Department of Computer and Electrical Engineering

Computer Networks

ENCS3320

Project 2 Report

Prepared by:

Ahmad Nidal Hamad 1180060

Baraa Atta 1180445

Supervised by:

Dr. Abdalkarim Awad

June 2021

Contents

Figures

Abstract

This project consists of two parts, first part is about tracing the transfer of packets using three different communication protocols, TCP, DHCP & ICMP, using Wireshark software. The second part is about designing and implementing a simple network with multiple subnets using the packet tracer software.

Procedure and Discussion

Part 1

This part is about tracing and capturing packets using Wireshark software.

A. Tracing TCP Packet:

   A TCP request was sent to IP address 104.17.244.204, the result is shown in the next figure.

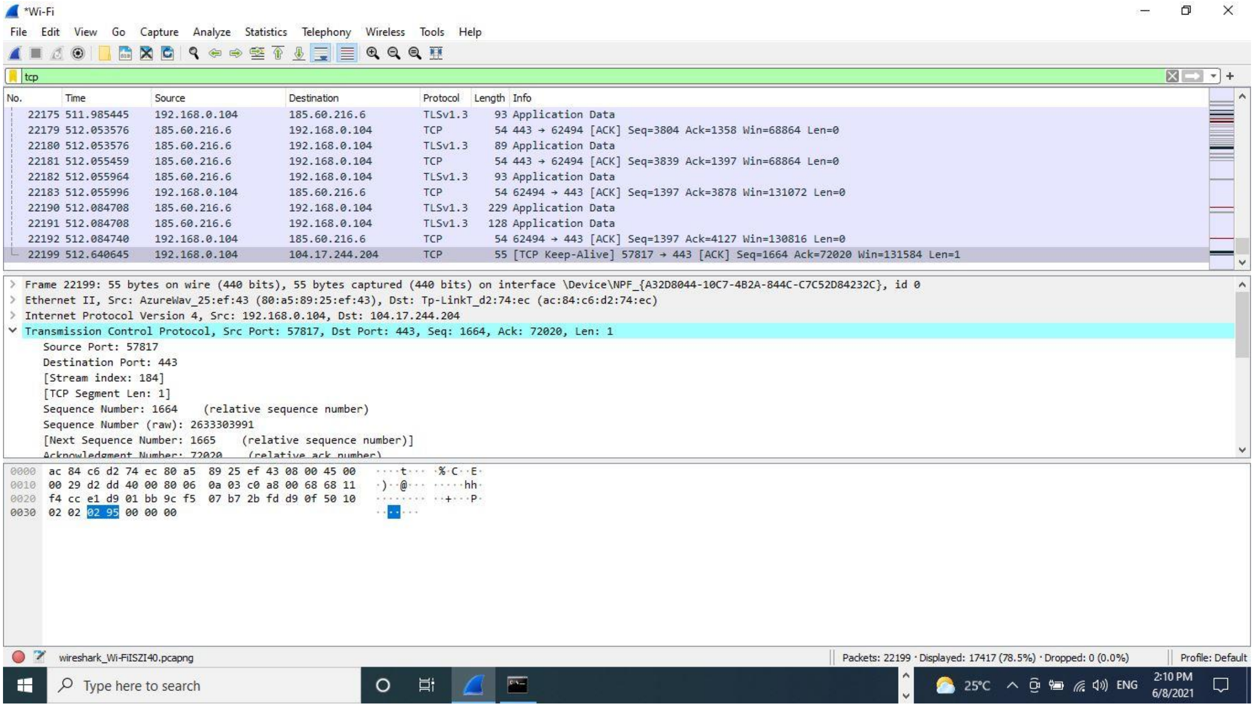

Figure 1: tracking TCP packets

As shown in the figure, the source IP which is my laptop's IP is 192.168.0.104 and the destination IP is 104.17.244.204. From the TCP header, we can see that the source port of the application that sent the request is 57817 and the destination port is 443 which is the port used for receiving HTTPS requests within secured websites. Also, sequence number is 1664 which is the byte number of the first byte that is sent in the request and it helps in reassembling the message at the receiver side when packets arrive out of order.

B. Tracing DHCP Request:

   A DHCP request is for requesting an IP address dynamically from the router and its done using the command: ipconfig/renew. The result is shown in the next figure.

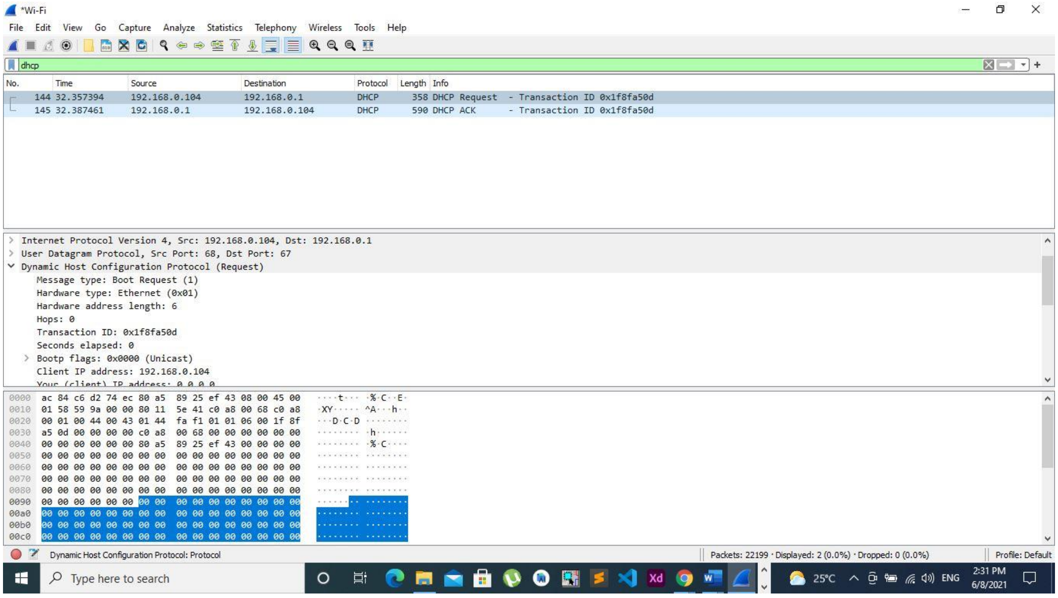

Figure2: tracking DHCP packets

As shown in the figure, the message type in the header of the request is 1 which means it’s a request message, while if it was 2 then it’s a reply message, the hardware type is ethernet which means the local network is using ethernet. In addition, the hardware address length is 6 bytes which means the MAC address of the message consists of 6 bytes.

C. Tracing ICMP Request:

ICMP requests are using ping command, the executed command is: ping www.google.com and the result is shown in the next figure.

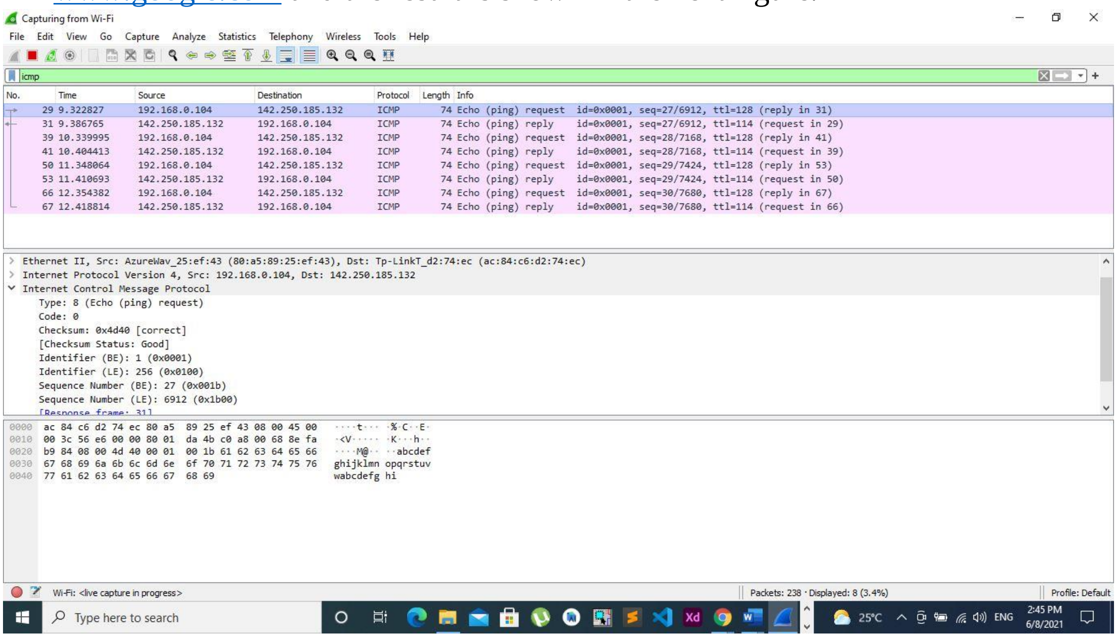

Figure 3: tracking ICMP packets

As shown in the figure, the type of this request is 8 which is echo request and it means the data that is sent in the echo request message must be returned in the echo reply message. The checksum is 0x4D40 and it’s used in the detection of error occurred during the transmission of the request. In addition, there is an identifier field that is used for matching the sent requests with the replies.

Part 2

In this part we are going to implement a simple network with 5 routers, 4 switches, 12 PCs, and 11 subnets.

Now we will start by assigning the IP addresses for each host and router's port. Before that we should pay your attention about the IP address class used in this implementation. In the project we were asked to fix the first 8 bits at a value of 118, but this won't work, since this implementation can only fit with class A IP address or with a classless implementation. The problem with class A is that it has 8 bits for the network and 118 requires 7 bits, so we weren't able to create more than two subnets, also the classless one is not acceptable by the RIP protocol in the packet tracer software. So, we decided to implement it using IP address type C starting with 218, because it doesn't have 118 in its available networks range.

First of all, the network was built as shown in figure1

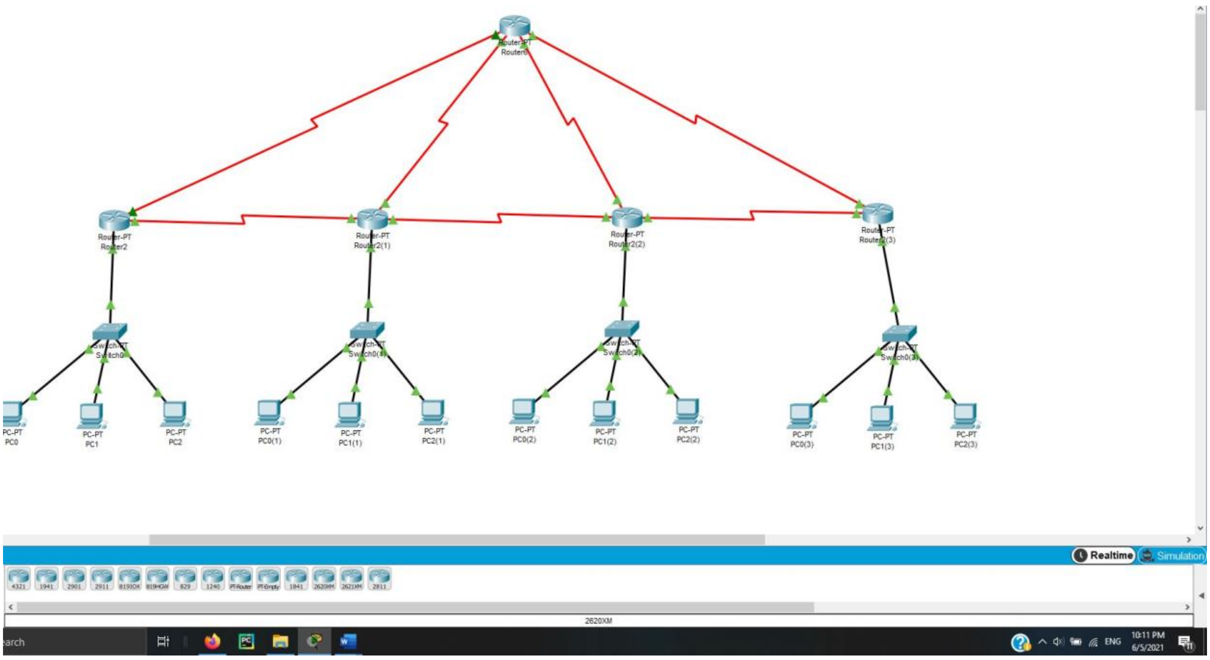

Figure 2:Network Design

The first subnet contains the first 3 left most PCs with the switch connecting them and the Ethernet port 0 of the first router from the left. For this subnet we decided to give a network address of 218.0.0.0, so the fast ethernet 0/0 port of the router takes the address 218.0.0.1, after that the PCs take the IP addresses 218.0.0.2,218.0.0.3, and 218.0.0.4 with a gateway of 218.0.0.1 for all of them, because the fast ethernet 0/0 port of the router will be their gateway outside their local network.

Note that the subnet mask for all devices is 255.255.255.0, because as we have already said the configuration is done using IP type C. Also, we can note that we didn't configure the switch, since it's a non-configurable device, it just connects the hosts together in a local area network.

Figure 2 shows the settings set for the fast ethernet 0/0 port of the router

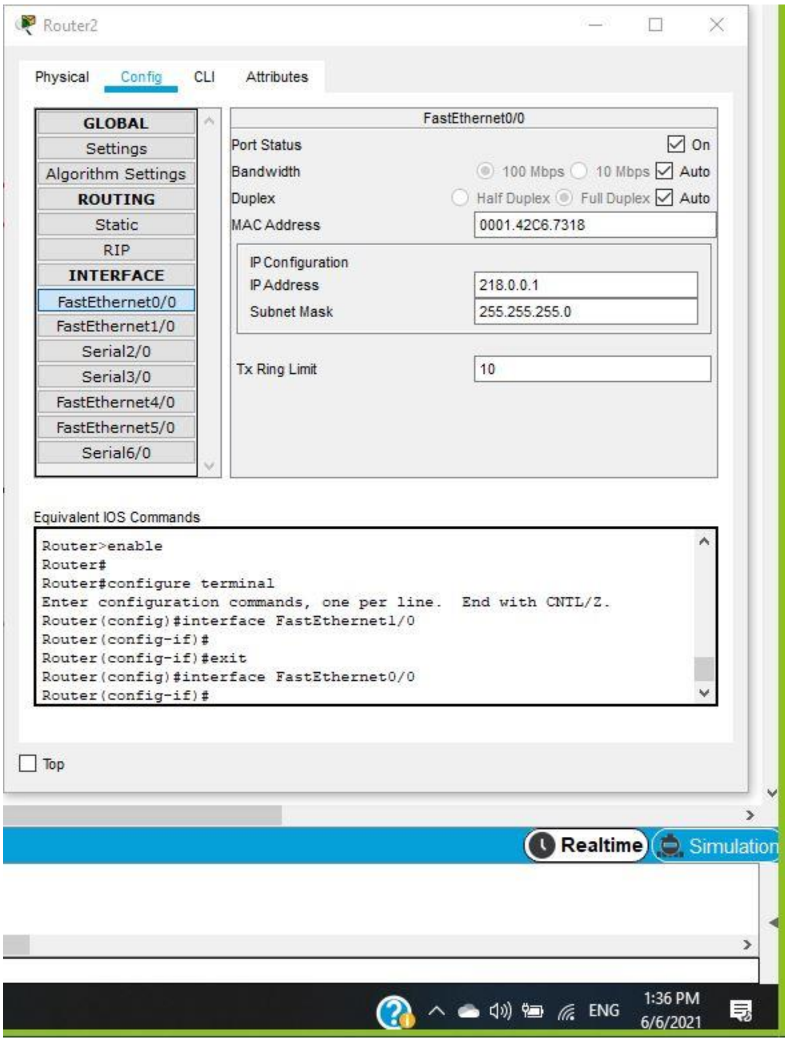

Figure 3:Router Configuration

As shown in the previous figure, the IP address was set to 218.0.0.1, which will act as the gate way for its subnet, moreover the subnet mask is the default one for the type C addresses.

Figure 3 shows the configuration of the first PC in the first subnet

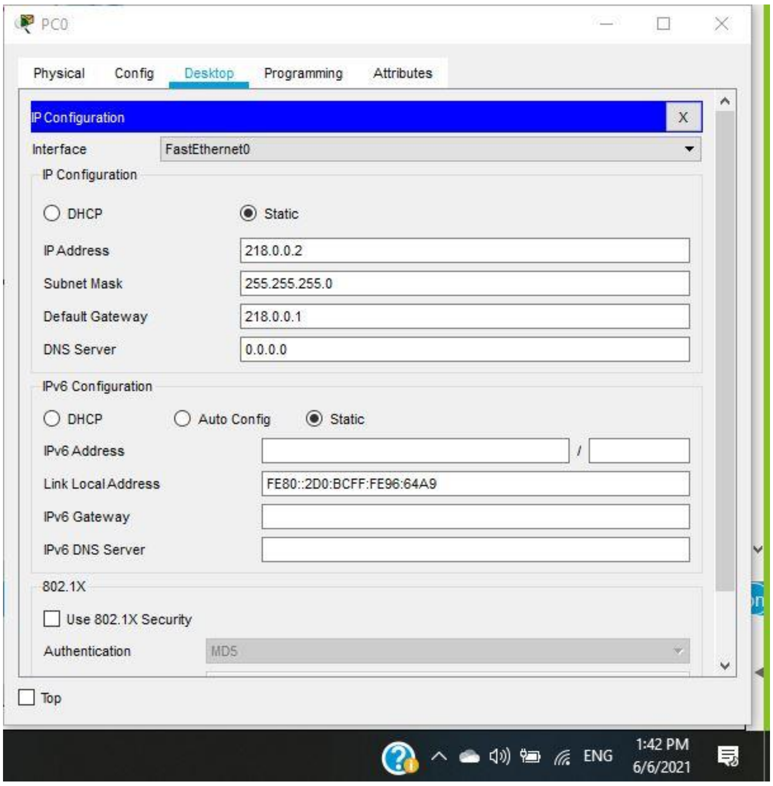

Figure 4:First Host Configuration

As shown in the previous figure, the IP address was set to 218.0.0.2, the subnet mask is the default one for the type C addresses, and finally the gate way was set to match the address of the router's port from this subnet side.

Note that the IP addresses for the other hosts in this subnet was given in the same way with changing the host part from 2 to 3 and 4, while keeping the gateway and the subnet mask the same, since the same port will act as the gateway for all the hosts in the same subnet.

The other subnets are configured in the same way, but by changing the network part of the address to become 218.1.0.0 for the second network and 218.2.0.0 for the second network, and so on.

The next step is to configure the subnets between the routers, which is done as same as configuring any new subnet, so I will configure the one connecting the first two routers from the left as follows:

Firstly, the serial port 2/0 for the first router was given an IP address of 218.4.0.1 and the serial port 2/0 of the second router, which is connected to the first router at the same pre-configured port was given an IP address of 2184.0.2, that's it the two routers are now connected to the same subnet.

Figure 3 and figure 4 show the configuration of those ports

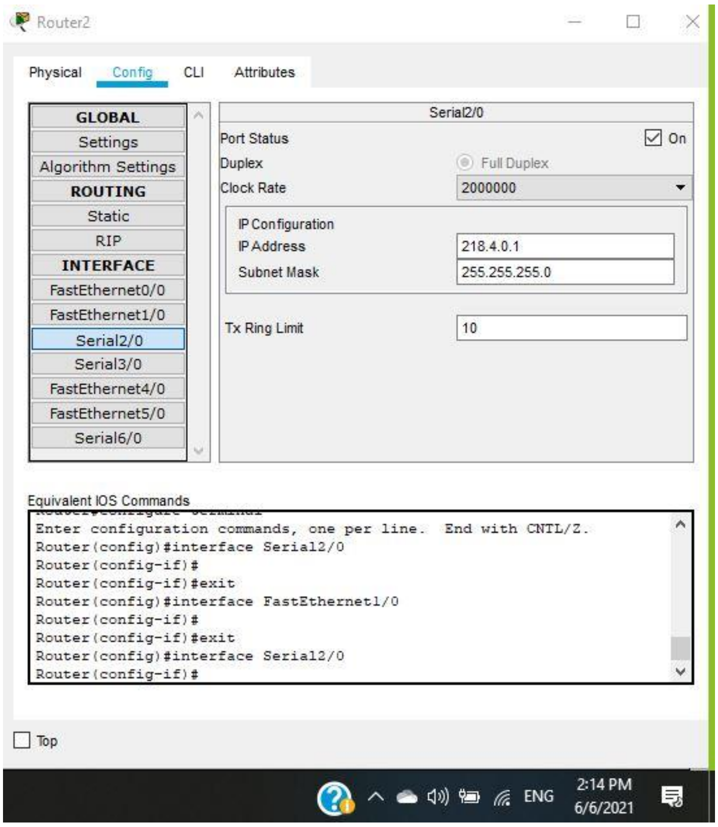

Figure 5:Configuration of serial port 2/0 of the first router

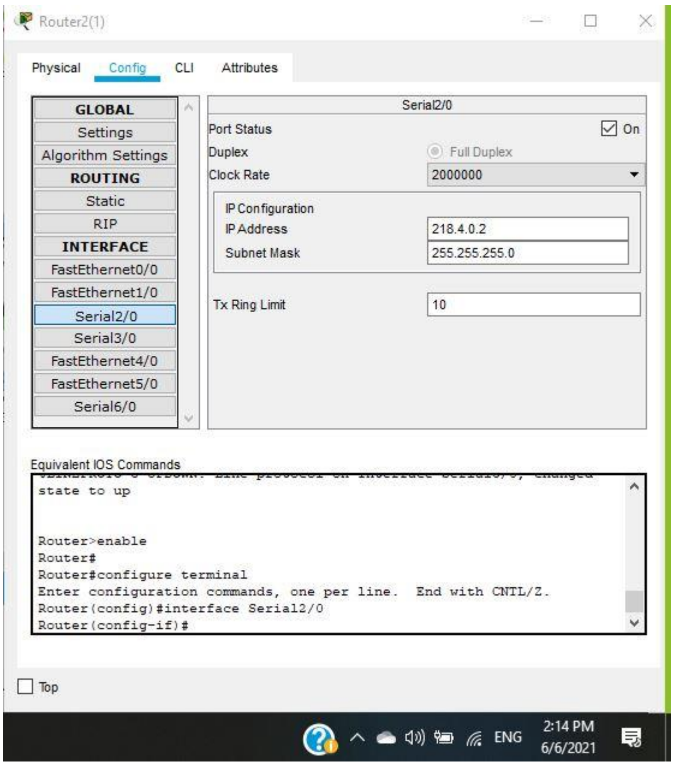

Figure 6:Configuration of serial port 2/0 of the second router

In the same fashion, all other subnets were implemented. Also, an important point to emphasize on is that the routers has only two serial ports by default, so we added other ones from the physical part of their configuration.

Finally figure 6 shows the detailed view of the network with its subnets.

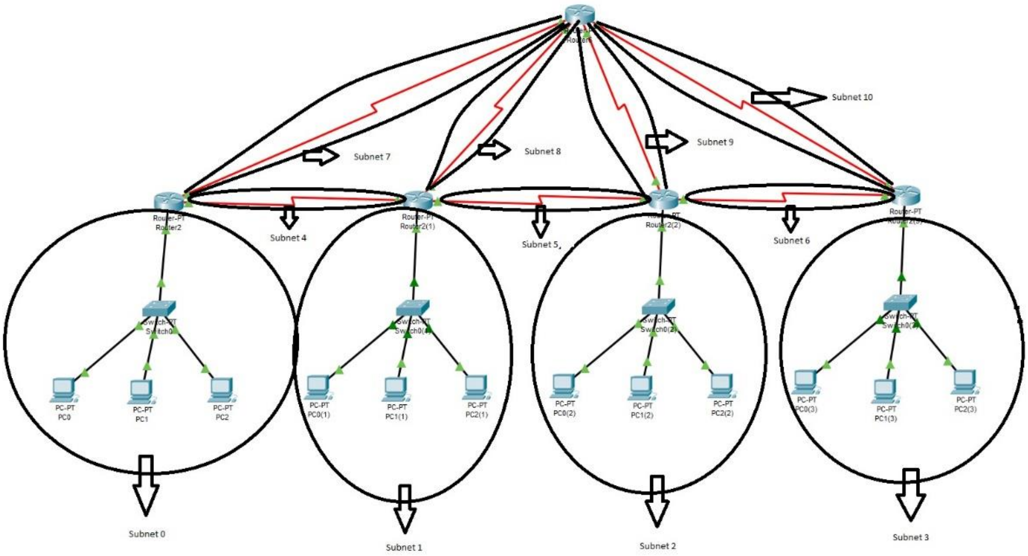

Figure 7:Detailed view of the network

After implanting all the subnets as seen before, we are going now to apply the RIP routing protocol on the network. This can be done by adding the addresses of all the network subnets to every router in the network.

As we have already seen, we end up with 11 subnets with the following addresses:

1- 218.0.0.0
2- 218.1.0.0
3- 218.2.0.0
4- 218.3.0.0
5- 218.4.0.0
6- 218.5.0.0
7- 218.6.0.0
8- 218.7.0.0
9- 218.8.0.0
10- 218.9.0.0
11- 218.10.0.0

So simply all those addresses should be added to the routers in the RIP protocol configuration area, figure 7 shows this process in one of the routers.

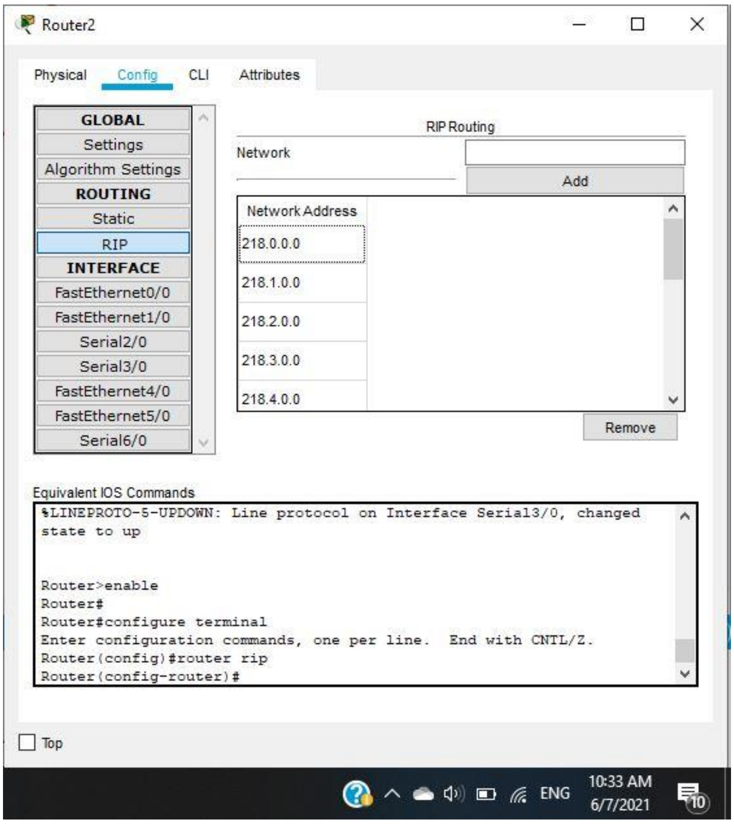

Figure 8:RIP protocol configuration for one router

The previous figure shows the implementation of the RIP protocol on one of the routers, note that the addresses continue to the last subnet address (218.10.0.0). In the same way all the other routers were configured.

Now we have our network fully implemented with its routing protocol, the final step is to test it by checking if we can reach a host in every subnet from the same subnet and from another one using the ping test. This process is done as shown in the next figures.

Testing all subnets

Subnet 0 testing

Pinging from two PCs in the same subnet

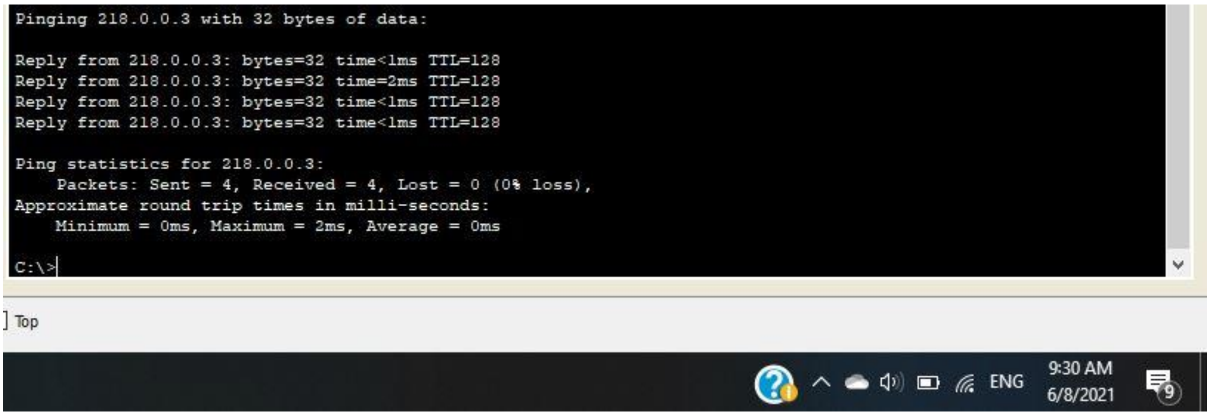

Figure 9:Pinging to host from same subnet 0

The previous figure shows a ping from the PC with IP 218.0.0.2 to the PC with the IP address 218.0.0.3, as we can see all the packets we sent have been received, so the PC is reachable from the same subnet.

Pinging from a pc from another subnet

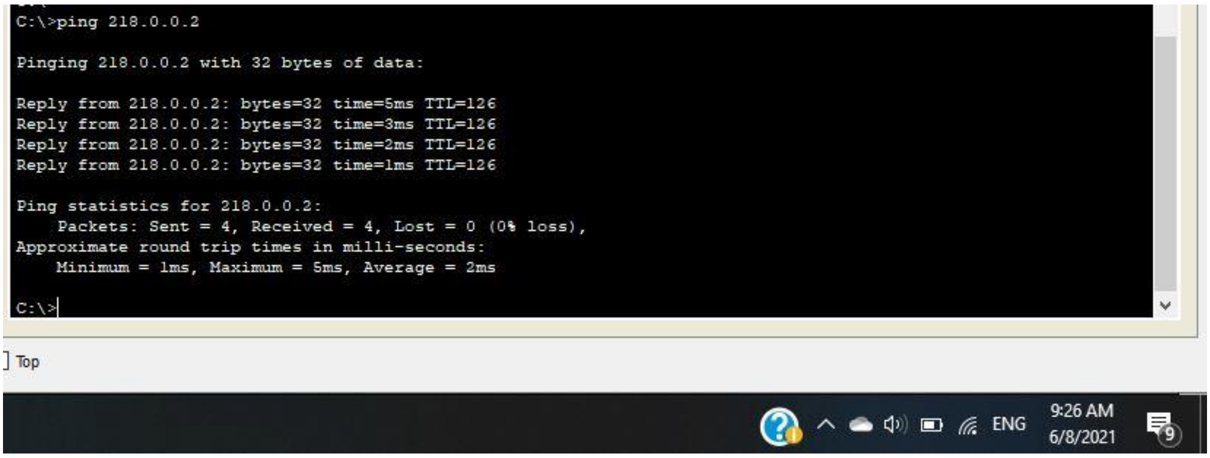

Figure 10:Pinging to host from another subnet 1

The previous figure shows a ping from the PC with IP 218.1.0.2 to the PC with the IP address 218.0.0.2, as we can see all the packets we sent have been received, so the PC is reachable from another subnet.

Subnet 1 testing

Pinging from two PCs in the same subnet

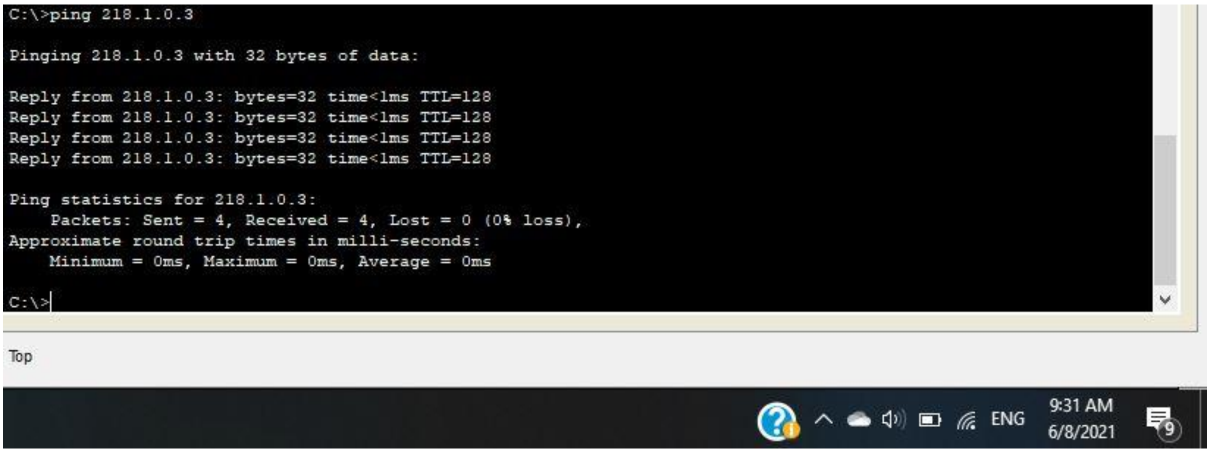

Figure 11:Pinging to host from same subnet 1

The previous figure shows a ping from the PC with IP 218.1.0.2 to the PC with the IP address 218.1.0.3, as we can see all the packets we sent have been received, so the PC is reachable from the same subnet.

Pinging from a pc from another subnet

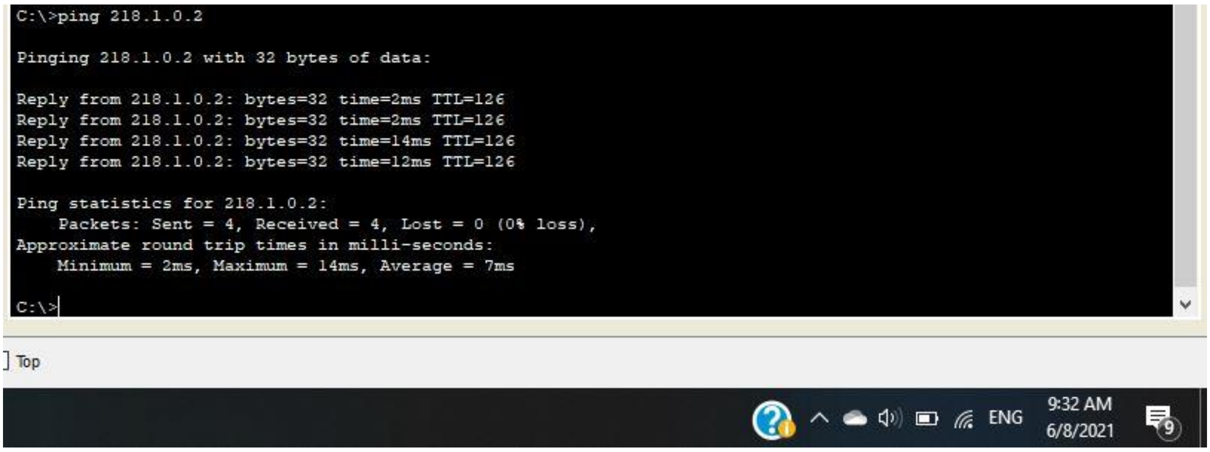

Figure 12: Pinging to host from another subnet 2

The previous figure shows a ping from the PC with IP 218.2.0.2 to the PC with the IP address 218.1.0.2, as we can see all the packets we sent have been received, so the PC is reachable from another subnet.

Subnet 2 testing

Pinging from two PCs in the same subnet

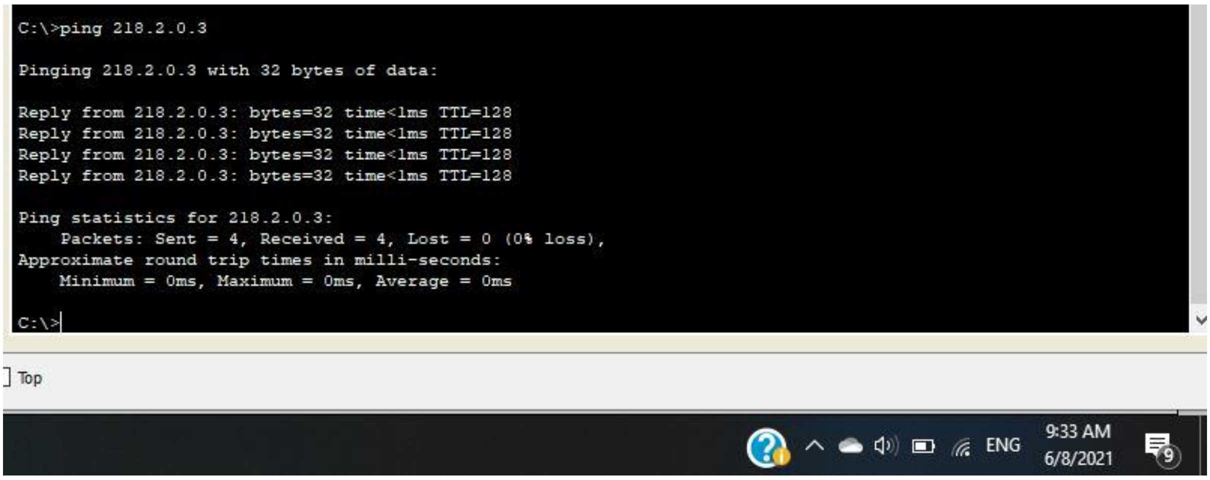

Figure 13: Pinging to host from same subnet 2

The previous figure shows a ping from the PC with IP 218.2.0.2 to the PC with the IP address 218.2.0.3, as we can see all the packets we sent have been received, so the PC is reachable from the same subnet.

Pinging from a pc from another subnet

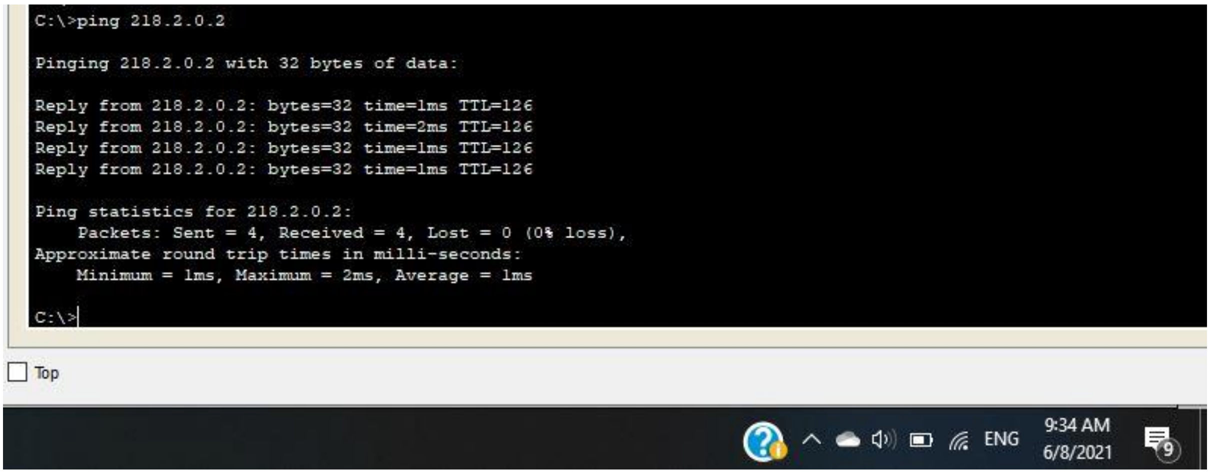

Figure 14: Pinging to host from another subnet 3

The previous figure shows a ping from the PC with IP 218.3.0.2 to the PC with the IP address 218.2.0.2, as we can see all the packets we sent have been received, so the PC is reachable from another subnet.

Subnet 3 testing

Pinging from two PCs in the same subnet

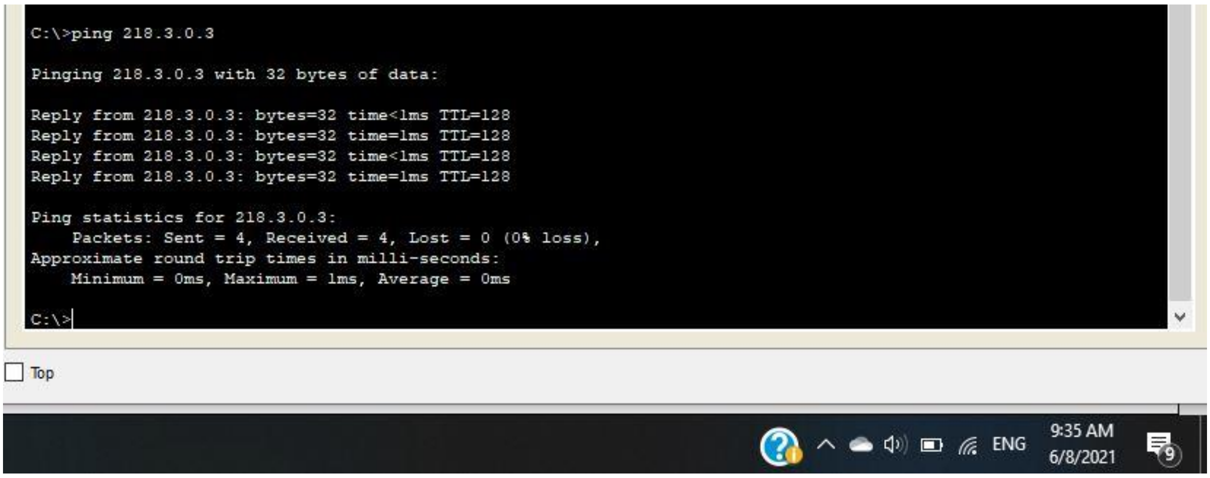

Figure 15: Pinging to host from same subnet 3

The previous figure shows a ping from the PC with IP 218.3.0.2 to the PC with the IP address 218.3.0.3, as we can see all the packets we sent have been received, so the PC is reachable from the same subnet.

Pinging from a pc from another subnet

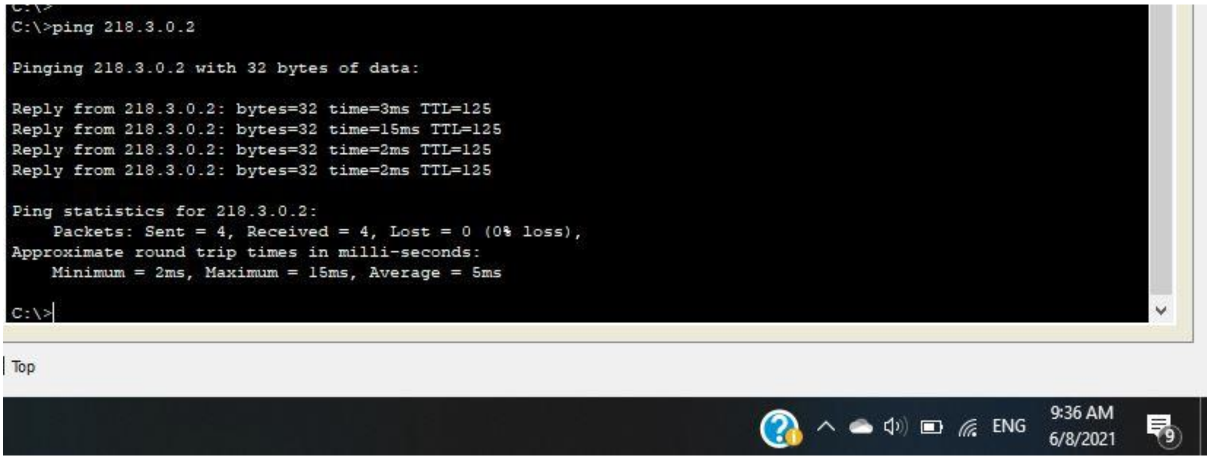

Figure 16: Pinging to host from another subnet 2

The previous figure shows a ping from the PC with IP 218.2.0.2 to the PC with the IP address 218.3.0.2, as we can see all the packets we sent have been received, so the PC is reachable from another subnet.

Conclusion

This project consists of two parts, in the first one we saw how to use Wireshark program to track packets on the network, which also gave us an idea about the main fields sent with three types of packets, TCP, DHCP, and ICMP.

In the second part we implemented a simple but full network with 11 subnets, moreover we learned how to apply the RIP protocol in order to route the packets to different subnets.

There are two points about the second part we should focus on, which are:

1- The program we were using didn’t accept a classless IP address for the RIP protocol, so we went with a class C.
2- It’s very important to configure the gateway for each PC in the network, in order to let them sent their packets to outer subnets.

We can say at the end that the project went on well, and we were excited doing it.