COMPUTER NETWORKS ASSIGNMENT 1

Question 1

PART A

Ping command **(Packet Internet Groper)**

This command is used to check the network connection between the host and the server.

This command takes the **IP address or the URL** as an input and sends a data packet to the target address with the message “PING” and gets a response from the server. If the response is not received successfully then that message is lost and is shown as lost in the output of the command. Various statistics are displayed for the **RTT** at the end of the output.

To check if the server is available or not the PING commands sends the request of a fixed size to it. The number of requests(data packets) and their sizes is customizable. It uses the **ICMP** protocol to establish the network and exchange information in the network by sending the request.

ICMP or Internet Control Message Protocol is used to provide the utility of sending error messages and is used by devices like Routers.

The ping command delivers the following information as output for each data packet:

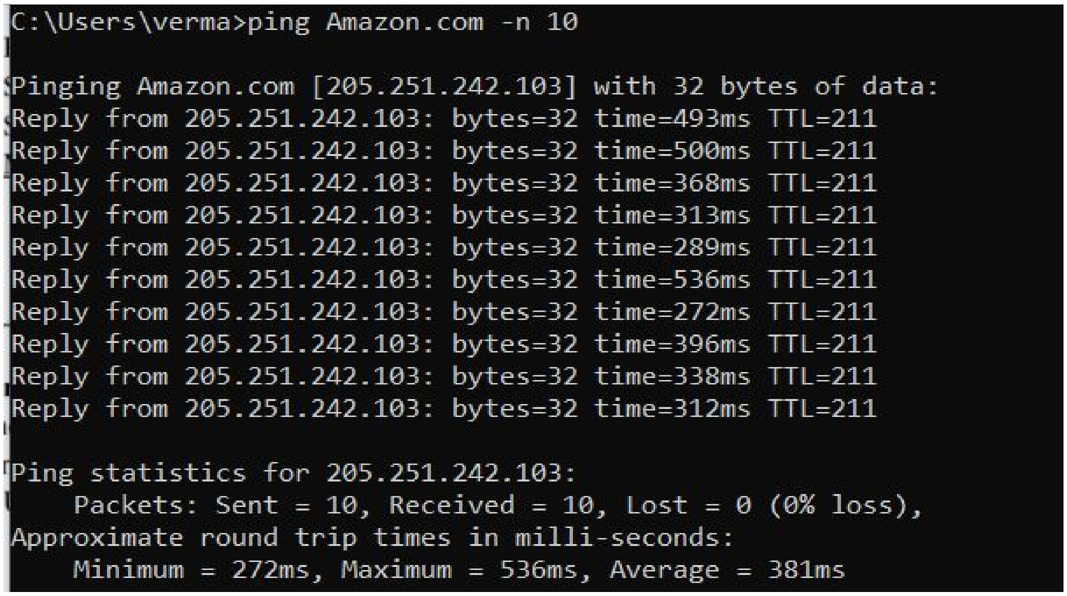
- Response time in milliseconds (ms) or RTT
- TTL
- Statistics of RTT

Response time is the total time taken by the data packet to go to the server and return back.TTL stands for **Time for Travel** which determines whether the data packet has been in the network for too long and should as a result needs to be discarded.

The two tasks assigned were to send a request of 10 packets to Amazon.com and then change the default packet size to 100 and record the responses such as minimum, maximum and average RTT.

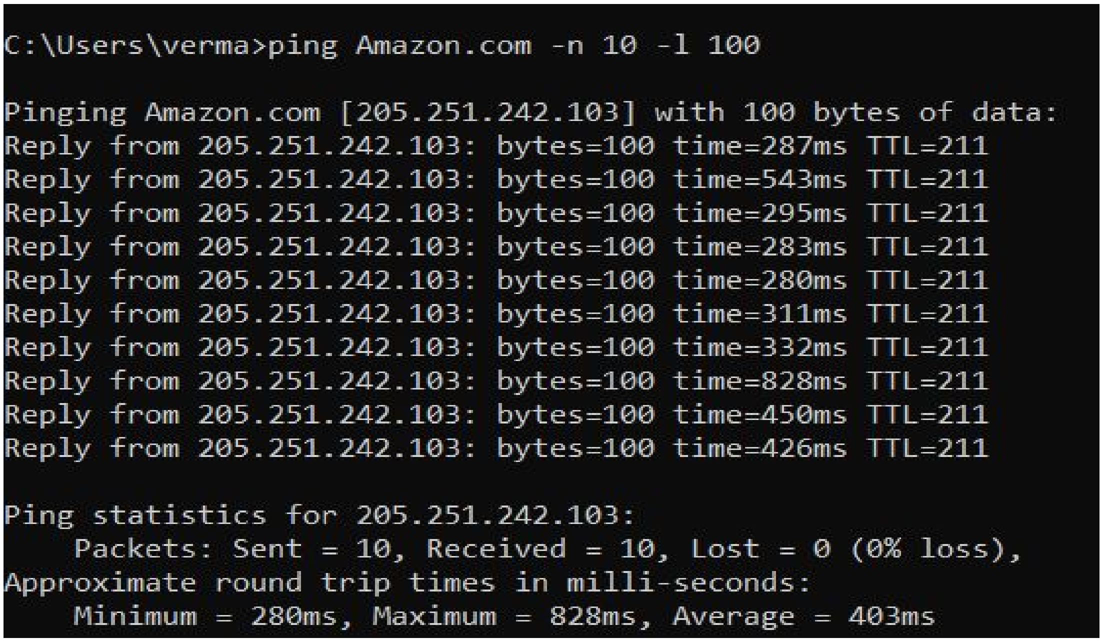
Here are the screenshots of the command prompt:

A) Here we had the sent 10 packets request to Amazon.com and received replies for all 10. The minimum RTT=272ms, maximum RTT=536ms and average RTT=381ms.The response time and TTL for all are given below.



```
C:\Users\verma>ping Amazon.com -n 10

Pinging Amazon.com [205.251.242.103] with 32 bytes of data:
Reply from 205.251.242.103: bytes=32 time=493ms TTL=211
Reply from 205.251.242.103: bytes=32 time=500ms TTL=211
Reply from 205.251.242.103: bytes=32 time=368ms TTL=211
Reply from 205.251.242.103: bytes=32 time=313ms TTL=211
Reply from 205.251.242.103: bytes=32 time=289ms TTL=211
Reply from 205.251.242.103: bytes=32 time=536ms TTL=211
Reply from 205.251.242.103: bytes=32 time=272ms TTL=211
Reply from 205.251.242.103: bytes=32 time=396ms TTL=211
Reply from 205.251.242.103: bytes=32 time=338ms TTL=211
Reply from 205.251.242.103: bytes=32 time=312ms TTL=211

Ping statistics for 205.251.242.103:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 272ms, Maximum = 536ms, Average = 381ms
```

B)Now we had to change the default size to 100 and note the values. The minimum RTT=280ms, maximum RTT=828ms and the average RTT=403ms.



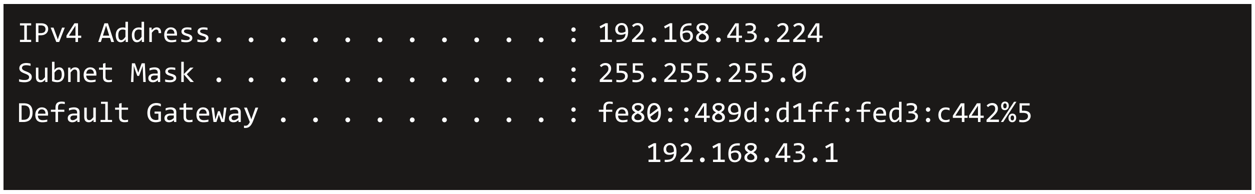
```
C:\Users\verma>ping Amazon.com -n 10 -l 100

Pinging Amazon.com [205.251.242.103] with 100 bytes of data:
Reply from 205.251.242.103: bytes=100 time=287ms TTL=211
Reply from 205.251.242.103: bytes=100 time=543ms TTL=211
Reply from 205.251.242.103: bytes=100 time=295ms TTL=211
Reply from 205.251.242.103: bytes=100 time=283ms TTL=211
Reply from 205.251.242.103: bytes=100 time=280ms TTL=211
Reply from 205.251.242.103: bytes=100 time=311ms TTL=211
Reply from 205.251.242.103: bytes=100 time=332ms TTL=211
Reply from 205.251.242.103: bytes=100 time=828ms TTL=211
Reply from 205.251.242.103: bytes=100 time=450ms TTL=211
Reply from 205.251.242.103: bytes=100 time=426ms TTL=211

Ping statistics for 205.251.242.103:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 280ms, Maximum = 828ms, Average = 403ms
```

All the requests in both the cases were received successfully and the average RTT slightly increased in case of larger packets being sent which could be justifiable as the larger the size of the message more resources would be needed at intermediate nodes and may result in overall time increase.

PART B

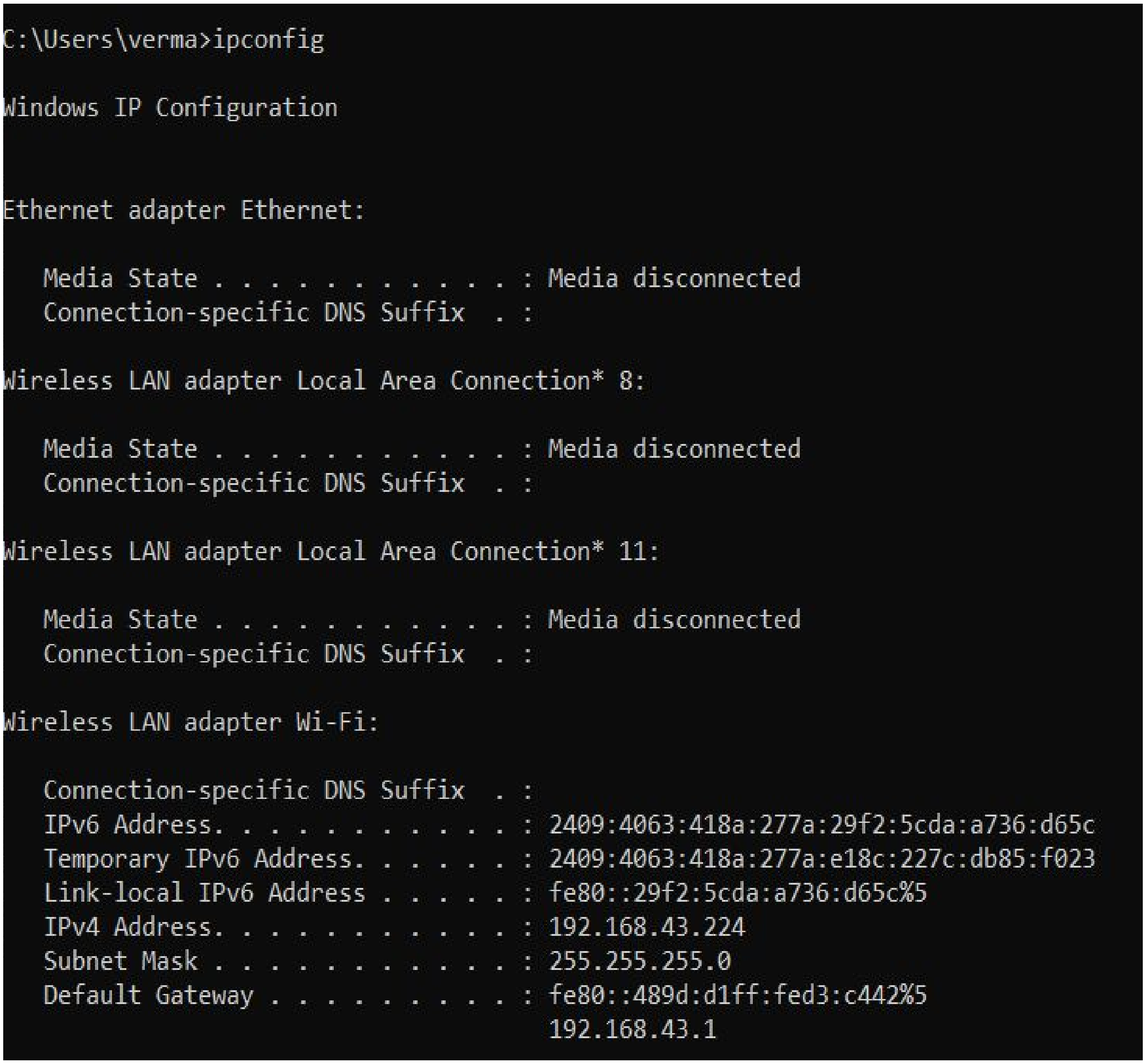
Ipconfig command

ipconfig stands for **Internet Protocol Configuration**. This command is used to list all the current TCP/IP network setting values of the computer. Ipconfig displays both the active and disabled network configurations for the host.
Thus, it is used to view, configure, and control the network connections in a computer. I have used two commands **ipconfig** and **ipconfig\all.**
TCP (Transmission Control Protocol) and **UDP** (User Datagram Protocol) are the most widely used Internet protocols through data is exchanged between applications.
TCP is connection-oriented and keeps a record of lost packets whereas **UDP** is a simpler, connectionless Internet protocol and no record of lost packets is there making it suitable for data exchange such as movies, streaming etc.TCP is slower as compared to UDP as it requires more resources as it keeps the record.
TCP eg include **HTTP** and UDP eg include **DNS**.
Ipconfig commands provide the IP address and all the TCP/IP networks along with their MAC addresses. The other command i.e. ipconfig\all provides additional information such as network establishment time and the host machine details.
Rest the output from both of them is same and the screenshots for both of them have been attached.
Both of them show the **IP address, the subnet mask** (used for identifying if a system is in the network or not as it breaks the IP address into host and networks address) and **gateway**(A gateway is a network node that forms a passage between two networks operating with different transmission protocols) details of the network being used.



```
IPv4 Address. . . . . . . . . . . : 192.168.43.224
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::489d:d1ff:fed3:c442%5
                                       192.168.43.1
```

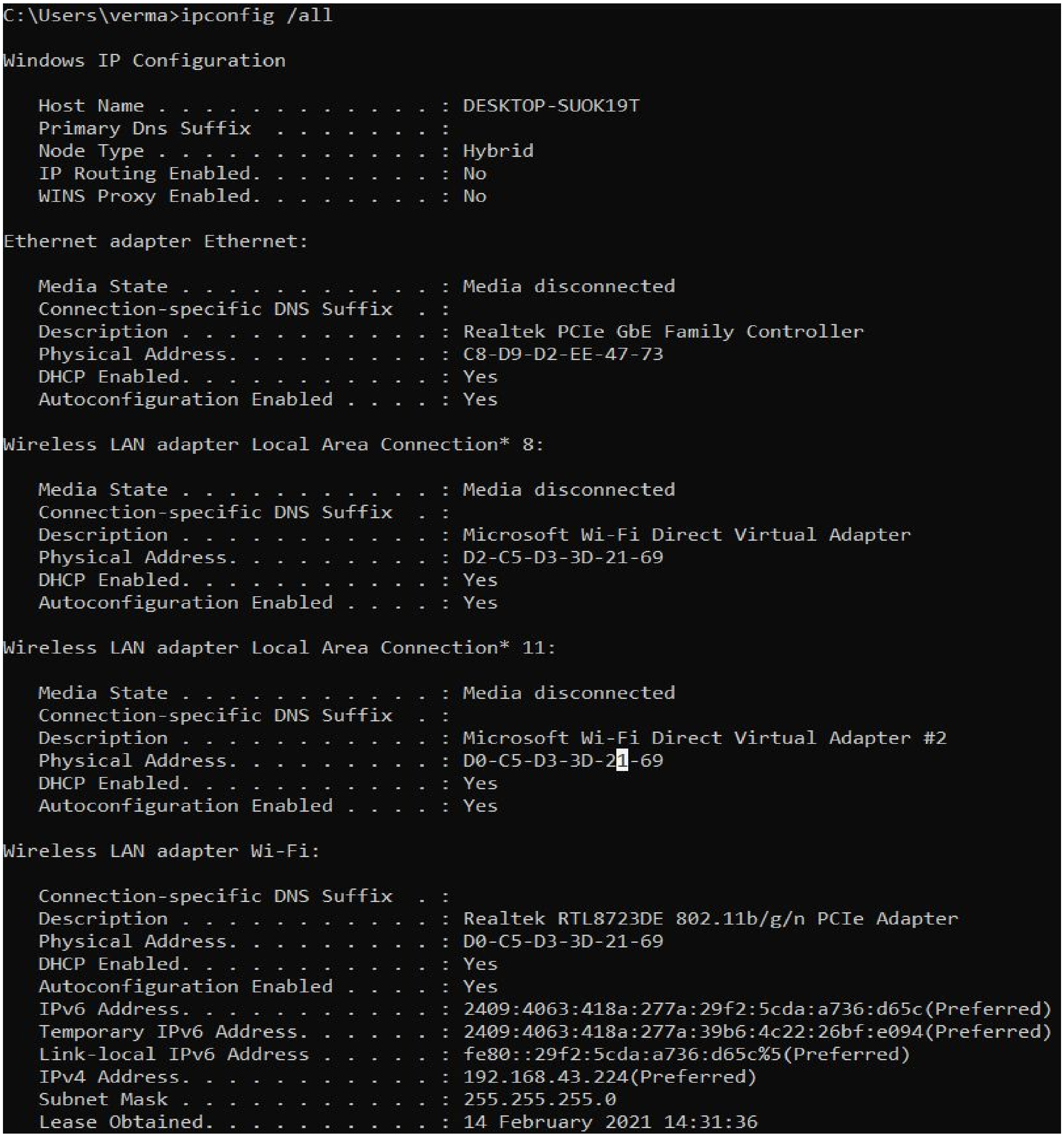
Both of these commands shows the various network configurations used by me to connect to the internet such as ethernet service and the 3 wireless LAN connections with one of the currently being active as my PC was connected to my internet through WIFI provided by my mobile and it lists the various network details of the same such as IP Address, Gateway.
A)Ipconfig command



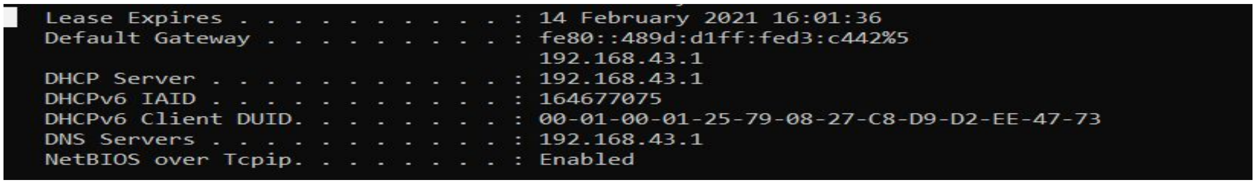
```
C:\Users\verma>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4063:418a:277a:29f2:5cda:a736:d65c
   Temporary IPv6 Address. . . . . . : 2409:4063:418a:277a:e18c:227c:db85:f023
   Link-local IPv6 Address . . . . . : fe80::29f2:5cda:a736:d65c%5
   IPv4 Address. . . . . . . . . . . : 192.168.43.224
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::489d:d1ff:fed3:c442%5
                                       192.168.43.1
```

B) Ipconfig /all

This commands also details all the network configurations for the system and provides details of the HOST system. This provides a vivid description of the network adapters.



```
C:\Users\verma>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-SUOK19T
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : C8-D9-D2-EE-47-73
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : D2-C5-D3-3D-21-69
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : D0-C5-D3-3D-21-69
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8723DE 802.11b/g/n PCIe Adapter
   Physical Address. . . . . . . . . : D0-C5-D3-3D-21-69
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2409:4063:418a:277a:29f2:5cda:a736:d65c(Preferred)
   Temporary IPv6 Address. . . . . . : 2409:4063:418a:277a:39b6:4c22:26bf:e094(Preferred)
   Link-local IPv6 Address . . . . . : fe80::29f2:5cda:a736:d65c%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.43.224(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 14 February 2021 14:31:36
```



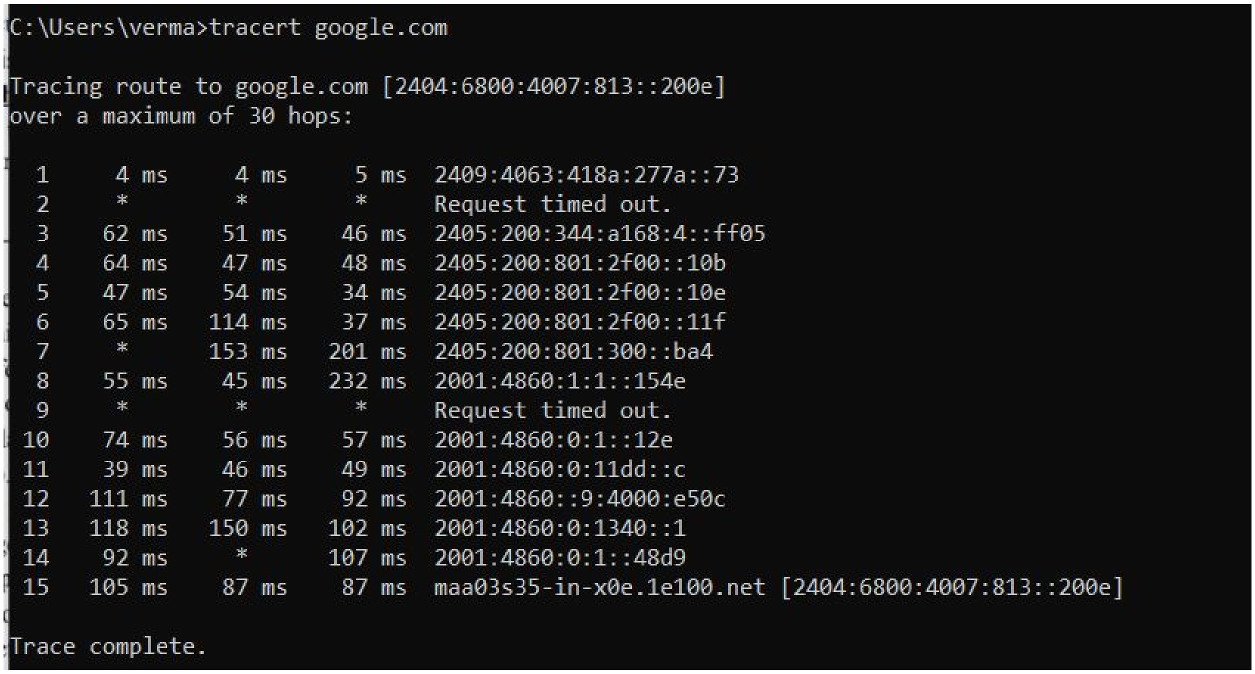
```
   Lease Expires . . . . . . . . . . : 14 February 2021 16:01:36
   Default Gateway . . . . . . . . . : fe80::489d:d1ff:fed3:c442%5
                                       192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DHCPv6 IAID . . . . . . . . . . . : 164677075
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-79-08-27-C8-D9-D2-EE-47-73
   DNS Servers . . . . . . . . . . . : 192.168.43.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

PART C

tracerrt command

This command helps us in knowing the path between the host and the server of request.
To achieve this the tracert command achieves this by sending a Request message from the host to the server with a TTL of 1 which increments by 1 on every subsequent transmission until the destination replies. The number of maximum nodes in the path is by default at 30.
The path is determined by examining the Time Exceeded messages returned by intermediate routers and the Reply message returned by the destination.
If some routers do not return the messages for packets and the time to live expires then these routers or nodes are not displayed in the path and are shown using (*) in the output.
Since the traceroute sends 3 different signal packets, each line contains the IP address of the hop, followed by three RTT values each for the 3 packets.

A) google.com

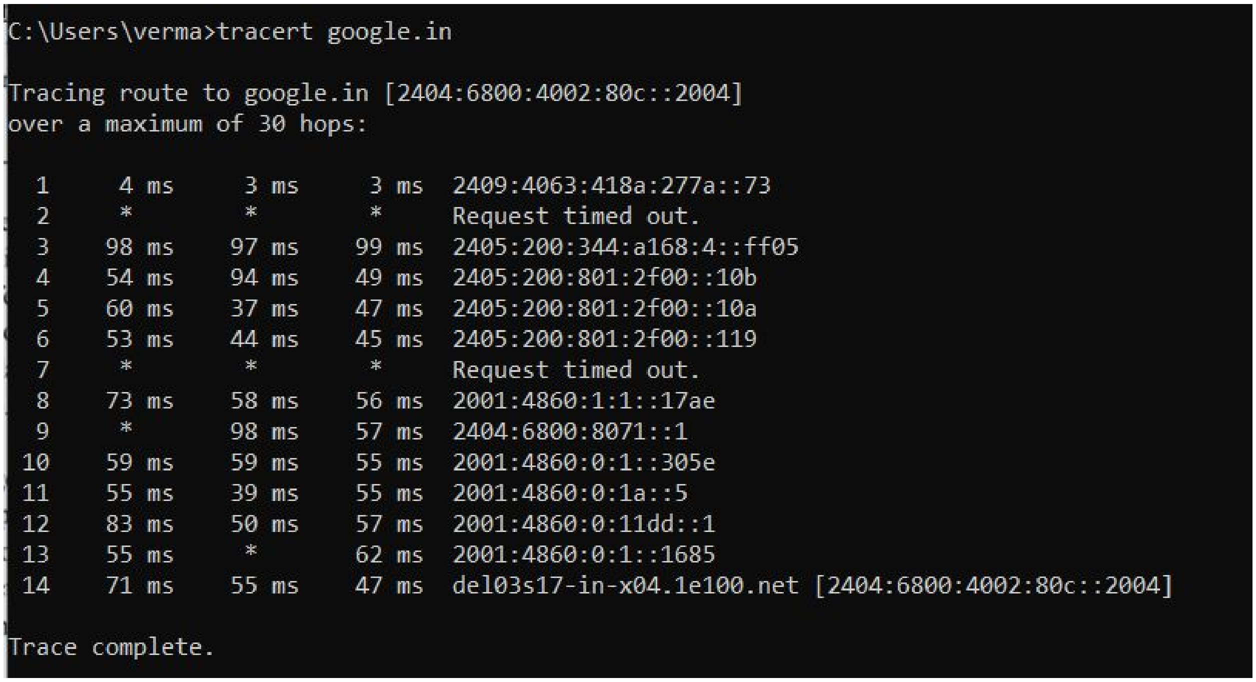


```
C:\Users\verma>tracert google.com

Tracing route to google.com [2404:6800:4007:813::200e]
over a maximum of 30 hops:

  1     4 ms     4 ms     5 ms  2409:4063:418a:277a::73
  2     *        *        *     Request timed out.
  3    62 ms    51 ms    46 ms  2405:200:344:a168:4::ff05
  4    64 ms    47 ms    48 ms  2405:200:801:2f00::10b
  5    47 ms    54 ms    34 ms  2405:200:801:2f00::10e
  6    65 ms   114 ms    37 ms  2405:200:801:2f00::11f
  7     *      153 ms   201 ms  2405:200:801:300::ba4
  8    55 ms    45 ms   232 ms  2001:4860:1:1::154e
  9     *        *        *     Request timed out.
 10    74 ms    56 ms    57 ms  2001:4860:0:1::12e
 11    39 ms    46 ms    49 ms  2001:4860:0:11dd::c
 12   111 ms    77 ms    92 ms  2001:4860::9:4000:e50c
 13   118 ms   150 ms   102 ms  2001:4860:0:1340::1
 14    92 ms     *      107 ms  2001:4860:0:1::48d9
 15   105 ms    87 ms    87 ms  maa03s35-in-x0e.1e100.net [2404:6800:4007:813::200e]

Trace complete.
```

The screenshot clearly shows all the middle nodes and the time elapsed and a few of them failed in returning in the time limit and are therefore omitted in the final output and shown as *.

The total number of hops done is 15.

B) google.in



```
C:\Users\verma>tracert google.in

Tracing route to google.in [2404:6800:4002:80c::2004]
over a maximum of 30 hops:

  1     4 ms     3 ms     3 ms  2409:4063:418a:277a::73
  2     *        *        *     Request timed out.
  3    98 ms    97 ms    99 ms  2405:200:344:a168:4::ff05
  4    54 ms    94 ms    49 ms  2405:200:801:2f00::10b
  5    60 ms    37 ms    47 ms  2405:200:801:2f00::10a
  6    53 ms    44 ms    45 ms  2405:200:801:2f00::119
  7     *        *        *     Request timed out.
  8    73 ms    58 ms    56 ms  2001:4860:1:1::17ae
  9     *       98 ms    57 ms  2404:6800:8071::1
 10    59 ms    59 ms    55 ms  2001:4860:0:1::305e
 11    55 ms    39 ms    55 ms  2001:4860:0:1a::5
 12    83 ms    50 ms    57 ms  2001:4860:0:11dd::1
 13    55 ms     *       62 ms  2001:4860:0:1::1685
 14    71 ms    55 ms    47 ms  del03s17-in-x04.1e100.net [2404:6800:4002:80c::2004]

Trace complete.
```

The total number of hops is 14.

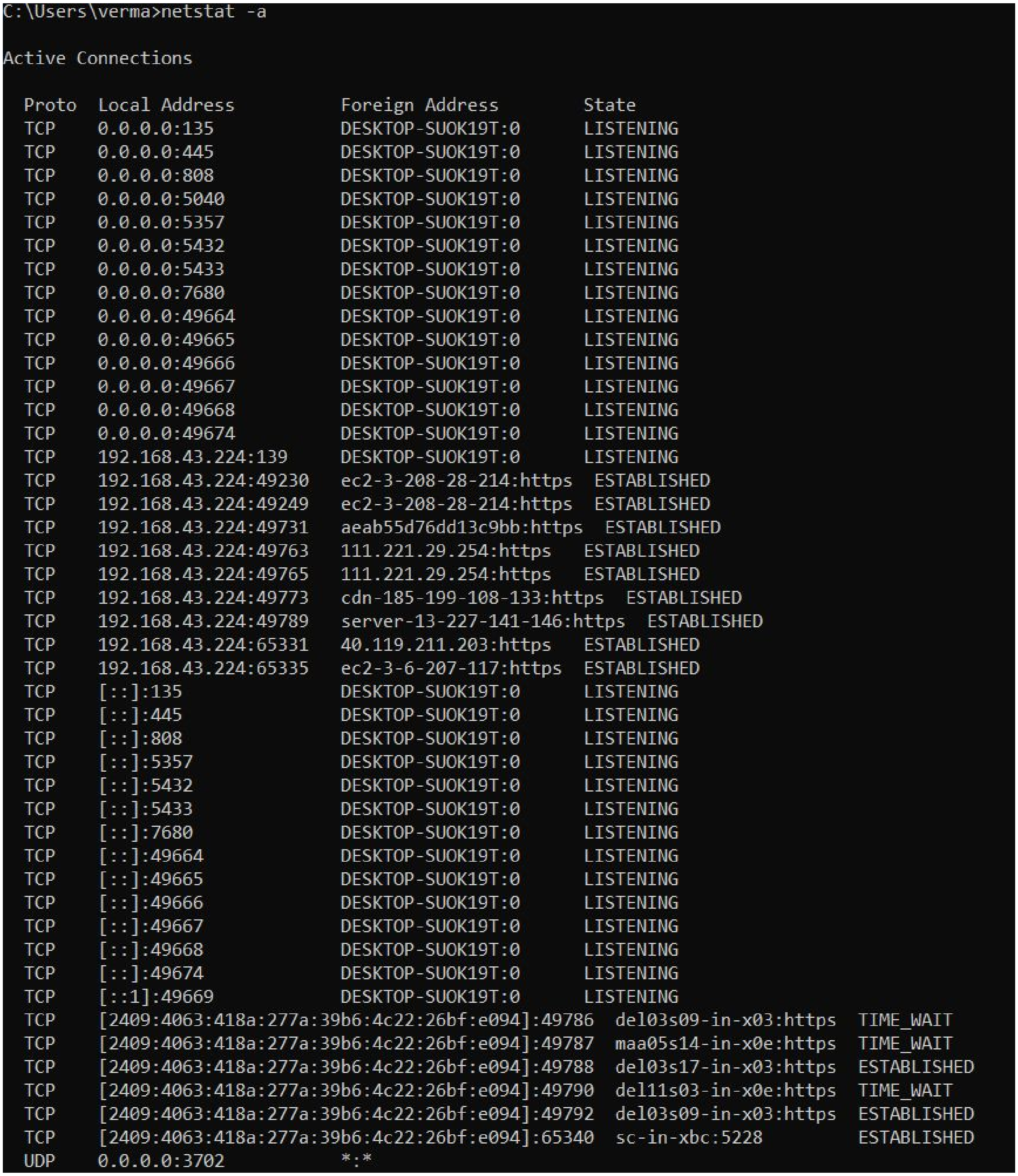
The path is shown in both the cases show that the initial hop is to the same node and thereafter they both differ as these both web addresses are provided by different servers.Google.com is the international version whereas google.in is the Indian one of the Google company and as such there are two different paths as shown in the screenshot. The total number of hops is also different showing that the way to connect them is different.

PART D

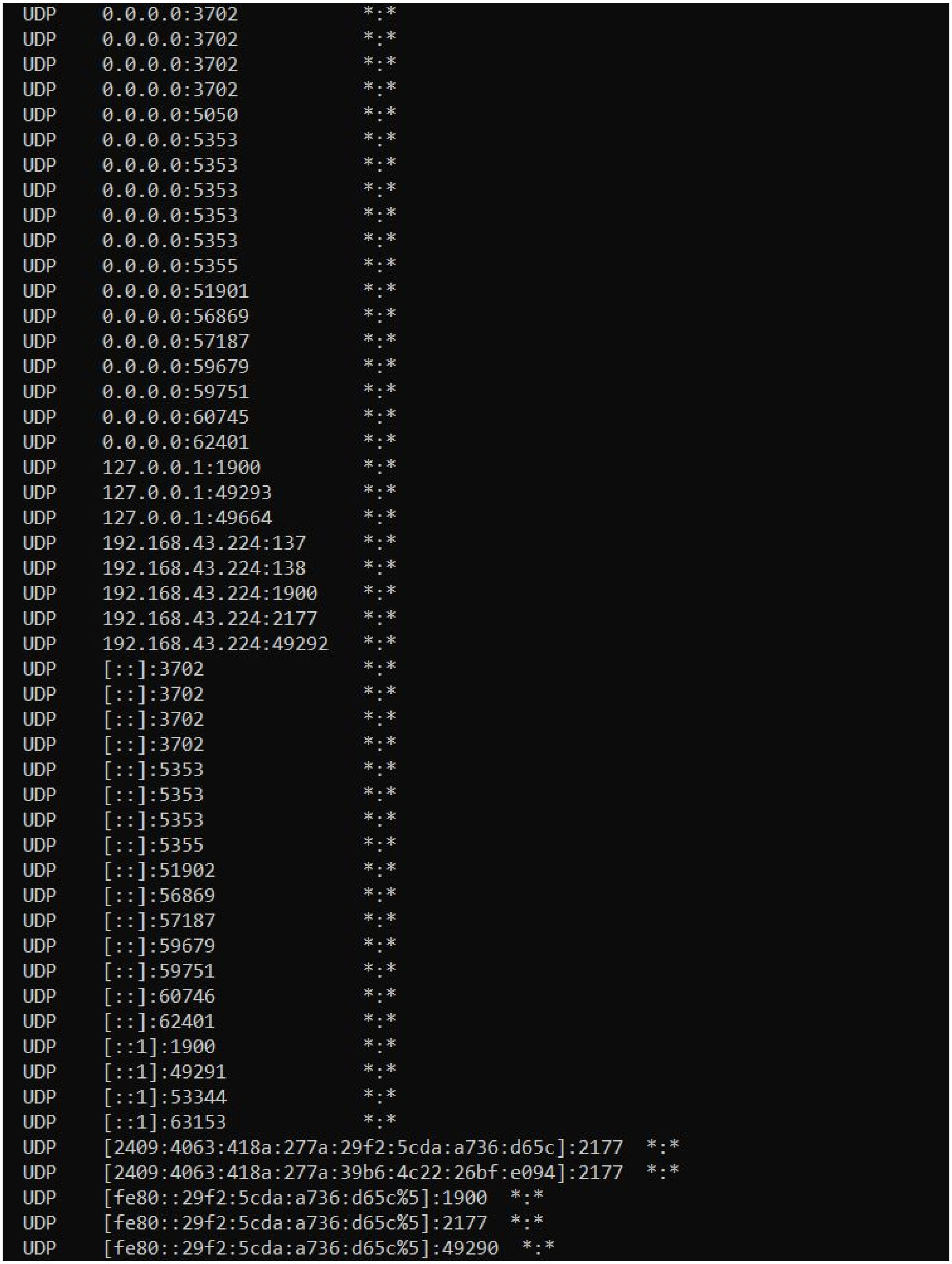
Netstat command

This command is used to show the active TCP connections, ports on which the computer is listening.TCP and UDP are defined above in the documents are the most common way of using the data exchange amongst the applications.

The screenshot attached shows all the listening UDP and TCP ports and the active TCP connections.



```
C:\Users\verma>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:808            DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:5432           DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:5433           DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-SUOK19T:0      LISTENING
  TCP    0.0.0.0:49674          DESKTOP-SUOK19T:0      LISTENING
  TCP    192.168.43.224:139     DESKTOP-SUOK19T:0      LISTENING
  TCP    192.168.43.224:49230   ec2-3-208-28-214:https  ESTABLISHED
  TCP    192.168.43.224:49249   ec2-3-208-28-214:https  ESTABLISHED
  TCP    192.168.43.224:49731   aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.43.224:49763   111.221.29.254:https   ESTABLISHED
  TCP    192.168.43.224:49765   111.221.29.254:https   ESTABLISHED
  TCP    192.168.43.224:49773   cdn-185-199-108-133:https  ESTABLISHED
  TCP    192.168.43.224:49789   server-13-227-141-146:https  ESTABLISHED
  TCP    192.168.43.224:65331   40.119.211.203:https   ESTABLISHED
  TCP    192.168.43.224:65335   ec2-3-6-207-117:https  ESTABLISHED
  TCP    [::]:135               DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:445               DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:808               DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:5357              DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:5432              DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:5433              DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:7680              DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49664             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49665             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49666             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49667             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49668             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::]:49674             DESKTOP-SUOK19T:0      LISTENING
  TCP    [::1]:49669            DESKTOP-SUOK19T:0      LISTENING
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:49786  del03s09-in-x03:https  TIME_WAIT
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:49787  maa05s14-in-x0e:https  TIME_WAIT
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:49788  del03s17-in-x03:https  ESTABLISHED
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:49790  del11s03-in-x0e:https  TIME_WAIT
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:49792  del03s09-in-x03:https  ESTABLISHED
  TCP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:65340  sc-in-xbc:5228         ESTABLISHED
  UDP    0.0.0.0:3702           *:*
```



```
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:51901          *:*
  UDP    0.0.0.0:56869          *:*
  UDP    0.0.0.0:57187          *:*
  UDP    0.0.0.0:59679          *:*
  UDP    0.0.0.0:59751          *:*
  UDP    0.0.0.0:60745          *:*
  UDP    0.0.0.0:62401          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49293        *:*
  UDP    127.0.0.1:49664        *:*
  UDP    192.168.43.224:137     *:*
  UDP    192.168.43.224:138     *:*
  UDP    192.168.43.224:1900    *:*
  UDP    192.168.43.224:2177    *:*
  UDP    192.168.43.224:49292   *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:51902             *:*
  UDP    [::]:56869             *:*
  UDP    [::]:57187             *:*
  UDP    [::]:59679             *:*
  UDP    [::]:59751             *:*
  UDP    [::]:60746             *:*
  UDP    [::]:62401             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:49291            *:*
  UDP    [::1]:53344            *:*
  UDP    [::1]:63153            *:*
  UDP    [2409:4063:418a:277a:29f2:5cda:a736:d65c]:2177  *:*
  UDP    [2409:4063:418a:277a:39b6:4c22:26bf:e094]:2177  *:*
  UDP    [fe80::29f2:5cda:a736:d65c%5]:1900  *:*
  UDP    [fe80::29f2:5cda:a736:d65c%5]:2177  *:*
  UDP    [fe80::29f2:5cda:a736:d65c%5]:49290  *:*
```

Question 2

For this question the files have been submitted and here are the screenshots of the various topologies.

Cisco Packet Tracer was used for the same.

Sample message simulation was also done and the result of the same can be seen in the screenshot.

For the same, I had first created the topology of interest by using Switches(Its a connecting device which is used to create networks and filters data before sending) and PC and had to assign every PC with a unique IP address (IP address are provided by the ISP and are unique and can be used to identify a system uniquely in a network.)Then I sent a message from 1 system to another to see if the message was successfully transferred and acknowledged by the switches.

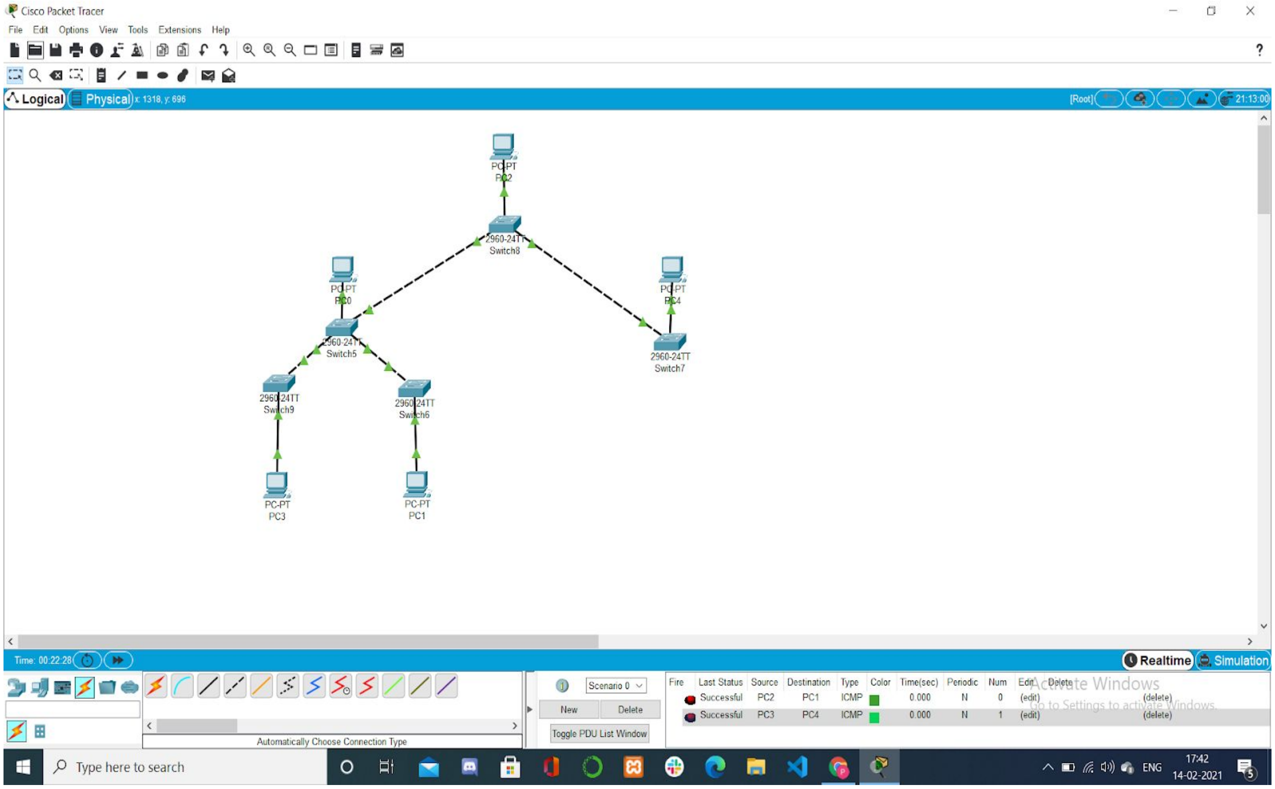
The three topologies taken were:

WAN:: Wide Area Network e.g. country

MAN:: Metropolitan Area Network e.g. city

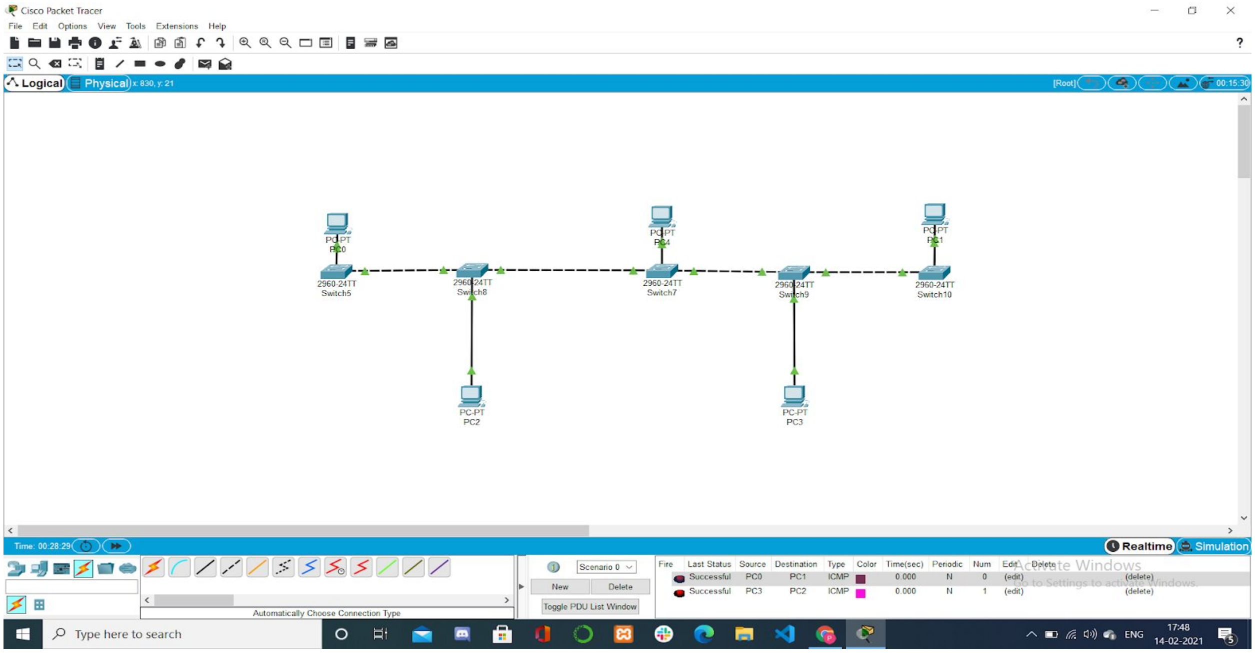
LAN:: Local Area Network e.g. hostels

A)Tree (used in WAN)



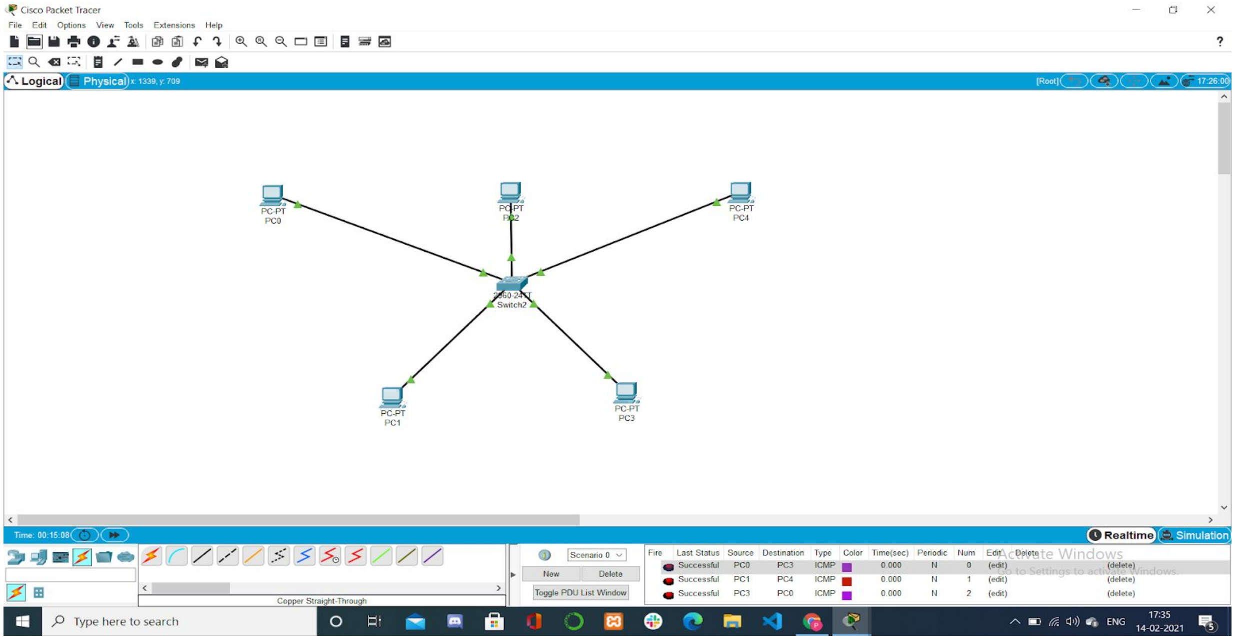
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC2	PC1	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	Successful	PC3	PC4	ICMP	🟩	0.000	N	1	(edit)	(delete)

B) BUS topology(used in MAN)



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	PC3	PC2	ICMP	■	0.000	N	1	(edit)	(delete)

C) Star topology (used in LAN)



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC3	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	PC1	PC4	ICMP	■	0.000	N	1	(edit)	(delete)
●	Successful	PC3	PC0	ICMP	■	0.000	N	2	(edit)	(delete)

References:

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/commands-by-server-role

https://www.netacad.com/courses/packet-tracer