB

ASSIGNMENT -1

By: - NIKIT BEGWANI (130101055)
ROHAN GUPTA (130101066)

1) The following readings were taken on 17/1/2016

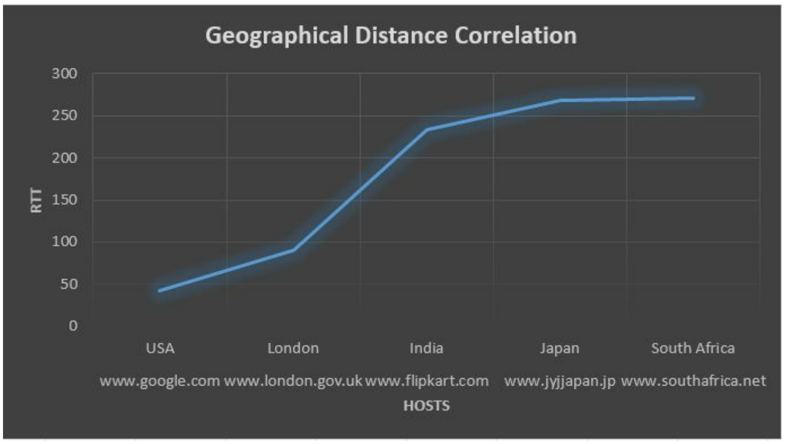
HOSTS	0000 hrs	1500 hrs	1800hrs
www.google.com	42.572/42.633/42.683	42.585/42.656/42.728	42.607/43.308/49.077
www.flipkart.com	233.632/233.934/235.195	233.649/233.763/233.894	232.956/233.620/233.807
www.london.gov.uk	89.356/89.433/89.505	88.700/89.327/89.461	88.511/89.400/89.926
www.jyjjapan.jp	209.249/227.006/270.935	218.811/239.428/268.494	211.201/244.967/270.622
www.southafrica.net	270.473/270.616/270.811	269.636/270.566/270.929	269.977/270.628/270.931

Each of the above reading represents the Minimum RTT/Average RTT/ Maximum RTT (all in ms). These data were gathered by pinging each host 20 times at three different times of a day. The packet size used was 64B for all ping request.

There was no case of packet loss while doing the above experiment with packet size of 64B. But there can be packet losses and the reason for the same could be:-

a) There are many hosts which don't respond to ping requests (Ex:- amazon.in)
b) Generally hosts reply for packet size of less than 1440B above that they don't respond.
c) There may be packet loss due to high traffic or congestion in network

Coming to the next question that whether measured RTTs are strongly or weakly correlated with the geographical distance of hosts.

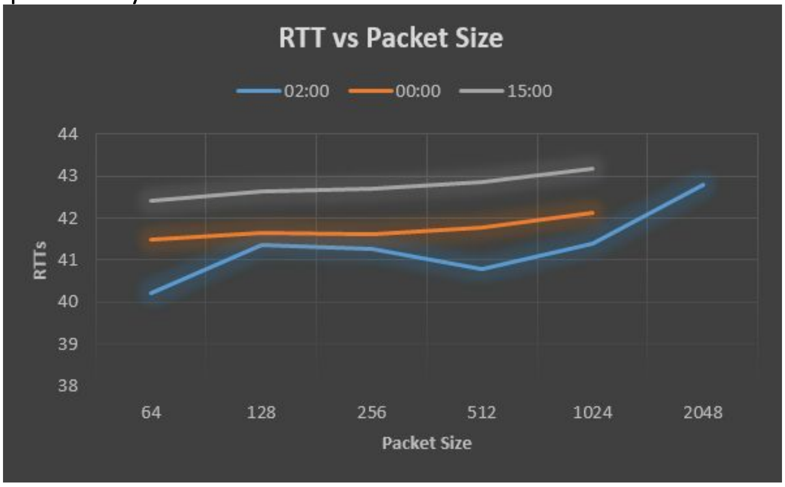


To answer this, we specifically choose the hosts located at different parts of world like USA, India, Japan, London and South Africa. We get the measured RTTs from spfld.com which is situated in USA so, it gives minimum RTT for USA and maximum for South Africa or Japan. From the graph, we can see that there is a strong positive correlation between measured RTTs and host's location.

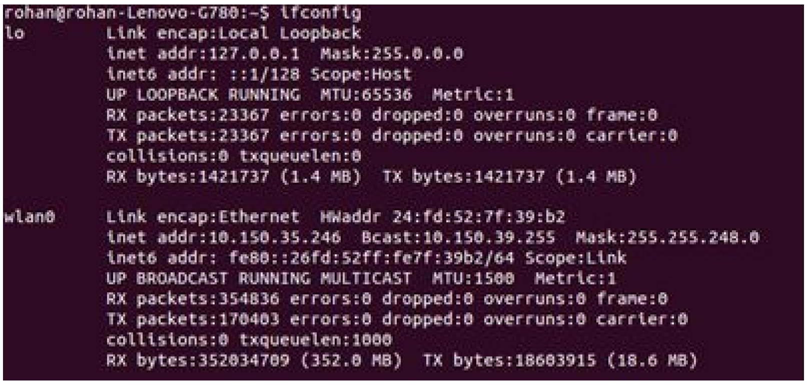
Different Packet Sizes and time of day

We chose www.google.com to repeat the experiment with different packet sizes from 64 bytes – 2048 bytes

We observed a change of nearly 2.5% in change of measured RTTs in a particular time period and we also observed that measured RTTs were different at different time of day. The probable reason for the first one could be due to larger packet size, it takes more time for transmission but the major part of RTTs is composed of connection establishment time and transmission time, it depends very less on the packet size though we can see a slight positive correlation. We also observe that RTTs change for different time of day it may be possible due to the network’s high usage and congestion, as it totally explains the observed data. We got a 100% packet loss for packet size > 1440 bytes at 00:00 and 15:00. At that time, due to high network usage, we did not get a response for ping for these packet sizes.



2) IFConfig Command



```
rohan@rohan-Lenovo-G780:~$ ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:23367 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1421737 (1.4 MB)  TX bytes:1421737 (1.4 MB)

wlan0     Link encap:Ethernet  HWaddr 24:fd:52:7f:39:b2
          inet addr:10.150.35.246  Bcast:10.150.39.255  Mask:255.255.248.0
          inet6 addr: fe80::26fd:52ff:fe7f:39b2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:354836 errors:0 dropped:0 overruns:0 frame:0
          TX packets:170403 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:352034709 (352.0 MB)  TX bytes:18603915 (18.6 MB)
```

Output given by ifconfig in a mchine running on Ubuntu OS and connected to IITG_WIFI wireless network

2a) **Output of ifconfig**

When used without any parameters, the command ifconfig shows details of the network interfaces that are up and running in your computer.

- **Link encap**:Ethernet - This denotes that the interface is an Ethernet related device.
- **Link encap**:Local Loopback - The loopback is a special, network interface that the computer uses to communicate with itself.
- **HWaddr** 24:fd:52:7f:39:b2 - This is the hardware address or MAC address. It is the address of the network interface card and is unique to it.
- **inet addr** - indicates the machine IP address. Since the machine is connected to IITG_WIFI, IP address is dynamically assigned to the machine.
- **Bcast** - denotes the broadcast address. A broadcast message is sent to all the devices connected to a particular network.
- **Mask** – It is network mask.
- **UP** - This flag indicates that the kernel modules related to the Ethernet interface has been loaded.
- **BROADCAST** - Denotes that the device supports broadcasting - a necessary characteristic to obtain IP address via DHCP.
- **MULTICAST** - This indicates that the Ethernet interface supports multicasting. Multicast allows a source to send a packet(s) to multiple machines as long as the machines are watching out for that packet.

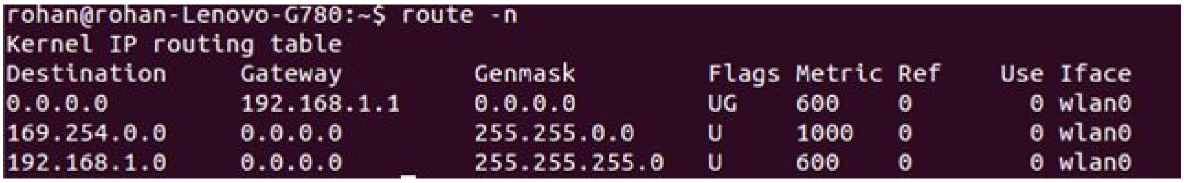
- **MTU** - short form for Maximum Transmission Unit is the size of each packet transferred by the Ethernet card. The value of MTU for all Ethernet devices by default is set to 1500.
- **Metric** - This option can take a value of 0,1,2,3... with the lower the value the more leverage it has. The value of this property decides the priority of the device. Setting this value using ifconfig has no effect on the priority of the card being chosen as Linux uses the Metric value in its routing table to decide the priority.
- **RX Packets, TX Packets** - The total number of packets received and transmitted respectively. The total errors are 0, no packets are dropped and there are no overruns. If the errors or dropped value is greater than zero, then it could mean that the Ethernet device is failing or there is some congestion in your network.
- **collisions** - If it has a value greater than 0, it could mean that the packets are colliding while traversing your network - a sure sign of network congestion.
- **txqueuelen** - This denotes the length of the transmit queue of the device.
- **RX Bytes, TX Bytes** - These indicate the total amount of data that has passed through the Ethernet interface either way.

2 b) **Various options in IFConfig:**

1. -a display all interfaces available(including the down interfaces)
2. -s display a short list with minimal required information
3. -v more verbose for some error conditions
4. IFConfig is primarily used to add alias to existing interfaces and change the existing ones. The following command adds a new alias with ipaddr 172.16.114.199 to the eth0 interface:
   ifconfig eth0:0 172.16.114.199
5. To change the settings of the existing interfaces, following keywords can be used in this format (ifconfig <name of the interface> <keyword>).
6. The available keywords are:
   a. up – to enable a network interface
   b. down – to disable a inteface
   c. <ip> - to change/assign a ip address to the inteface
   d. netmask <netmask> - to assign a netmask
   e. broadcast <broadcast addr> - to assign a braodcast addr
   f. mtu <size in octets> - to set the mtu value

2 c) **Route**

Route command is used to view and also modify the IP routing table.



```
rohan@rohan-Lenovo-G780:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlan0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlan0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlan0
```

Output of route

- Destination : The destination network or destination host.
- Gateway : The gateway address or '*' if none set.
- Genmask : The netmask for the destination net.
- Flags :
  U (route is up)
  G (use gateway)
- Metric : The distance to the target (usually counted in hops). It is not used by recent kernels.
- Ref : Number of references to this route.
- 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.

2 d)**Some of the relevant options of route used are**

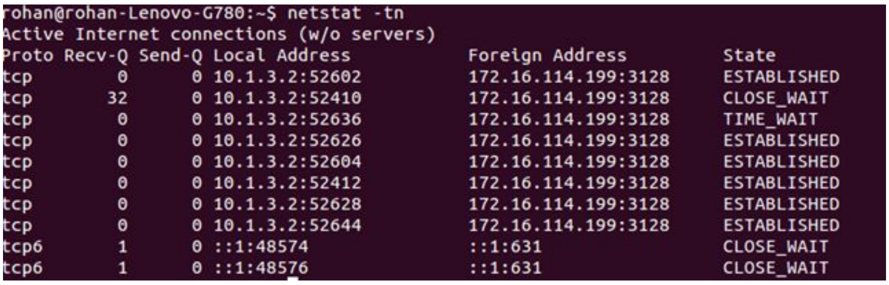
1. -n is used to show numerical addresses instead of trying to determine the symbolic host names.
2. -v verbose option
3. del to delete a route
4. add to add new route

3) **Netstat**

Netstat is a command line utility that can be used to list out all the network (socket) connections on a system. It is essentially collection of multiple tools together.

3 a) To list all TCP connections

netstat -tn

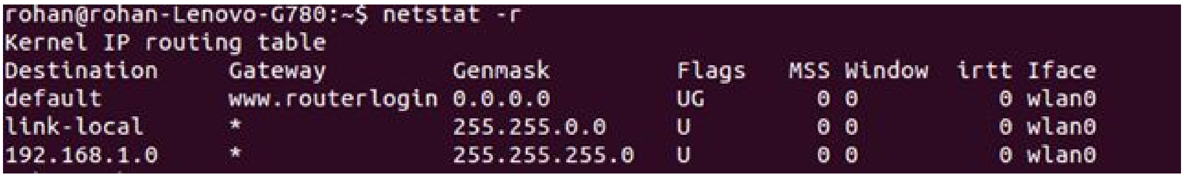


```
rohan@rohan-Lenovo-G780:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.1.3.2:52602          172.16.114.199:3128     ESTABLISHED
tcp       32      0 10.1.3.2:52410          172.16.114.199:3128     CLOSE_WAIT
tcp        0      0 10.1.3.2:52636          172.16.114.199:3128     TIME_WAIT
tcp        0      0 10.1.3.2:52626          172.16.114.199:3128     ESTABLISHED
tcp        0      0 10.1.3.2:52604          172.16.114.199:3128     ESTABLISHED
tcp        0      0 10.1.3.2:52412          172.16.114.199:3128     ESTABLISHED
tcp        0      0 10.1.3.2:52628          172.16.114.199:3128     ESTABLISHED
tcp        0      0 10.1.3.2:52644          172.16.114.199:3128     ESTABLISHED
tcp6       1      0 ::1:48574               ::1:631                 CLOSE_WAIT
tcp6       1      0 ::1:48576               ::1:631                 CLOSE_WAIT
```

Various features are:

1. Proto: The protocol used for the given connection
2. **The “Recv-Q” and “Send-Q” columns** tell us how much data is in the queue for that socket, waiting to be read (Recv-Q) or sent (Send-Q).
3. **The “Local Address” and “Foreign Address” columns** tell to which hosts and ports the listed sockets are connected. The local address is the adsress of the machine on which netstat is run, and the foreign end is the other computer.
4. **The “State” column** tells in which state the listed sockets are.

3 b) netstat -r



```
rohan@rohan-Lenovo-G780:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         www.routerlogin 0.0.0.0         UG        0 0          0 wlan0
link-local      *               255.255.0.0     U         0 0          0 wlan0
192.168.1.0     *               255.255.255.0   U         0 0          0 wlan0
```

This option is used to list the kernel routing table.

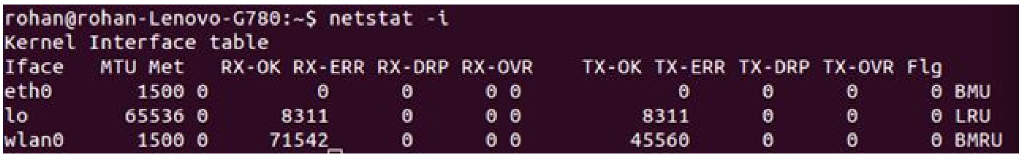
- **The “Destination” column** indicates the pattern that the destination of a packet is compared to. When a packet has to be sent over the network, this table is examined top to bottom, and the first line with a matching destination is then used to determine where to send the packet.
- **The “Gateway” column** tells the computer where to send a packet that matches the destination of the same line. An asterisk (*) here means “send locally”, because the destination is supposed to be on the same network.
- **The “Genmask” column** is the subnet mask that is used for the connection
- **The “Flags” column** shows which flags apply to the current table line. “U” means Up, indicating that this is an active line. “G” means this line uses a Gateway.
- **The “MSS” column** lists the value of the Maximum Segment Size for this line. Nowadays, most computers have no problems with the most commonly used maximum packet sizes, so this column usually has the value of 0, meaning “no changes”.
- **The “Window” column** is like the MSS column in that it gives the option of altering a TCP parameter. In this case that parameter is the default window size, which indicates how many TCP

packets can be sent before at least one of them has to be ACKnowledged. Like the MSS, this field is usually 0, meaning “no changes”.

- **The “irtt” column** stands for Initial Round Trip Time and may be used by the kernel to guess about the best TCP parameters without waiting for slow replies. In practice, it’s not used much, so 0 here.
- **The “Iface” column** tells which network interface should be used for sending packets that match the destination. If your computer is connected to multiple subnets on multiple network cards.

3 c). Showing interface statistics

netstat -i is used

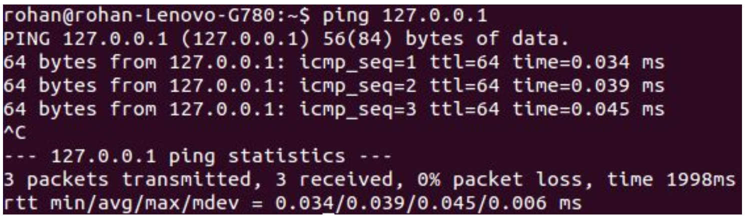


```
rohan@rohan-Lenovo-G780:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500 0         0      0      0 0          0      0      0      0 BMU
lo       65536 0      8311      0      0 0       8311      0      0      0 LRU
wlan0     1500 0     71542      0      0 0      45560      0      0      0 BMRU
```

3 d) **The loopback interface**

The loopback device is a virtual network interface that computer uses to communicate with itself. It is used for diagnostics and troubleshooting, and to connect to servers running on local machine.

If we ping the virtual address of the machine then it loopbacks till keyboard interrupt is given.



```
rohan@rohan-Lenovo-G780:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.045 ms
^C
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.034/0.039/0.045/0.006 ms
```

4) a)

Host Name	***Hop Counts***			***No. of Common Hops***	***Common Hops***
	14:00	***18:00***	***23:00***		
www.google.com	7	7	7	2	google-level3-3x10g.dallas.level3.net dfw25s08-in-f14.1e100.net
www.flipkart.com	21	21	21	0	
www.london.gov.uk	12	12	12	4	121.244.37.178.static.chennai.vsnl.net ae-3-80.edge5,dallas3.level3.net ix-19-0.tcore2.dt8-dallas.as6453.net if-8-2.tcore1.lvw-los-angeles.as6453.net
www.jyjjapan.jp	17	17	17	1	ae-1-60.edge2.losangeles9.level3.net
www.southafrica.net	13	13	13	8	ae-3-8.bear1.johannesburg2.level3.net workiline.bear1.johannesburg2.level3.net esr1-isd-cr1-gi0-0-22.wolcomm.net 14-71-148-197.as37497.za.net 11-66-148-197.as37497.za.net 250-71-148-197.as.as37497.za.net core-access-switch1.jnb1.host-h.net row-access-switch1-row7-8.jnb1.host-h.net

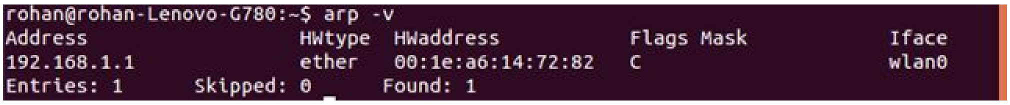
4) b) Route to same host changes at different time of the day due to differing traffic pattern. Routing may change due to considerations of different servers along the way, such as server load and availability. If the routing is not dynamic and let’s say a server is down, it will lead to undelivered requests. Some servers are extremely busy during day time due to heavy computations or too many request while during night, they may be ideal so in such case we may route the requests to these servers at night and change during day time.

4) c) There are cases when traceroute doesn’t provide the complete path, at times the request is acknowledged but the host name is not provided and at times timeout is returned. The primary reason could be existence of firewall which is configured to block these packets or a secondary (very unlikely though) reason could be that router is dropping packets going through it. This is

usually caused by three reasons either the router is overloaded, the router having a software or physical failure or the router is configured to do so (null route/blackholes).

4) d) Yes, it is possible to find the route to certain hosts which fail to respond with ping experiment (e.g. www.amazon.in). Ping works on straight ICMP (Internet control Message Protocol) Traceroute works very different from ping even though it uses ICMP. Traceroute works by targeting the final hop, but limiting the TTL (Time To Live) and waiting for a time exceeded message, and then increasing it by one for the next iteration. Therefore the response it gets is not an ICMP echo reply to the ICMP echo request from the host along the way, but a time exceeded message from the host. There are some hops, which don't give an ICMP echo reply so, we don't get a reply for ping request but we are able to trace the route.

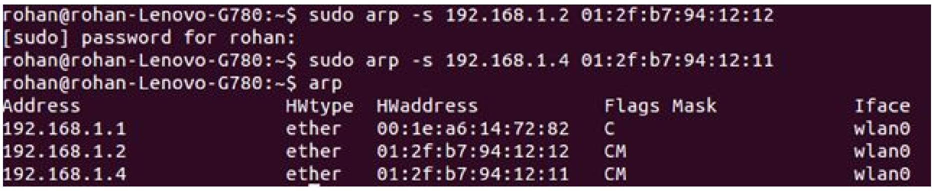
5 a)ARP table can be seen using the arp command. The output of arp command:



```
rohan@rohan-Lenovo-G780:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1e:a6:14:72:82   C                     wlan0
Entries: 1      Skipped: 0      Found: 1
```

1. Address column of the table shows the IP addr of the machine connected to a network
2. Hwtype specifies the type of hardware.
3. Hwaddress column shows the mac address corresponding the particular entry in the table.
4. ARP cache entries may be marked with the following flags: **C** (complete), **M** (permanent).
5. Interface shows the network interface type for the corresponding entry.

5 b) Option **To add a new entry** to the arp table: *arp -s <ip address> <hardware address>*
To delete an entry: *arp -d <ip address>*



```
rohan@rohan-Lenovo-G780:~$ sudo arp -s 192.168.1.2 01:2f:b7:94:12:12
[sudo] password for rohan:
rohan@rohan-Lenovo-G780:~$ sudo arp -s 192.168.1.4 01:2f:b7:94:12:11
rohan@rohan-Lenovo-G780:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1e:a6:14:72:82   C                     wlan0
192.168.1.2              ether   01:2f:b7:94:12:12   CM                    wlan0
192.168.1.4              ether   01:2f:b7:94:12:11   CM                    wlan0
```

5 c)The refresh time of arp cache can be found using the following command:
"cat /proc/sys/net/ipv4/neigh/default/gc_stale_time". It is 60 seconds for the current machine.
Trial And Error method to find the timeout:
An approach similar to the binary search can be used to get the desired value.
1. Connect the machine to a new network and then after every 5 mins, check of the entry in table is updated.
2. Let the entry be updated in the ith check. This means that the cache was refreshed between the i-1 and the i check.
3. Now disconnect from this network and wait for (i-1)*5 minutes + 2min + 30 sec. If the entry still exist at this time that means that the cache is cleared after this time and before 5*i minutes.
4. Apply this approach iteratively to get the result.

5 d)Yes, a single ethernet card can have multiple IP's assigned to it, this process is known as IP aliasing. With this, one node on a network can have multiple connections to a network, each serving a different purpose. In a lot of scenarios, multiple IP addresses are used such as when a single server hosts multiple domain names, when we use two operating system simultaneously one background and another as virtual machine we use different two different ip addresses to communicate among them, even though the MAC address is same(MAC address of our machine).
But conflict will arise when multiple ethernet addresses are mapped to single ip address. Whenever host say B wants to communicate to another host A and it doesn't have its mac address but only ip address it sends out a broadcast message "Who has mac address of A?". The reply to above request can be given by either the host A itself or any other host who has A's MAC address