Faculty of Engineering and Technology

Electrical and Computer Engineering Department

Computer Network

ENCS3320

Project No. 2

Student's Name: Aseel Deek.	**ID:** 1190587.	**Sec**: 4.
Student's Name: Lojain Abdalrazaq**.**	**ID:** 1190707.	**Sec**: 4.
Student's Name: Eman Maraita**.**	**ID:** 1190768.	**Sec**: 4.

Instructor:

Dr. Imad Tartir.

15th Jan 2022

Abstract

The aim of this project is to be familiar with network protocols such as DHCP, ICMP and TCP protocols, to capture few packets for each protocol, and to understand the basic idea for each one of them, all of this will be done using Wireshark software. Then to learn a lot about network connections, which will be using network components such as switches, routers and hosts (end systems), and the connection will be using Packet tracer software.

Table of contents

Introduction

- ## Network protocols

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.[1]

- ## Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.[2]

- ## Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks. [3]

- ## Transmission Control Protocol (TCP)

A connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network. It is the most common protocol in networks that use the Internet Protocol (IP); together they are sometimes referred to as TCP/IP. TCP takes messages from an application/server and divides them into packets, which can then be forwarded by the devices in the network – switches, routers, security gateways – to the destination. TCP numbers each packet and reassembles them prior to handing them off to the application/server recipient. Because it is connection-oriented, it ensures a connection is established and maintained until the exchange between the application/servers sending and receiving the message is complete. [4]

Procedure

▪ Part 1: Wireshark network protocol analyzer

The First Question asked to capture few DCHP and ICMP packets and explain at least three fields of each packets using Wireshark. Also required capturing a TCP session for transferring a large file, show the sequence number of three packets, their ACK numbers and the data size on two packets.

1) Dynamic Host Configuration Protocol (DHCP):

To capture the **DHCP** packets, two commands were implemented in the command prompt. The first one is the **ipconfig /release**, this command requests to release the old IP address, make the client IP-address (**0.0.0.0).** And the second command is the **ipconfig/renew** command that requests the **DHCP** server for another IP address for the client.

After implementing the two commands in the cmd, while the Wireshark is opened, the Wireshark captures the **DHCP packets**. Using the filter option in the Wireshark, the following figure 1.1 shows the **DHCP packets only** when writing **dhcp** as a filter.

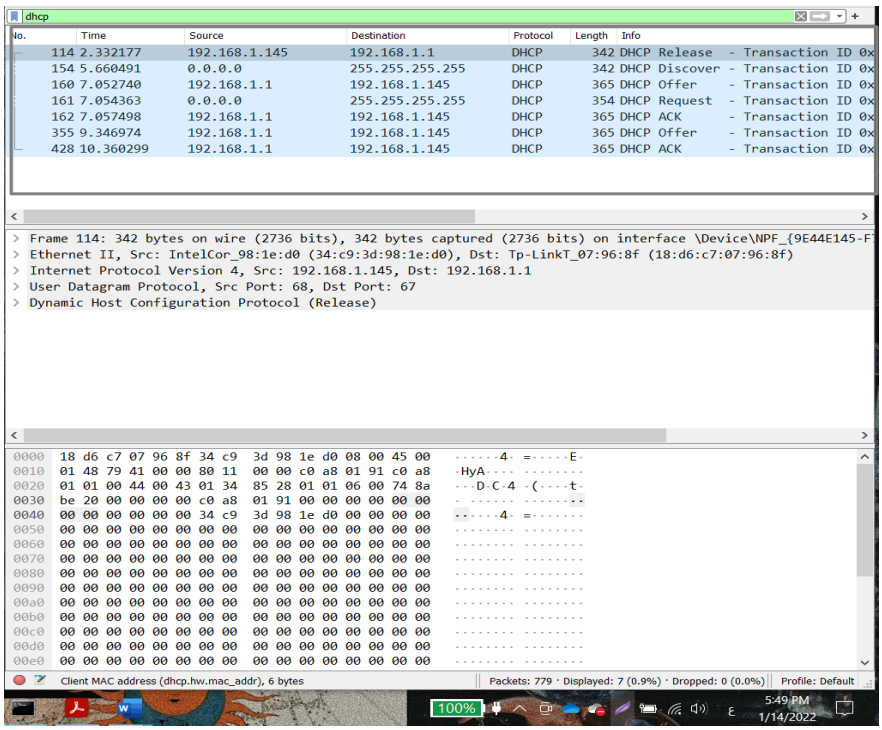

Figure1. 1 (shows the DHCP packets from Wireshark capturing)

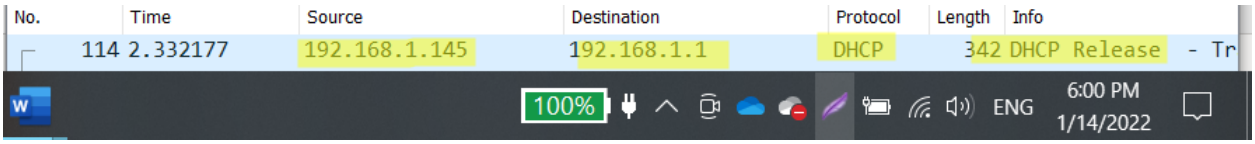

Figure1. 2 (the DHCP release packet)

The heighted packet in figure (1.2) is the **DHCP Release packet.** It was sent when the command **ipconfig /release** was written in the cmd. Here, the client computer (my computer) trying to find a **DHCP** server telling it to release its current IP address (release the 192.168.1.145 IP address).

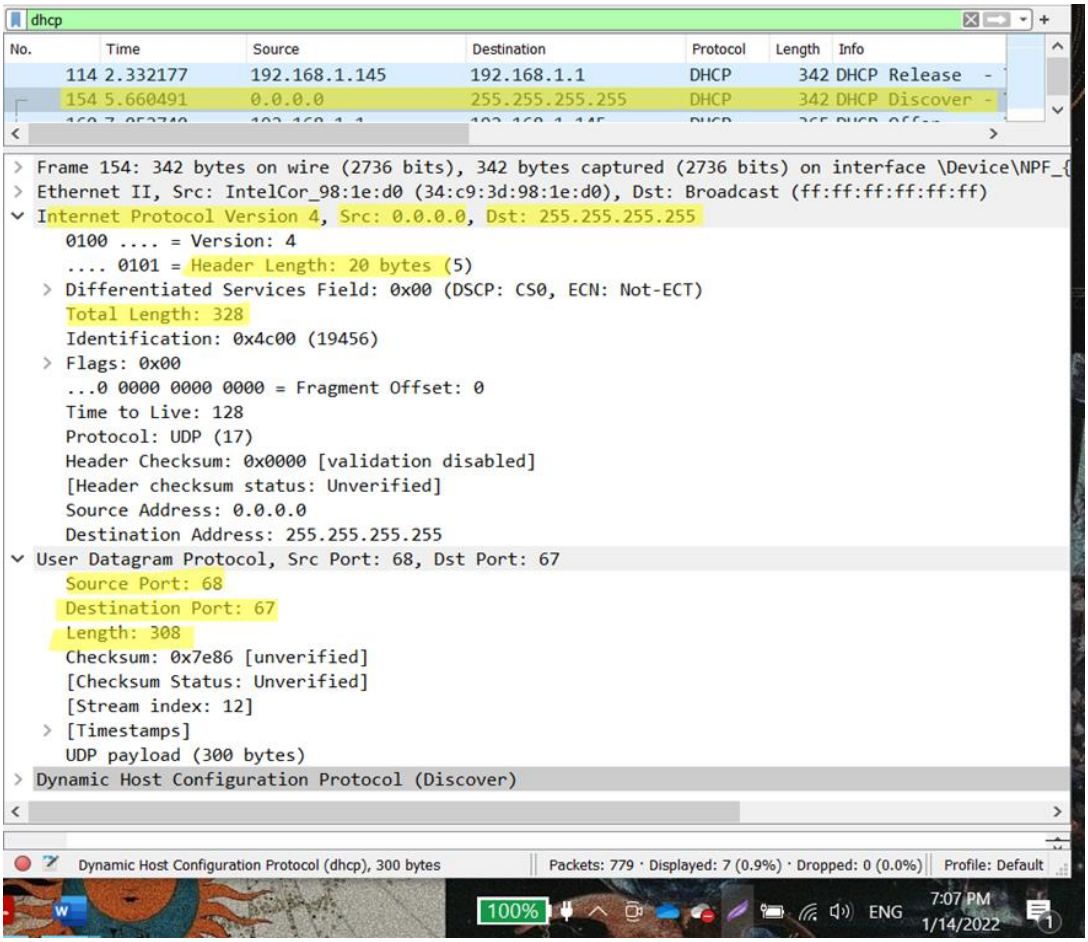

Figure1. 3 (shows information of the DHCP Discover packet)

The second Packet is the **DHCP Discover packet, this** packet requests a message from the client to the DHCP server asking for a new IP address after the new source IP now equals **0.0.0.0**. (The client has no IP-address). The **destination IP address** is the broadcast address **255.255.255.255** as shown in figure (1.3). The **UDP port for the source** is **68** and for the **destination,** the **UDP port** is **67** (for the DHCP server). Note that IP address version is **IPV 4**, the total length is equals **328**, the header length is **20** bytes and it's **time to live is 128** routers to travel through.

2) Internet Control Message Protocol (ICMP):

ICMP is used to check the reachability of a host router in a network. Ping and tracerout use ICMP echo request and ICMP echo reply messages to check whether the destination host is reachable or not. To capture ICMP packets, the device was connected to the internet and the Ping command ***ping ritaj.birzeit.edu*** was implemented in the cmd. The Ping command in the source host sends an ICMP packet to the target IP destination which is **Ritaj** site, and the ping in the target IP destination responds by sending an ICMP packet back to the source host. The following figure (Figure2.1) represents the output of running the ping command, it is noticed that the number of ICMP sent packets is 4, while the number of received ICMP packets is 4, 8 packets in total.

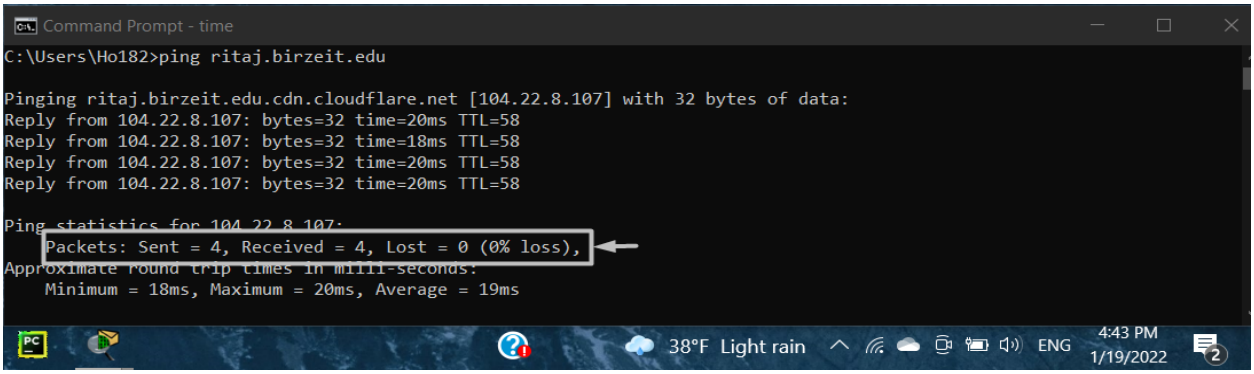

*Figure2. 1 (cmd after implementing ping **ritaj.birzeit.edu**.)*

After implementing the Ping command in the cmd, the Wireshark is opened, and the **'ICMP'** protocol has been entered into the filter display. From the following figure (Figure2.2), it is noticed that the total number of packets is 8 ICMP packets, 4 ping requests sent by this PC which is the source with IP address ***(192.168.1.7),*** and 4 Ping responses received from the destination which is Ritaj site with IP address ***(104.22.8.107).***

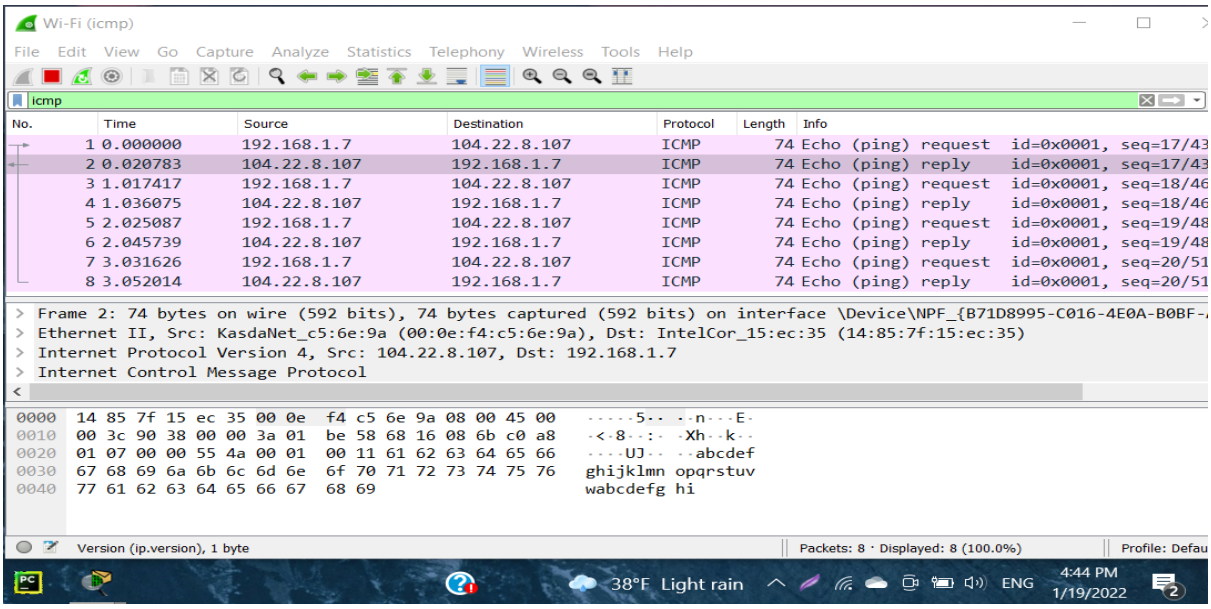

*Figure2. 2(Wireshark output with Ping command **ritaj.birzeit.edu.**)*

The following figure (Figure2.3) represents the first packet sent by the PC (client), this packet is **the *ICMP request packet***. The packet contents area provides information about this packet, it is noticed that the source IP address ***(192.168.1.7)*** while the destination address is Ritaj IP address ***(104.22.8.107)*** which means that the packet sent by the client, with **version 4 of Internet Protocol Addressing**, and 20 bytes **header length**.

In addition, this ICMP request packet **Time to Live (TTL)** is 128 which means that the packet can travel and move through 128 routers before being discarded by the device and the **checksum** with 0x4d4a [correct] which means that there is no error in the received packets.

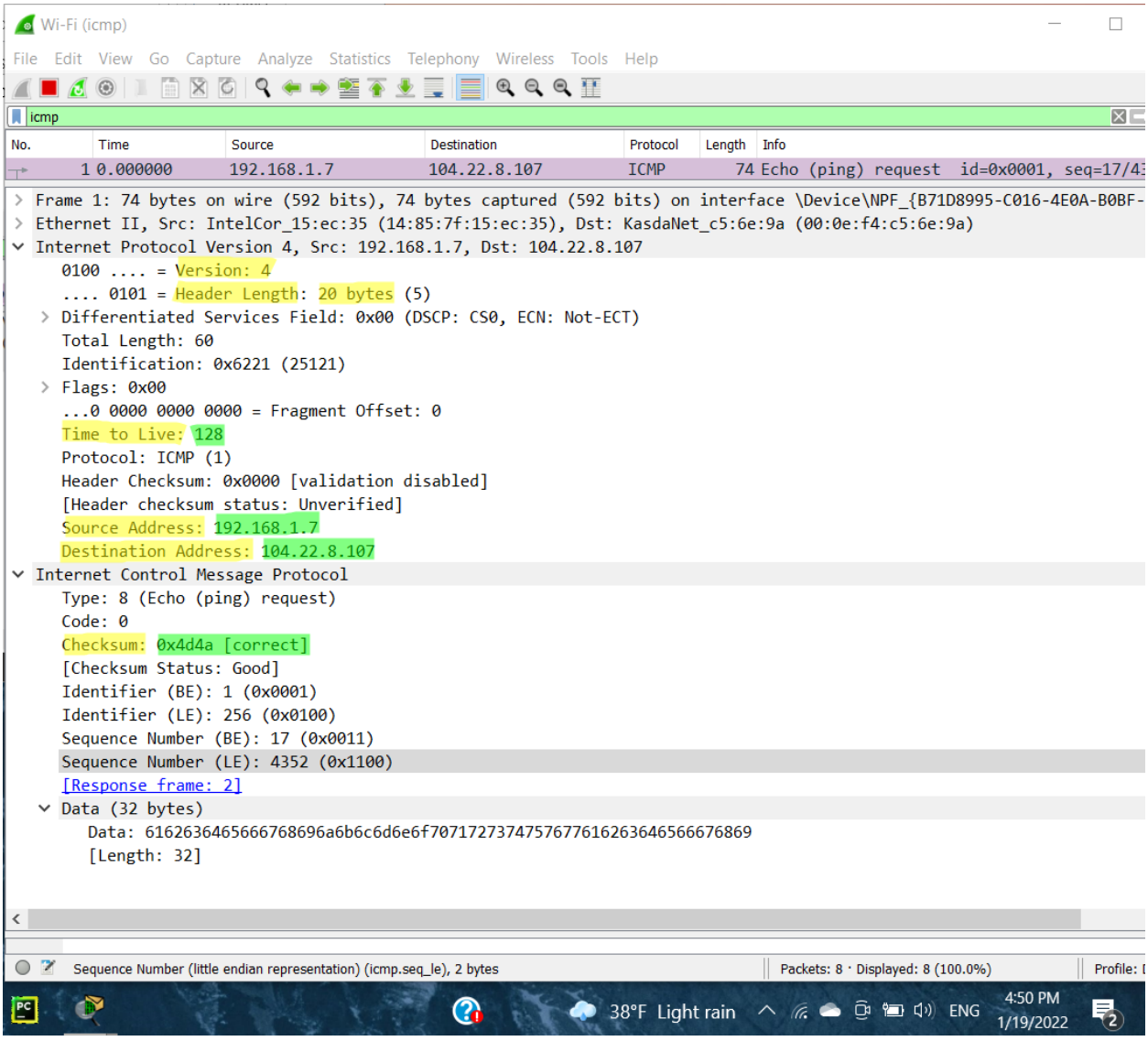

Figure2. 3 (Wireshark capture of the first ICMP Packet.)

The second packet is sent by the source address which is Ritaj site with IP address ***(104.22.8.107)*** and the destination is this PC with IP address ***(192.186.1.7)*** as shown in the figure (Figure2.4) below, this is the ICMP reply packet, with 20 bytes **Header Length** and **version 4 of Internet Protocol Addressing,** the same as the ICMP request packet, while the **Time to Live (TTL)** for this packet is 58.

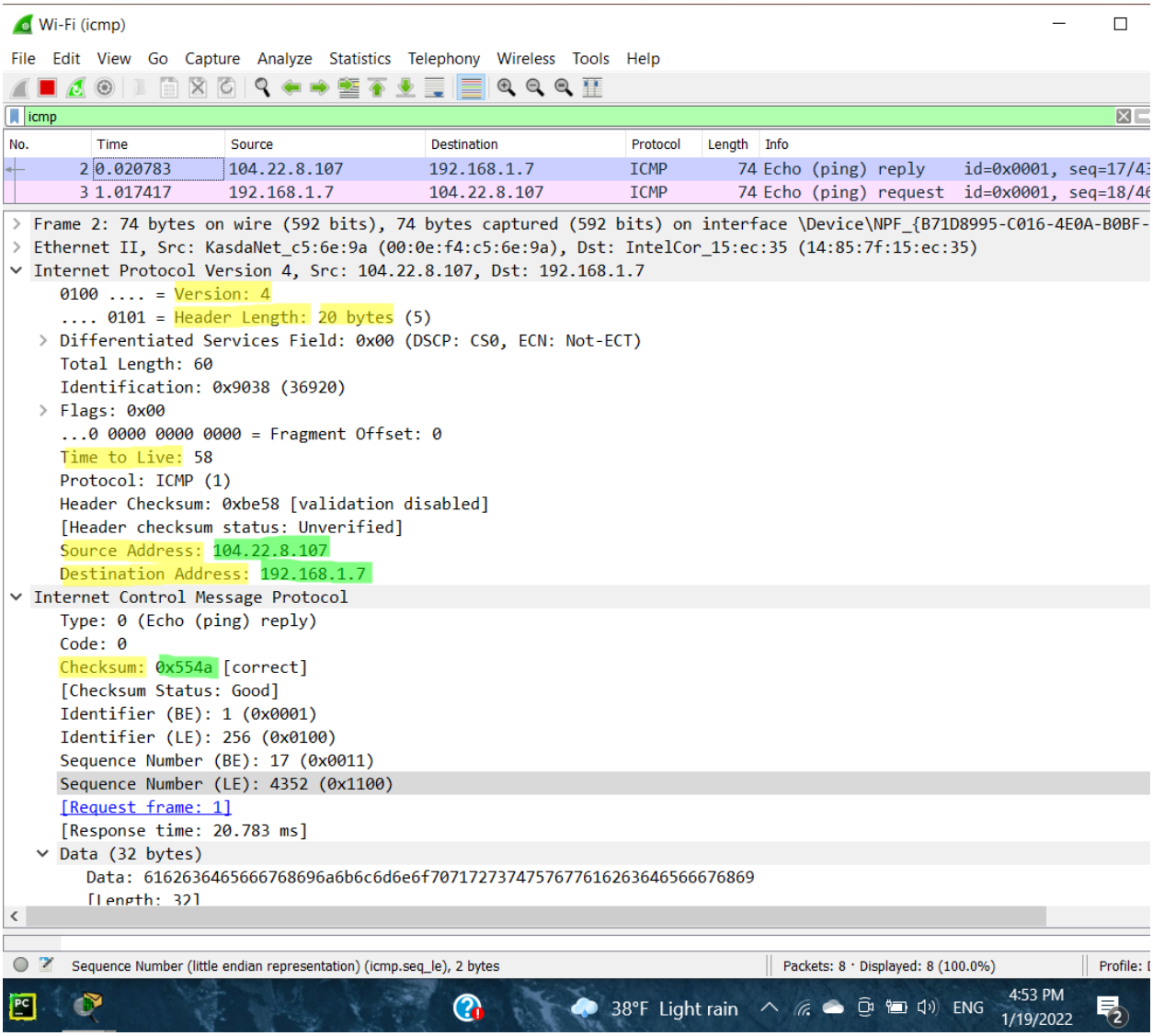

Figure2. 4 (Wireshark capture of the second ICMP Packet).

3) Transmission Control Protocol (TCP)

In order to capture a TCP session for transferring a large file, a large file is sent form the computer with IP address 192.168.1.10 to someone using Ritaj site, which have an IP address 104.22.9.107, when sending the file, the Wireshark is open to capture the TCP transmission session, as showing below:

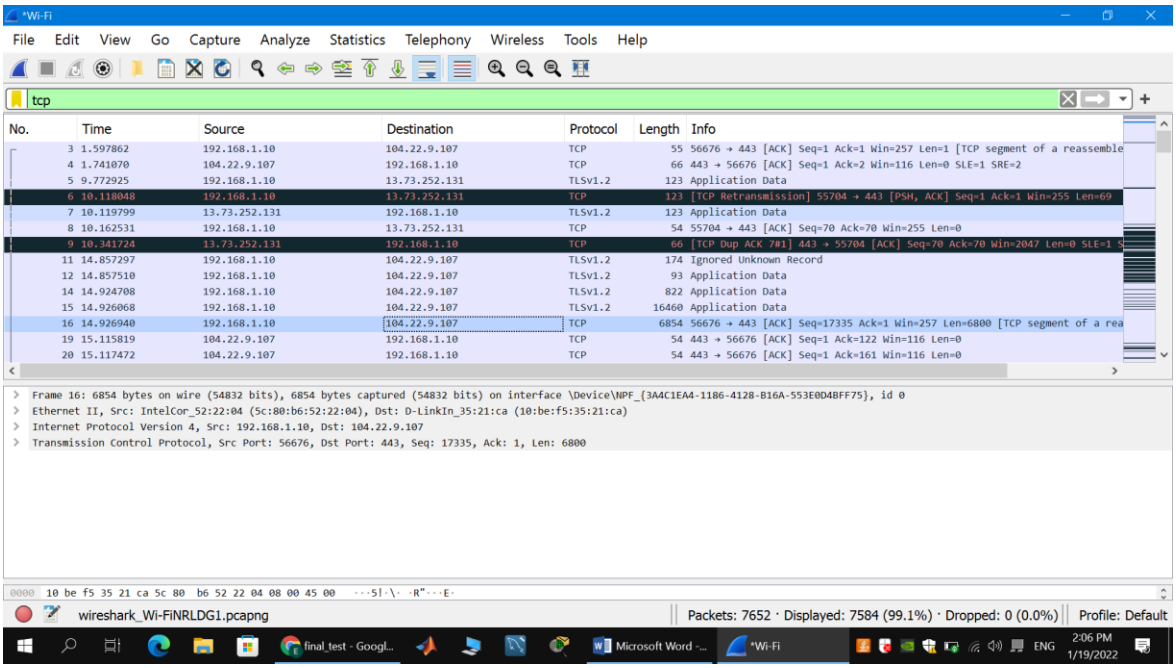

Figure3. 1 (TCP transmission packets)

This is the start of transmission operation, the **first packet** is described below:

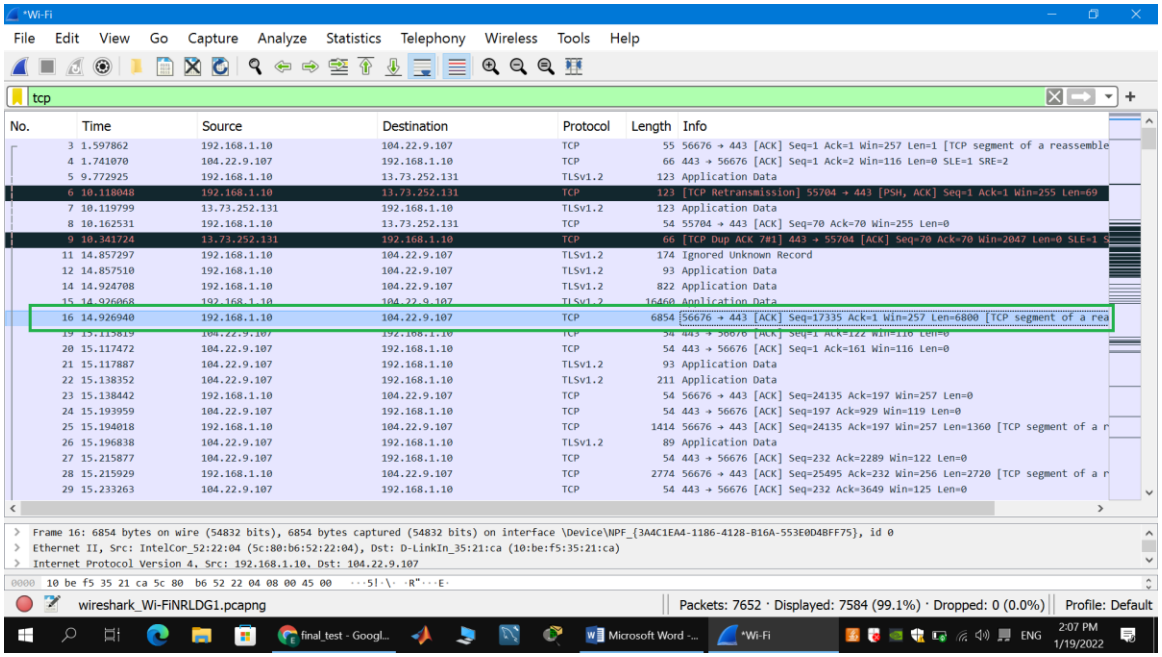

Figure3. 2 (first TCP packet)

This is the first packet sent with TCP protocol, as can see, the **sequence number is 17335**, and the **acknowledgment number is 1**, the information about sending this packet is as below:

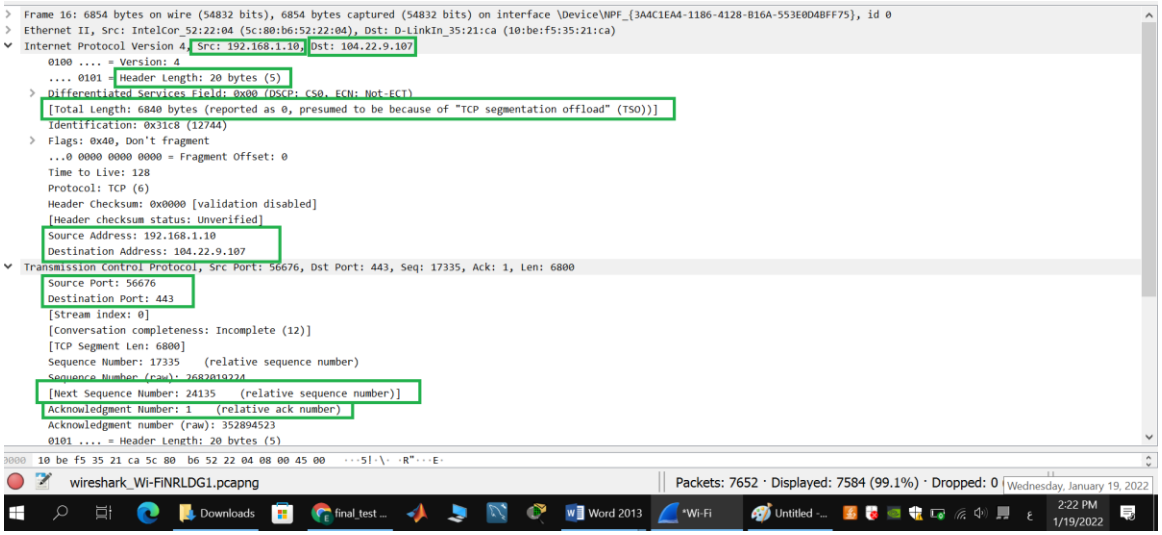

Figure3. 3 (first TCP packet information)

This is to show that the internet protocol version used is IPv4, and to show the source and destination IP addresses, which they are the IP address for the sending device (in this case a laptop) and the destination, which is a site called retag. The header length is 20 bytes, and the total length of the packet is 6840 bytes, so that to find the data size for this packet, the header

length is subtracted from the total length, which will give **6820 bytes as a data size**. The next expected sequence number is shown as 24135.

The **second packet** with sequence number 24135 is as shown below:

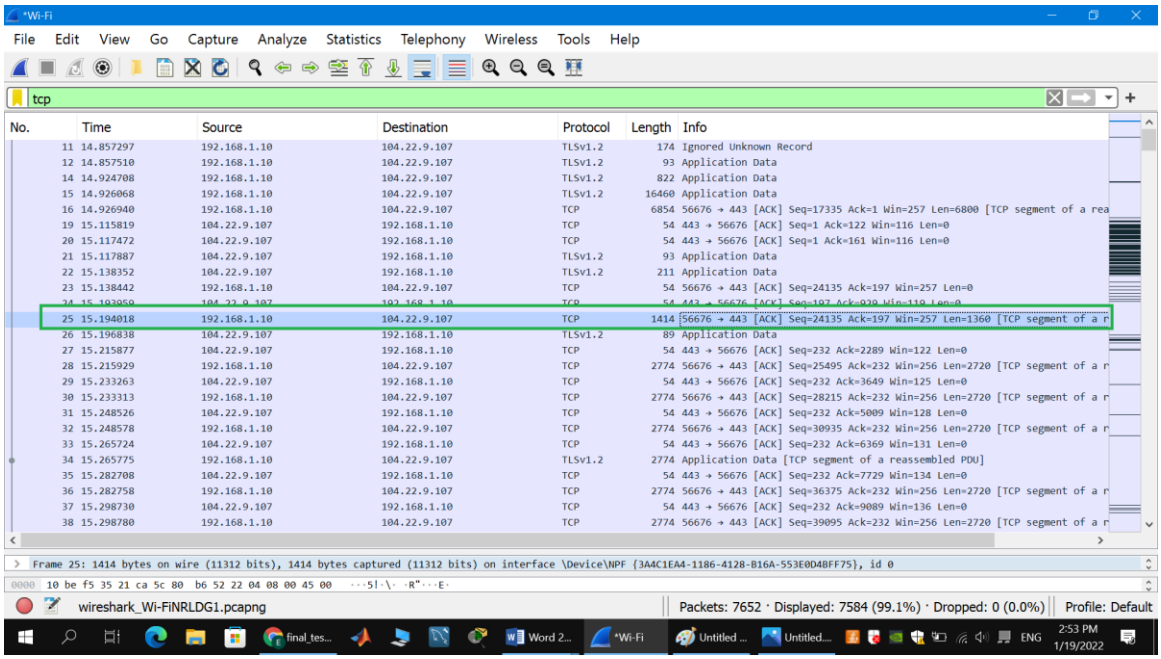

Figure3. 4 (second TCP packet)

The **sequence number is 24135**, and **the acknowledgment number is 197**, the information about sending this packet is as below:

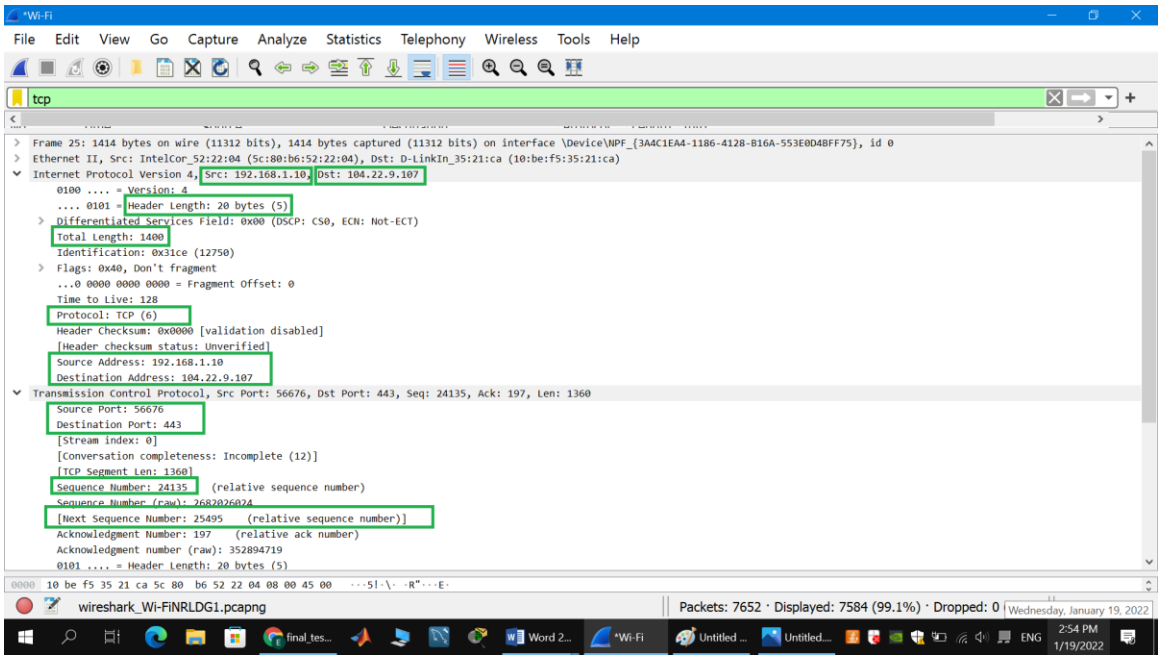

Figure3. 5 (second TCP packet information)

As the previous packet, the internet protocol version used is IPv4, and the source and destination IP address are the same. The header length is 20 bytes, and the total length of the packet is 1400 bytes, so as the previous packet, the **data size is 1400 – 20 = 1380 bytes**. The next expected sequence number is shown as 25495.

The **third packet** with sequence number 25495 is as shown below:

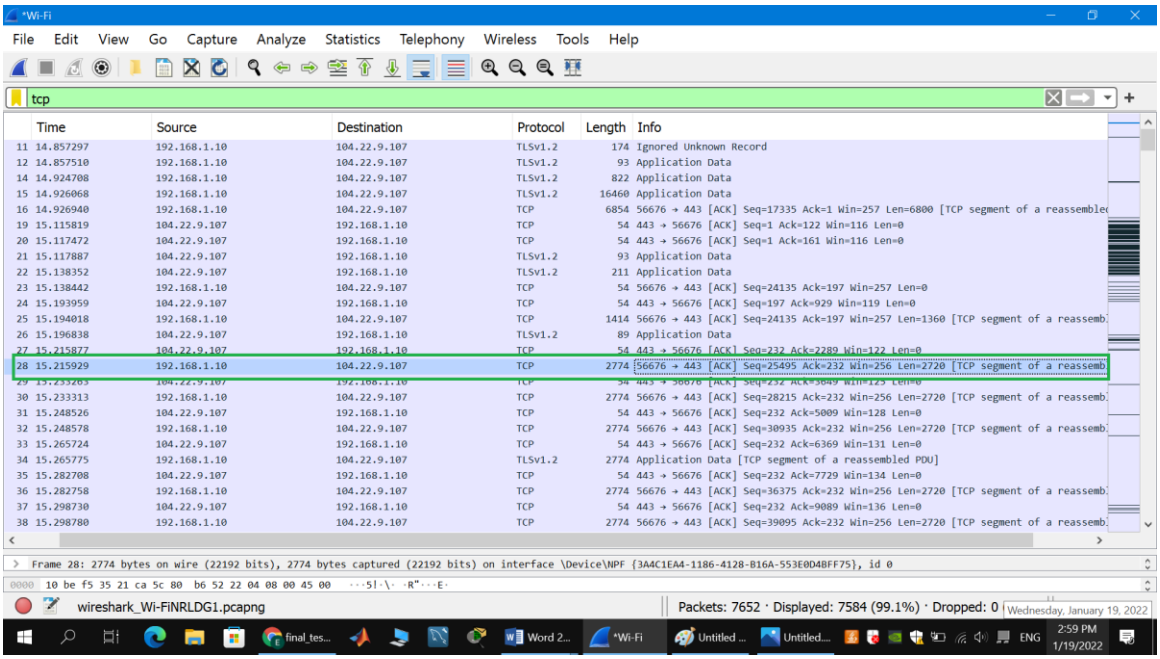

Figure3. 6 (third TCP packet)

The **sequence number is 25495**, and the **acknowledgment number is 232**, the information about sending this packet is as below:

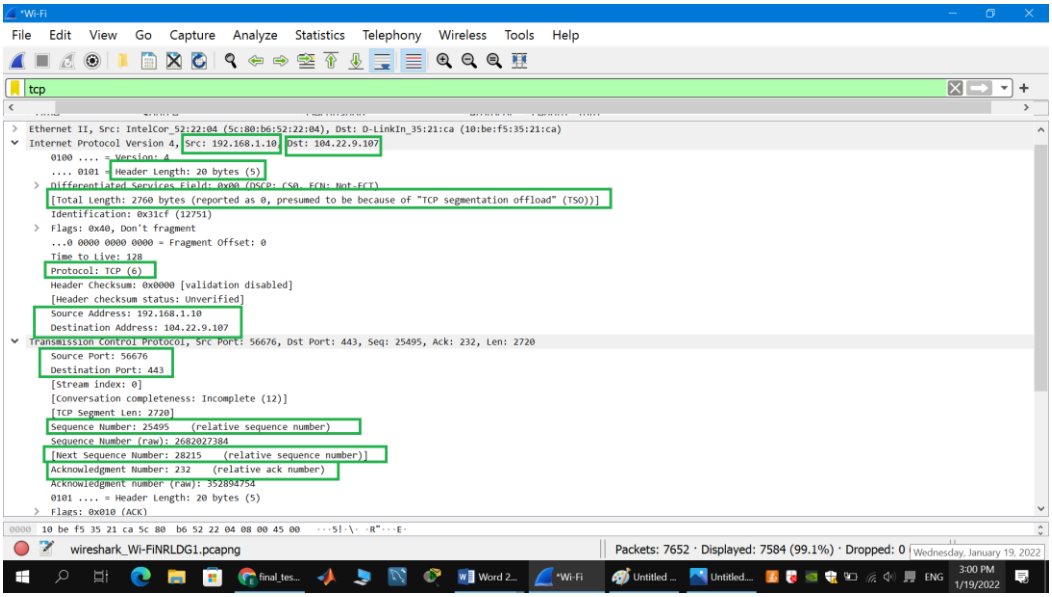

Figure3. 7 (third TCP packet information)

This is to show that the internet protocol version used is IPv4, and to show the source and destination IP addresses, which they are the IP address for the sending device (in this case a laptop) and the destination is a site called Ritaj, also the header length is 20 bytes, and the total length of the packet is 2760 bytes, so as the previous packet, **the data size is 2760 – 20 = 2740** bytes. The next expected sequence number is shown as 28215.

▪ Part 2: Cisco Packet Tracer

Question two required to implement a network topology and implement some operation on this network. Also, this question asked for using specific IP addressing criteria. The new IP addresses of the routers and PCs should be from a student ID number. In this project, the ID was used Is ***1190587***, and here are the new IPs for all routers and PCs in the required Question.

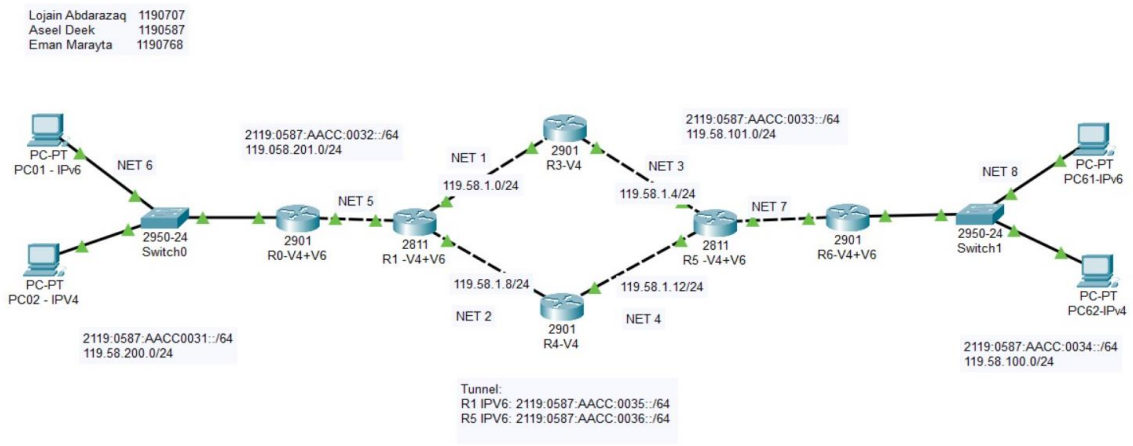

Figure2. 5 (network implementation)

1. **For the PC01 & PC02:**
   - ✓ *IPv4:* 192.168.200.2/24 → **119.58.200.2 /24**
   - ✓ *IPv6:* 2001:0DB8:AACC:0031::2 / 64 → **2119:0587:AACC:0031::2 /64**

2. For R0:

- ✓ *IPv4:* 192.168.201.1 /30 → **119.58.201.1 /30**
- ✓ *IPv4:* 192.168.200.1/24 → **119.58.200.1/24**
- ✓ *IPv6:* 2001:0DB8:AACC:0031::1 /64 → **2119:0587:AACC:0031::1 /64**
- ✓ *IPv6:* 2001:0DB8:AACC:0032::1 /64 → **2119:0587:AACC:0032::1 /64**

3. For R1:

- ✓ *IPv4:* 192.168.201.2/30 → **119.58.201.2 /30**
- ✓ *IPv4:* 192.168.1.9 /30 → **119.58.1.9/30**
- ✓ *IPv4:* 192.168.1.2/30 → **119.58.1.2 /30**
- ✓ *IPv6:* 2001:0DB8:AACC:0032::2 /64 → **2119:0587:AACC:0032::2 /64**
- ✓ *IPv6:* 2001:0DB8:AACC:0035::1 /64 → **2119:0587:AACC:0035::1 /64**

4. For R3:

- ✓ *IPv4:* 192.168.1.6/30 → **119.58.1.6 /30**
- ✓ *IPv4:* 192.168.1.1/30 → **119.58.1.1 /30**

5. For R4:

- ✓ *IPv4:* 192.168.1.14/30 → **119.58.1.14/30**
- ✓ *IPv4:* 192.168.1.10/30 → **119.58.1.10/30**

6. For R5:

- ✓ *IPv4:* 192.168.101.2/30 → **119.58.101.2 /30**
- ✓ *IPv4:* 192.168.1.5/30 → **119.58.1.5 /30**
- ✓ *IPv4:* 192.168.1.13/30 → **119.58.1.13 /30**
- ✓ *IPv6:* 2001:0DB8:AACC:0036::1 /64 → **2119:0587:AACC:0036::1 /64**
- ✓ *IPv6:* 2001:0DB8:AACC:0033::2 /64 → **2119:0587:AACC:0033::1 /64**

7. For R6:

- ✓ *IPv4:* 192.168.101.1/30 → **119.58.101.1/30**
- ✓ *IPv4:* 192.168.100.1/24 → **119.58.100.1/24**
- ✓ *IPv6:* 2001:0DB8:AACC:0033::1 /64 → **2119:0587:AACC:0033::1 /64**
- ✓ *IPv6:* 2001:0DB8:AACC:0034::1 /64 → **2119:0587:AACC:0034::1 /64**

8. For the PC61 & PC62:

- ✓ *IPv4:* 192.168.100.2/24 → **119.58.100.2/24**
- ✓ *IPv6:* 2001:0DB8:AACC:0034::2 /64 → **2119:0587:AACC:0034::2 /64**

1. Assigning IP Addresses to all PC's:

In the first part, it is required to assign IP addresses to all PC's into the following network topology. According to specific IP addressing criteria as explained previously, the PC's which are connected to router R0, **PC01–Ipv6** and **PC02–Ipv4** will be given **2119:0587:AACC:0031::2/64** and **119.58.200.2/24** with subnet mask **255.255.255.0** respectively, while the PC's connected to R6, **PC61–IPv6** and **PC62–IPv4** will be given **2119:0587:AACC:0034::2** and **119.58.100.2/24** with subnet mask **255.255.255.0** sequentially.

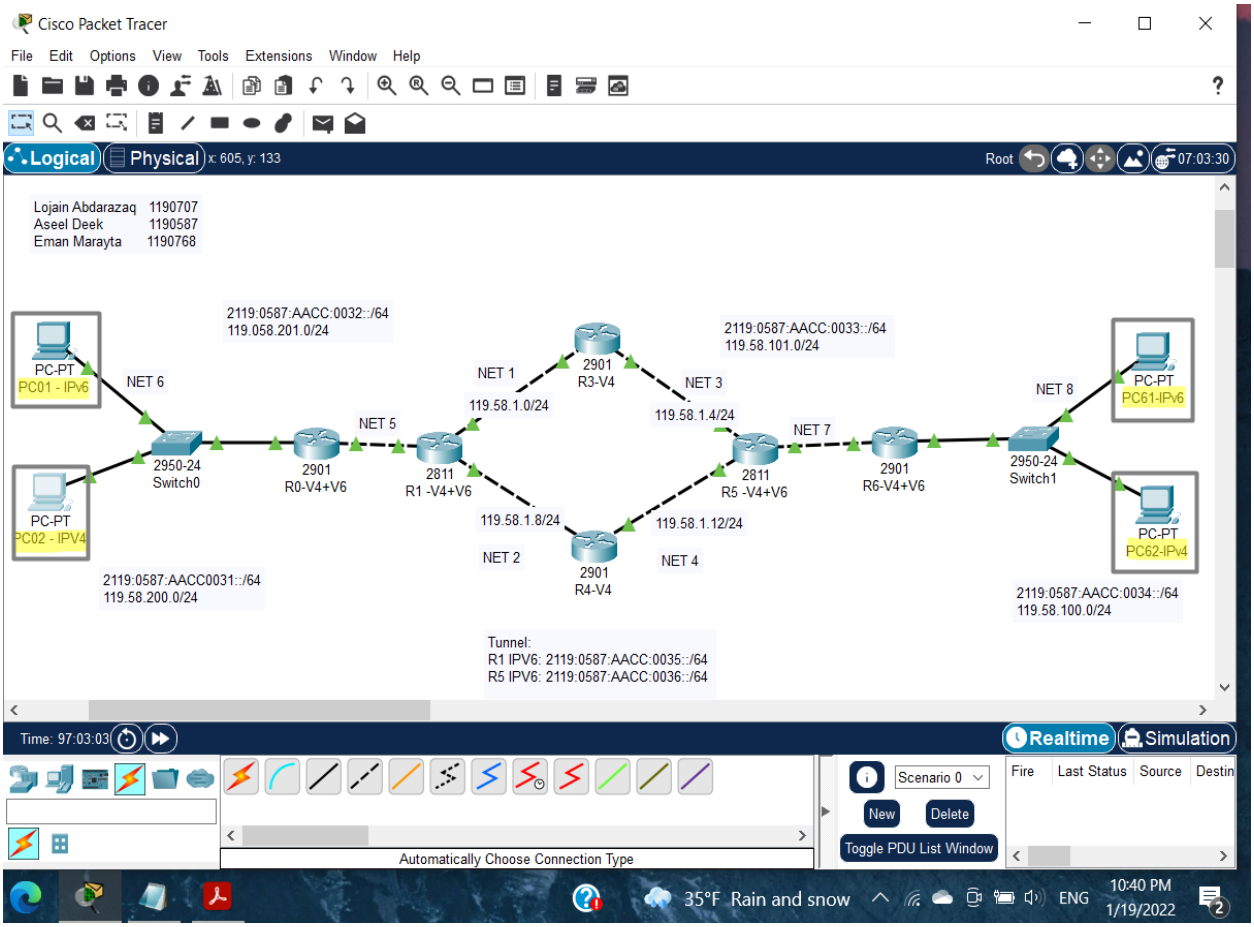

Figure2.1 1 (Network Topology)

✓ **For PC01-IPv6:**

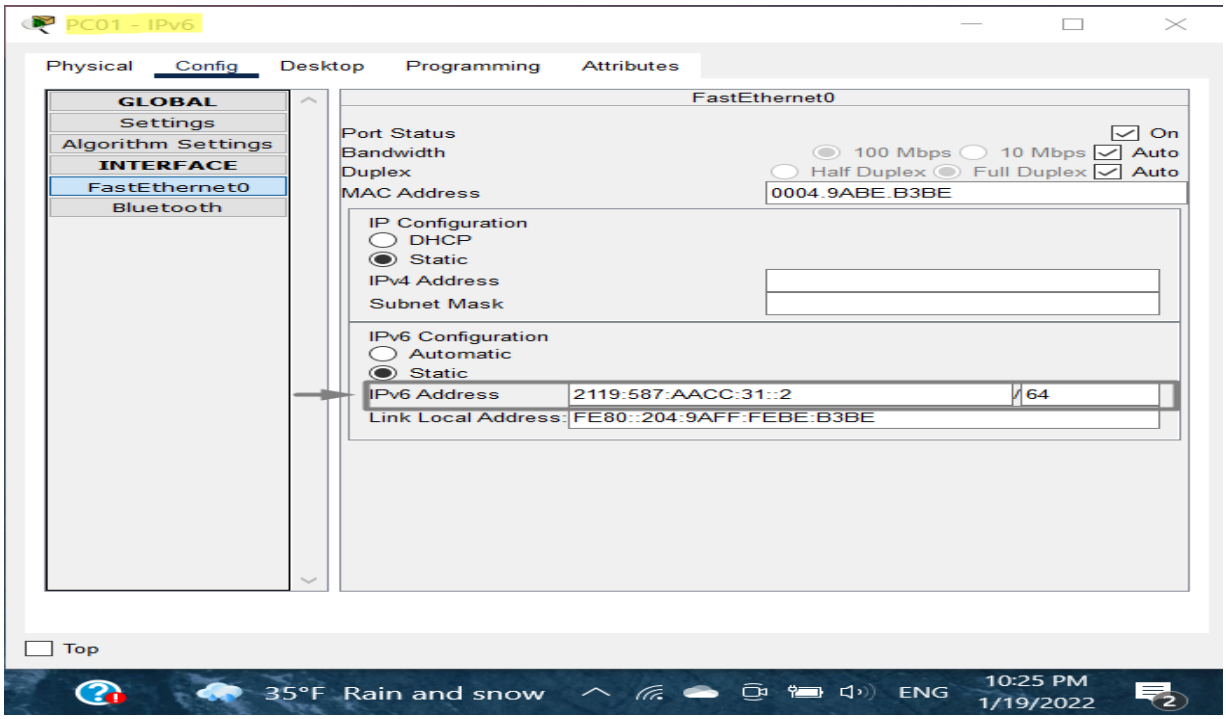

Figure2.1 2 (Assigning IPv6 Address to PC01)

✓ **For PC02 –IPv4:**

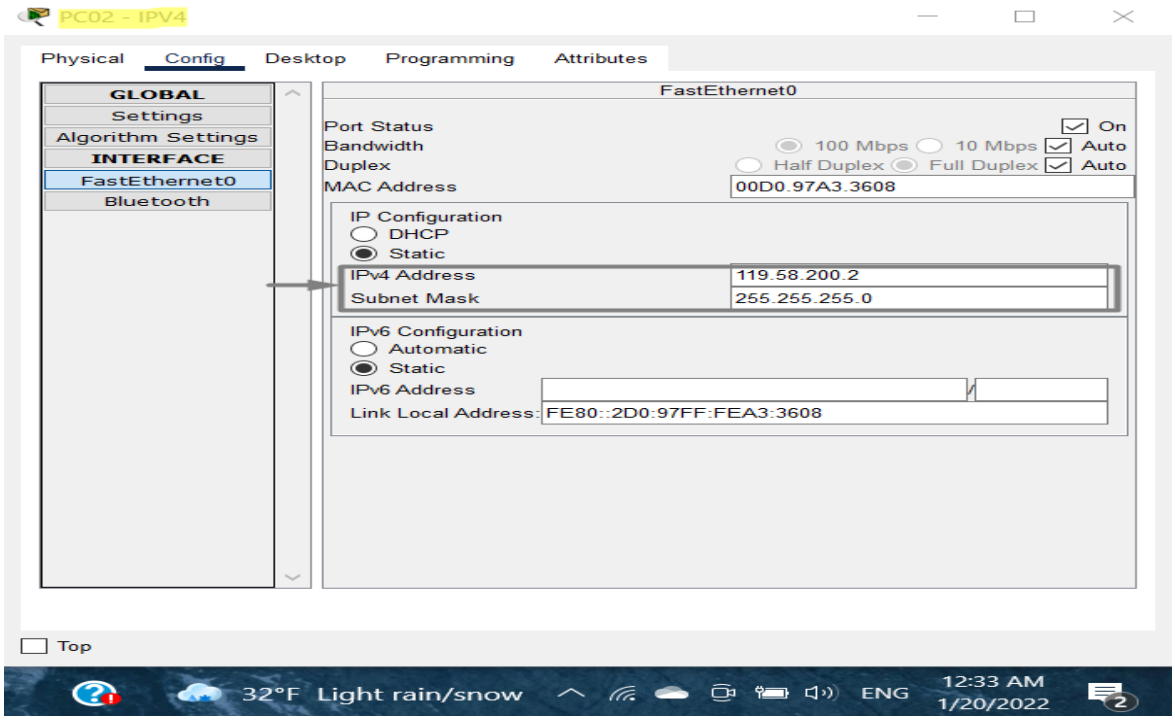

Figure2.1 3 (Assigning IPv4 Address to PC02)

✓ **For PC62 –IPv4:**

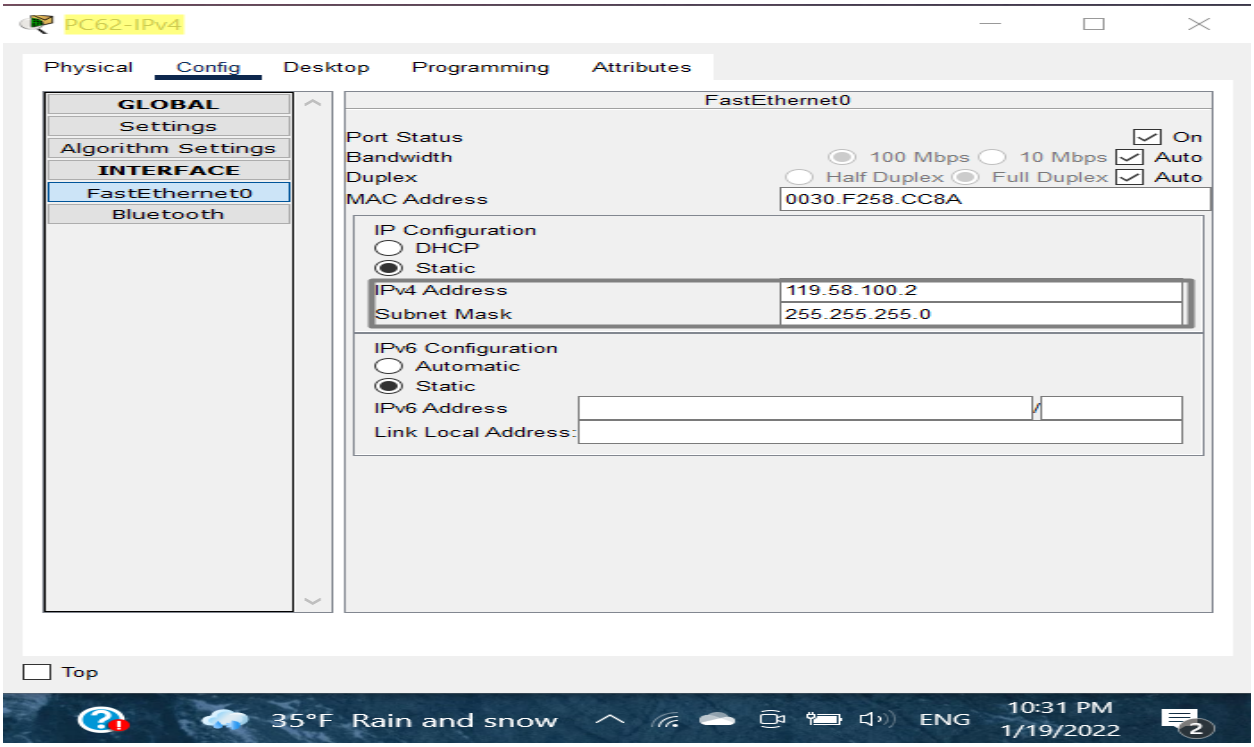

Figure2.1 4 (Assigning IPv4 Address to PC62)

✓ **For PC61 –IPv6:**

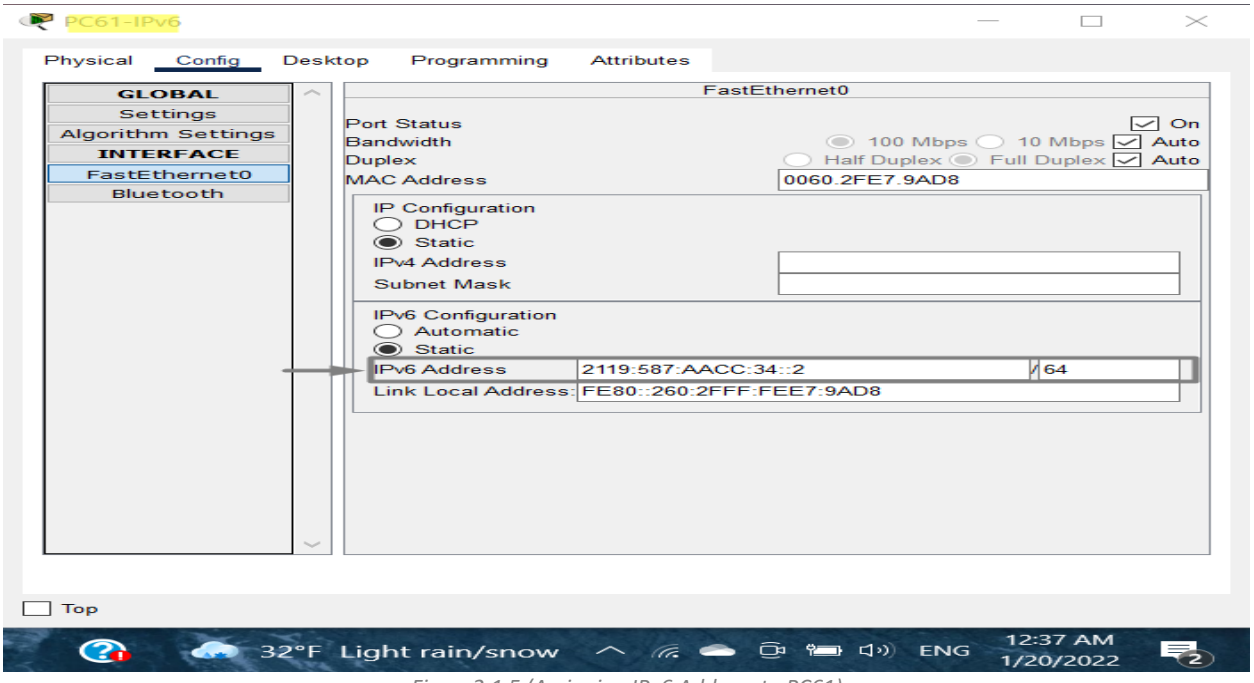

Figure2.1 5 (Assigning IPv6 Address to PC61)

2. Assign IP addresses to all router interfaces:

In this part, it is required to assign IP addresses to all routers interfaces in the network according to specific criteria explicated previously, the ID number ***"1190587"*** was used. The following figures represent assigning IP addresses to all router interfaces.

- ✓ **<u>For R0:</u>** this router is connected to the two PCs from the left side with IP address **119.058.200.1/24**, and the router R1 from the right side **119.058.201.1/24**.

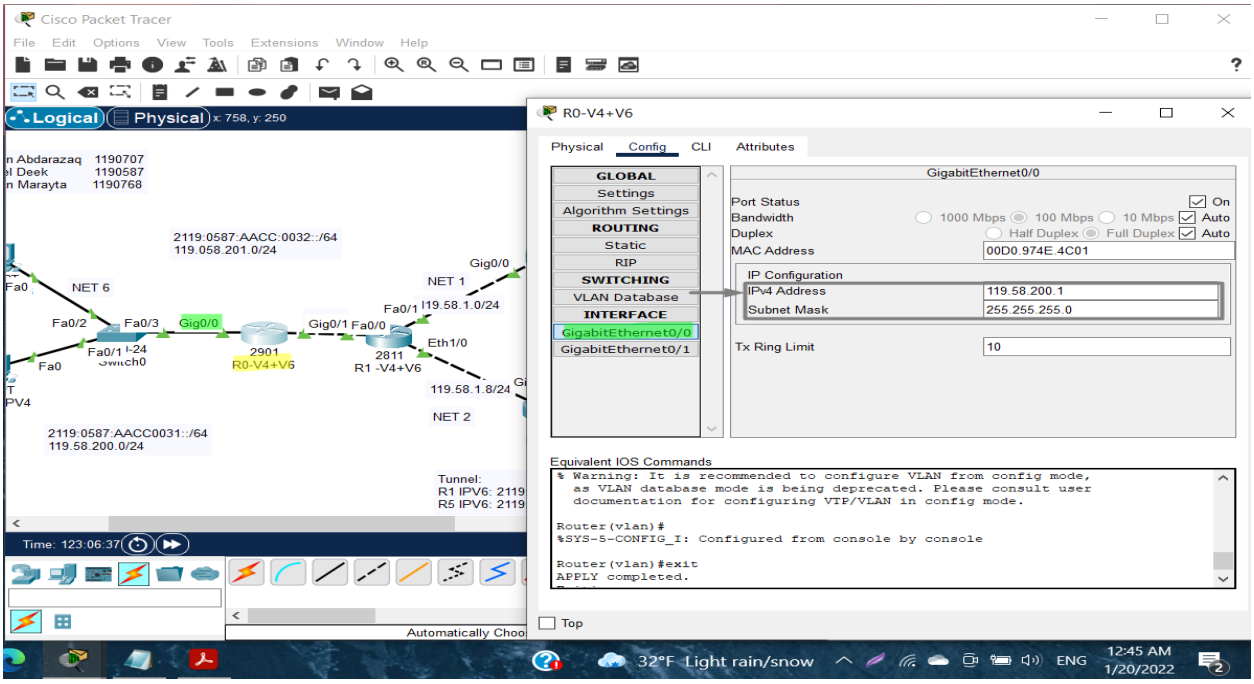

*Figure2.2. 1 (Assigning IPv4 Address **119.058.200.1** between router R0 and the PCs)*

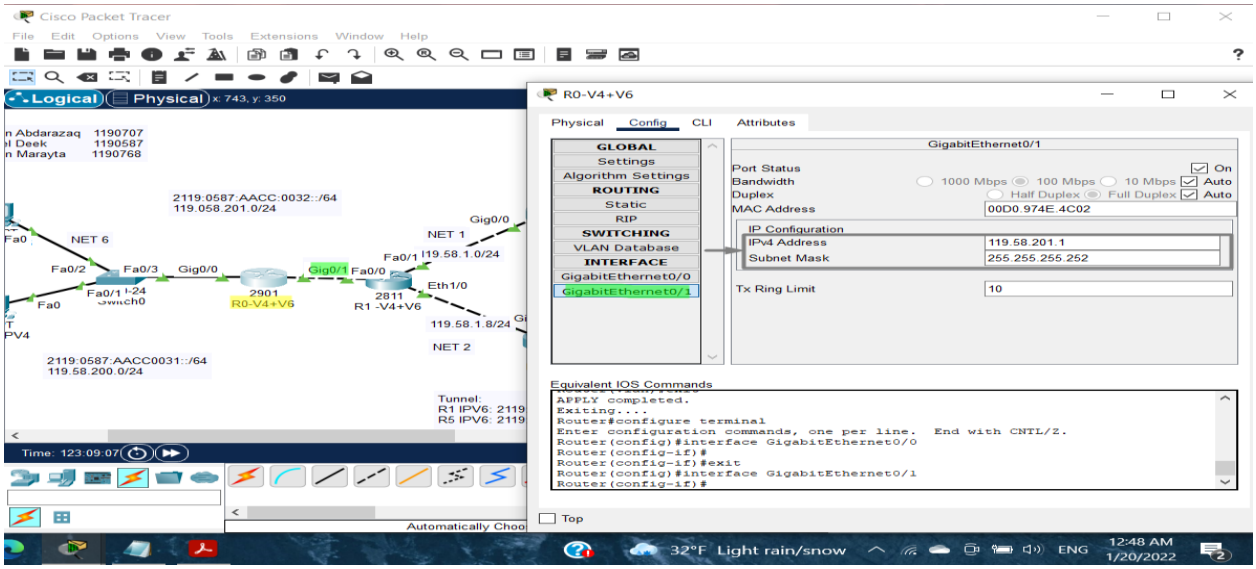

*Figure2.2. 2 (Assigning IPv4 Address **119.058.201.1** between the router R0 and router R1)*

- ✓ **<u>For R1:</u>** it is connected to the three routers (R0,R3, and R4). The IP address assigned to router R1 and R0 is**119.58.201.2/24,** while the IP address between the router R1 and R3 is **119.058.1.2/24**, and finally the IP address between R1 and R4 is **119.058.1.9/24**.

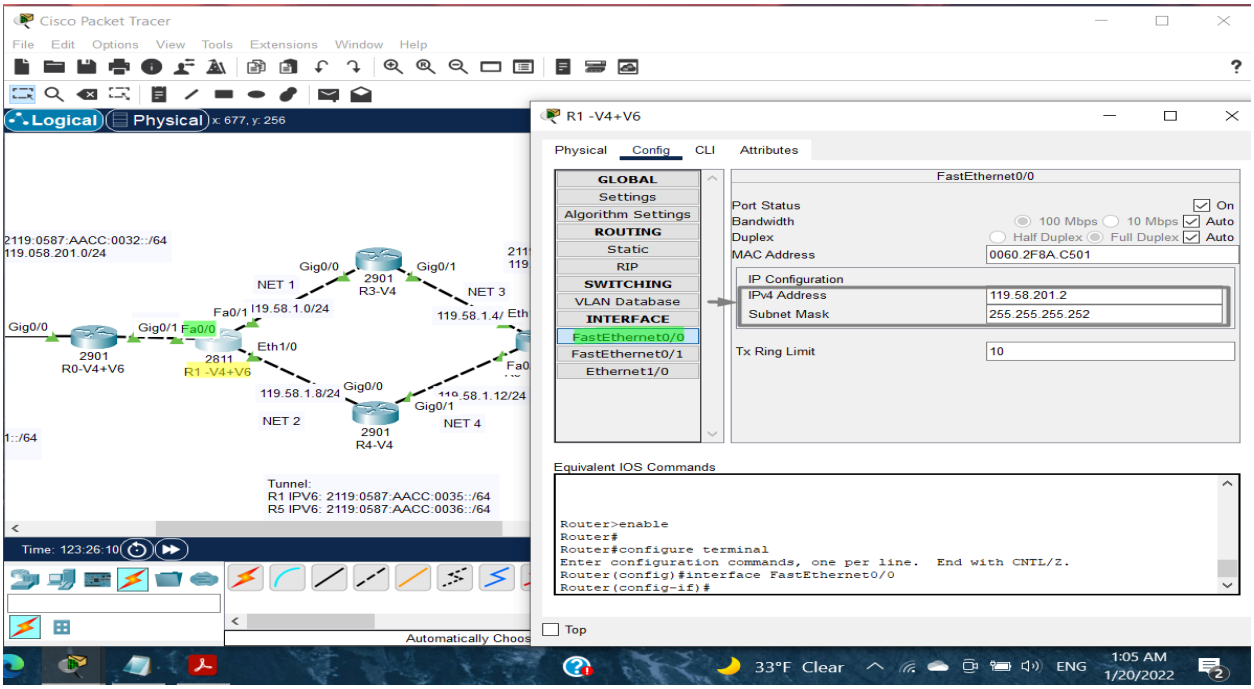

*Figure2.2. 3 (Assigning IPv4 Address **119.058.201.2** between the router R0 and router R1)*

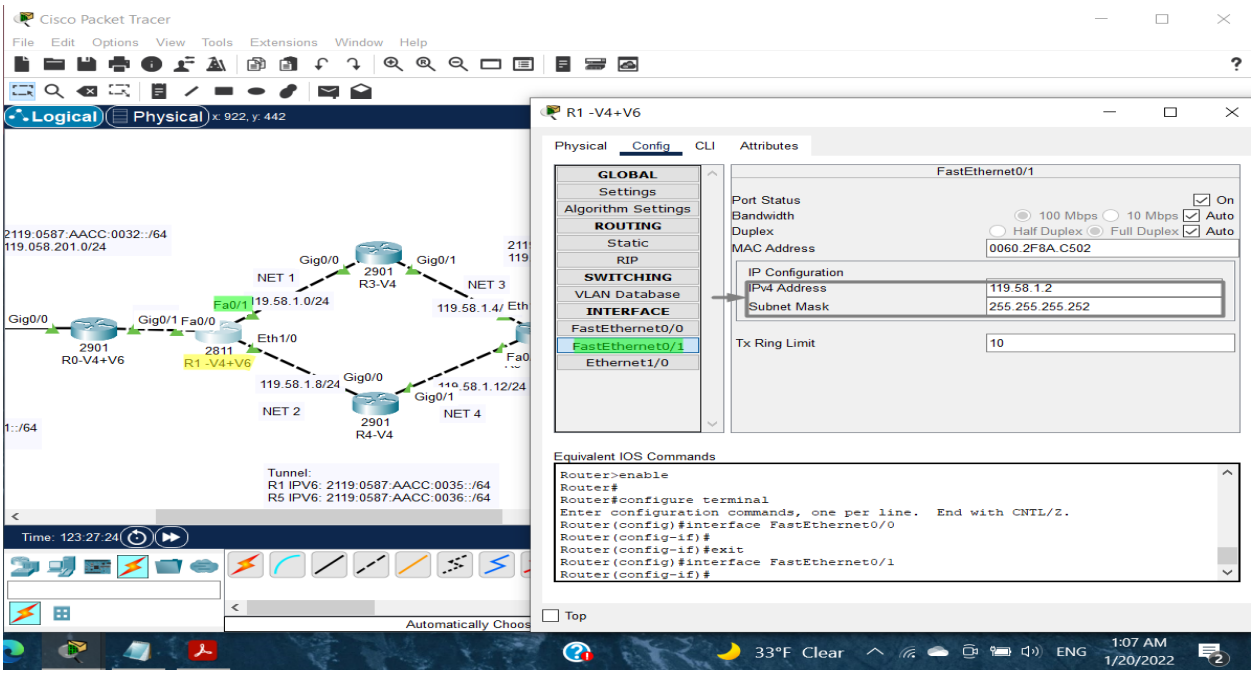

*Figure2.2. 4 (Assigning IPv4 Address **119.058.1.2** between the router R1 and router R3)*

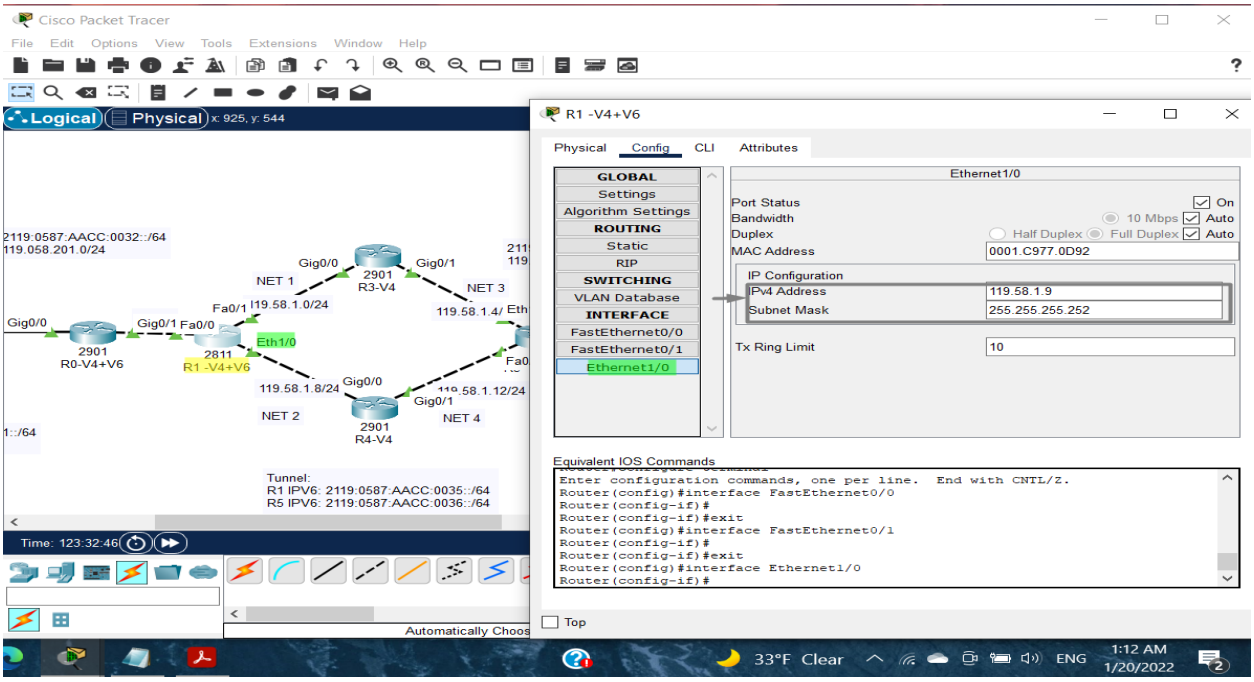

*Figure2.2. 5 (Assigning IPv4 Address **119.058.1.9** between the router R1 and router R4)*

- ✓ **For R3:** The router R3 is connected to two routers, R1 and R5. The IP address **119.58.1.1/24** is assigned between R3 and R1, while the IP address **119.58.1.6/24** is assigned between R3 and R5.

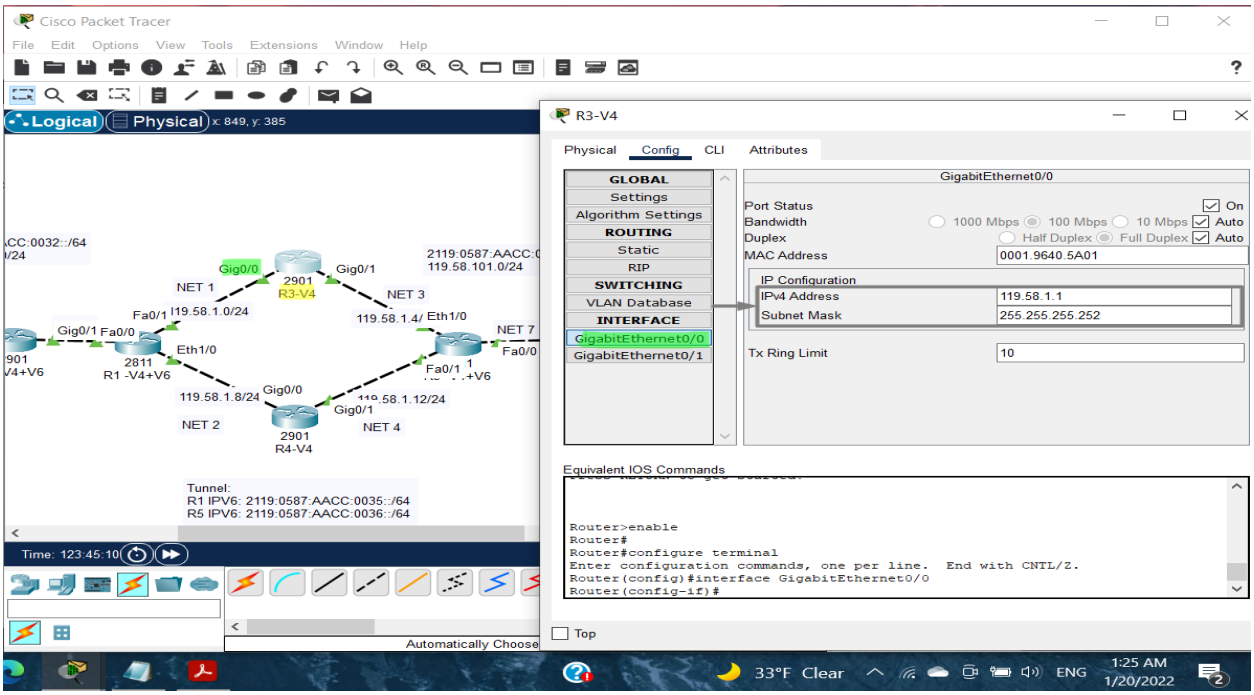

*Figure2.2. 6 (Assigning IPv4 Address **119.058.1.1** between the router R3 and router R1)*

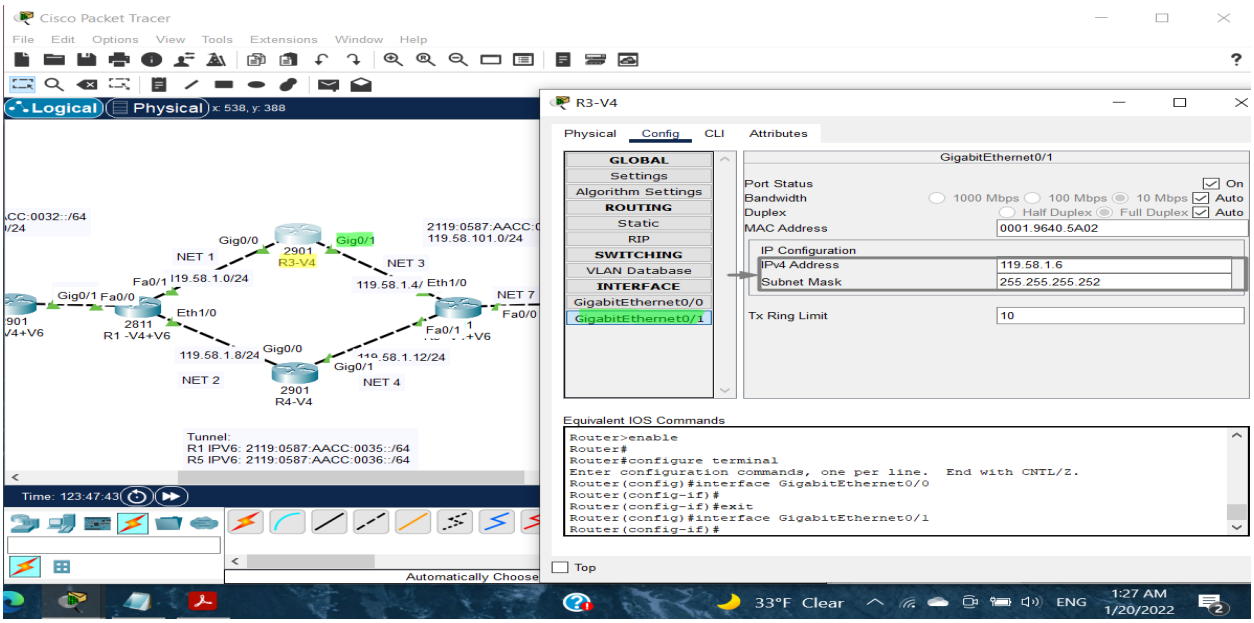

*Figure2.2. 7 (Assigning IPv4 Address **119.058.1.6** between the router R3 and router R5)*

- ✓ **<u>For R4</u>**: For router R4, its similar to router R3, it's connected to R1 and R5. The IP address **119.58.1.10/24** is assigned between the router R4 and R1, while **119.58.1.14/24** is assigned between R4 and R5.

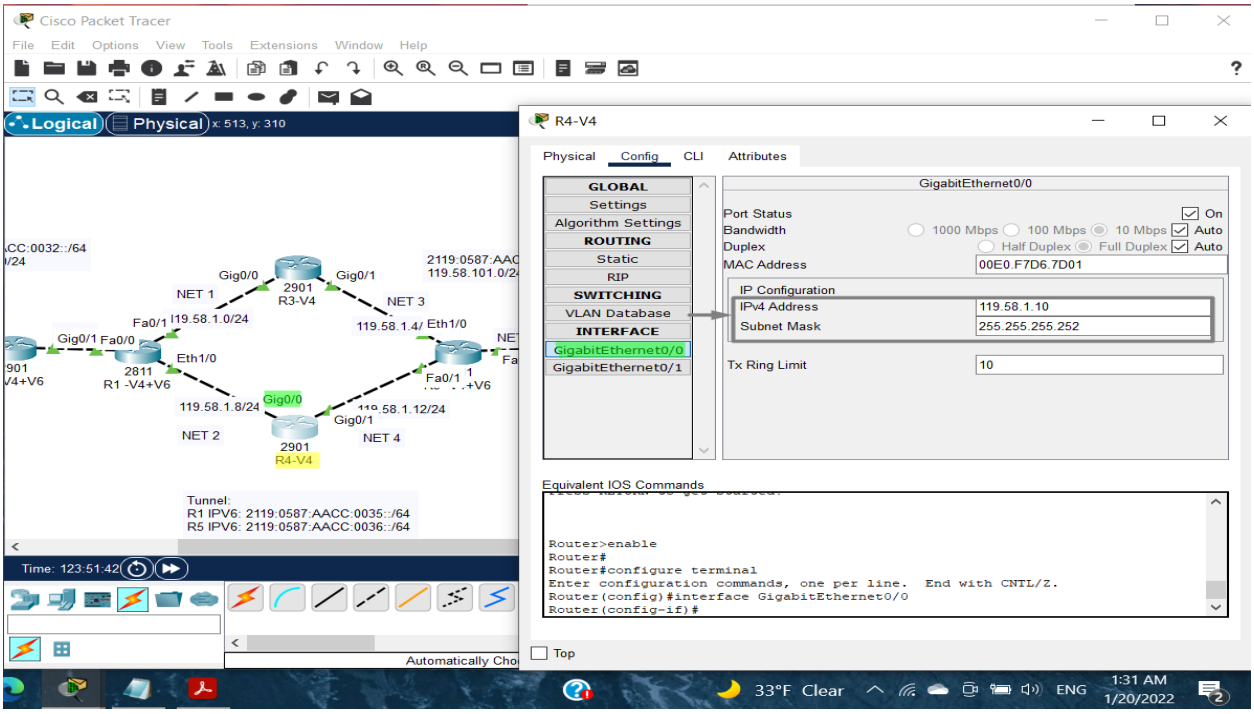

*Figure2.2. 8 (Assigning IPv4 Address **119.58.1.10** between the router R4 and router R1)*

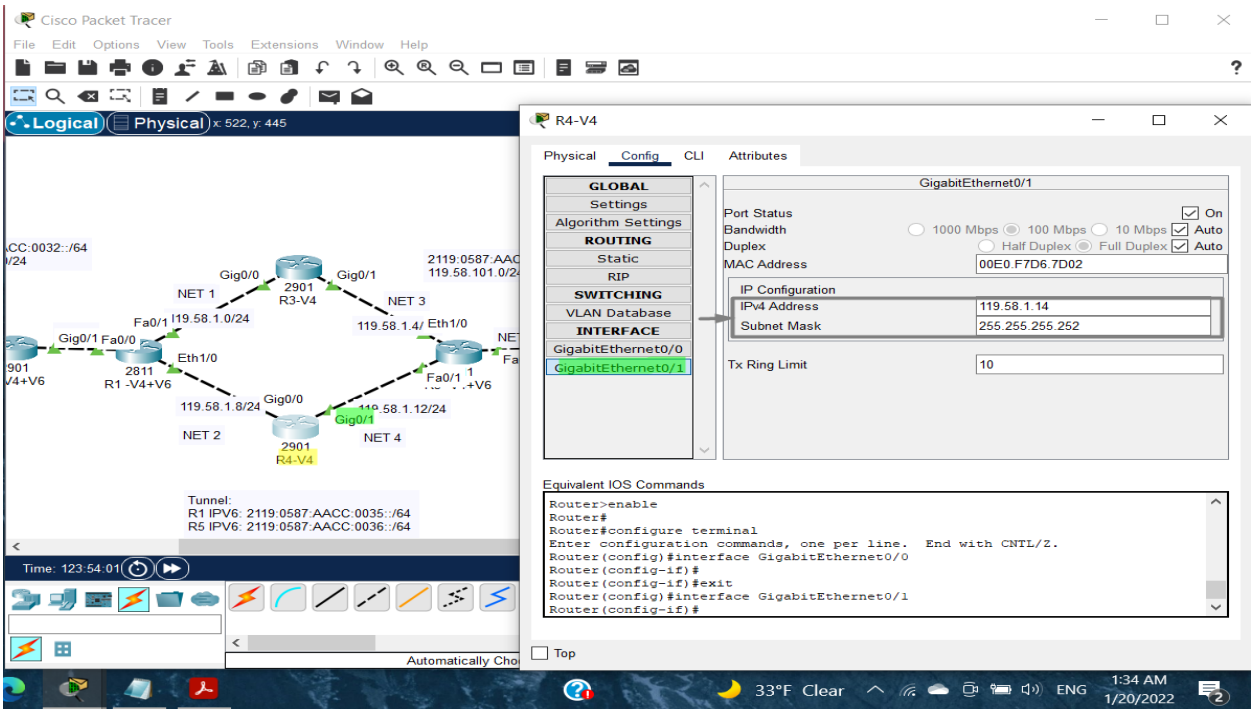

*Figure2.2. 9 (Assigning IPv4 Address **119.58.1.14** between the router R4 and router R5)*

- ✓ **<u>For R5:</u>** R5 is connected with 3 other routers, R6, R4 and R3. The IP addresses **119.58.101.2/24, 119.58.1.13/24** and **119.58.1.5/24 respectively.**

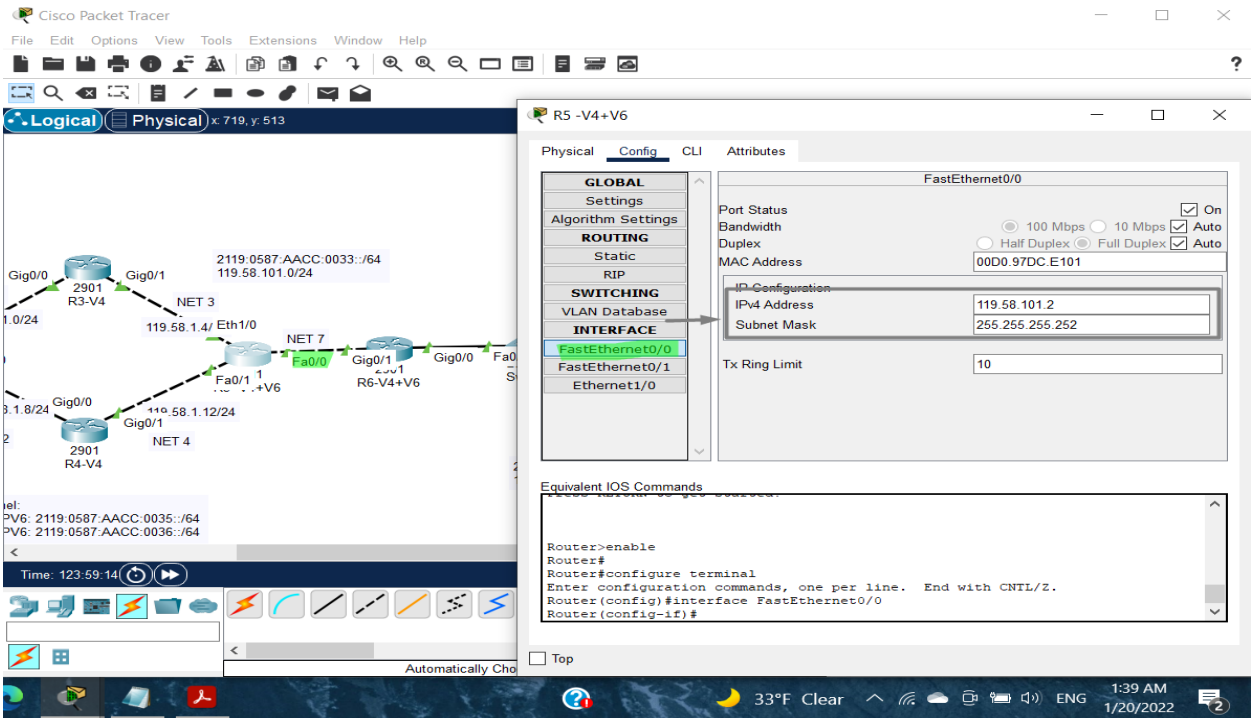

*Figure2.2. 10 (Assigning IPv4 Address **119.58.101.2** between the router R5 and router R6)*

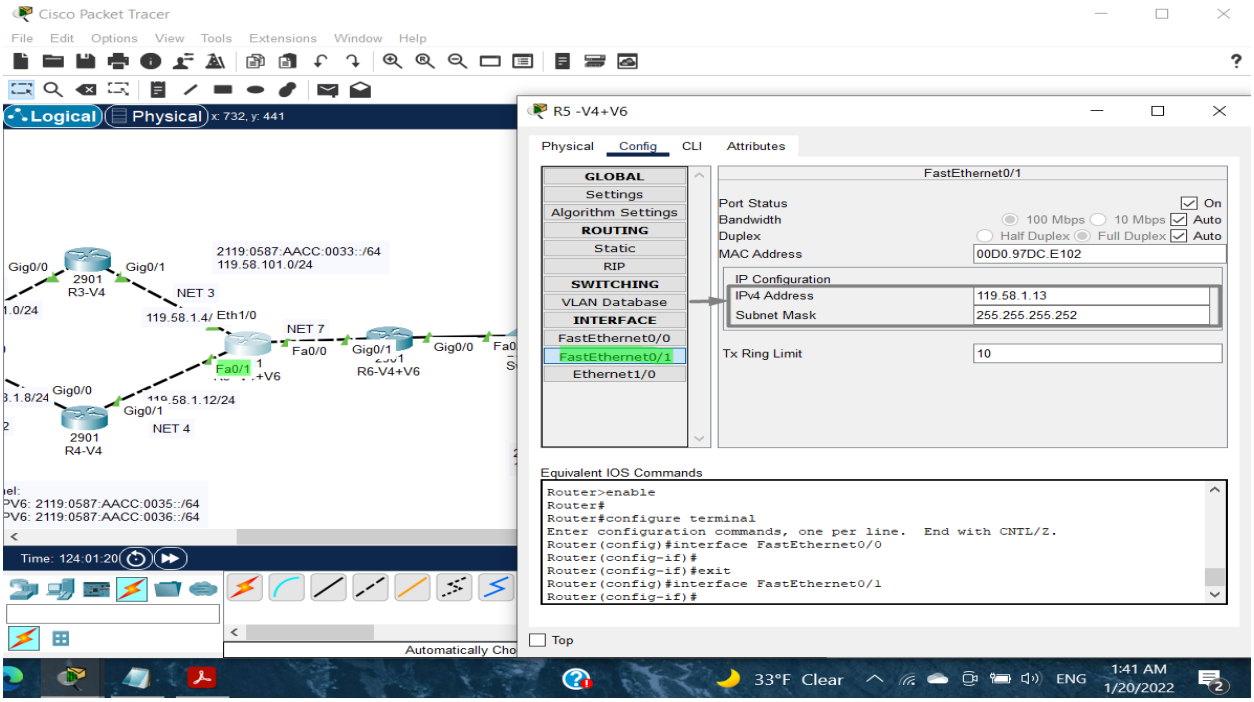

*Figure2.2. 11 (Assigning IPv4 Address **119.58.1.13** between the router R5 and router R4).*

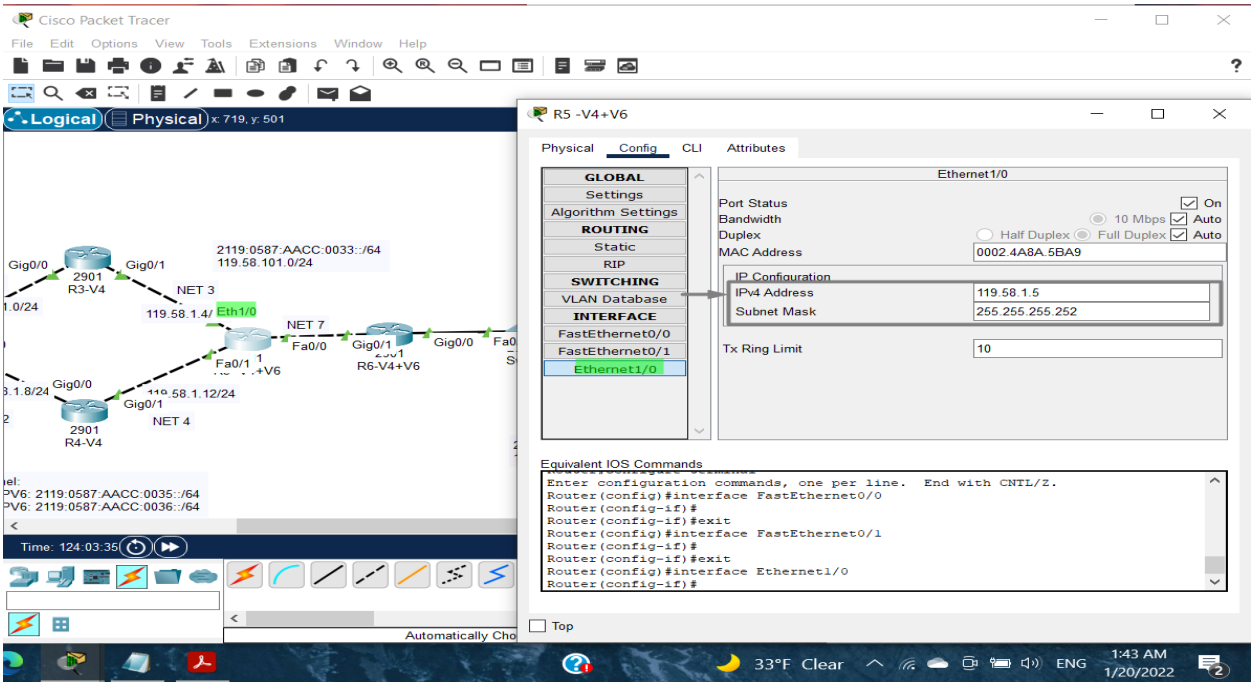

*Figure2.2. 12 (Assigning IPv4 Address **119.58.1.5** between the router R5 and router R3).*

✓ **For R6:** The last router R6 is connected to 2 sides, the first side with R5 while the second side with two PC's. The IP addresses **119.58.100.1/24** and **119.58.101.1/24** is assigned to router R6.

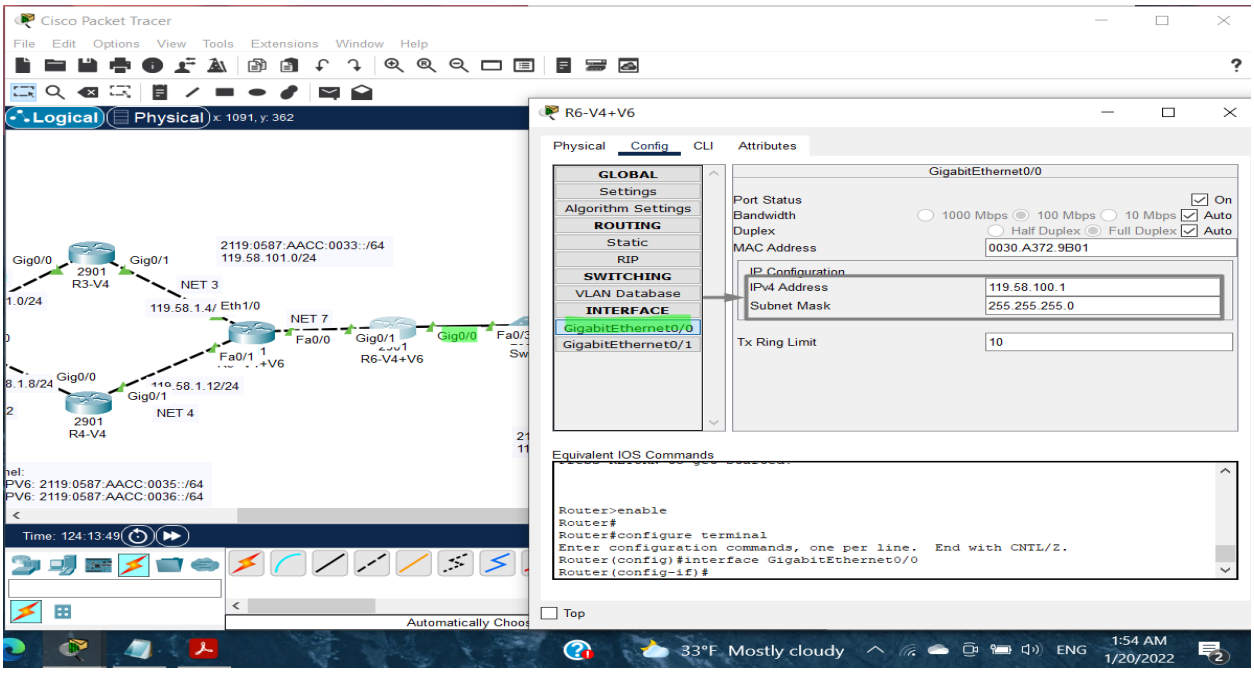

*Figure2.2. 13 (Assigning IPv4 Address **119.58.100.1/24** between the router R6 and two PCs)*

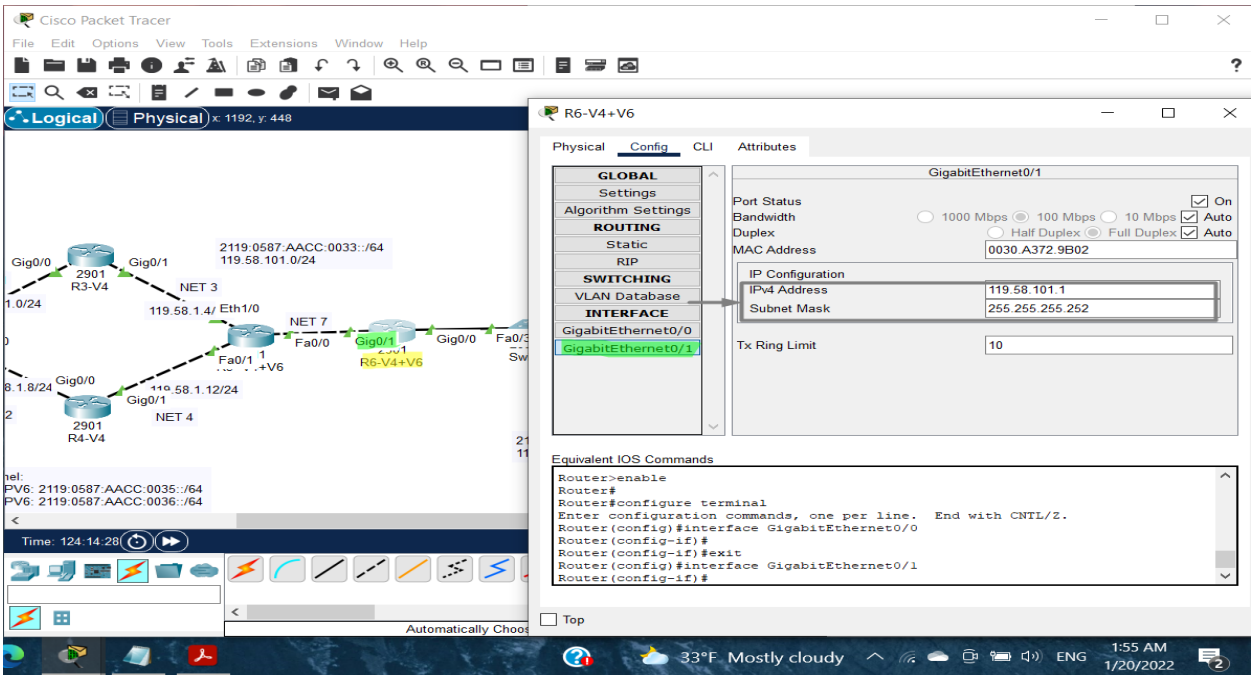

*Figure2.2. 14 (Assigning IPv4 Address **119.58.101.1** between the router R6 and router R5)*

3. Each host can ping at least one host in the same network.

To make sure that each host can connect with at least one other host in the same network, the ***Ping command*** will be used to check the reachability in each network.

- ✓ **For Network 1:**

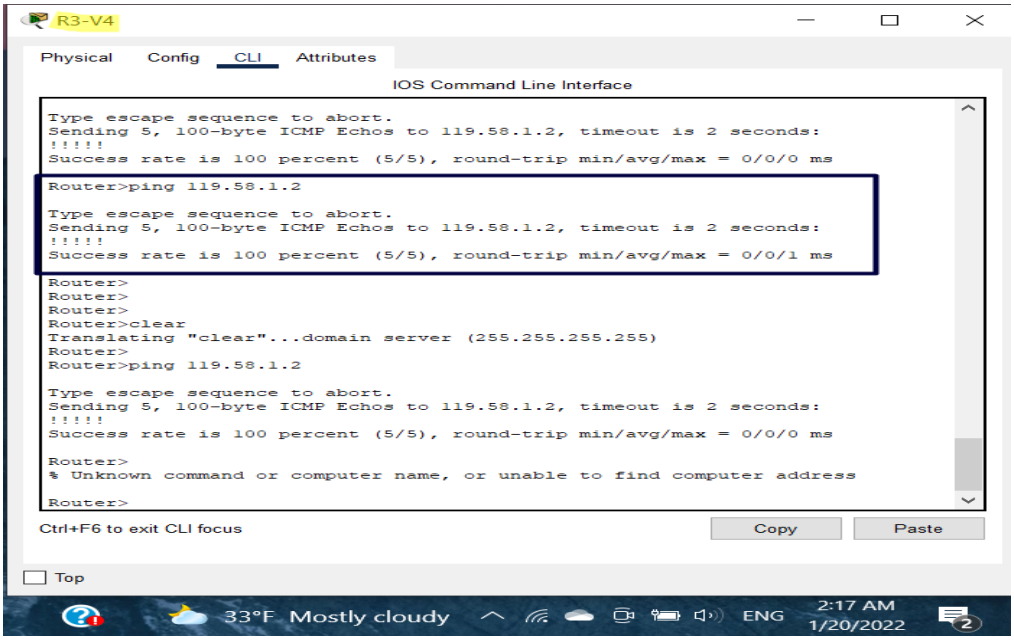

Figure2.3. 1 (Pinging R1 from R3 in network 1)

- ✓ **For Network 2:**

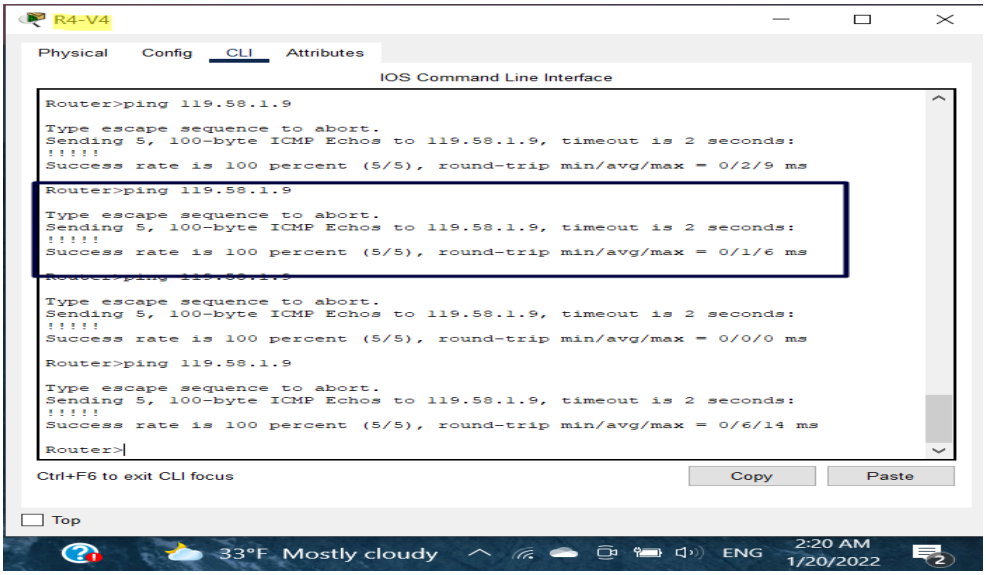

Figure2.3. 2 (Pinging R1 from R4 in network 2)

✓ **For Network 3:**

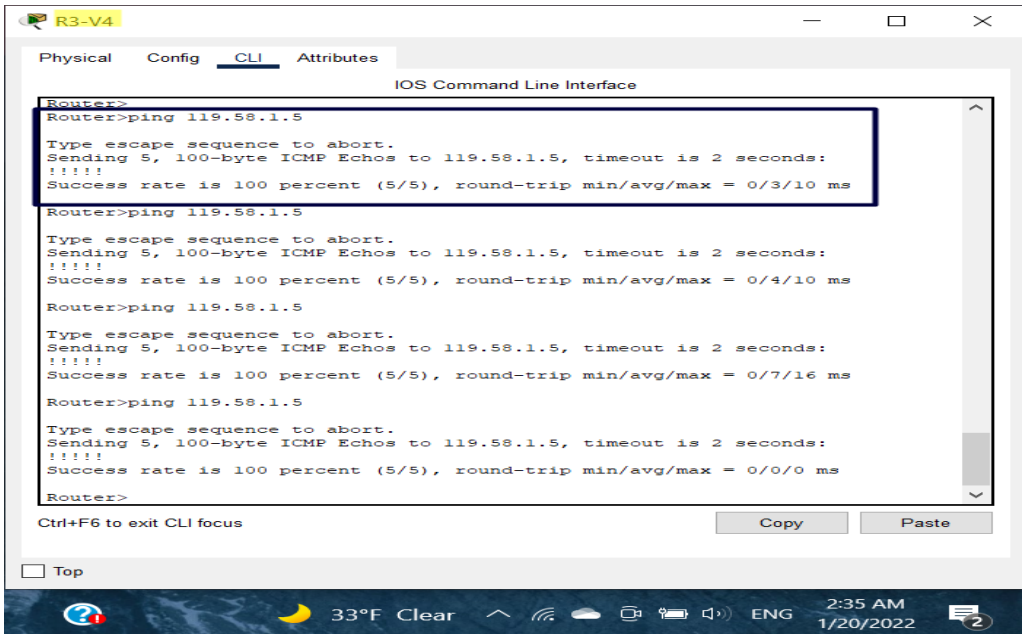

Figure2.3. 3 (Pinging R5 from R3 in network 3)

✓ **For Network 4:**

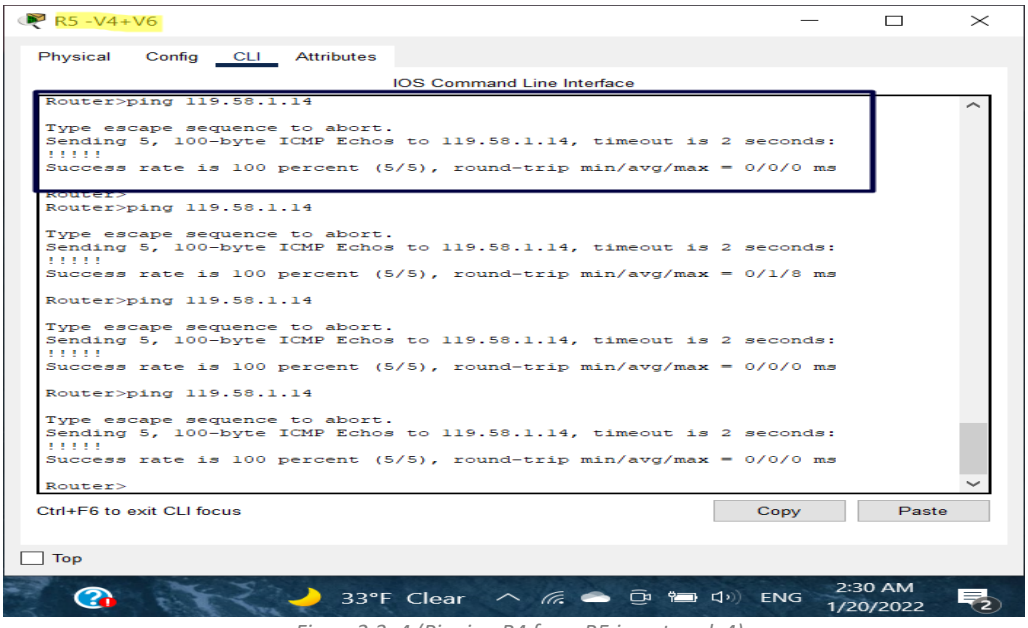

Figure2.3. 4 (Pinging R4 from R5 in network 4)

✓ **For Network 5:**

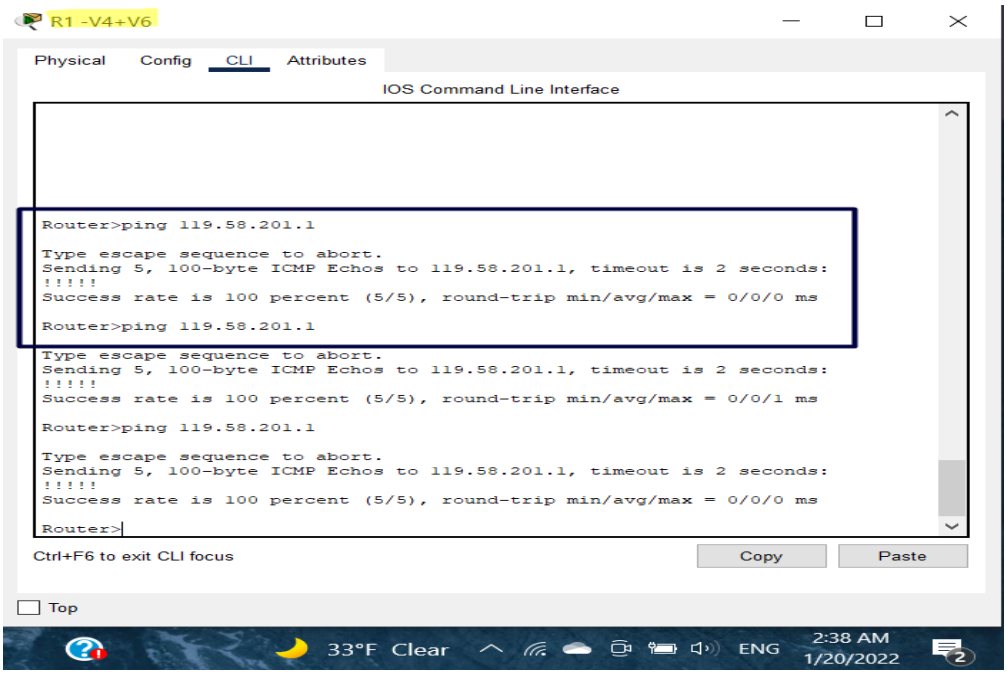

Figure2.3. 5 (Pinging R0 from R1 in network 5)

✓ **For Network 6:**

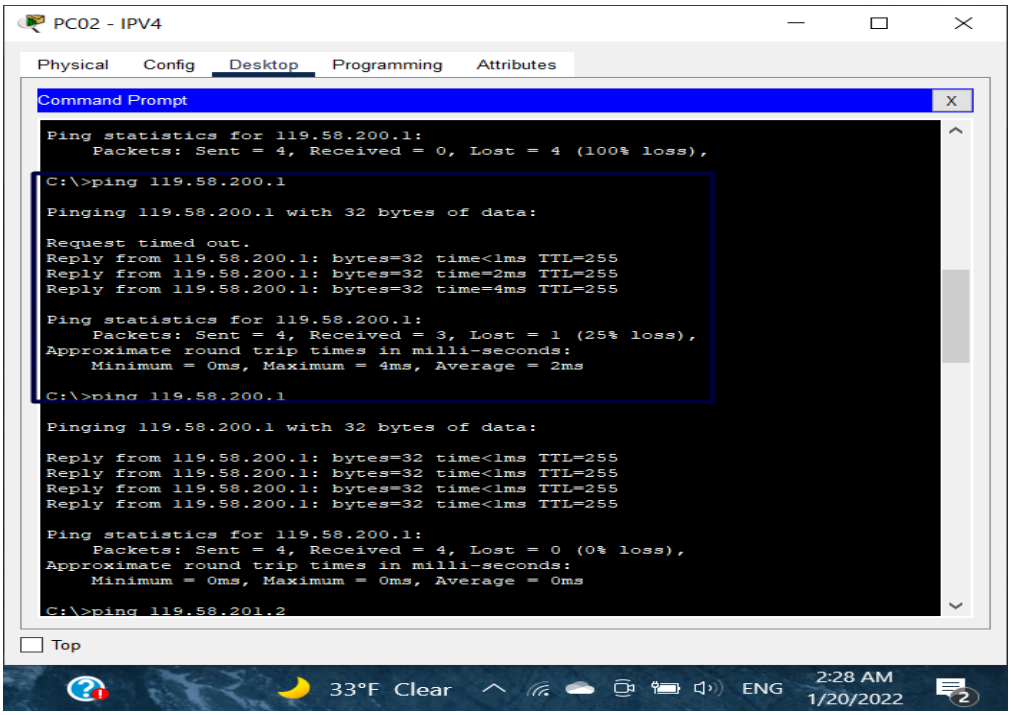

Figure2.3. 6 (Pinging R0 from PC02 in network 6)

4. Implementing single area OSPF routing protocol for IPv4.

To implement a single area OSPF protocol, the command ***(#router ospf 1)*** is applied into the **CLI window** for each router in the topology network. The following figures represent implementing the ospf routing protocol for both R0 and R3.

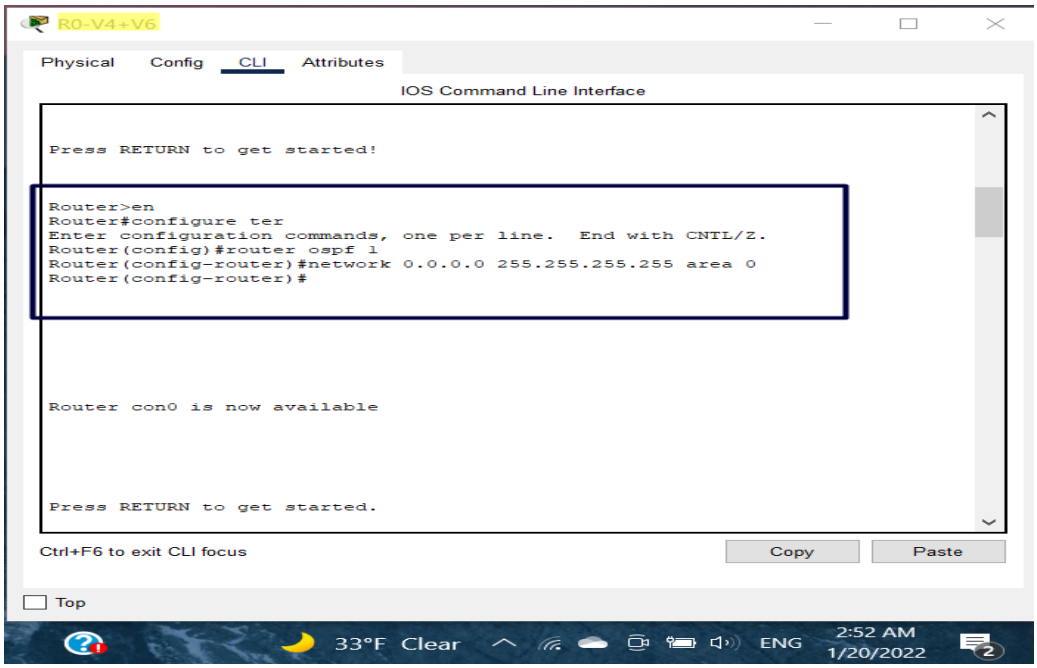

*Figure2.4. 1 (Applying **OSPF** routing protocol to R0)*

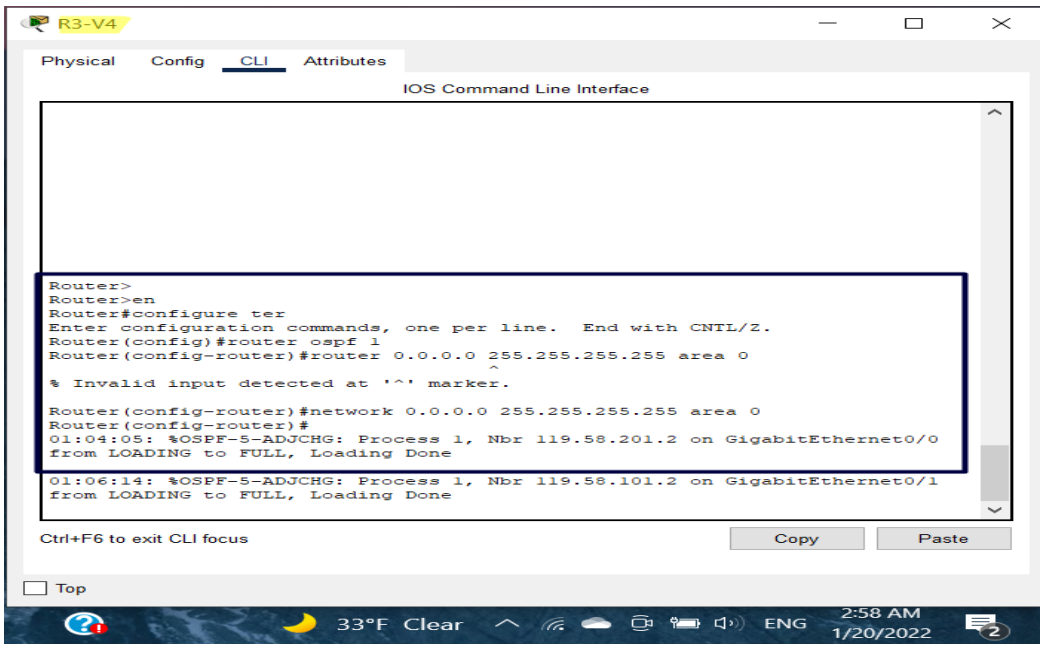

*Figure2.4. 2 (Applying **OSPF** routing protocol to R3)*

5. IPv4 packets routed all over the network.

To be sure that the IPv4 packets are correctly routed all over the network, the ***Ping command*** must be implemented. In the following figures, the ping command used to check the reachability between networks. The PC02 with **119.58.200.2/24** address is connected router R3, which outside of the PC's network, the ping command is used, and it's the connection was created clearly as shown:

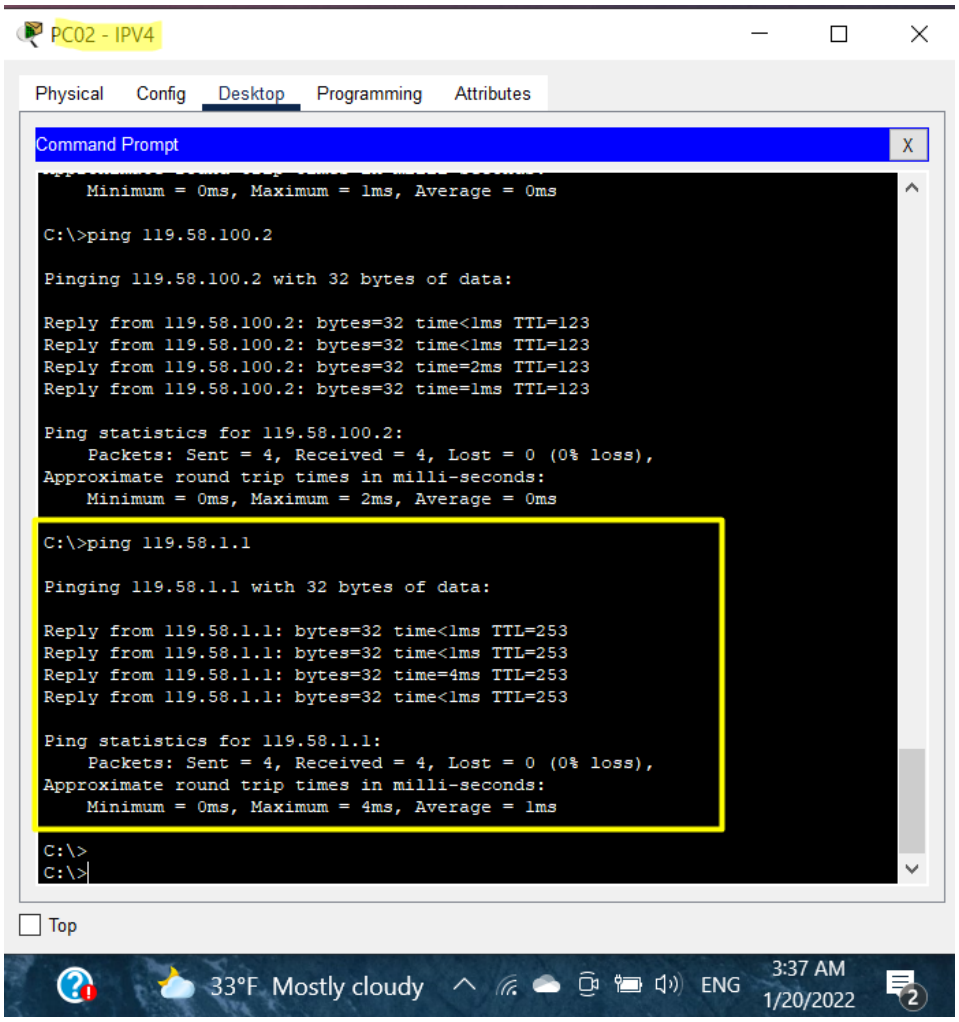

Figure2.5. 1 (Pinging R3 from PC02)

The PC02 with IPv4 address ***119.58.200.2/24*** connected with the PC62 with Ipv4 address ***119.58.100.2/24*** using Ping command, and the operation is done **successfully** (4 received packets with 0 lost packets) which leads that the Ipv4 packets routed all over the topology network.

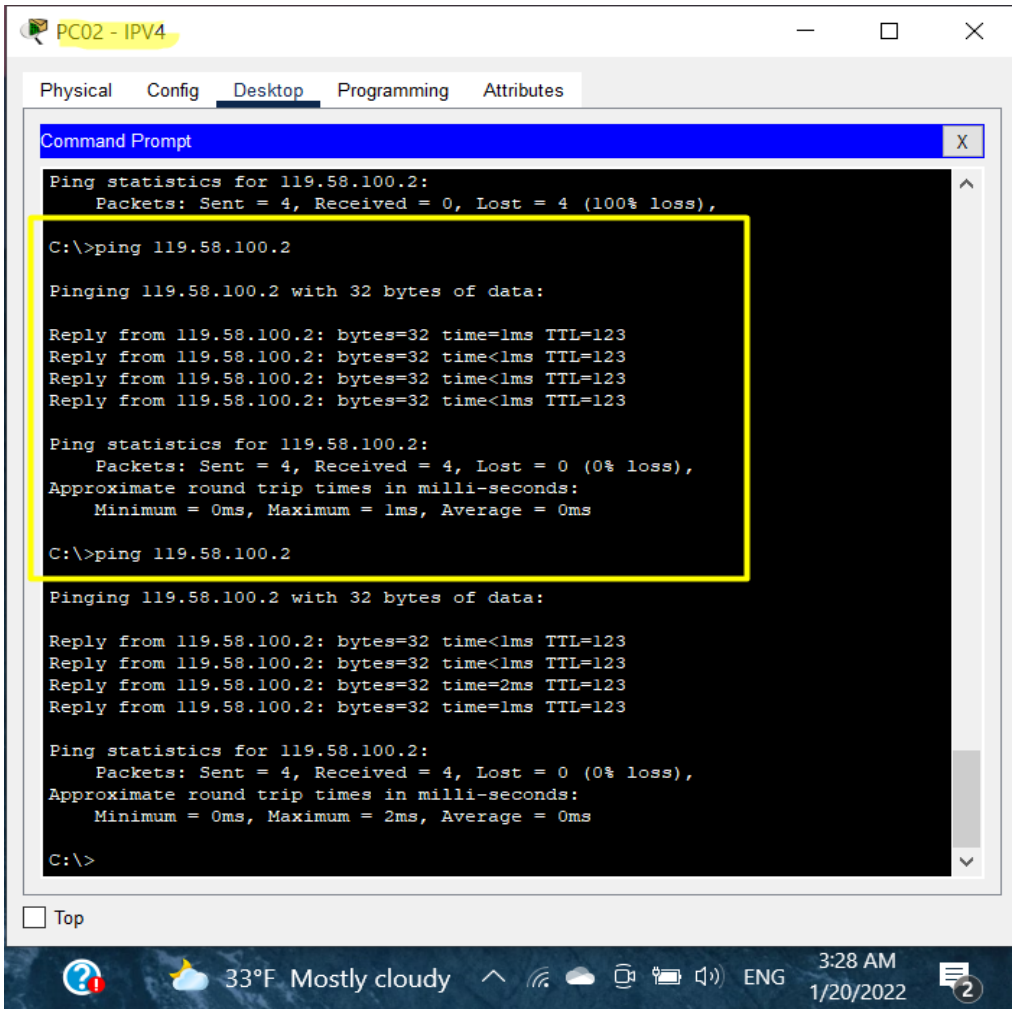

Figure2.5. 2 (Pinging PC62 from PC02)

In addition, using ping command, the connection between the router R0 with ***119.58.201.1/24*** and R5 with ***119.58.100.2/24***, and the router R4 ***119.58.1.14/24*** and R6 ***119.58.101.1/24*** was checked, and it's created successfully as shown in the following figures:

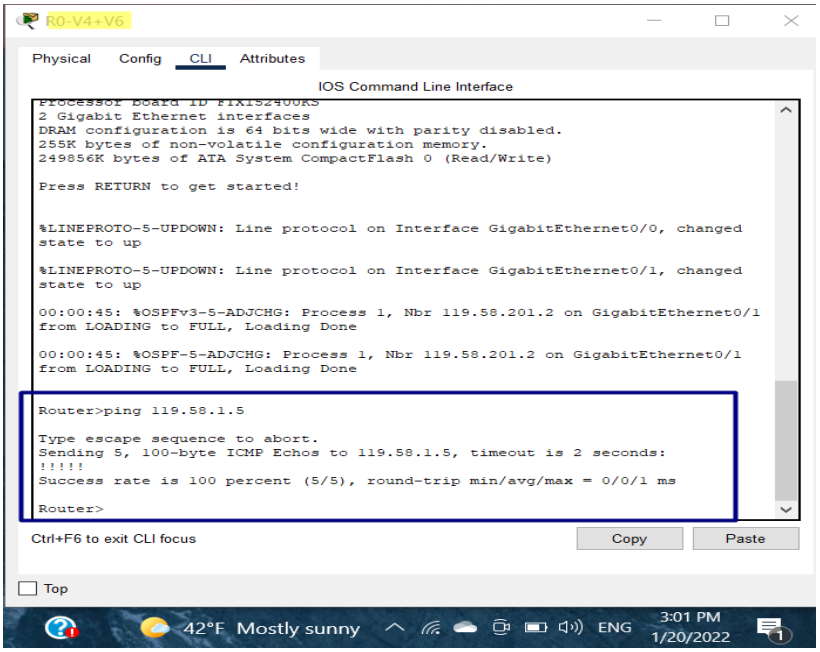

Figure2.5. 3 (*Pinging R5 from R0)*

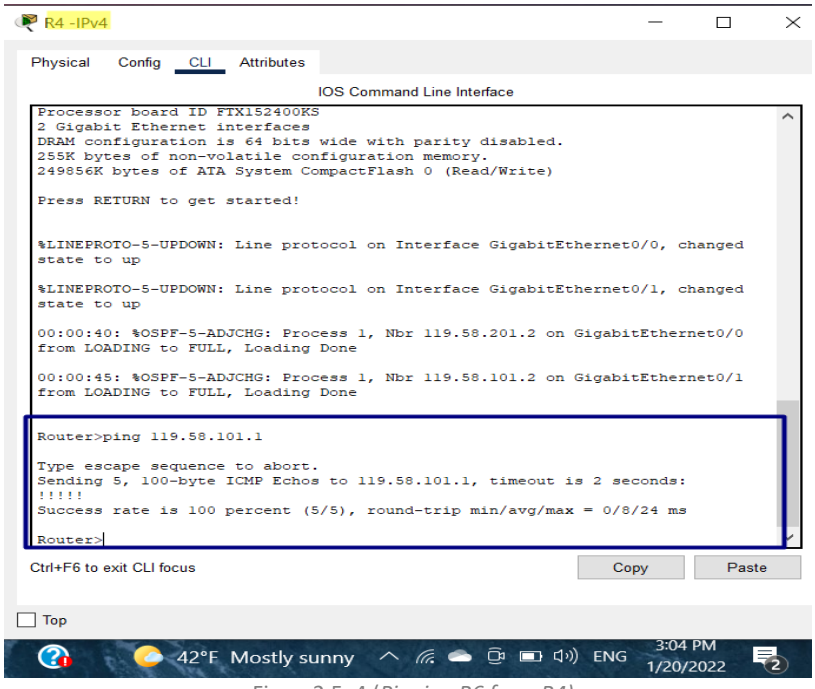

Figure2.5. 4 (*Pinging R6 from R4)*

6. Assigning IPv6 to Routers (R0, R1, R5, R6):

To assign the IPv6 to all the mentioned router, some commands were implemented, the below figures show how to activate the IPv6 in each router using commands.

- **For R0:**

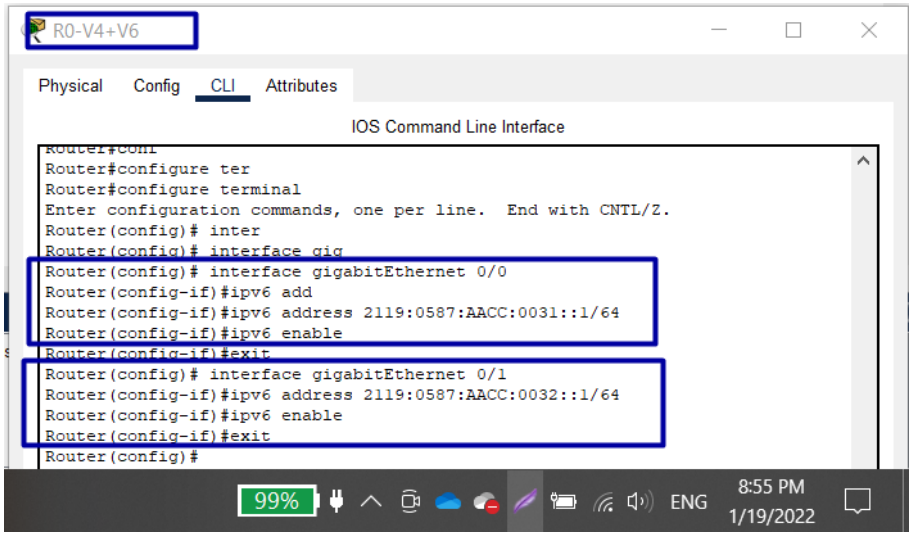

*Figure2.6. 1 (*Assigning IPv6 to Router R0)

- **For R1:**

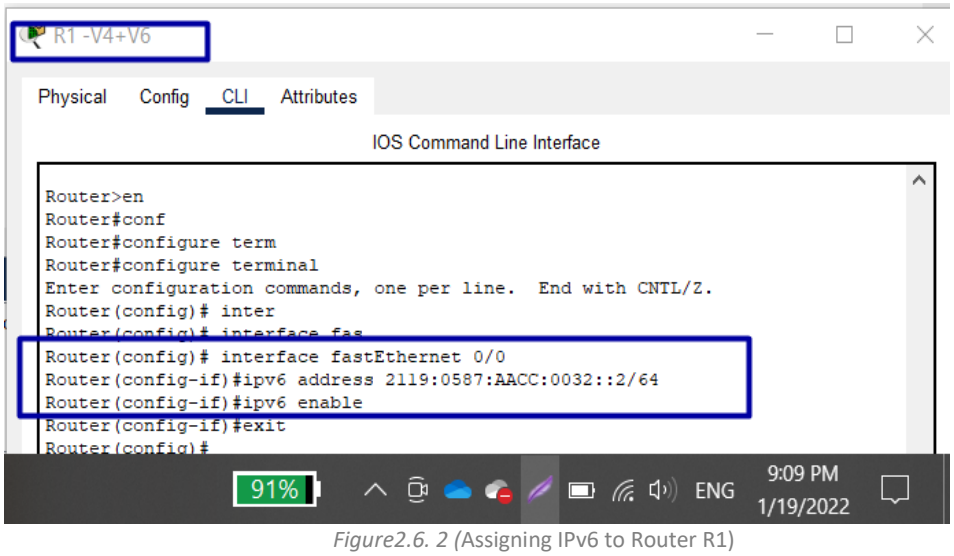

*Figure2.6. 2 (*Assigning IPv6 to Router R1)

- **For R5:**

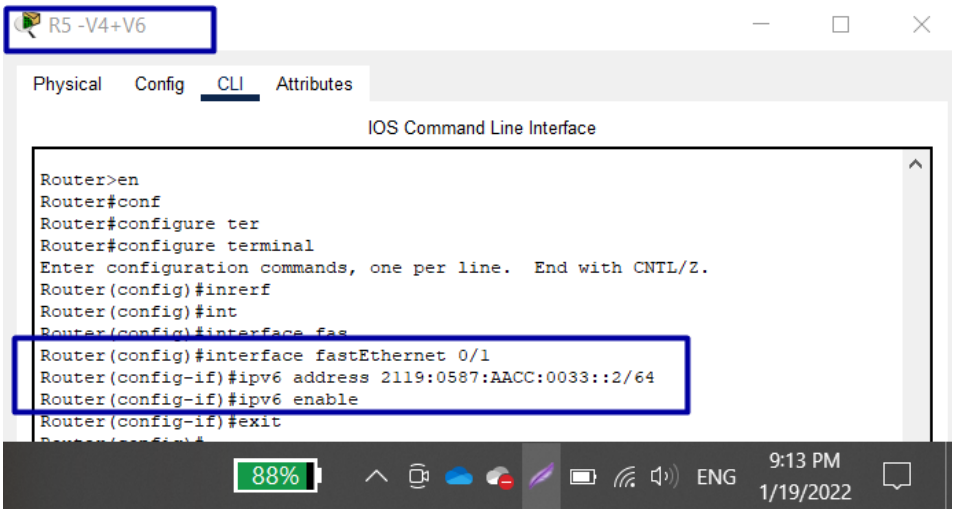

*Figure2.6. 3 (*Assigning IPv6 to Router R5)

- **For R6:**

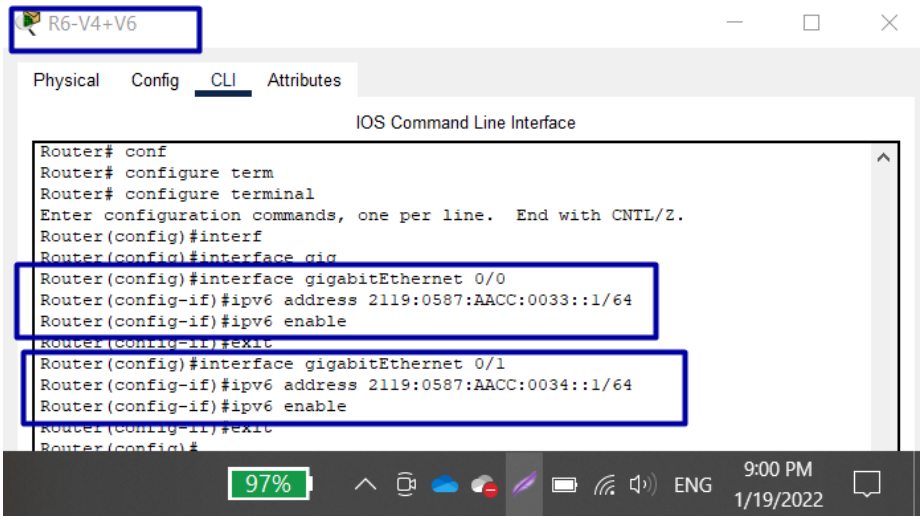

*Figure2.6. 4 (*Assigning IPv6 to Router R6)

7. Implementing OSPF routing protocol for IPv6.

To implement a single area OSPF for IPv6, this command ***#ipv6 ospf 1 area 0***, should be implemented in each interface for the router. Figure (1.3) and figure (1.4) shows the OSFP in each R0 and R6.

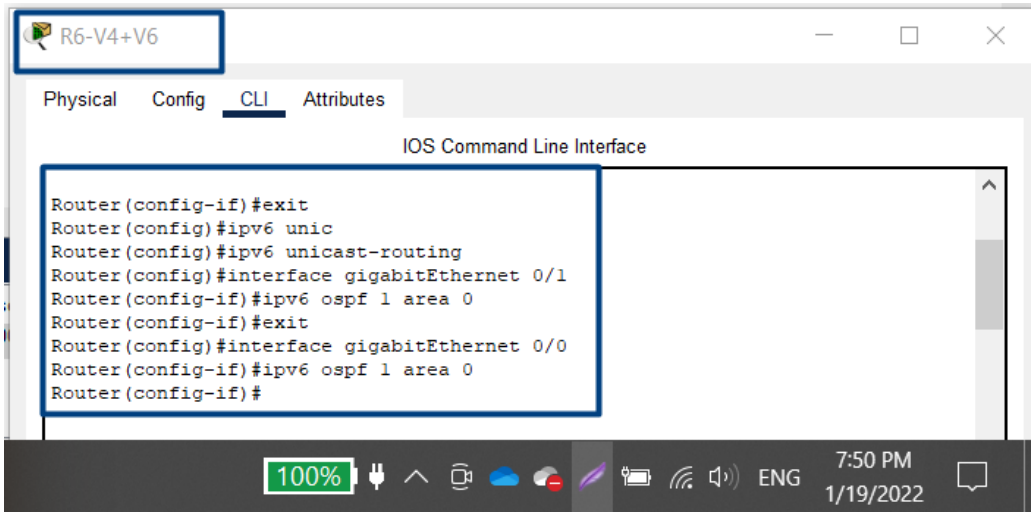

*Figure2.7. 1 (*Assigning OSPF to Router R6)

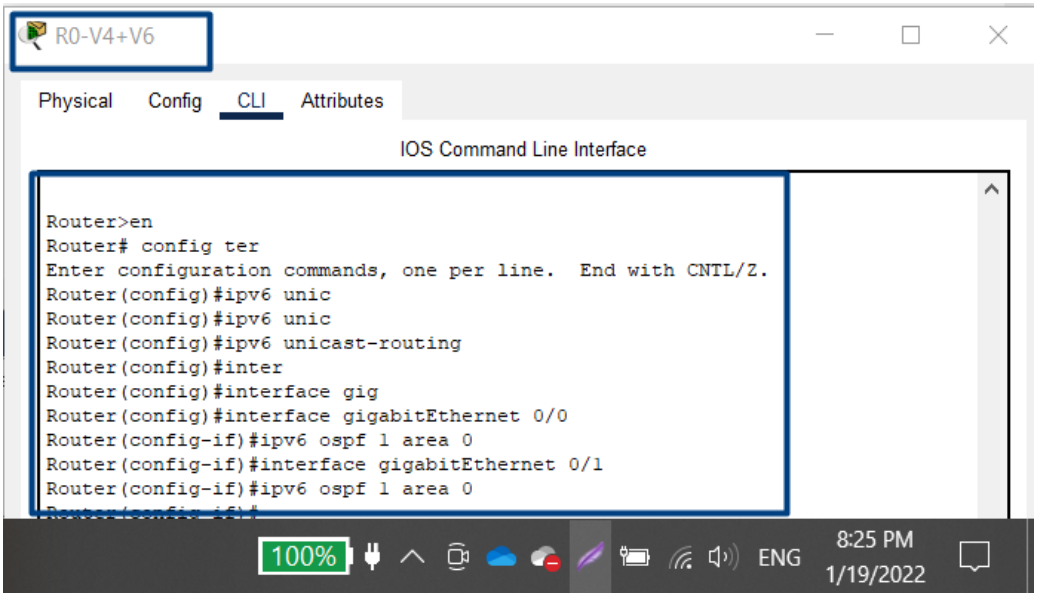

*Figure2.7. 2 (*Assigning OSPF to Router R0)

Note, the same thing done to R1 & R5 .

8. Applying Tunnel between R1 and R5.

The main idea of creating the tunnel is to specify the source IP address of the tunnel and the destination IP-address. The tunnel importance is to allow the IPv6 packets travel through IPv4 routers by encapsulating the IPv6 datagram as a payload in IPv4 datagram**.[5]**

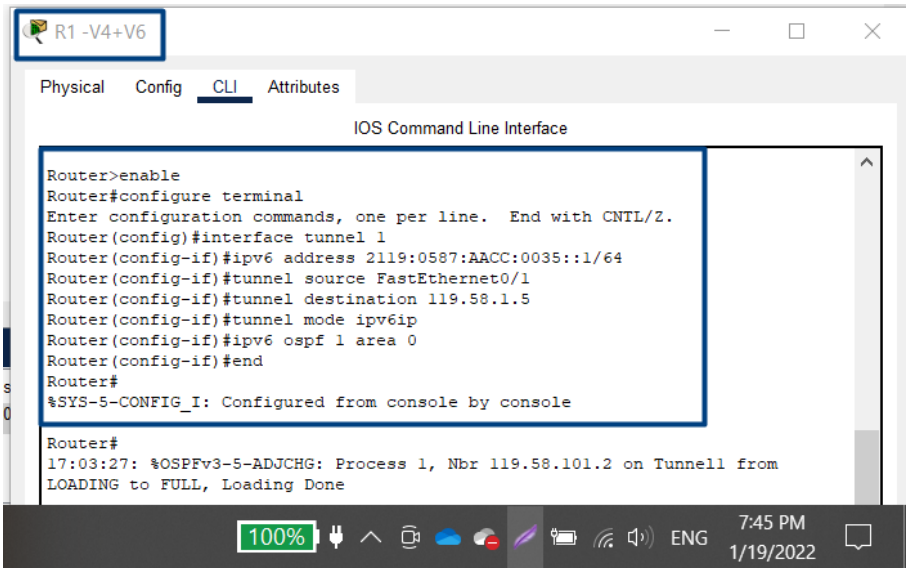

*Figure2.8. 1 (*Tunneling in R1)

Tunnel 1 was created in Router R1 side, the source IP -address is the interface **fastEthernet 0/1** and the destination IP-address was specified using the **IP 119.58.1.5.** After creating the tunnel, the OSPF was implemented to let the tunnel communicate with any network.

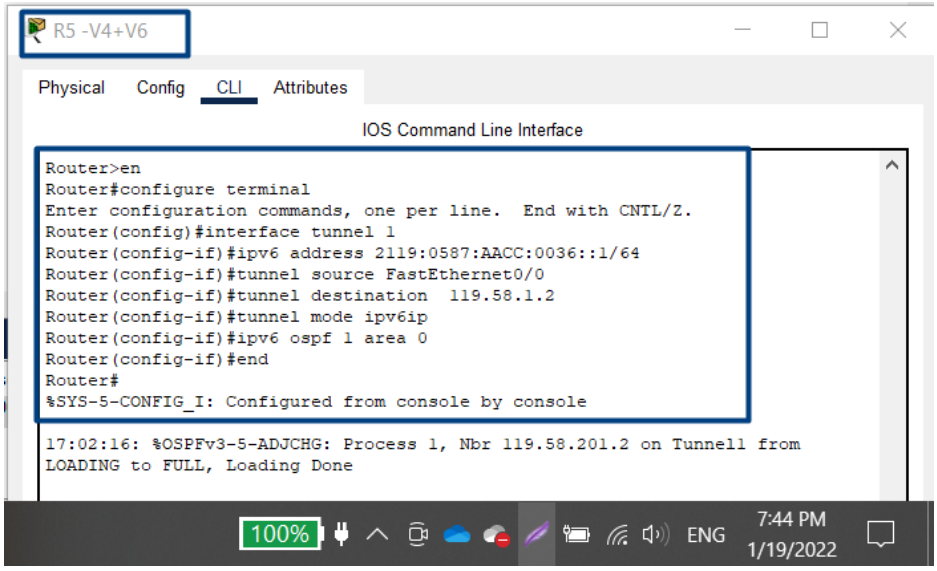

*Figure2.8. 2 (*Tunneling in R5)

Same thing to router (R5) But with different source and destination IPs.

9. Ping IPv6 in R6 from R0.

To check if the tunnel is working or not, the ping command between R0 and any IPv6 in R6 shows the network is connected.

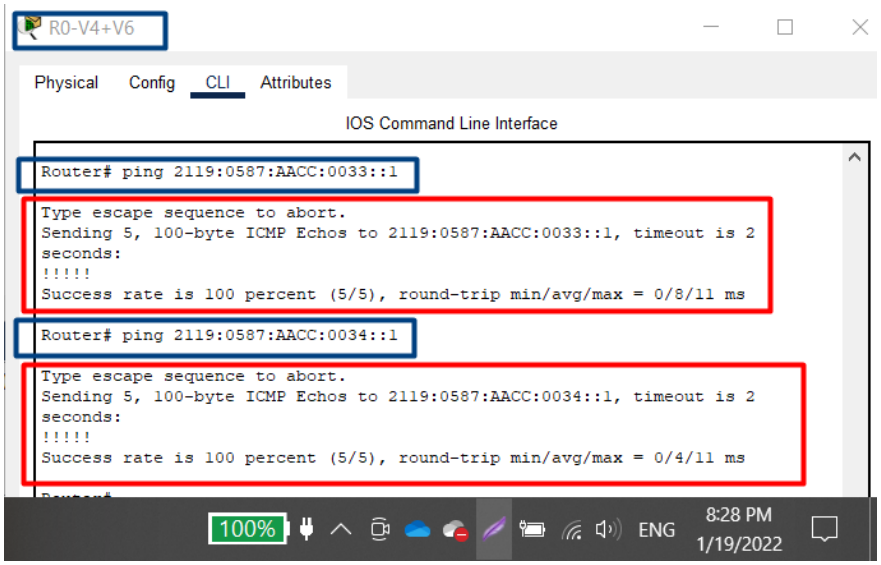

Figure2.9. 1 (result of pinging R6 from R0)

10. Ping from PC01 to PC61

Pinging PC61 from PCP1 is working 100% since the network is connected.

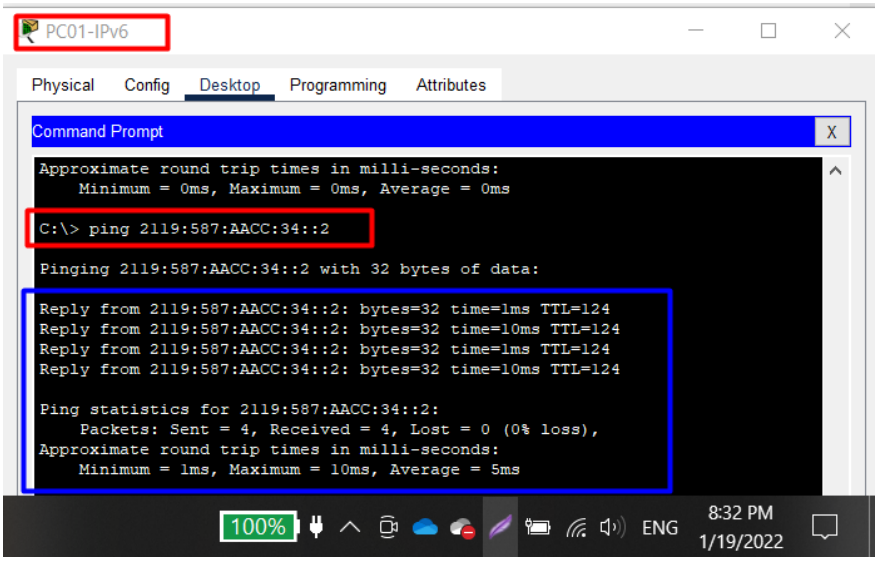

Figure2.10. 1 (result of pinging PC61 from PC01)

11. Ping from PC02 to PC62.

The ping command succeed. The lost is 0% and the received packets are 100%.

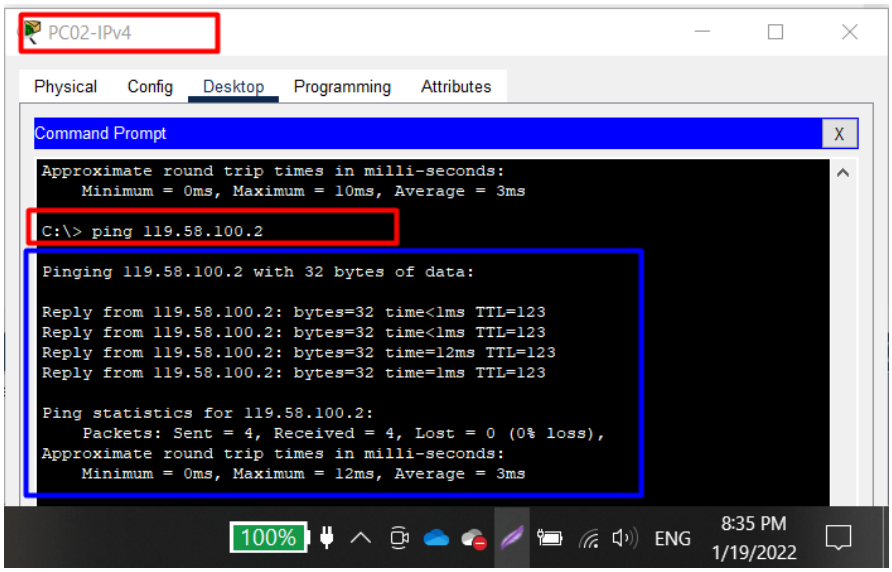

Figure2.11. 1 (result of pinging PC62 from PC02)

12. Ping from PC01 to PC62.

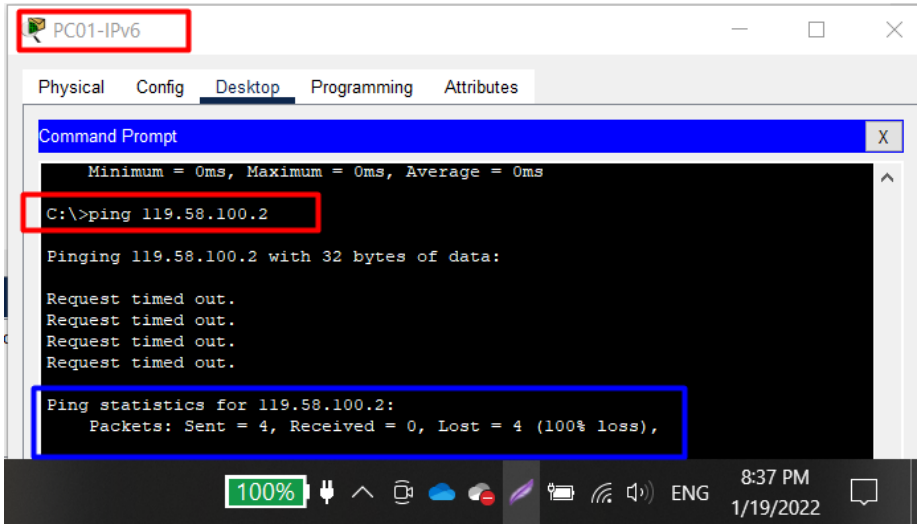

Figure2.12. 1 (result of pinging PC62 from PC02)

This command will not work, because the PC01 is IPv4 and the PC62 is IPv6. ***(Different protocols).*** **[6]**

Conclusion

In this project, we learnt more and more about computer network protocols, especially DHCP, ICMP and TCP protocols, how they work, how to get information about each one of them. In the second part, a network was implemented, with all components such as routers, switches and hosts, we learnt a lot how to assign IP addresses to routers and host, with two version of IP, which are IP version4 and IP version6, also we learnt how to be able to transmit data between two PC's in the same network, and also in different networks, and how to implement a Tunnel between two routers in order to exchange data easily.

References

[1] https://www.comptia.org/content/guides/what-is-a-network-protocol [Accessed on 18-1-2022]

[2] https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top [Accessed on 18-1-2022]

[3] https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/ [Accessed on 18-1-2022]

[4] https://www.sdxcentral.com/resources/glossary/transmission-control-protocol-tcp/

[Accessed on 18-1-2022]

[5] Cisco. (2017, June 5). *IPv6 tunnel through an ipv4 network*. Cisco. Retrieved January 19, 2022, from https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6/25156-ipv6tunnel.html

[6] Cisco Learning Network. (2017, June 11). Retrieved January 19, 2022, from https://learningnetwork.cisco.com/s/question/0D53i00000Kt6hhCAB/ping-from-ipv4-to-ipv6