FACULTY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER ENGINEERING

Computer Networks
ENCS3320

Project 2 Report

Prepared by:

Tariq Odeh	1190699
Qays Safa	1190880
Mahmoud Samara	1191602

Sec: 2

Instructor: Dr. Abdalkarim Awad

Date: 14th January 2022

Table of Contents

1. Part I:

Using Wireshark, capture few DHCP and ICMP packets. Show the packets, write some comments about each picture and explain at least 3 fields of each packet. Capture a TCP session for transferring a large file, show the sequence number of three packets and the ACK numbers, conclude the data size on two packets.

1.1. DHCP

First of all, we will use Wireshark program to capture DHCP packets. Now to make this first we will open CMD and write (ipconfig /release) this command used to release current IP address. After that, we write (ipconfig /renew) this command used to obtain a new IP address. Finally, we go to Wireshark program and write DHCP and start capturing to get the result as shown in the following picture.

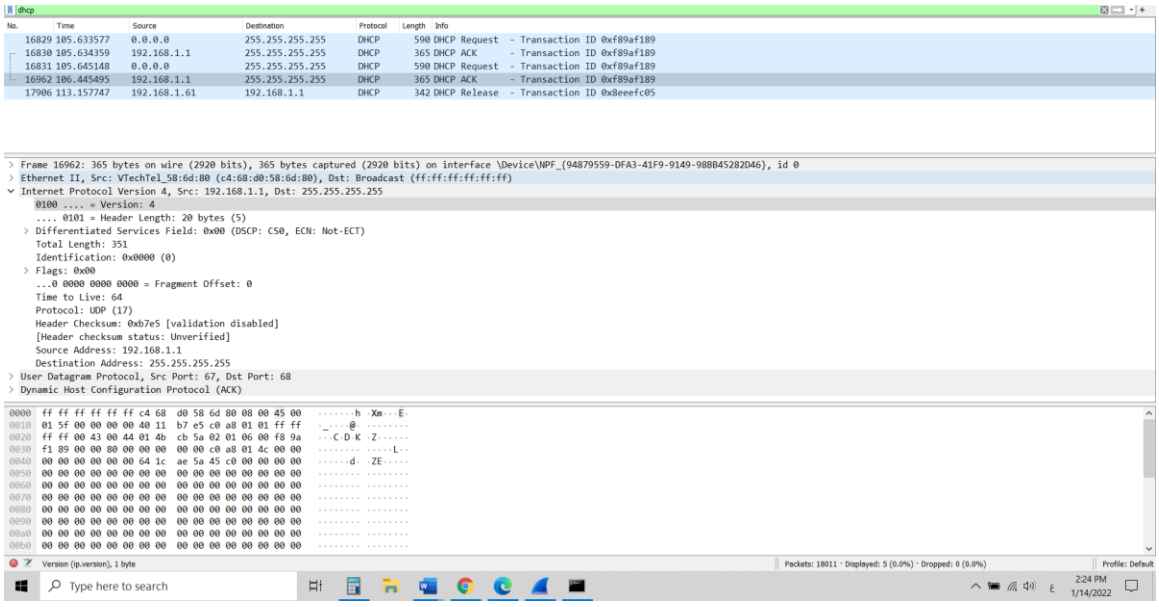


Figure 1: DHCP result

For the fields we will explain are: the internet protocol addressing version is IPV4. In addition, for DHCP the total length of the packets is 351 bits. Moreover, the source port of the packets equal 67, while the destination port of the packets equal 68. Finally, the packet can travel through 64 routers (TTL).

1.2. ICMP

First of all, we will use Wireshark program to capture ICMP packets. Now to make this first we will open CMD and write the following command (ping www.youtube.com). Finally, we go to Wireshark program and write ICMP and start capturing to get the result as shown in the following picture.

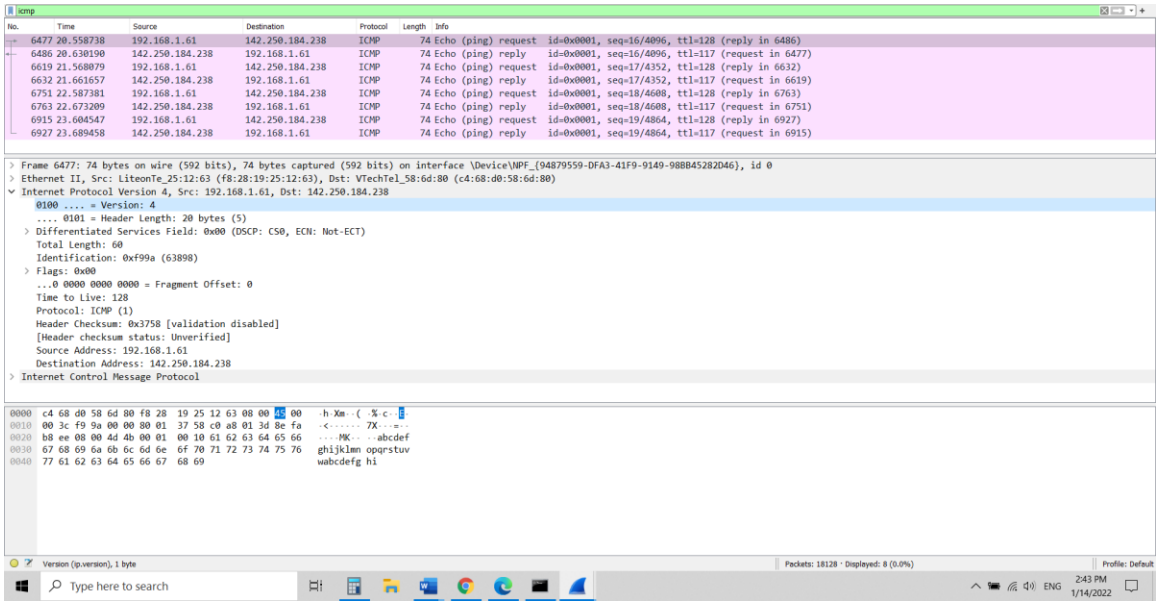


Figure 2: : ICMP result

For the fields we will explain are: the internet protocol addressing version is IPV4. In addition, for ICMP the total length of the packets is 60 bits. Moreover, the local IP address of my PC = 192.168.1.61, while the destination the IP address of the destination = 142.250.184.238 which is YouTube address. Finally, the packet can travel through 128 routers (TTL).

1.3. TCP

First of all, we will use Wireshark program to capture TCP session. Now to make this first we will open CMD and write the following command (ipconfig) to get my pc ip address 192.186.1.158, and then write the following command (nslookup) to get Ritaj ip address 104.22.8.107 where we had sent the file via Ritaj. Finally, we go to Wireshark program and write TCP to filtering the results and start capturing to get the result as shown in the following pictures.

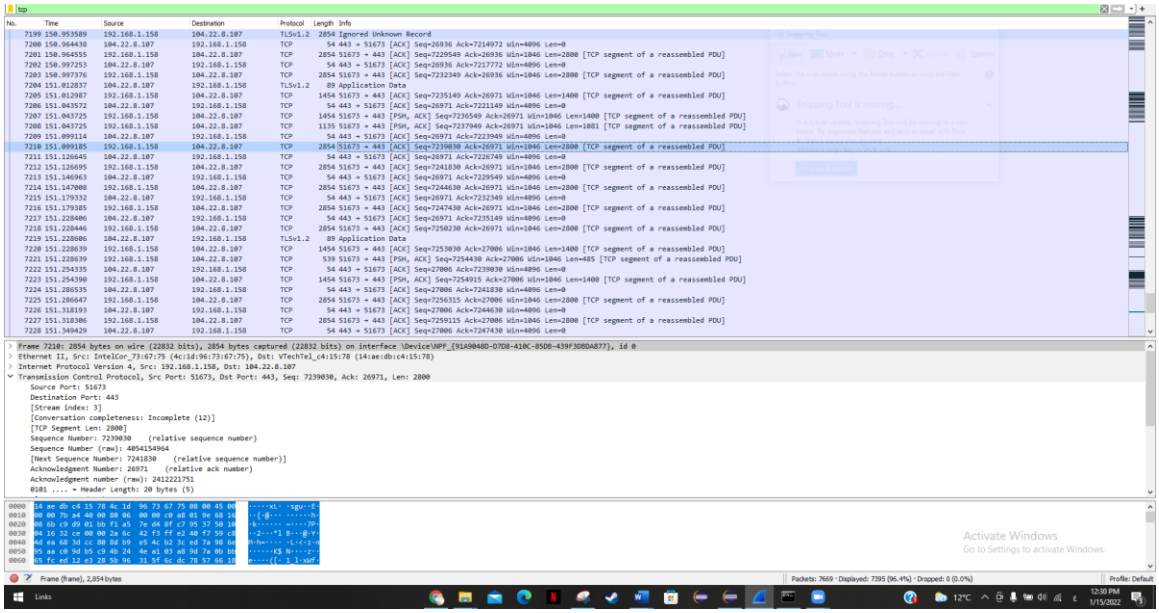


Figure 3: first packet

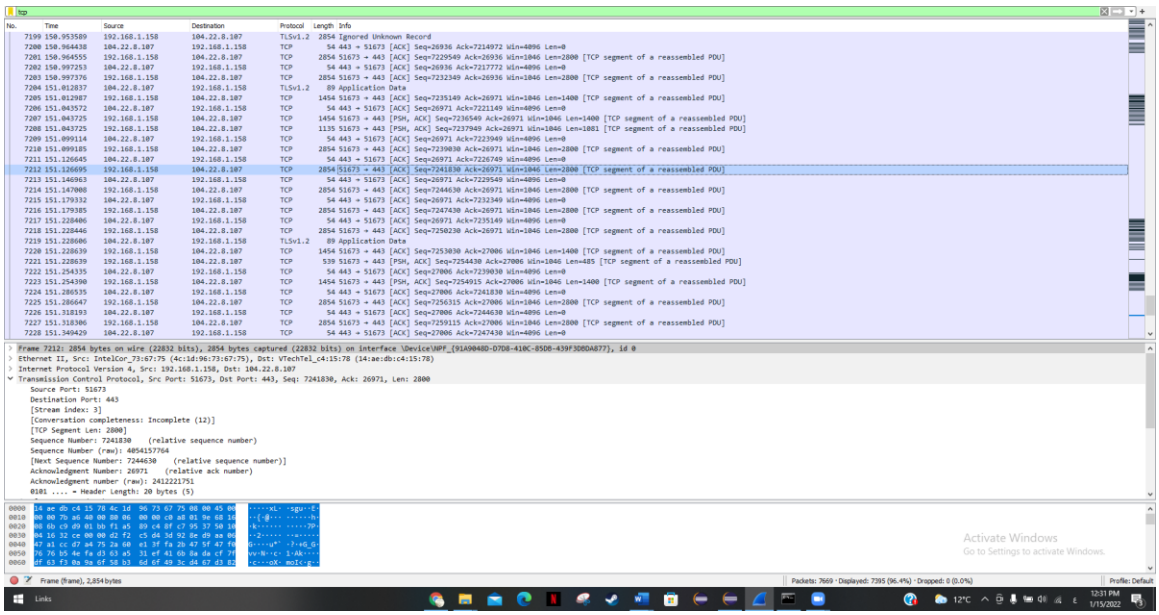


Figure 4: second packet

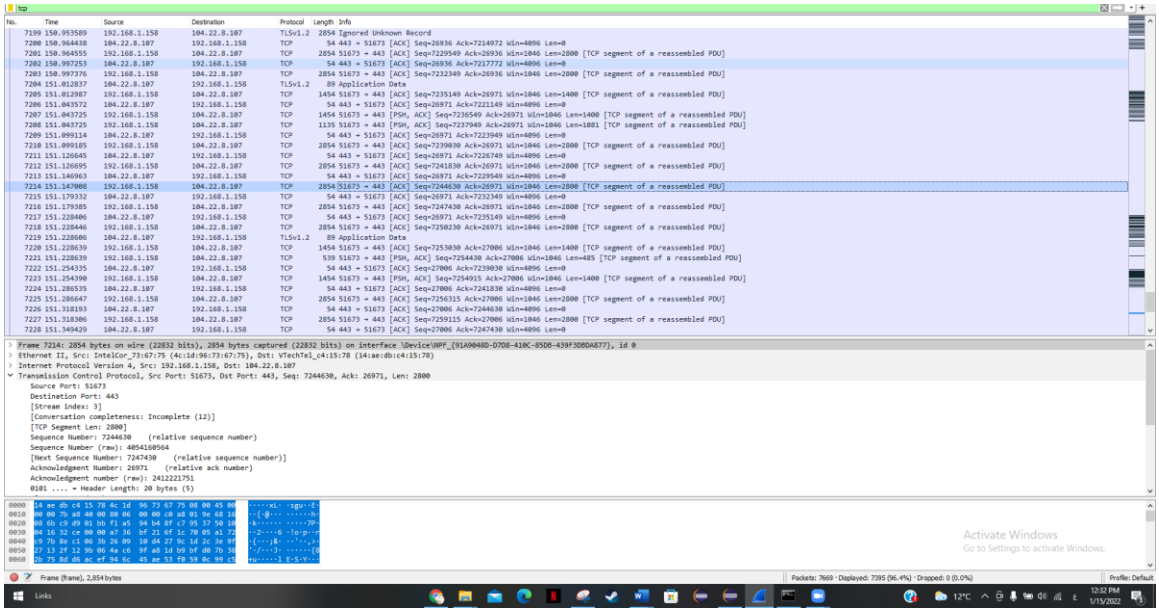


Figure 5: third packet

From the figure 3 we can see that the sequence number of the first packet we choose is (7239030) and we can see that the next seq number is (7241830) and from the seq number and the next seq number we can see from the difference between them we got number (2800) and this number is the TCP segment length (data size). We can also see the Acknowledgment number (26971).

And from the figure 4 we can see that the sequence number of the second packet we choose is (7241830) and we can see that the next seq number is (7244630) and from the seq number and the next seq number we can see from the difference between them we got number (2800) and this number is the TCP segment length (data size). We can also see the Acknowledgment number (26971).

And from the figure 5 we can see that the sequence number of the third packet we choose is (7244630) and we can see that the next seq number is (7247430) and from the seq number and the next seq number we can see from the difference between them we got number (2800) and this number is the TCP segment length (data size). We can also see the Acknowledgment number (26971).

2. Part II

2.1. Implementation steps

step 1: We connected all the devices such as what is required and given. In addition, we are repairing IPs based on IP addressing criteria that given. The student ID they used is (1191602).

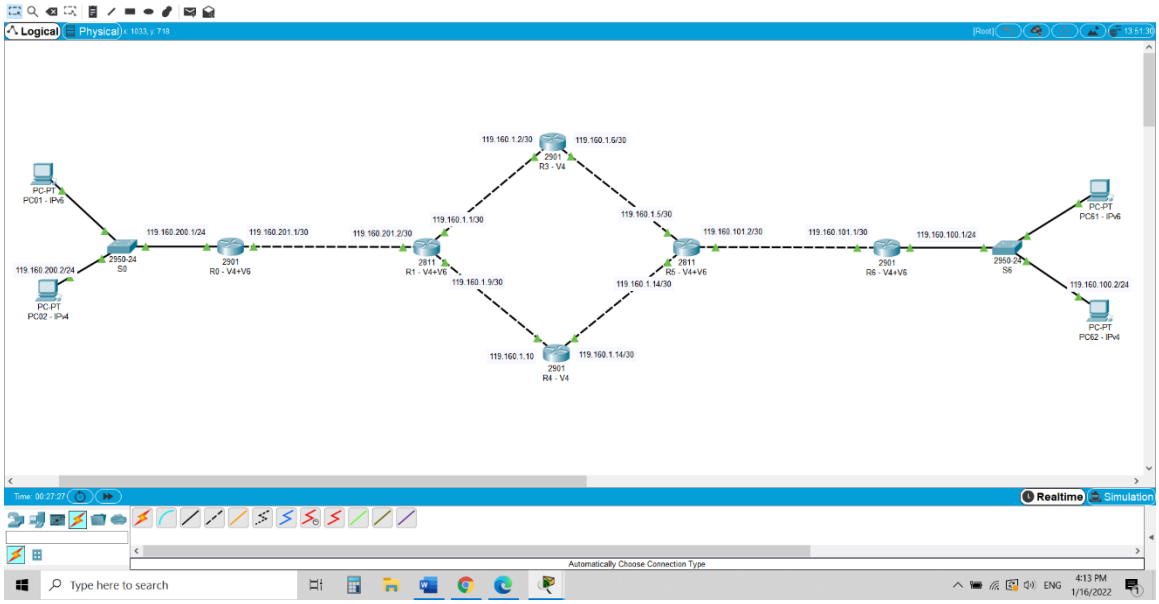


Figure 6: implement the network

step 2: We Assign IP addresses to all PCs. Moreover, we assigned IP addresses to all router interfaces and we added the gateways to PCs.

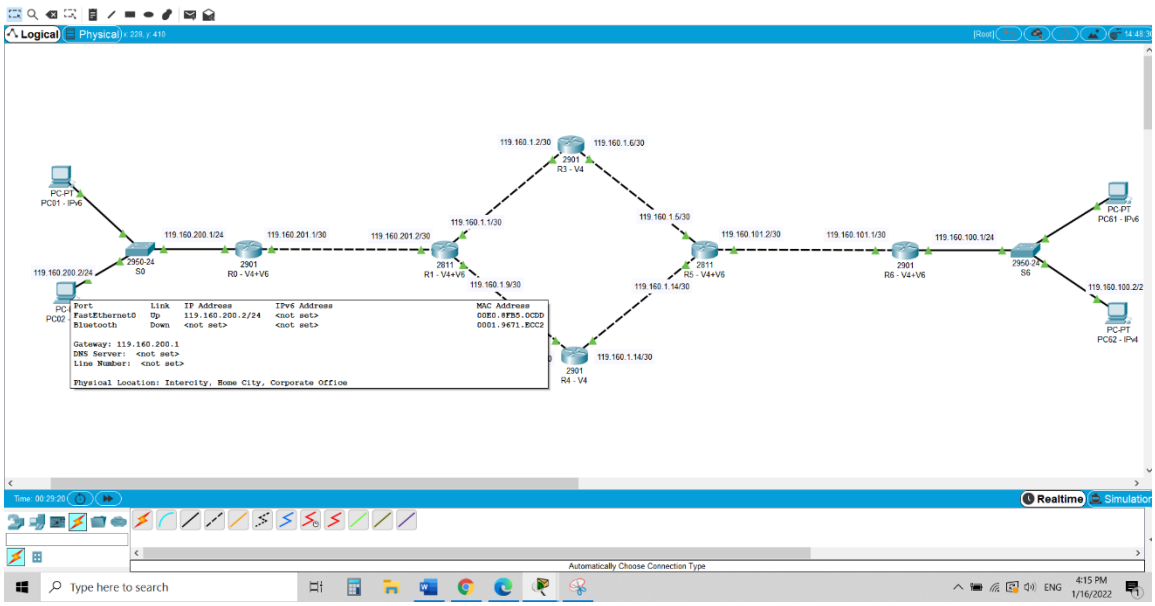


Figure 7: Assign IP addresses

step 3: We have done OSPF for all routers that include IPV4 which is (R0, R1, R3, R4, R5, R6).

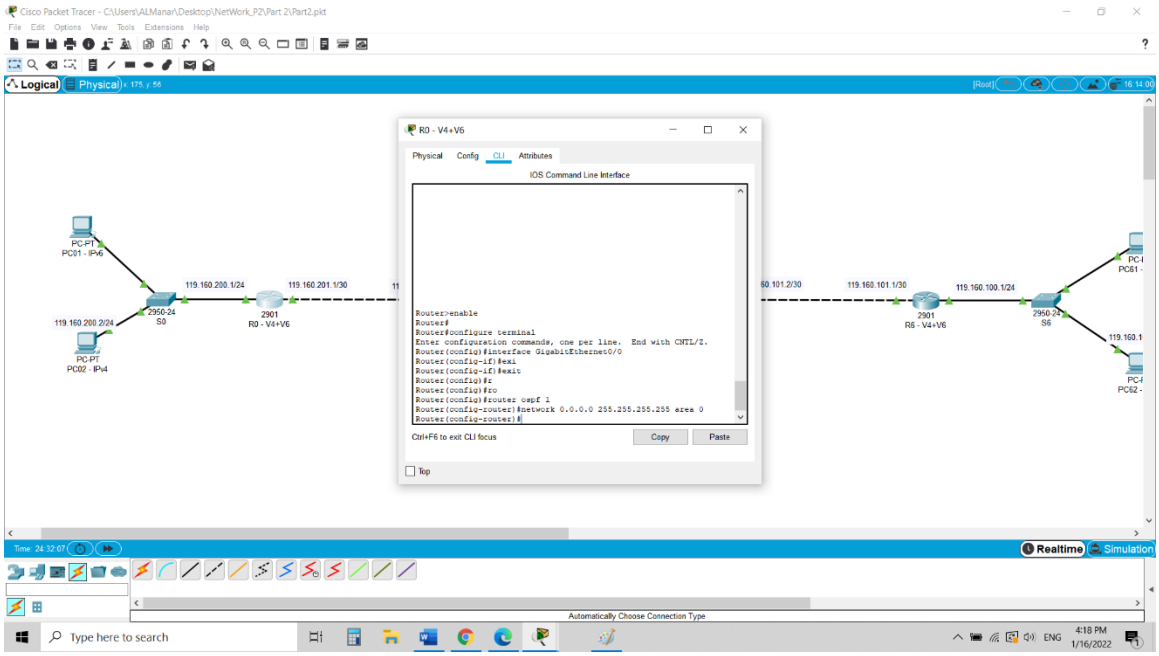


Figure 8: Implement single area OSPF routing protocol for IPv4

step 4: We made a check between the routers and other devices to ensure the correctness of the work (by using ping). To make that we checked the connection between PC02 and PC62 with all routers and between each other.

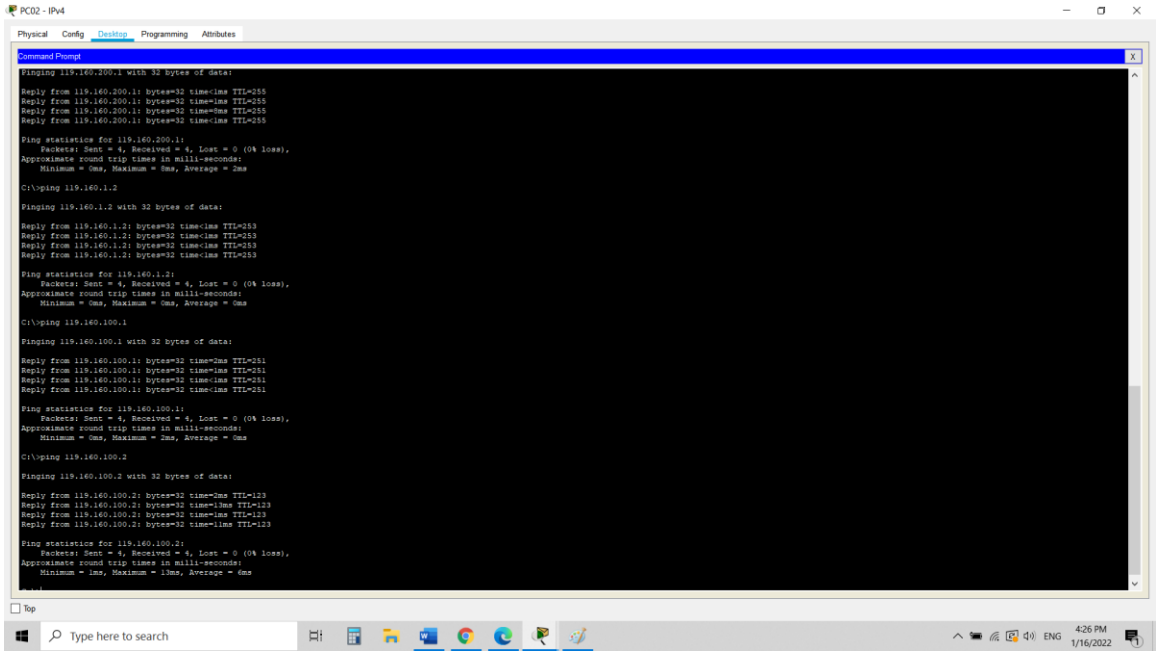


Figure 9: Make sure Pc02 can ping

step 5: We assigned the IP addresses that relate to IPV6 and also set the gateway for PCs that deal with IPV6.

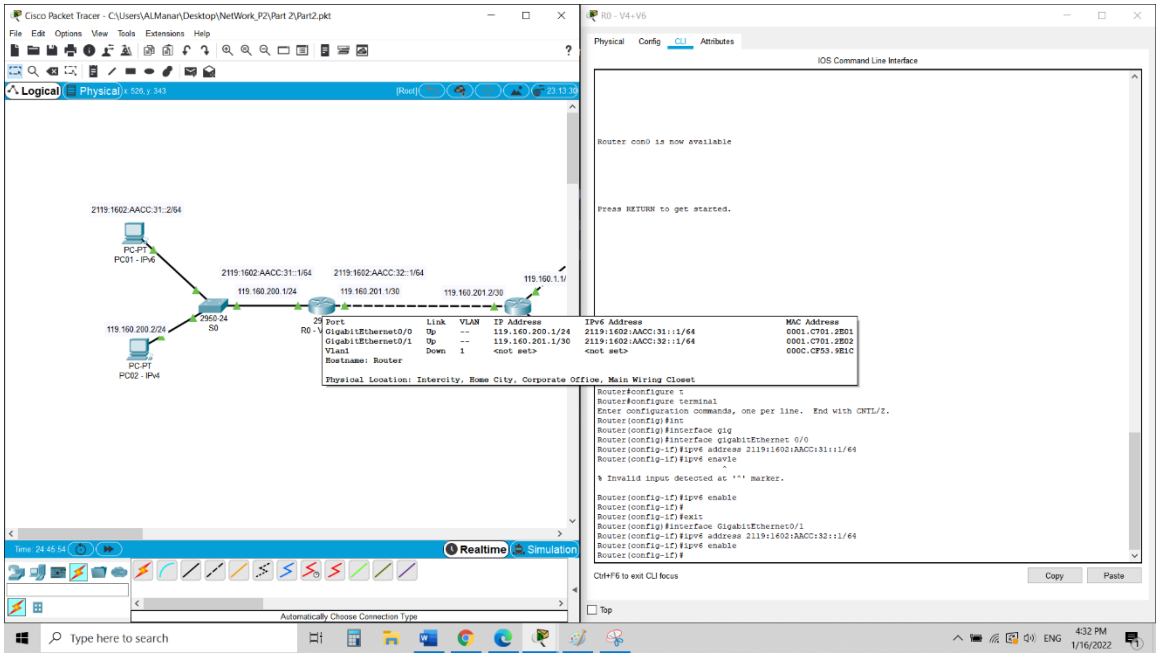


Figure 10: assigned the IP addresses that relate to IPV6

step 6: we have done OSPF for all routers that include IPV6 which is (R0, R1, R5, R6).

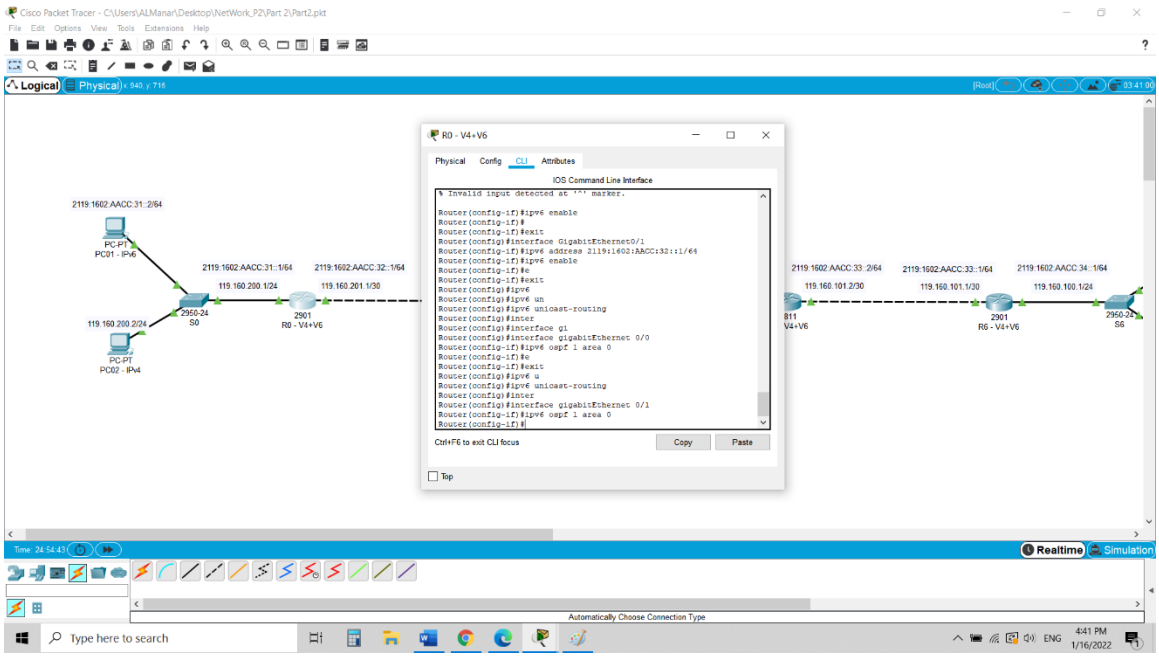


Figure 11: Implement single area OSPF routing protocol for IPv6

step 7: We implement a tunnel (IPv6 over IPv4) between R1 and R5, and this help us to allow IPv6 traffic to pass through these routers. In addition, we will do OSPF in order to do ping in IPV6 through this tunnel.

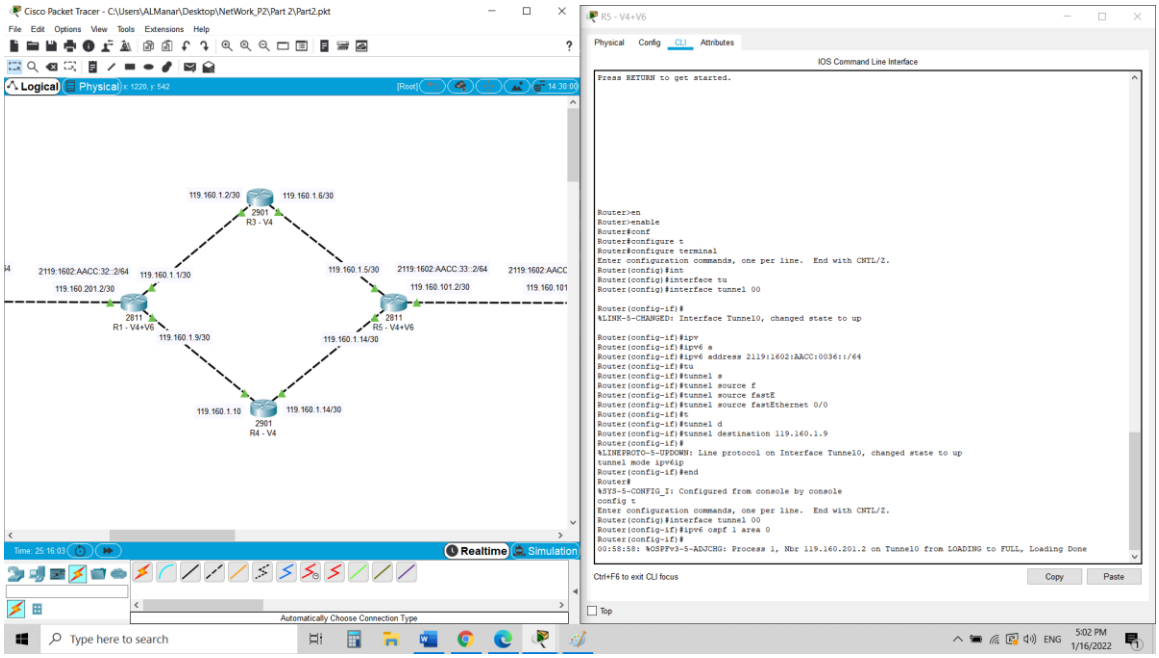


Figure 12: implement a tunnel

step 8: We made a check between the routers and other devices to ensure the correctness of the work (by using ping), so we checked the connection between PC01 and PC61 with all routers and between each other.

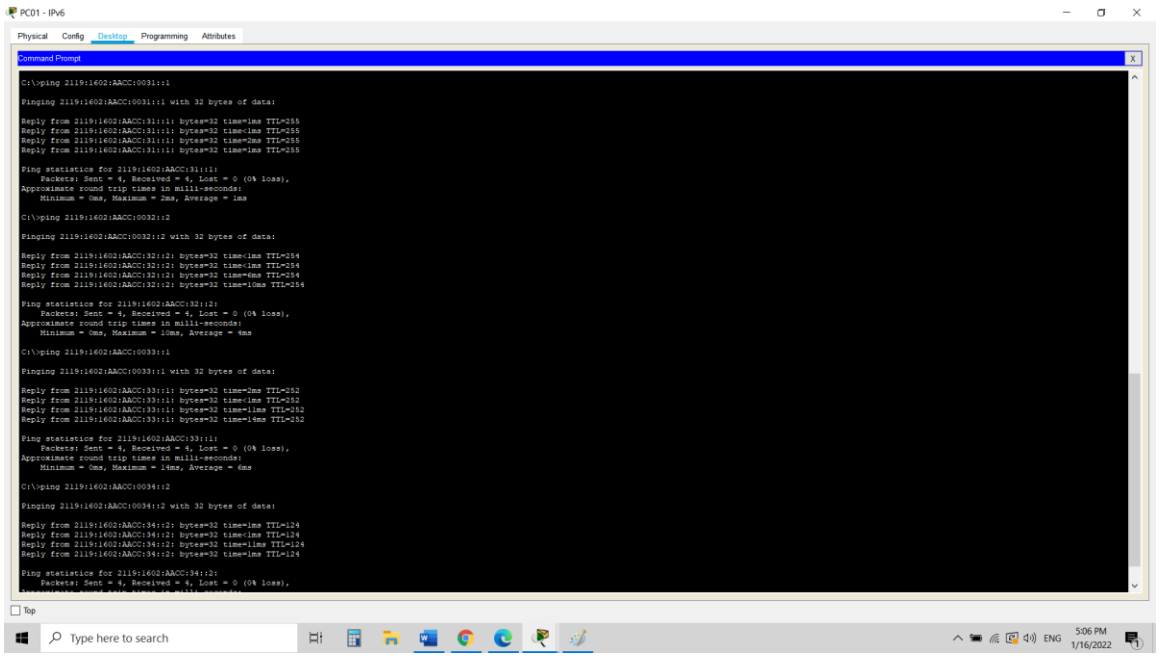


Figure 13: Make sure Pc01 can ping

2.2. Assign IP addresses to all PCs

We can see in the figure below the IP addresses assigned to PC02, and in the same way the IP addresses assigned to the rest of the PCs were defined.

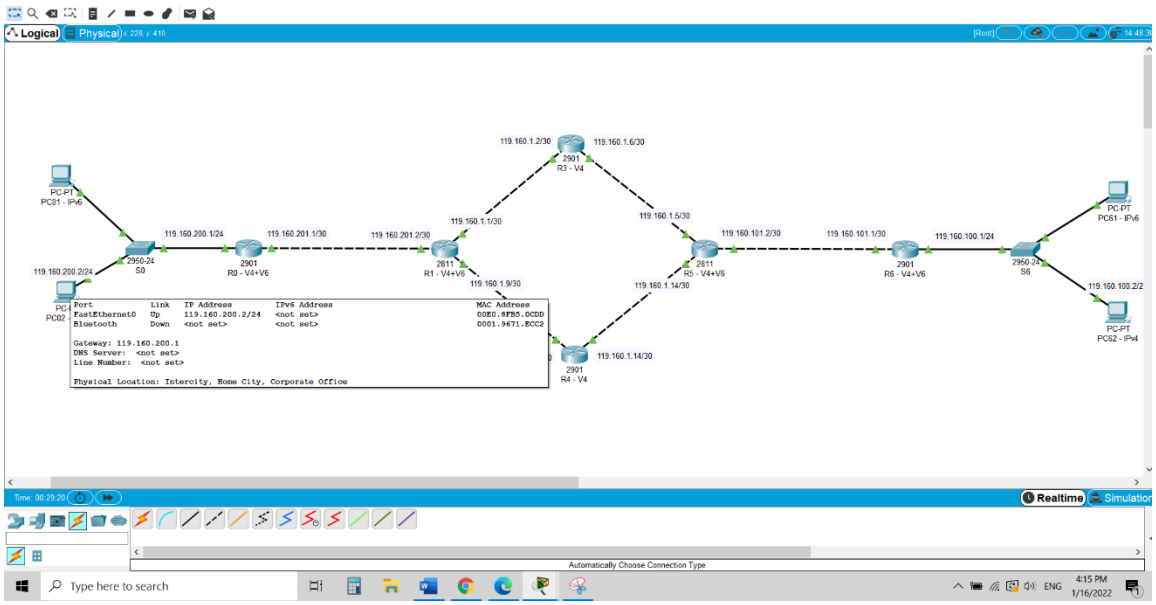


Figure 14: Assign IP addresses to PC02

2.3. Assign IP addresses to all router interfaces

We can see in the figure below the IP addresses assigned to R1, and in the same way the IP addresses assigned to the rest of the routers were defined.

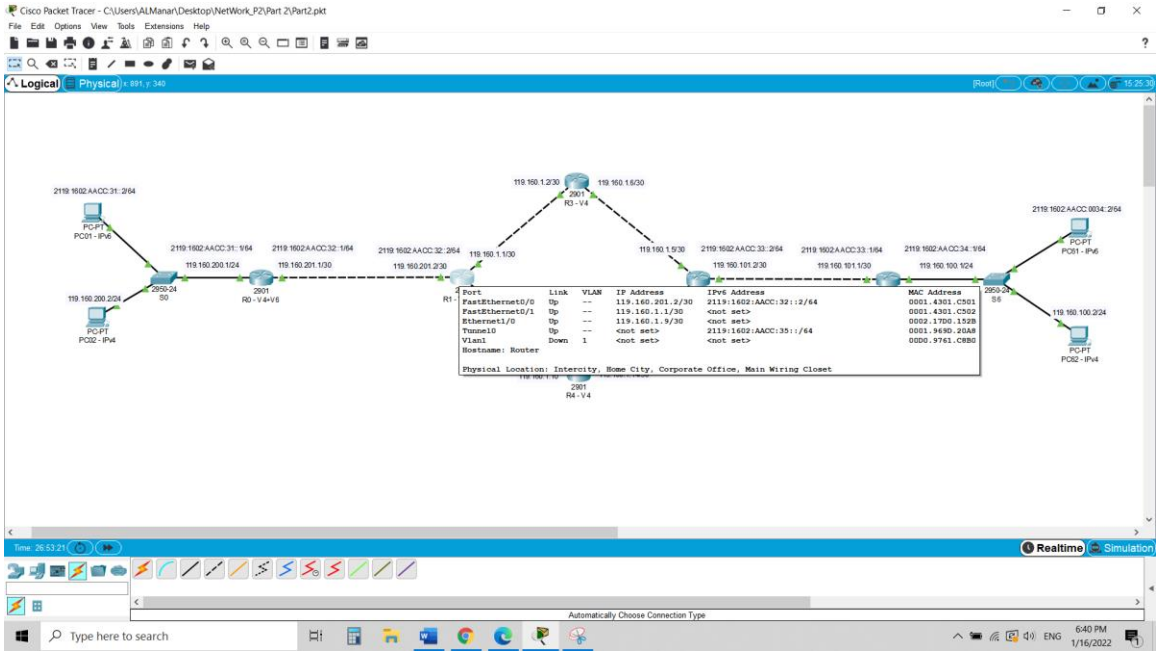
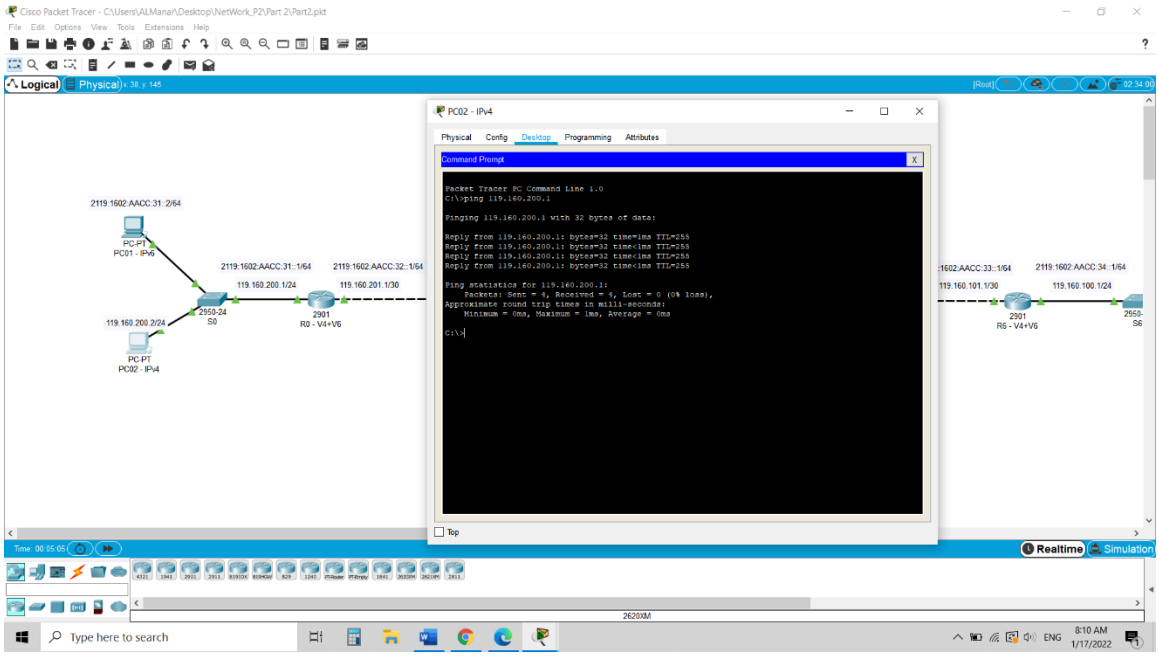
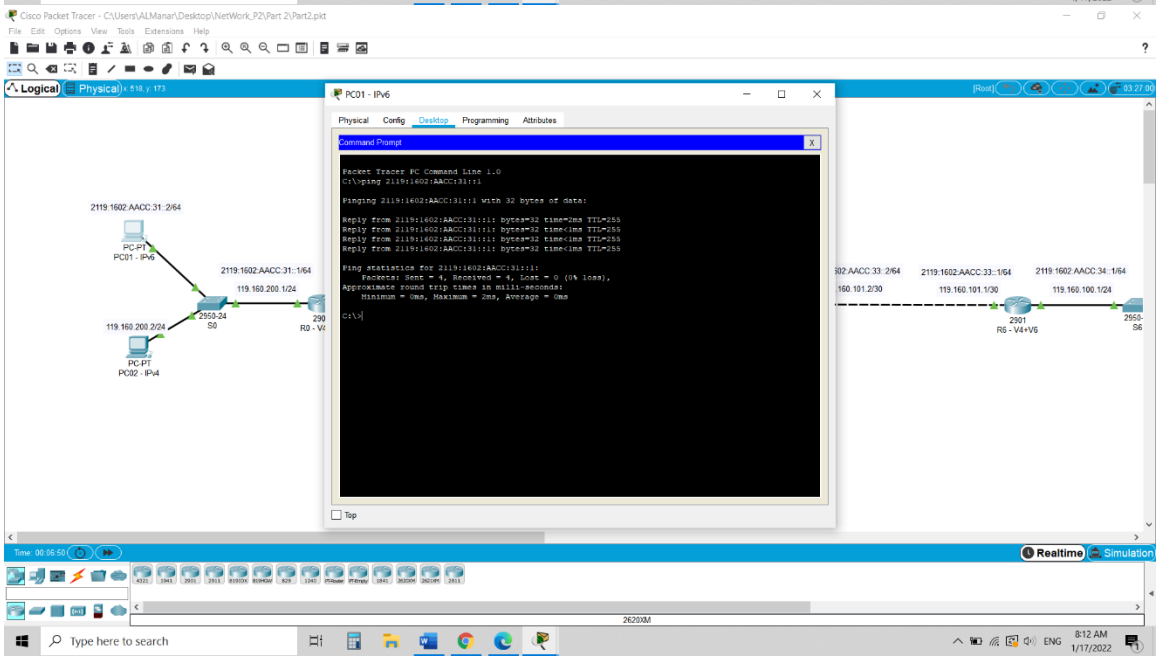


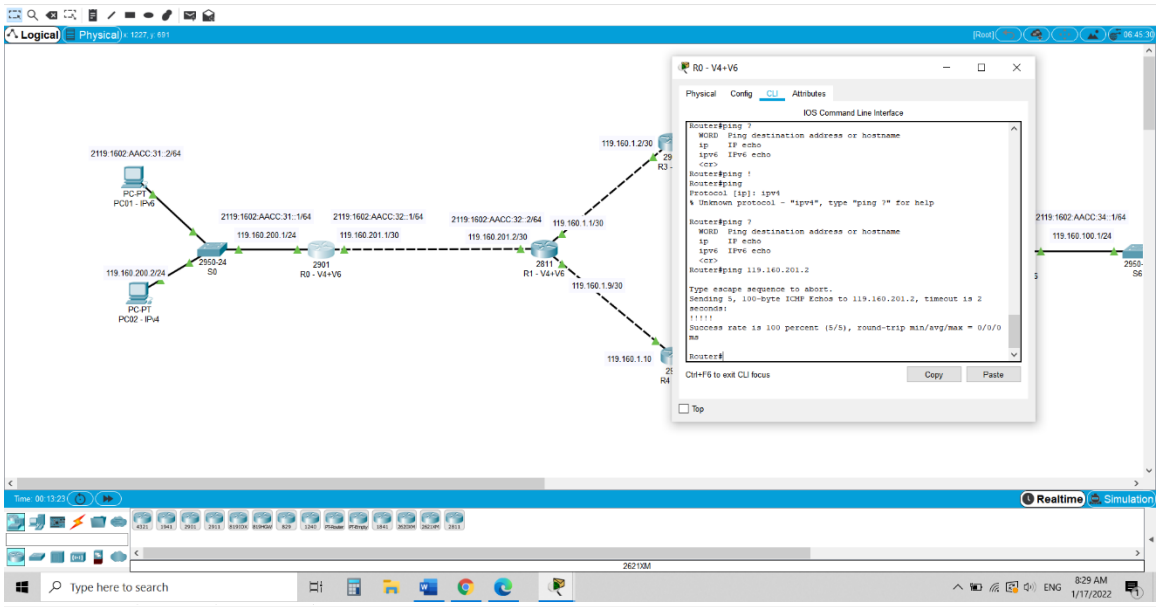
Figure 15: Assign IP addresses to R1

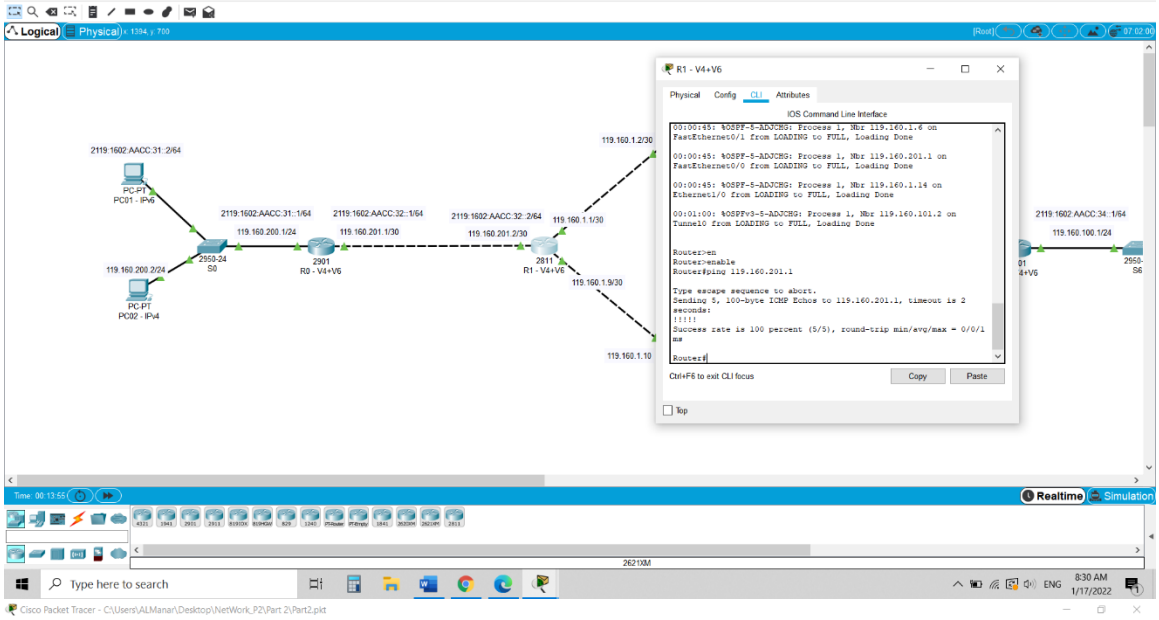
2.4. Make sure each host can ping at least one other host in the same network.

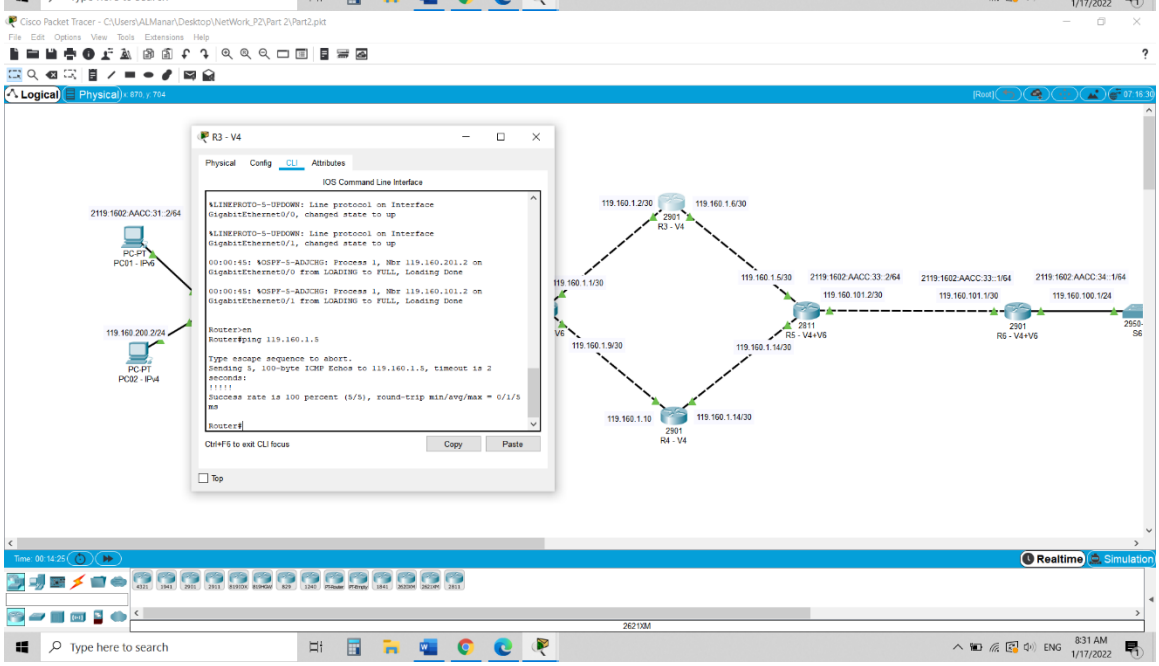
We made sure that each host can ping at least one other host in the same network, where we made sure of all PCs (PC01, PC02, PC61 and PC62), and we made sure of all routers (R0, R1, R3, R4, R5and R6). The pictures below explain this to each host.

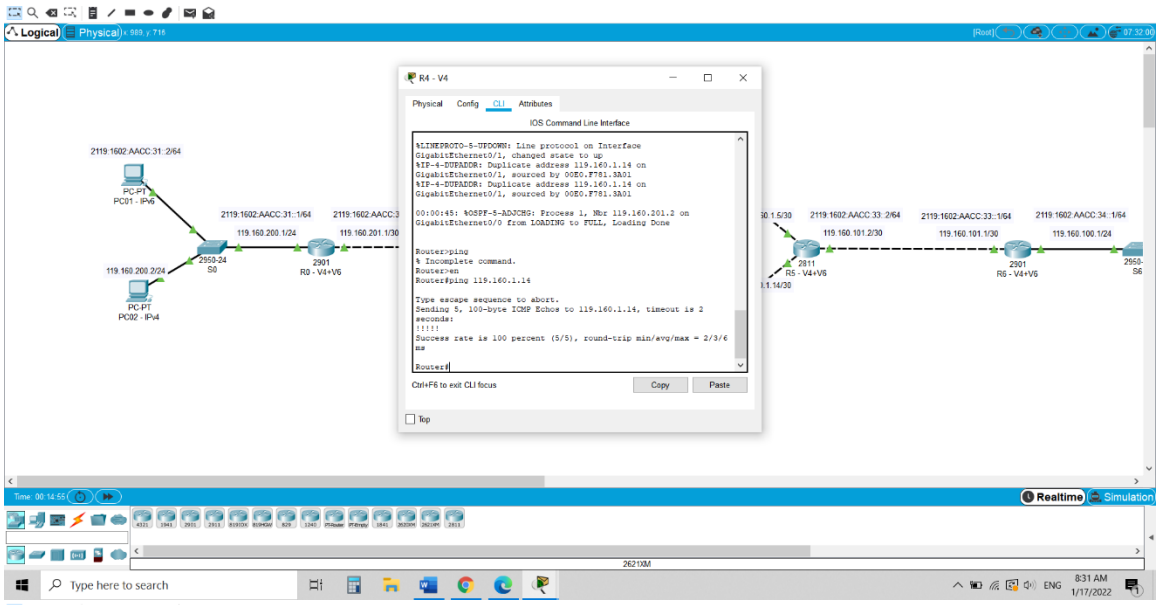


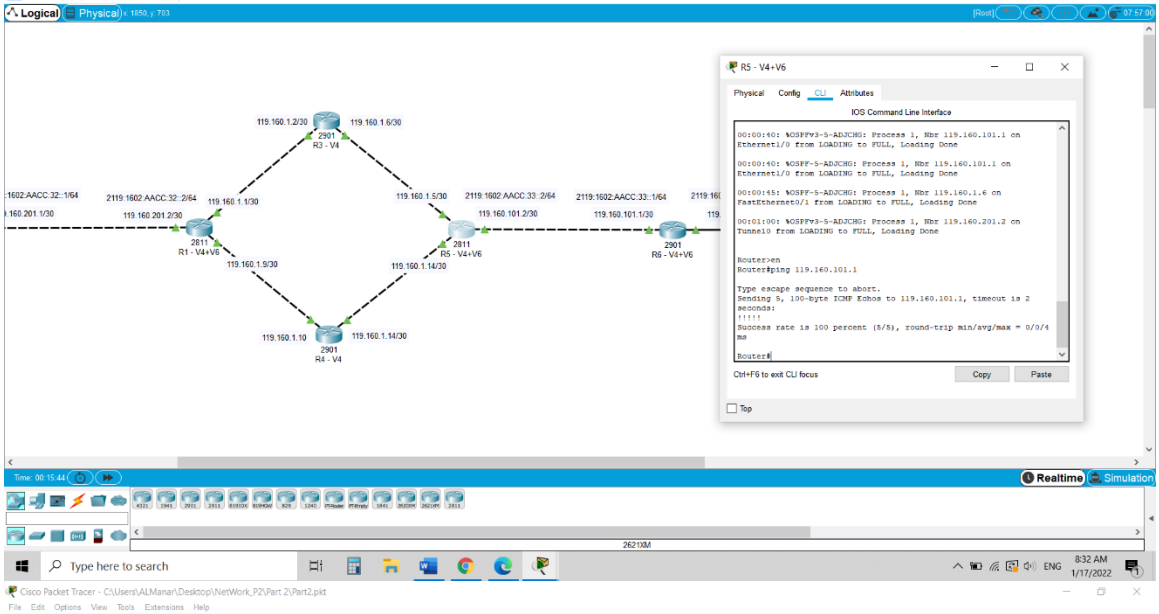


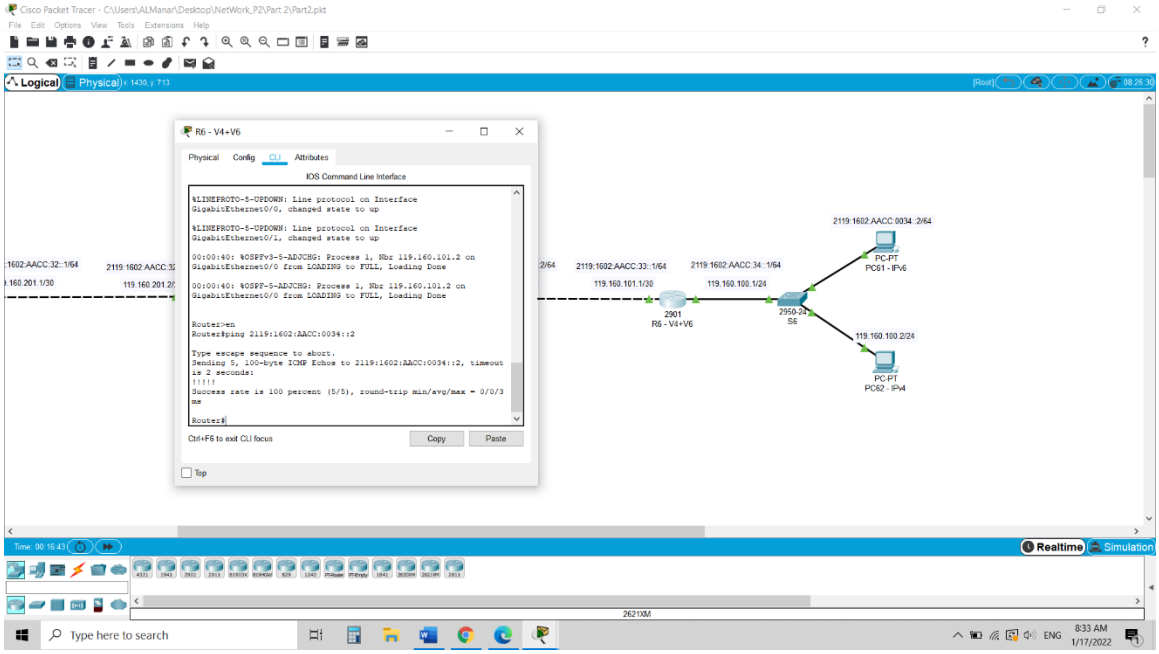

R0 - V4+V6
Physical Config CLI Attributes
IOS Command Line Interface
Router#ping ?
WORD Ping destination address or hostname
ip IP echo
ipv6 IPv6 echo
<cr>
Router#ping !
Router#ping
Protocol [ip]: ipv4
% Unknown protocol - "ipv4", type "ping ?" for help
Router#ping ?
WORD Ping destination address or hostname
ip IP echo
ipv6 IPv6 echo
<cr>
Router#ping 119.160.201.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 119.160.201.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
2119:1602:AACC:31::2/64
PC-PT PC01 - IPv6
119.160.200.2/24
PC-PT PC02 - IPv4
2950-24 S0
2119:1602:AACC:31::1/64
119.160.200.1/24
2901 R0 - V4+V6
2119:1602:AACC:32::1/64
119.160.201.1/30
2119:1602:AACC:32::2/64
119.160.201.2/30
2811 R1 - V4+V6
119.160.1.1/30
119.160.1.2/30
119.160.1.9/30
119.160.1.10
2119:1602:AACC:34::1/64
119.160.100.1/24
Realtime Simulation
Type here to search
8:29 AM 1/17/2022


R1 - V4+V6
Physical Config CLI Attributes
IOS Command Line Interface
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.1.6 on FastEthernet0/1 from LOADING to FULL, Loading Done
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.201.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.1.14 on Ethernet1/0 from LOADING to FULL, Loading Done
00:01:00: %OSPFv3-5-ADJCHG: Process 1, Nbr 119.160.101.2 on Tunnel0 from LOADING to FULL, Loading Done
Router>en
Router#enable
Router#ping 119.160.201.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 119.160.201.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
2119:1602:AACC:31::2/64
PC-PT PC01 - IPv6
119.160.200.2/24
PC-PT PC02 - IPv4
2950-24 S0
2119:1602:AACC:31::1/64
119.160.200.1/24
2901 R0 - V4+V6
2119:1602:AACC:32::1/64
119.160.201.1/30
2119:1602:AACC:32::2/64
119.160.201.2/30
2811 R1 - V4+V6
119.160.1.1/30
119.160.1.2/30
119.160.1.9/30
119.160.1.10
2119:1602:AACC:34::1/64
119.160.100.1/24
Realtime Simulation
Type here to search
8:30 AM 1/17/2022


Cisco Packet Tracer - C:\Users\ALManar\Desktop\NetWork_P2\Part 2\Part2.pkt
R3 - V4
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.201.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.101.2 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
Router>en
Router#ping 119.160.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 119.160.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
2119:1602:AACC:31::2/64
PC-PT PC01 - IPv6
119.160.200.2/24
PC-PT PC02 - IPv4
119.160.1.2/30
2901 R3 - V4
119.160.1.6/30
119.160.1.1/30
119.160.1.5/30
2119:1602:AACC:33::2/64
119.160.101.2/30
2119:1602:AACC:33::1/64
119.160.101.1/30
2119:1602:AACC:34::1/64
119.160.100.1/24
2811 R5 - V4+V6
2901 R6 - V4+V6
119.160.1.9/30
119.160.1.14/30
119.160.1.10
2901 R4 - V4
Realtime Simulation
Type here to search
8:31 AM 1/17/2022


R4 - V4
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%IP-4-DUPADDR: Duplicate address 119.160.1.14 on GigabitEthernet0/1, sourced by 00E0.F781.3A01
%IP-4-DUPADDR: Duplicate address 119.160.1.14 on GigabitEthernet0/1, sourced by 00E0.F781.3A01
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.201.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
Router>ping
% Incomplete command.
Router>en
Router#ping 119.160.1.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 119.160.1.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
2119:1602:AACC:31::2/64
PC-PT PC01 - IPv6
119.160.200.2/24
PC-PT PC02 - IPv4
2950-24 S0
119.160.200.1/24
119.160.201.1/30
2901 R0 - V4+V6
2119:1602:AACC:33::2/64
119.160.101.2/30
2811 R5 - V4+V6
119.160.101.1/30
2901 R6 - V4+V6
119.160.100.1/24
2950- S6


R5 - V4+V6
Physical Config CLI Attributes
IOS Command Line Interface
00:00:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 119.160.101.1 on Ethernet1/0 from LOADING to FULL, Loading Done
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.101.1 on Ethernet1/0 from LOADING to FULL, Loading Done
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.1.6 on FastEthernet0/1 from LOADING to FULL, Loading Done
00:01:00: %OSPFv3-5-ADJCHG: Process 1, Nbr 119.160.201.2 on Tunnel0 from LOADING to FULL, Loading Done
Router>en
Router#ping 119.160.101.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 119.160.101.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
119.160.1.2/30
119.160.1.6/30
2901 R3 - V4
2811 R1 - V4+V6
119.160.1.1/30
119.160.1.5/30
2811 R5 - V4+V6
119.160.1.9/30
119.160.1.14/30
119.160.1.10
2901 R4 - V4
2119:1602:AACC:33::1/64
2901 R6 - V4+V6


Cisco Packet Tracer - C:\Users\ALManar\Desktop\NetWork_P2\Part 2\Part2.pkt
R6 - V4+V6
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
00:00:40: %OSPFv3-5-ADJCHG: Process 1, Nbr 119.160.101.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 119.160.101.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done
Router>en
Router#ping 2119:1602:AACC:0034::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2119:1602:AACC:0034::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
Router#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
2119:1602:AACC:0034::2/64
PC-PT PC01 - IPv6
119.160.100.2/24
PC-PT PC02 - IPv4
2901 R6 - V4+V6
119.160.101.1/30
119.160.100.1/24

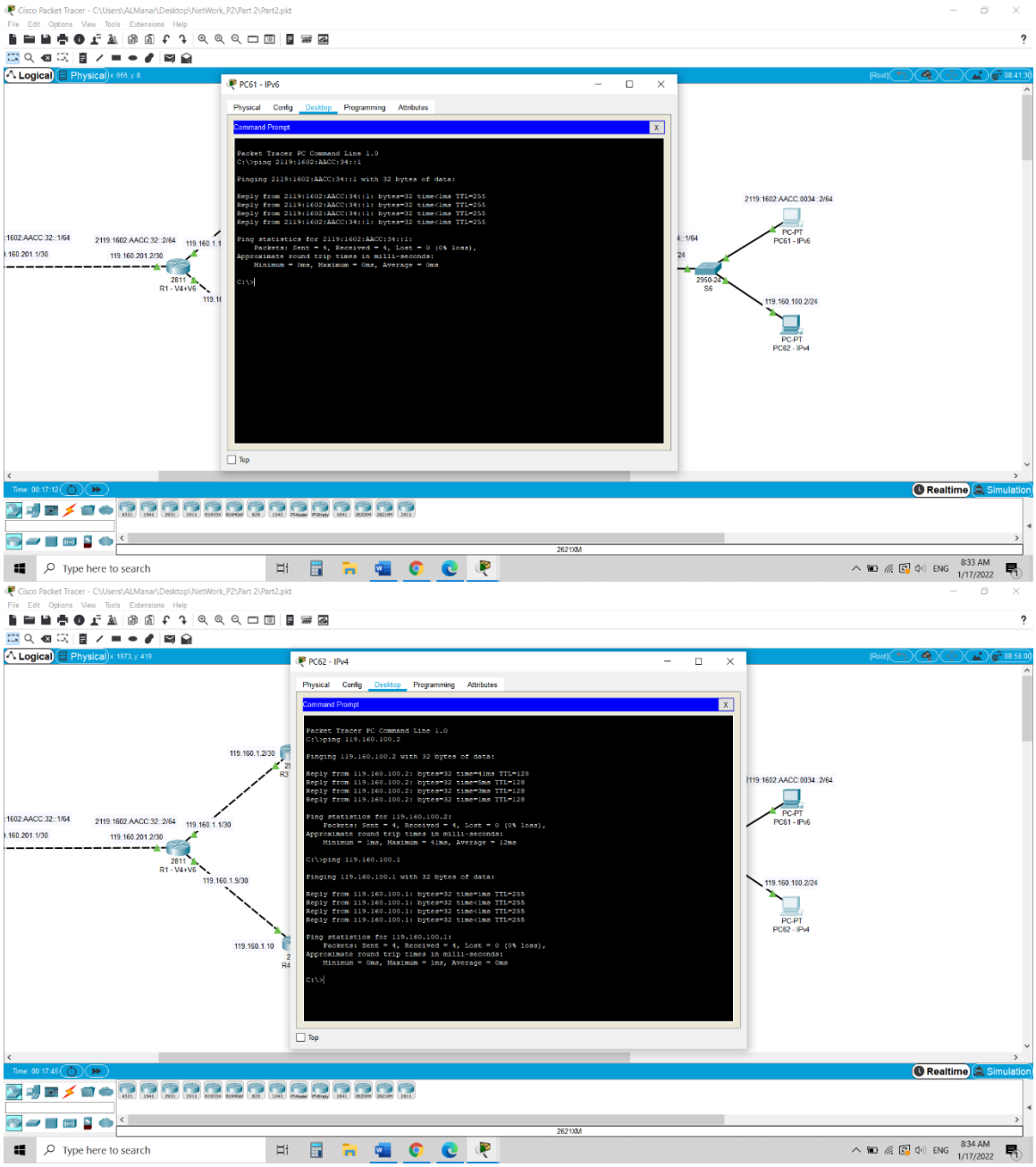


Figure 16: pinging from each host to other host in the same network

2.5. Implement single area OSPF routing protocol for IPv4

We can see in the figure below Implement single area OSPF routing protocol for IPv4 for R0, and in the same way the single area OSPF routing protocol for IPv4 Implemented to the R1, R3, R4, R5 and R6.

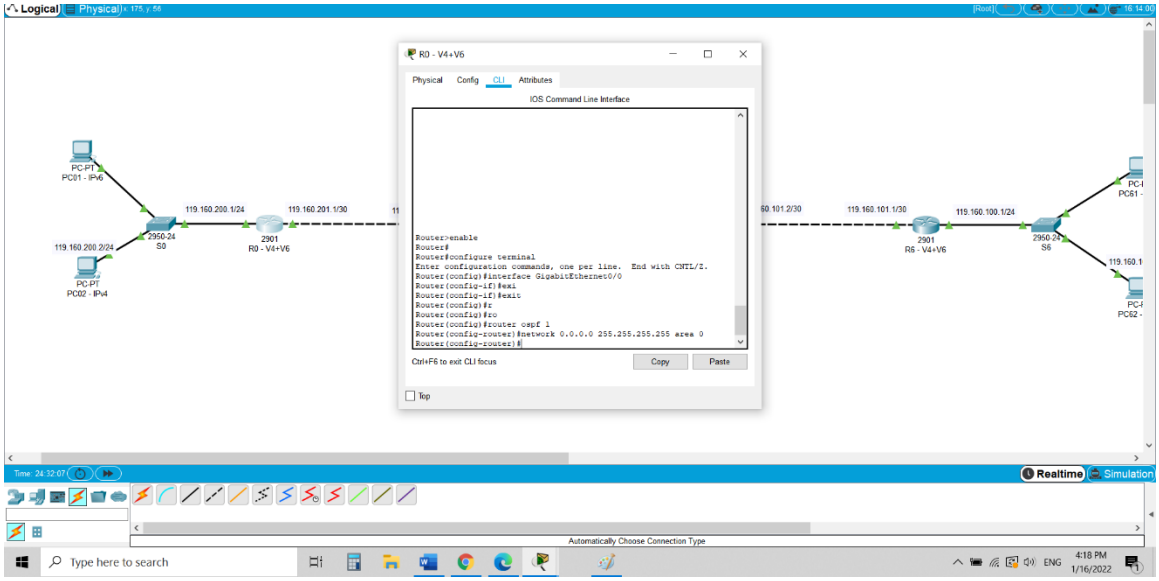


Figure 17: Implement single area OSPF for IPv4

2.6. IPv4 packets are correctly routed all over the network topology

In the section 2.5 we implemented single area OSPF routing protocol for IPv4 in order to guarantee that IPv4 packets are correctly routed all over the network topology. And from the figure below we can see that we pinging from PC02 to PC62 and we can see that IPv4 packets are correctly routed all over the network topology.

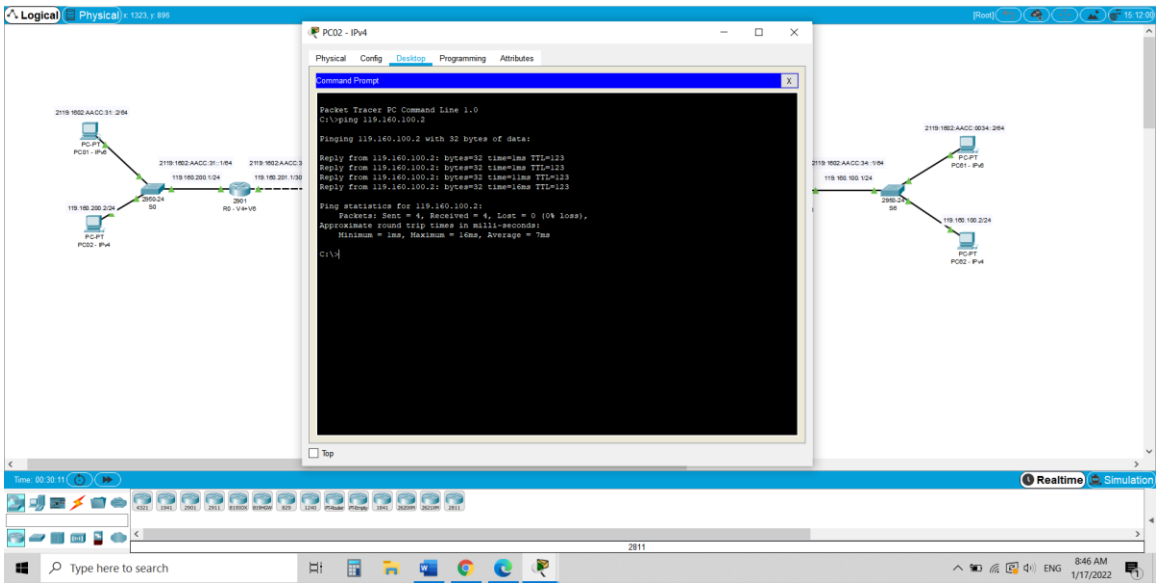


Figure 18: pinging from PC02 to PC62

2.7. Assign IPv6 addresses all connected interfaces on routers (R0, R1, R5 and R6)

We can see in the figure below assigned IPv6 addresses all connected interfaces on router R0, and in the same way the IPv6 addresses assigned to the rest of the routers were defined.

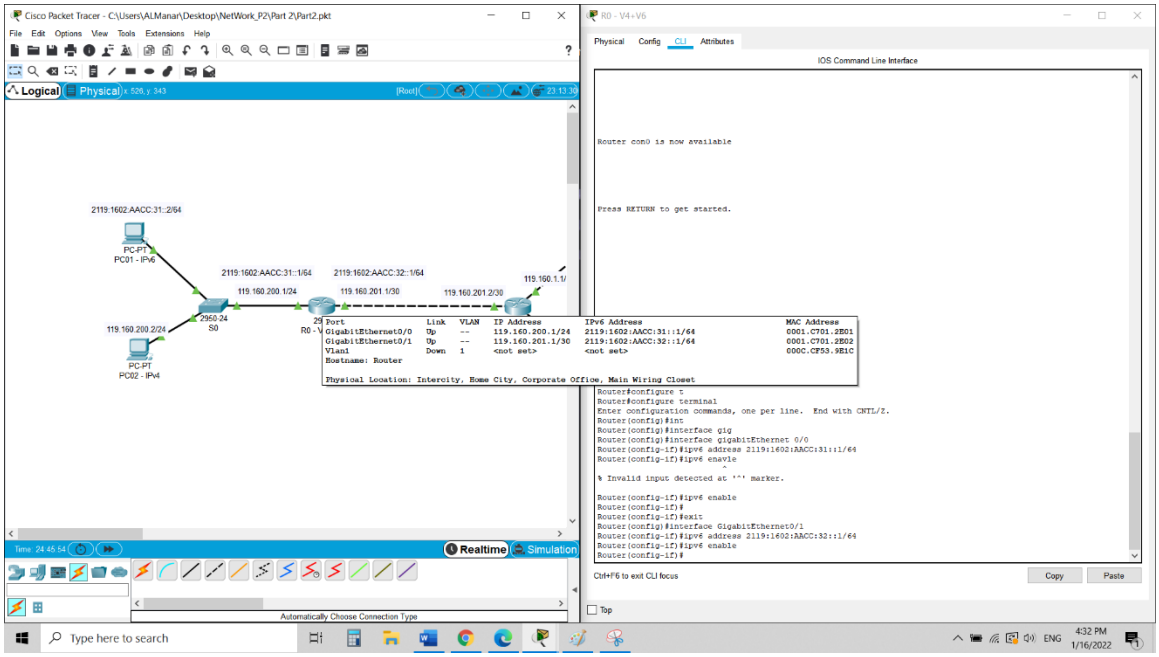


Figure 19: assigned IPv6 addresses all connected interfaces on router R0

2.8. Implement single area OSPF routing protocol for IPv6

We can see in the figure below Implement single area OSPF routing protocol for IPv6 for R0, and in the same way the single area OSPF routing protocol for IPv6 Implemented to the R1, R5 and R6.

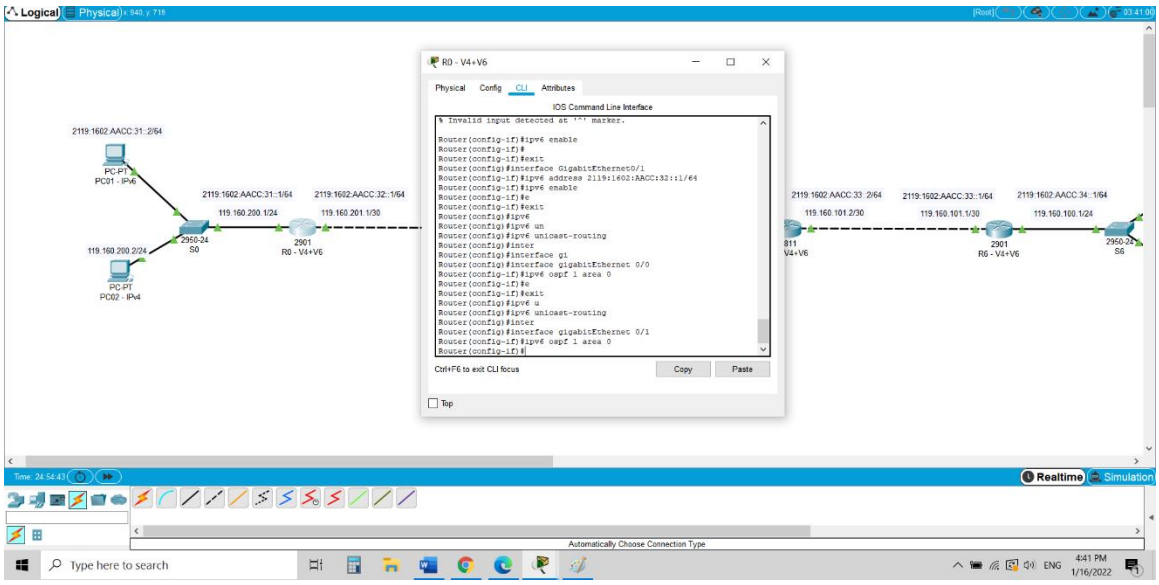


Figure 20: Implement single area OSPF for IPv6

2.9. Implement a tunnel (IPv6 over IPv4)

We implement a tunnel (IPv6 over IPv4) between R1 and R5, and this help us to allow IPv6 traffic to pass through these routers. In addition, we will do OSPF in order to do ping in IPV6 through this tunnel.

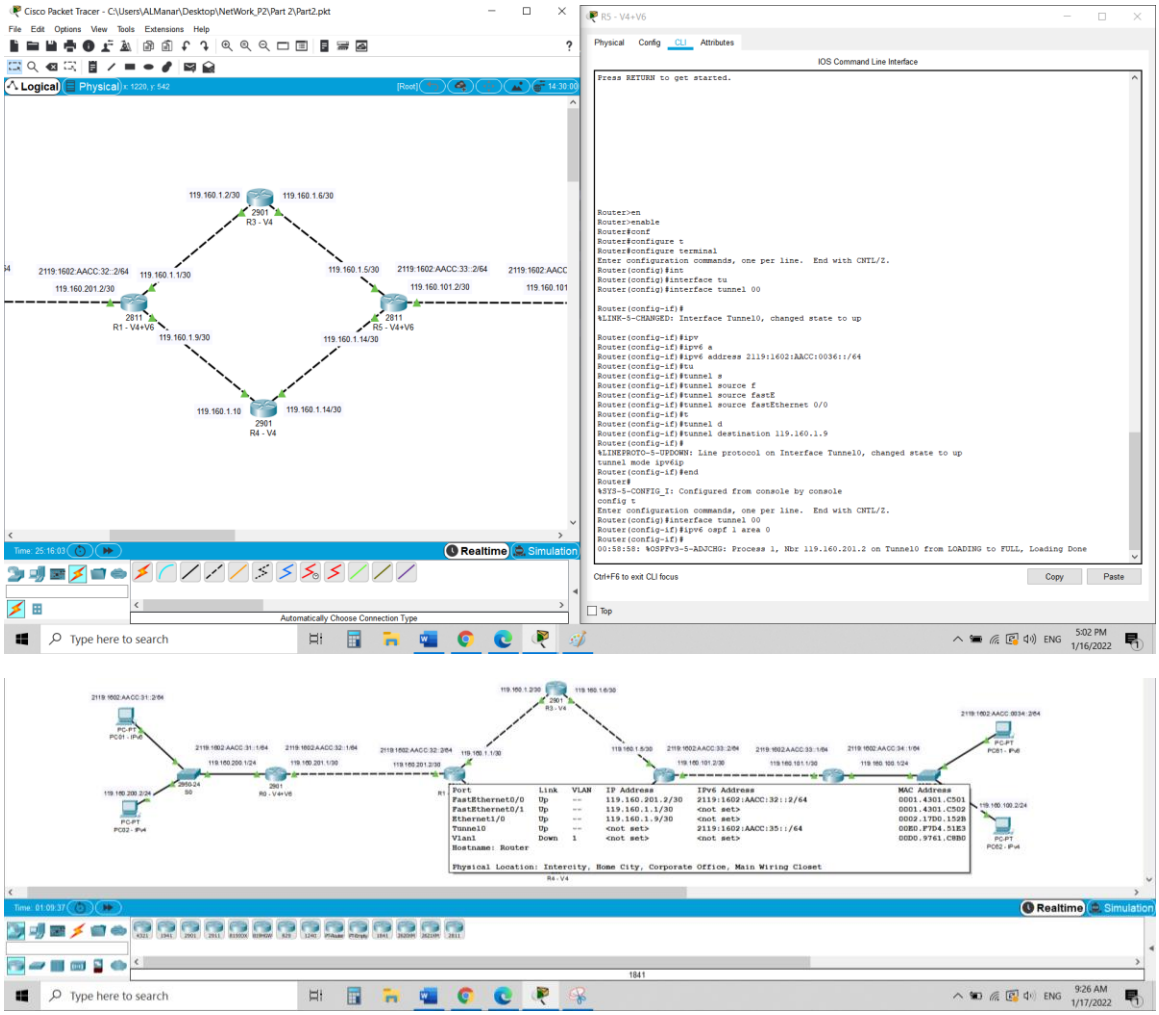


Figure 21: implement a tunnel (IPv6 over IPv4)

2.10. From router R0 ping the IPv6 IP address of any interface on R6

We can see that success rate of 100% (5/5) and no packets were lost, and we can see the approximate round-trip times in milliseconds.

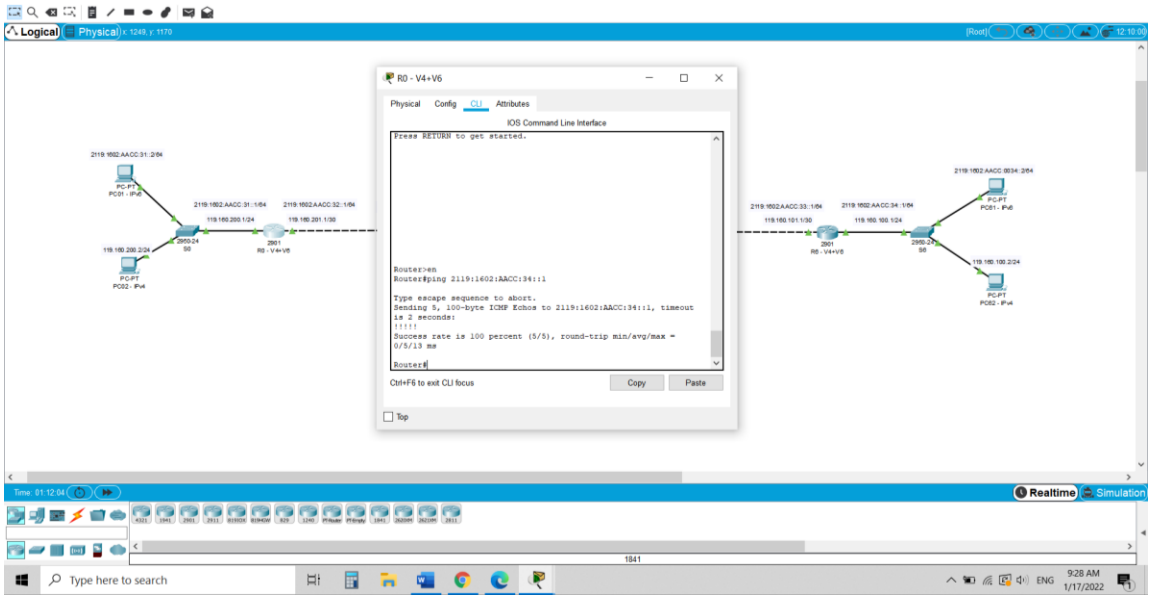


Figure 22: ping from R0 to IPv6 IP address (2119:1602:AACC:34::1/64) on R6

2.11. Ping from PC01 to PC61

We can see that 4 packets were sent and 4 packets arrived, meaning a success rate of 100% and no packets were lost, and we can see the approximate round-trip times in milliseconds and TTL.

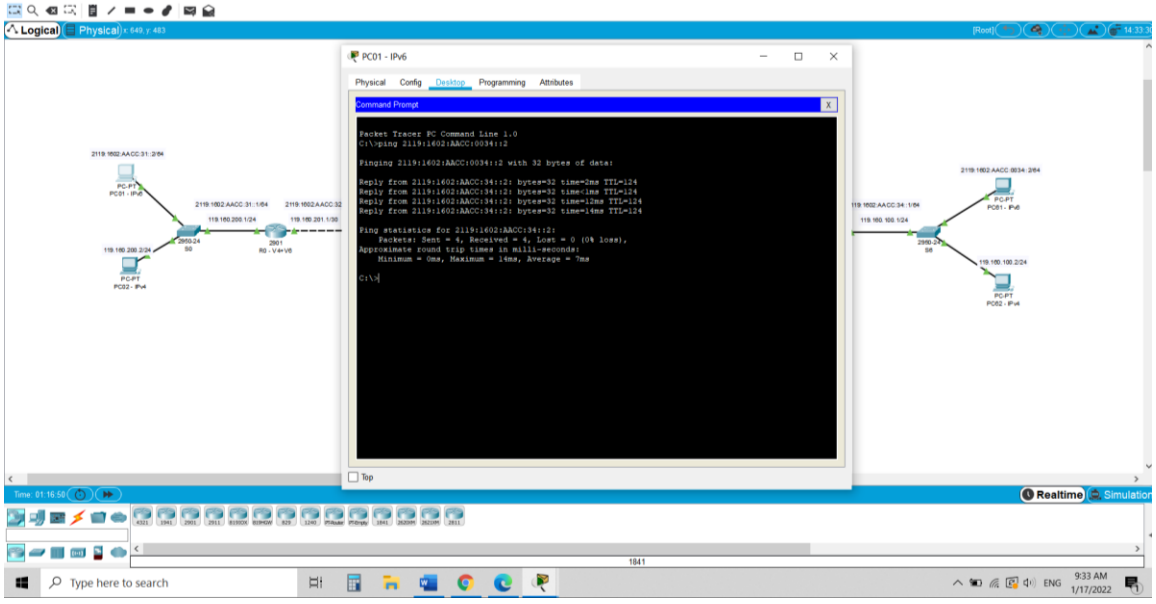


Figure 23: Ping from PC01 to PC61

2.12. Ping from PC02 to PC62

We can see that 4 packets were sent and 4 packets arrived, meaning a success rate of 100% and no packets were lost, and we can see the approximate round-trip times in milliseconds and TTL.

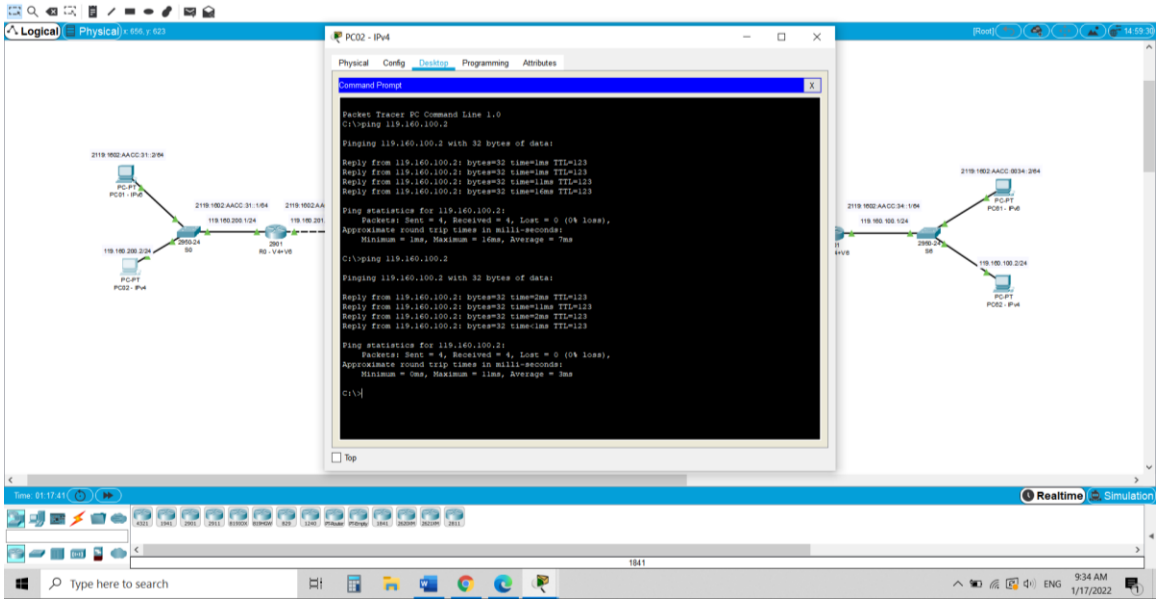


Figure 24: Ping from PC02 to PC62

2.13. Ping from PC01 to PC62

IPv4 and IPv6 are two completely separate protocols, and an IPv6-only device can't directly communicate with an IPv4-only device, or vice versa. And we can see in figure below that we sent 4 packets from device IPv6 to device IPv4 and all packets lost and showed us request timed out.

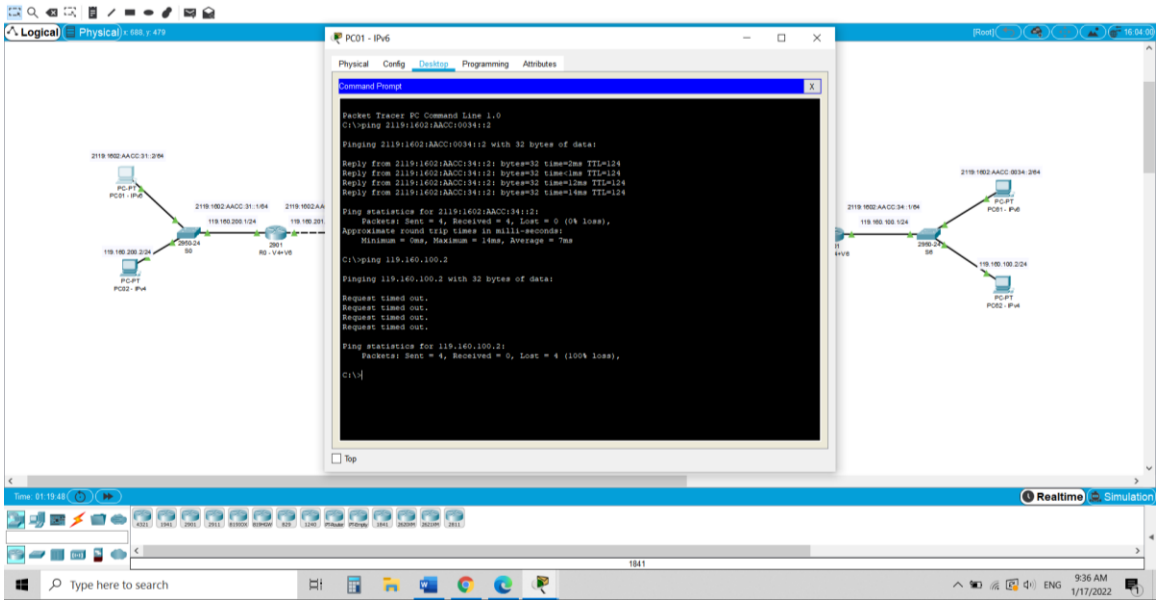


Figure 25: Ping from PC01 to PC62

3. References

Part 1:

[1] Kurose, J. F., & Ross, K. W. (2022). *Computer networking: A top-down approach*. Pearson Education Limited.

[2] *profitap*. http://profitap.com/wp-content/uploads/Chappell-TCP-Architecture.pdf?hss_channel=fbp-937557376324166&fbclid=IwAR0I_5daY5ClRWYbDsojtvJWcDz1tvLRog-CfNOI0fDO175pdIcjZwNGIMU. (2020, April 4). Retrieved January 14, 2022.

[3] YouTube. (2019, September 22). *DHCP packets capture using Wireshark*. YouTube. Retrieved January 16, 2022, from https://www.youtube.com/watch?v=88whguJCeSA

[4] YouTube. (2019, September 22). *ICMP packets capture using Wireshark*. YouTube. Retrieved January 16, 2022, from https://www.youtube.com/watch?v=i5C68u4gmeo

Part 2:

[1] *3 steps GRE Tunnel configuration with Cisco Packet Tracer ⋆*. IpCisco. (2021, August 25). Retrieved January 16, 2022, from https://ipcisco.com/lesson/gre-tunnel-configuration-with-cisco-packet-tracer/?fbclid=IwAR3mxlSPaqWLBI1vrwtvOWNMXzM0kimhV3dTBrkQZMWTglLvdUnv7hnvnlE

[2] Kimanzi, S. (2019, November 10). *Configuring ipv6 tunneling over an ipv4 network in packet tracer*. Computer Networking Tips. Retrieved January 16, 2022, from https://computernetworking747640215.wordpress.com/2019/10/20/ipv6-tunneling-over-an-ipv4-network-2/?fbclid=IwAR3VrAqXJLm-_2qz8B-QLcippPDNa81Q6mkn4cOSFSCXi-0sulIhb_spwIg

[3] YouTube. (2017, October 22). *OSPF(Open shortest path First) - configuration in Cisco packet tracer*. YouTube. Retrieved January 16, 2022, from https://www.youtube.com/watch?v=B7-7RcZCIbM

[4] YouTube. (2022, January 4). *ENCS3320 computer networks: Anycast broadcast subnetting packet tracer project2*. YouTube. Retrieved January 16, 2022, from https://www.youtube.com/watch?v=V3GBFdBWrY8&list=PL7YSA38ZxcXzG529R9e2ahWzp6YYMkJmT&index=24&t=18s

[5] zerocold40. (2021, February 24). *GRE طريقة ربط فرعين عن طريق - lab 3.4.2.6 configure a point-to-point gre VPN tunnel*. YouTube. Retrieved January 16, 2022, from https://www.youtube.com/watch?v=brJ7fTOJ_fE&t=38s