Task 8.1p

Active class 7: Who is Instructing What

The learning objective of this class is to learn about routing and routing algorithms.

At the end of this activity, you should be able to:

1. Explain the control plane operation of the Network layer

2. Build a simple network in Cisco Packet Tracer and simulate static routing and dynamic routing.

Activity 1

Routing Role Play:

In this group activity, we're tasked with discussing and role-playing scenarios related to routing. We'll simulate a network with two routers and separate LANs connected to each router. Each group member will take on specific roles, such as representing LANs, routers' data planes, or control planes. We'll work together to support a message transmission from one PC to another and discuss subnetting and the responsibilities of router control planes.

Activity 2

Packet Tracer Implementation:

Following our discussions from Activity 1, we'll apply what we've learned by implementing the network scenario in Cisco Packet Tracer. We'll configure the devices based on our previous discussions, ensuring communication between specific PCs. We'll also make network adjustments and verify communication using simulation tools.

Activity 3

Alternative Routing Algorithms:

Reflecting on our experiences in Activity 2, we'll discuss alternatives to manual routing table configuration and explore the latest routing algorithms. We'll then implement the network scenario again in Packet Tracer, this time utilizing the routing algorithm available in the routers. We'll analyze network connections, compare results with Activity 2, and observe how routing algorithm changes impact packet transmission.

Throughout these activities, collaboration, note-taking, and active engagement are encouraged to deepen understanding and practical application of routing concepts. Completing these tasks not only reinforces theoretical knowledge but also enhances practical skills essential for network management and troubleshooting.

Active class 8: Internet is full of Network Protocols

The learning objective of this class is to learn the role of Network Address Translation (NAT) protocol, Dynamic Host Configuration Protocol (DHCP) and Internet Control Message Protocol (ICMP) which are (perhaps considered as) significant network layer protocols.

At the end of this activity, you should be able to:

1. Explain the functionalities of the mentioned protocols

2. Build a simple network and analyse the protocols.

Activity 1

Group Discussion:

We're discussing the challenges related to the scarcity of IPv4 addresses and exploring solutions to conserve the global IP address space. This includes considering a protocol, like NAT, that can help in this regard.

Activity 2

DHCP Role Play and Implementation:

We're simulating a DHCP environment within our group, where one member acts as a router with a DHCP server, and others act as host devices trying to connect to the network. We're setting up the network and establishing connections using DHCP, then analyzing the message sequence with a timing diagram. Later, we're implementing DHCP server functionality in Cisco Packet Tracer, configuring network pools, default gateways, and IP addresses to understand DHCP's practical application.

Activity 3

ICMP Exploration:

Using Cisco Packet Tracer's simulation tool, we're exploring ICMP by sending packets between hosts in the network implemented in Activity 2. We're examining the details of ICMP messages, including their format and types, and comparing ICMP behavior between a ping and a traceroute.

Throughout these activities, active participation, collaboration, and practical experimentation are encouraged to deepen our understanding of these protocols and their roles in networking. Completing these tasks will not only reinforce theoretical knowledge but also enhance our practical skills in network management and troubleshooting.

Evidences: Quiz 4

Which of the following statement is true regarding the routing algorithms? 10/10

- ○ Distributed routing algorithms compute the least-cost path from a source to destination by using the complete global knowledge about the network.
- ○ In centralised algorithms, no network node has the complete information about the costs of all links.
- ◉ Centralised routing algorithms compute the least-cost path from a source to destination by using the complete global knowledge about the network.
- ○ The distributed algorithms need to have the complete knowledge of the connectivity between all nodes and the costs of all links.

What is the correct order of DHCP to obtain an IP address? 10/10

- ○ 1) DHCP Request; 2) DHCP Offer; 3) DHCP Discover; 4) DHCP Acknowledgement.
- ○ 1) DHCP Discover; 2) DHCP Request; 3) DHCP Offer; 4) DHCP Acknowledgement.
- ◉ 1) DHCP Discover; 2) DHCP Offer; 3) DHCP Request; 4) DHCP Acknowledgement.
- ○ 1) DHCP Request; 2) DHCP Discover; 3) DHCP Offer; 4) DHCP Acknowledgement.

What are the advantageous of using NAT? There could be more than one answer. 10/10

- [x] Help conserving the global IPV4 address space
- [x] Provide security by hiding the internal IP addresses
- [ ] Provide more options for network management
- [ ] Help dynamically allocate IP addresses

OSPF is implemented using 10/10

- (•) Dijkstra's algorithm
- ( ) Vector space algorithm
- ( ) Path finder algorithm
- ( ) Bellman-ford algorithm

Which of the following algorithms can be considered as Intra-AS routing algorithms? 10/10

- [x] OSPF
- [x] IS-IS
- [x] RIP
- [ ] BGP

Which are the two fields in ICMP header that used to identify the purpose of the ICMP message? 10/10

- ( ) Type and control flag
- ( ) Code and control flag
- (•) Type and code
- ( ) IP address and type

Consider the following scenario: Router "a" has only two directly attached neighbouring Routers "b" and "c". The cost to connect Router "a" and "b" is 3, "a" to "c" cost is 6 and "b" to "c" cost is 2. Router "b" has a minimum cost path to another Router "d" and the cost is 5. Router "c" also has a minimum cost path to Router "d" and the cost id 8. 10/10

What is the Router a's distance vector for destination b, c, and d?

- ○ Da(b) = 3, Da(c) = 4 , Da(d) = 9
- ○ Da(b) = 3, Da(c) = 5 , Da(d) = 5
- ○ Da(b) = 3, Da(c) = 4 , Da(d) = 8
- ◉ Da(b) = 3, Da(c) = 5 , Da(d) = 8

The following table contains the first line of a Dijkstra's algorithm solution to a shortest path problem. 10/10

By looking at the table, we can identify that some nodes are not directly connected to the starting node. What are those nodes?

Destination	Path	Distance
B	A→B	2
C	A→C	6
D		∞
E	A→E	6
F		∞

- ◉ D and F
- ○ A, D, and F
- ○ A and F
- ○ B, C and E

The following table contains the solution of a shortest path problem that obtained using Dijkstra's algorithm. 10/10

What is the length of the shortest path from A to F? what is the route?

Destination	Path	Distance	Next Hop
B	A → B	2	B
C	A → B → C	4	B
D	A → B → C → E → F → D	8	B
E	A → B → C → E	5	B
F	A → B → C → E → F	6	B

- ○ 6, A->B->C->D->E->F
- ○ 2, A->B->C->D->E->F
- ○ 4, A->B->C->E->F
- ◉ 6, A->B->C->E->F

Consider the count-to-infinity problem in the distance vector routing. The count-to-infinity problem occur if we decrease the cost of a link. Is the above statement true/false? 10/10

- ○ True
- ◉ False

Notes

Network Layer Functions

Forwarding: This is the process of moving packets from a router's input to the appropriate output based on the routing table. It occurs in the data plane.

Routing: The control plane is responsible for determining the route packets take from source to destination. It involves running routing algorithms to populate the forwarding tables.

Control Plane Structures

Per-Router Control: Traditional method where each router has its own control plane and runs an individual routing algorithm.

Logically Centralized Control (SDN): In Software-Defined Networking (SDN), a remote controller computes and installs forwarding tables in routers, centralizing control.

ICMP Protocol

Purpose: The Internet Control Message Protocol (ICMP) is used for network-level communication, including error reporting (e.g., unreachable host/network/port/protocol) and operational queries like echo requests/replies used by the ping utility.

Functionality: ICMP messages, which are carried in IP datagrams, contain a type, code, and the first 8 bytes of the IP datagram that caused the error.

Ping Utility

Usage: Ping verifies the availability of a destination host and measures the round-trip time (RTT).

Process: It sends an ICMP type 8 code 0 message (echo request) and awaits a type 0 code 0 reply (echo reply), with the RTT measured in milliseconds.

Key algorithms and protocols used in the control plane of a network layer:

Routing Algorithms

These are algorithms that determine the best path for data packet transmission. Two main types of routing algorithms are:

Link-State Algorithm: This algorithm has each router maintain a comprehensive map of the network's topology. Each router independently calculates the best next hop from it for every possible destination in the network using Dijkstra's algorithm.

Distance Vector Algorithm: In this algorithm, each router does not possess explicit knowledge of the network topology. Instead, the router only knows the distance and direction to its directly connected neighbors. Bellman-Ford Algorithm is an example of a distance vector algorithm.

Routing Protocols

These are protocols that implement the routing algorithms and facilitate the exchange of routing information between routers. Some of the commonly used routing protocols include:

OSPF (Open Shortest Path First): This is a link-state routing protocol which uses Dijkstra's algorithm to compute the shortest path tree.

BGP (Border Gateway Protocol): This is a distance-vector protocol which is used for routing between autonomous systems.

MPLS (Multiprotocol Label Switching): This is a protocol for efficient network traffic flow between multiple sites.

SDN Control Plane

In Software-Defined Networking (SDN), the control plane is logically centralized, and a remote controller compute and installs forwarding tables in routers.

These algorithms and protocols play a crucial role in managing the control plane of the network layer, ensuring efficient and reliable data transmission across networks.

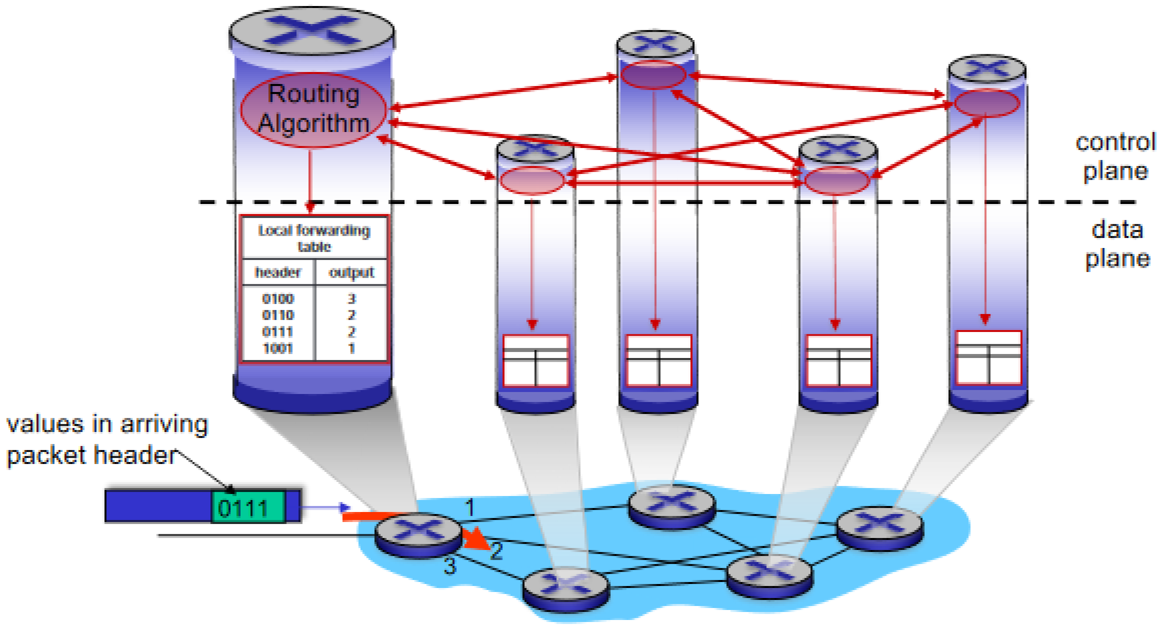
Some external resources I referred to

1. *What is the control plane? | Control plane vs. data plane | Cloudflare*. (n.d.).

   https://www.cloudflare.com/learning/network-layer/what-is-the-control-plane/

2. Chapter 5 Network Layer: The Control Plane. (2016). *Computer Networking: A Top Down Approach*.

   http://courses.washington.edu/ee565/handouts/chapter5.pdf



Active class 7: Who is Instructing What

Activity 1: Group discussion

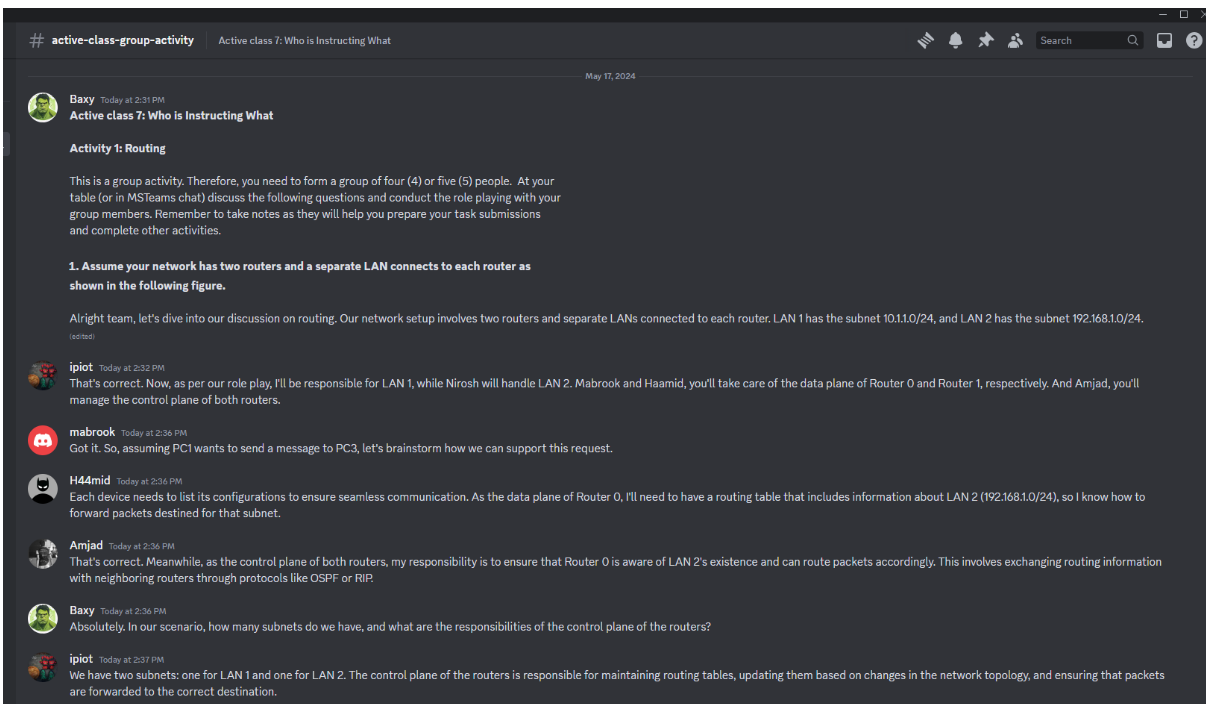
In Activity 1, we gather as a group to discuss routing concepts and simulate a network scenario. We form a team of four or five people and engage in discussions and role-playing exercises.

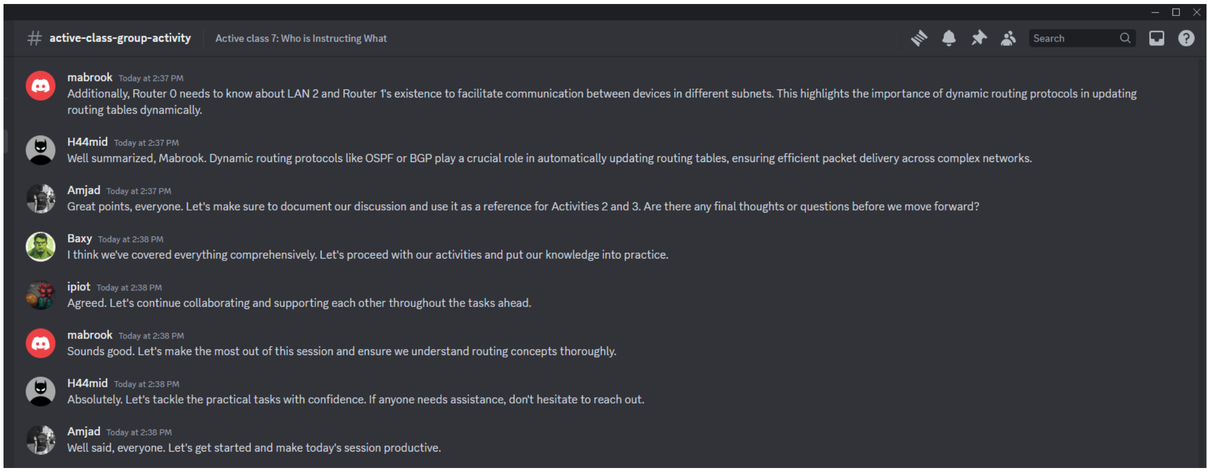
We start by envisioning a network with two routers and separate LANs. Each LAN has its own IP address range: LAN1 with 10.1.1.0/24 and LAN2 with 192.168.1.0/24.

To simulate the network, some of us act as LANs, responsible for PCs in each LAN, while others represent the data plane of Router 0 and Router 1. One member takes on the role of the control plane for both routers.

We simulate a scenario where PC1 needs to send a message to PC3, requiring coordination and configuration among all devices involved.

During our discussion, we analyze the network's subnet structure and discuss the responsibilities of the control plane in routers, including how Router 0 learns about LAN2 and Router 1.





\# active-class-group-activity | Active class 7: Who is Instructing What

Search

mabrook Today at 2:37 PM
Additionally, Router 0 needs to know about LAN 2 and Router 1's existence to facilitate communication between devices in different subnets. This highlights the importance of dynamic routing protocols in updating routing tables dynamically.

H44mid Today at 2:37 PM
Well summarized, Mabrook. Dynamic routing protocols like OSPF or BGP play a crucial role in automatically updating routing tables, ensuring efficient packet delivery across complex networks.

Amjad Today at 2:37 PM
Great points, everyone. Let's make sure to document our discussion and use it as a reference for Activities 2 and 3. Are there any final thoughts or questions before we move forward?

Baxy Today at 2:38 PM
I think we've covered everything comprehensively. Let's proceed with our activities and put our knowledge into practice.

ipiot Today at 2:38 PM
Agreed. Let's continue collaborating and supporting each other throughout the tasks ahead.

mabrook Today at 2:38 PM
Sounds good. Let's make the most out of this session and ensure we understand routing concepts thoroughly.

H44mid Today at 2:38 PM
Absolutely. Let's tackle the practical tasks with confidence. If anyone needs assistance, don't hesitate to reach out.

Amjad Today at 2:38 PM
Well said, everyone. Let's get started and make today's session productive.

Activity 2: Cisco Packet Tracer Implementation

After our discussion, we transition to Activity 2, where we implement the network scenario using Cisco Packet Tracer.

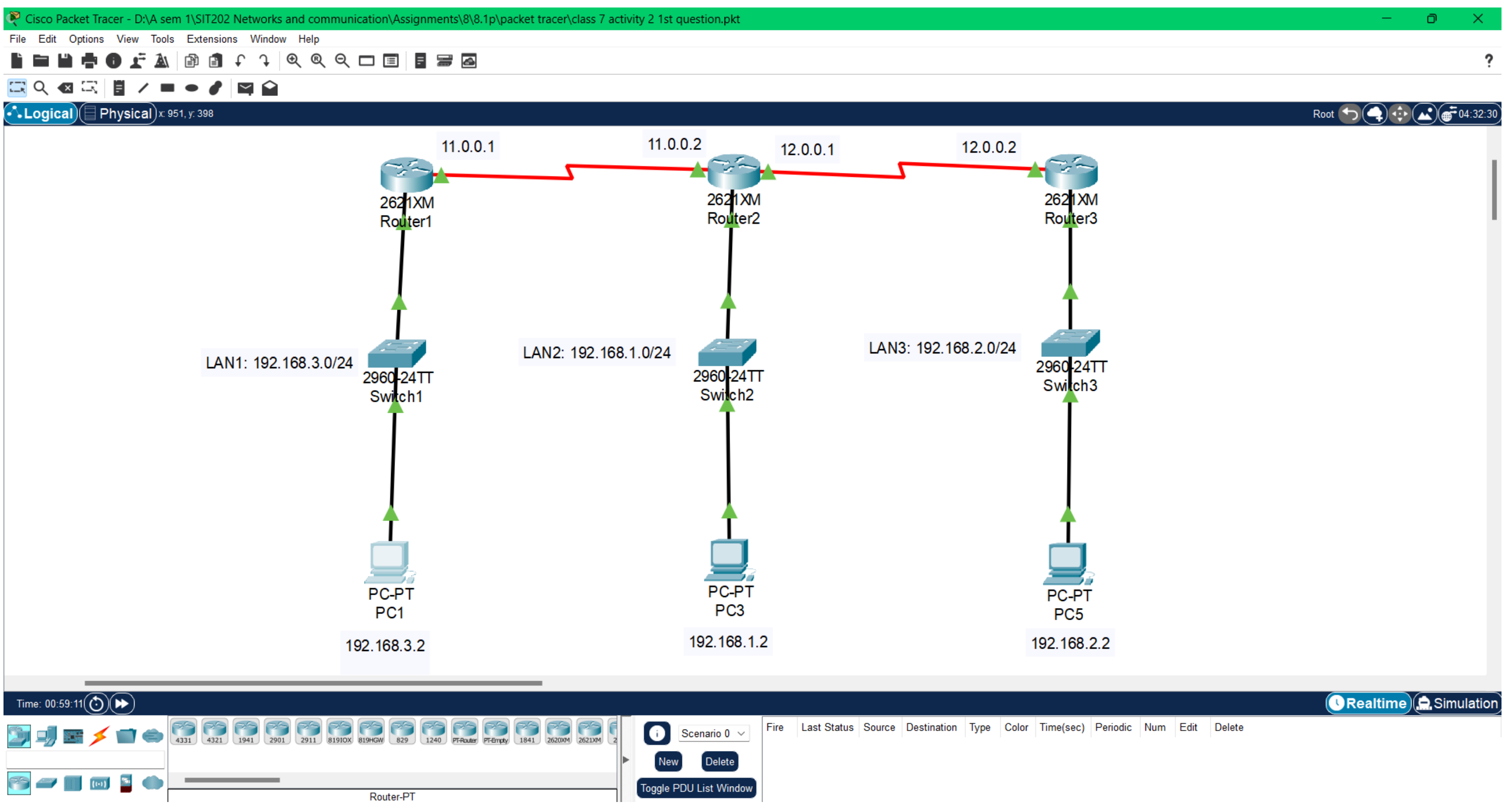
Working collaboratively, we configure each device in the network based on our earlier discussions. We ensure PC1, PC3, and PC5 can communicate by adding static routes to each router.

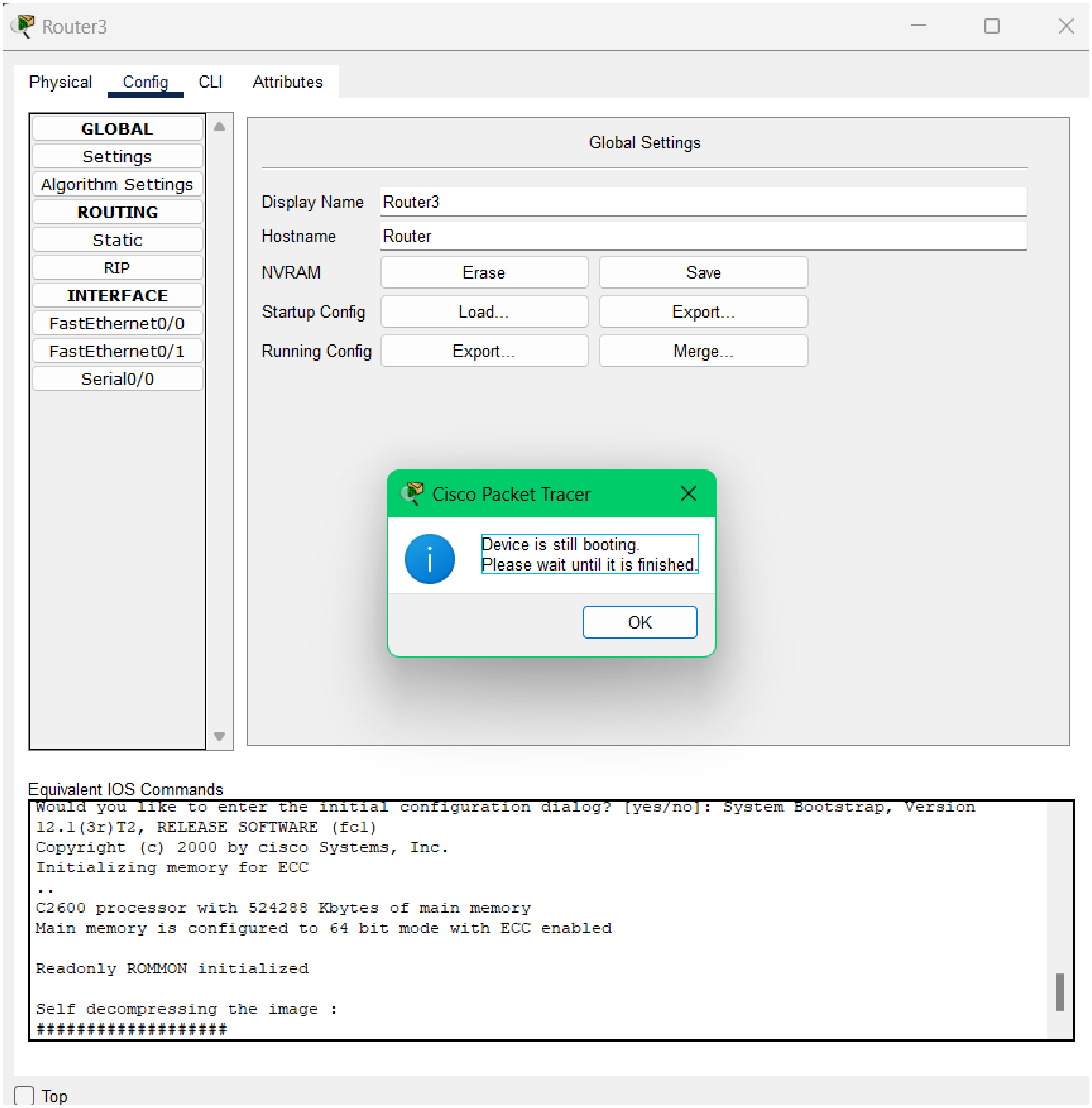
Using Cisco Packet Tracer, we verify connectivity between PC1, PC3, and PC5 by executing PING commands and simulations.

First, I launched Cisco Packet Tracer on my computer, ensuring that all group members have access to the software.

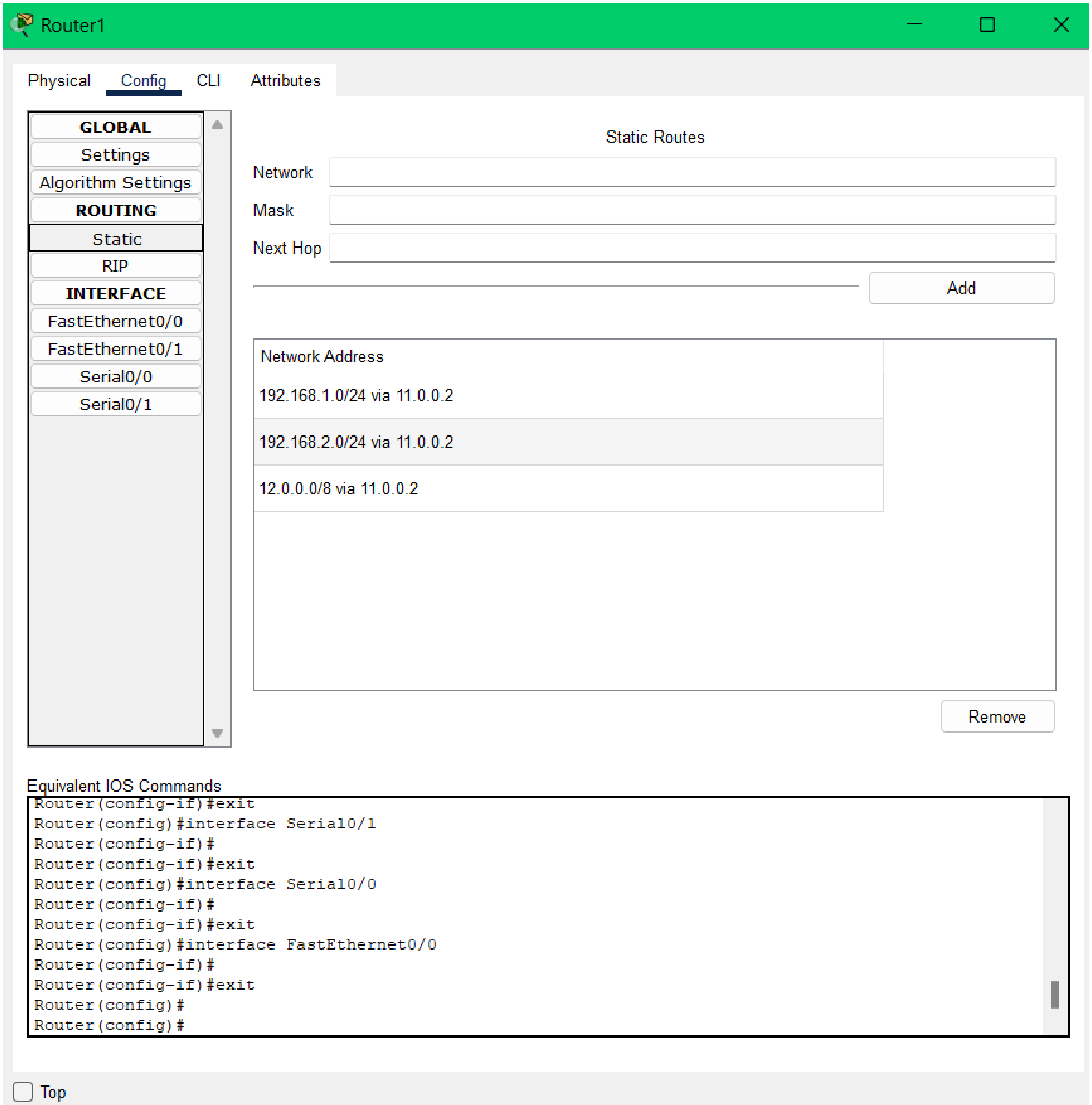
Using the insights gained from our group discussion in Activity 1, I would start by designing the network topology in Cisco Packet Tracer. I would place the 2621XM routers and connect them via serial connections as specified in the task requirements.

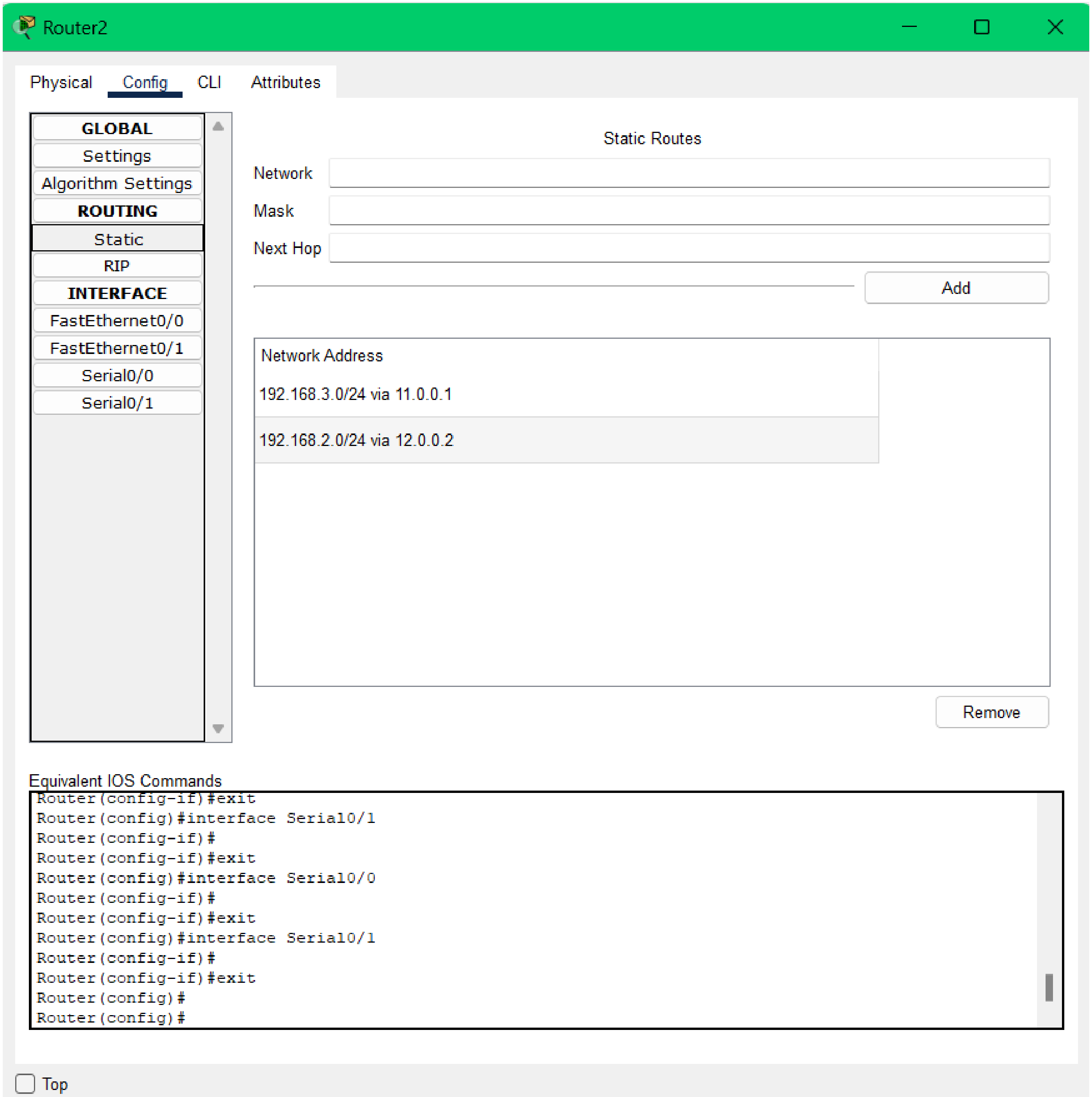
Question 1

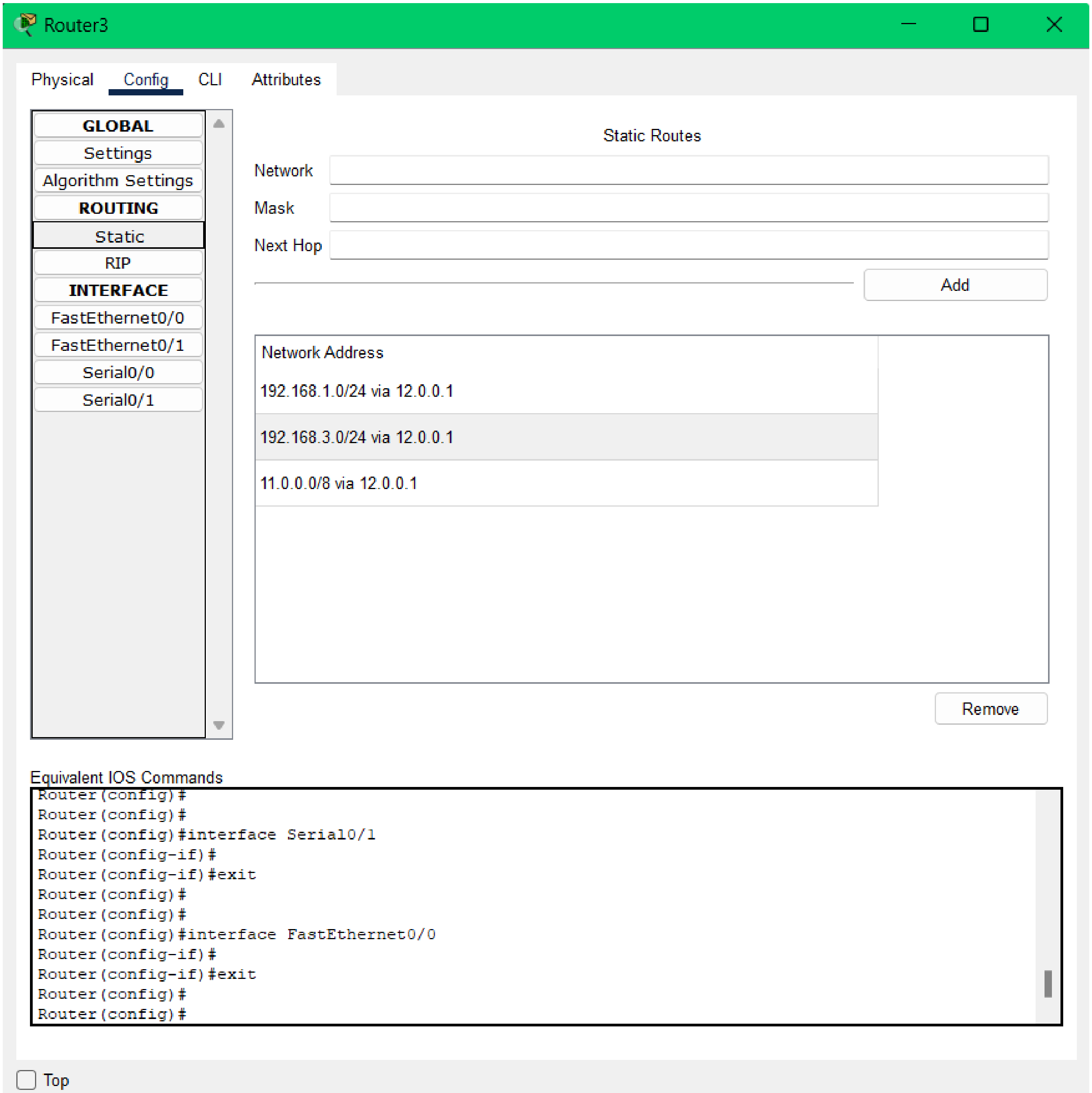



Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0
Global Settings
Display Name
Router3
Hostname
Router
NVRAM
Erase
Save
Startup Config
Load...
Export...
Running Config
Export...
Merge...
Cisco Packet Tracer
Device is still booting.
Please wait until it is finished.
OK
Equivalent IOS Commands
Would you like to enter the initial configuration dialog? [yes/no]: System Bootstrap, Version
12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Initializing memory for ECC
..
C2600 processor with 524288 Kbytes of main memory
Main memory is configured to 64 bit mode with ECC enabled
Readonly ROMMON initialized
Self decompressing the image :
###################
Top

Leveraging the discussions from Activity 1, I configured each device in the network. This includes setting up IP addresses, subnet masks, default gateways, and static routes on the routers to ensure communication between PC1, PC3, and PC5.



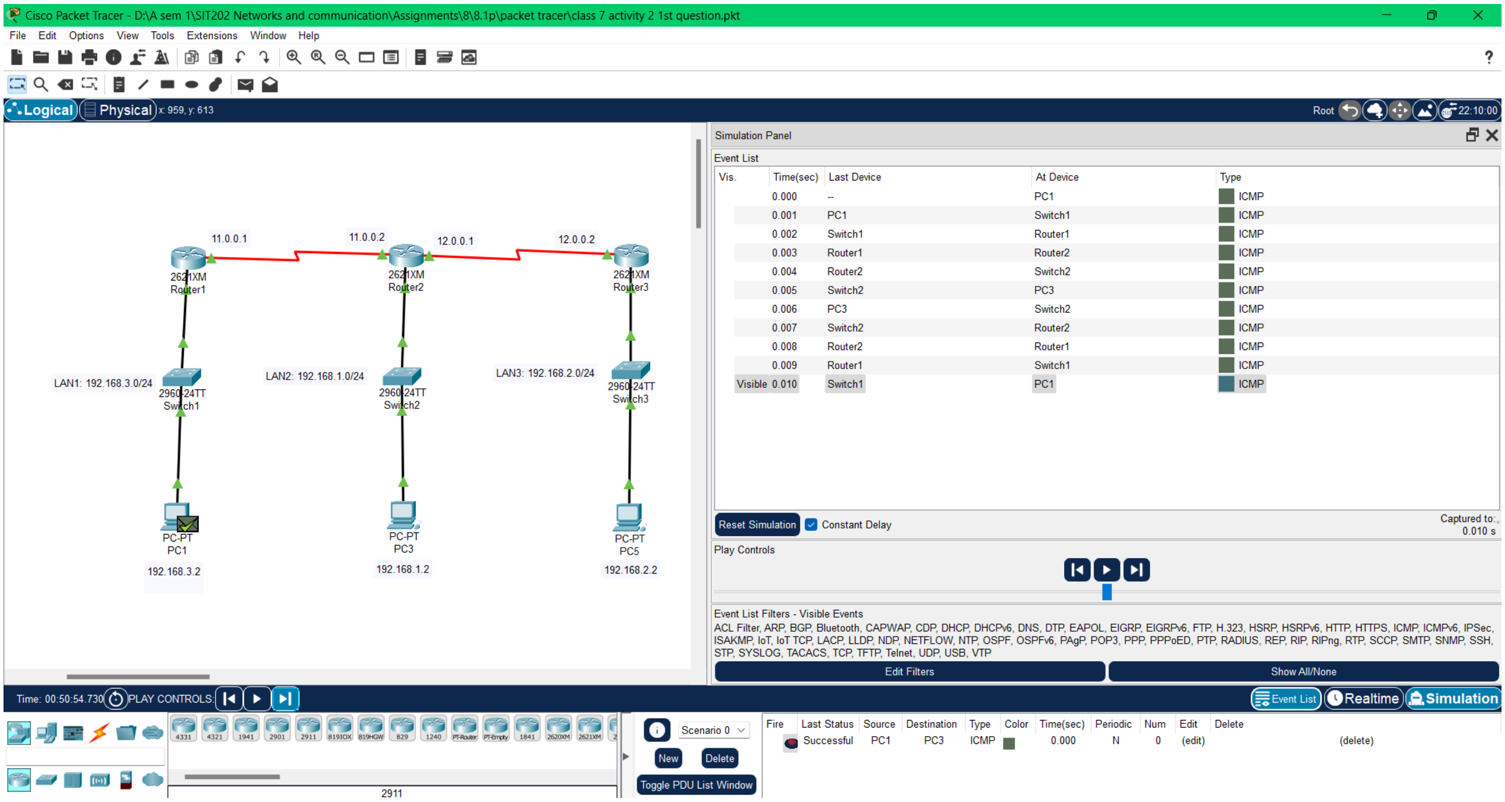

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0
Serial0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.3.0/24 via 11.0.0.1
192.168.2.0/24 via 12.0.0.2
Remove
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Top


Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0
Serial0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.1.0/24 via 12.0.0.1
192.168.3.0/24 via 12.0.0.1
11.0.0.0/8 via 12.0.0.1
Remove
Equivalent IOS Commands
Router(config)#
Router(config)#
Router(config)#interface Serial0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Top

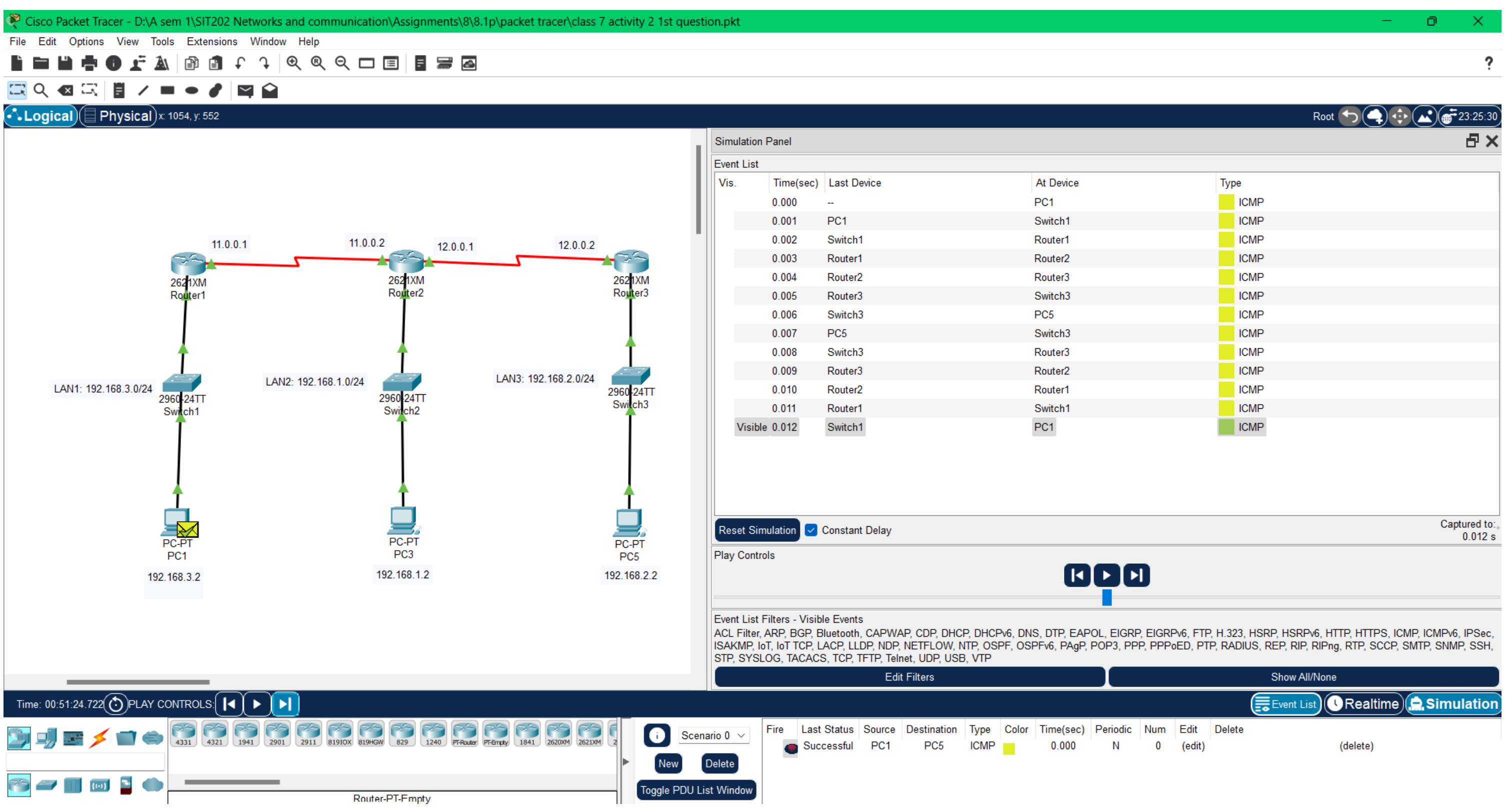
Once the configuration is complete, I verified that PC1 can communicate with both PC3 and PC5 using the PING command and simulations within Cisco Packet Tracer. This involves sending test packets between the devices and confirming successful communication.

Simulation

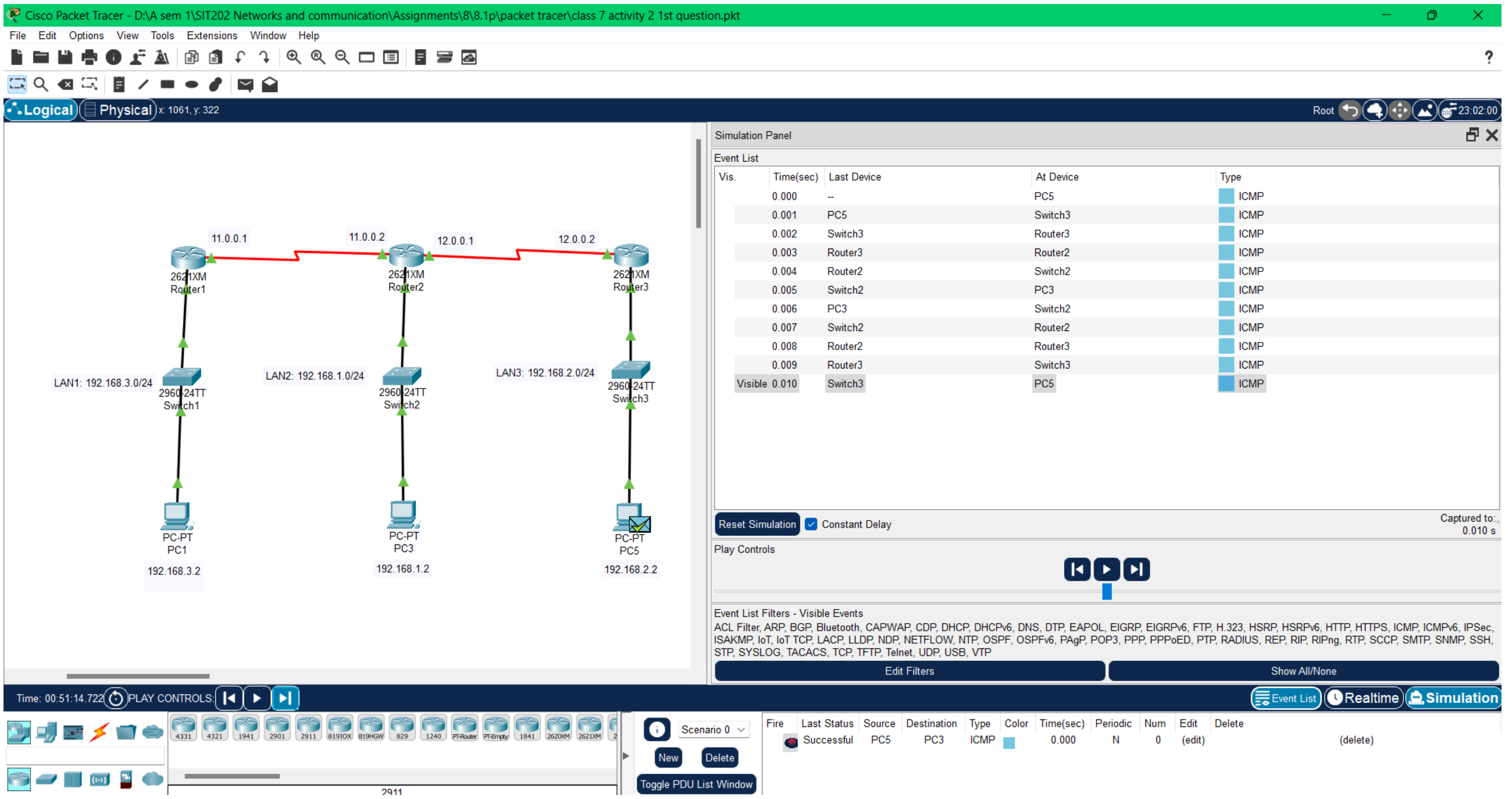
PC1 – PC3



PC1 – PC5

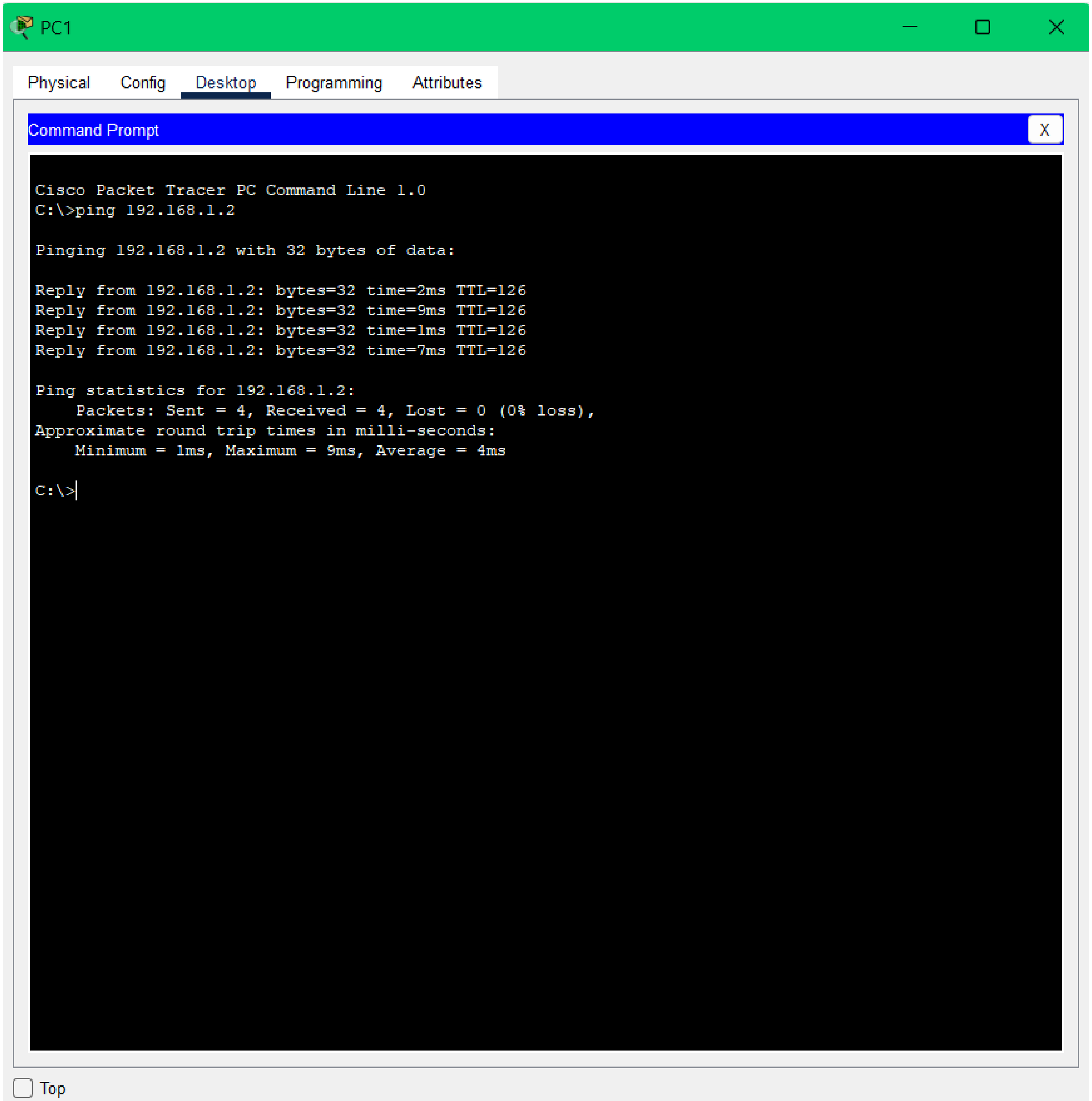


PC5 – PC3

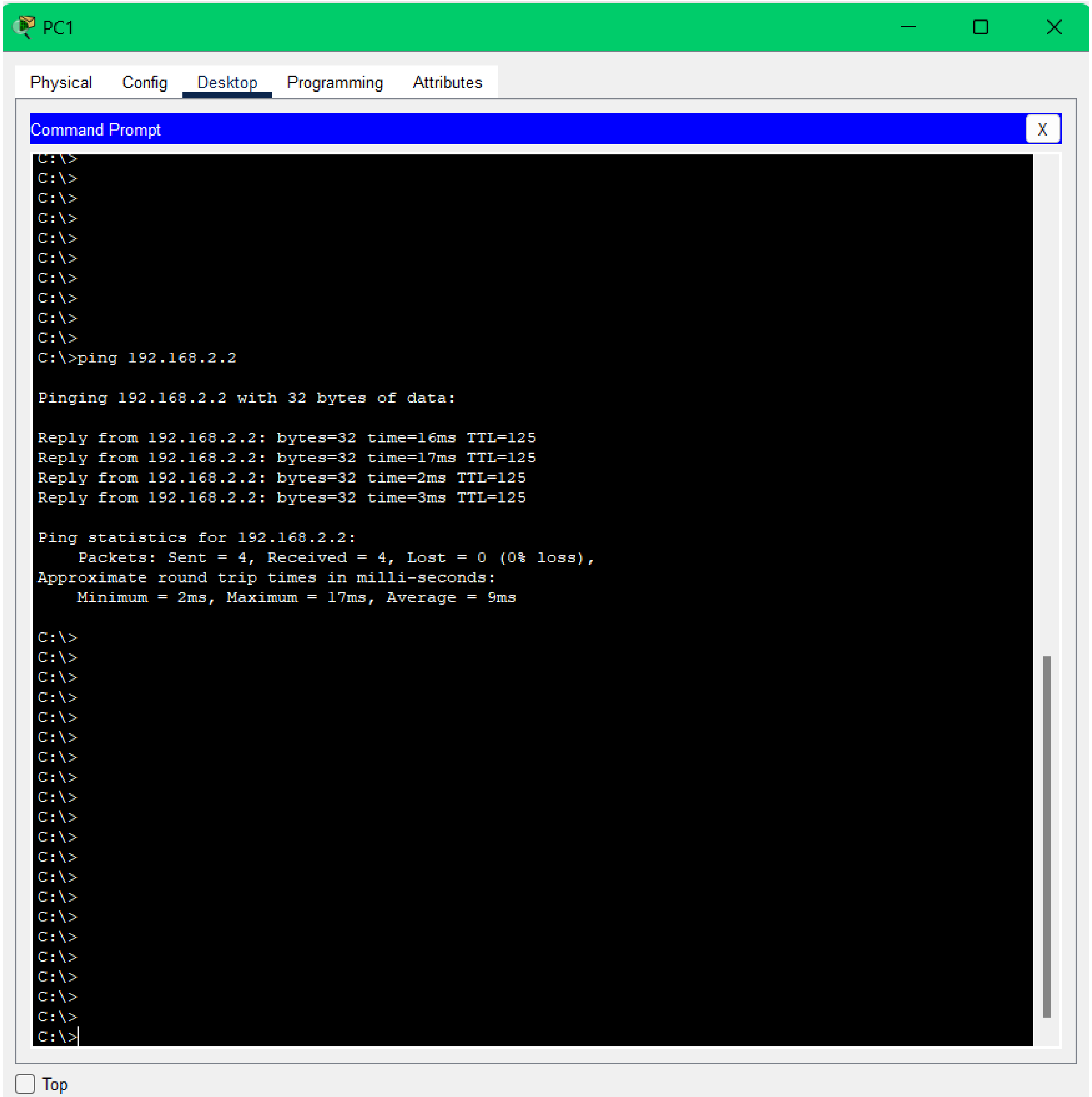

Cisco Packet Tracer - D:\A sem 1\SIT202 Networks and communication\Assignments\8\8.1p\packet tracer\class 7 activity 2 1st question.pkt
Simulation Panel
Event List
Vis. | Time(sec) | Last Device | At Device | Type
0.000 | -- | PC5 | ICMP
0.001 | PC5 | Switch3 | ICMP
0.002 | Switch3 | Router3 | ICMP
0.003 | Router3 | Router2 | ICMP
0.004 | Router2 | Switch2 | ICMP
0.005 | Switch2 | PC3 | ICMP
0.006 | PC3 | Switch2 | ICMP
0.007 | Switch2 | Router2 | ICMP
0.008 | Router2 | Router3 | ICMP
0.009 | Router3 | Switch3 | ICMP
Visible 0.010 | Switch3 | PC5 | ICMP
11.0.0.1
11.0.0.2
12.0.0.1
12.0.0.2
2621XM Router1
2621XM Router2
2621XM Router3
LAN1: 192.168.3.0/24
LAN2: 192.168.1.0/24
LAN3: 192.168.2.0/24
2960-24TT Switch1
2960-24TT Switch2
2960-24TT Switch3
PC-PT PC1
PC-PT PC3
PC-PT PC5
192.168.3.2
192.168.1.2
192.168.2.2
Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete
Successful | PC5 | PC3 | ICMP | 0.000 | N | 0 | (edit) | (delete)

Pinging

PC1 – PC3



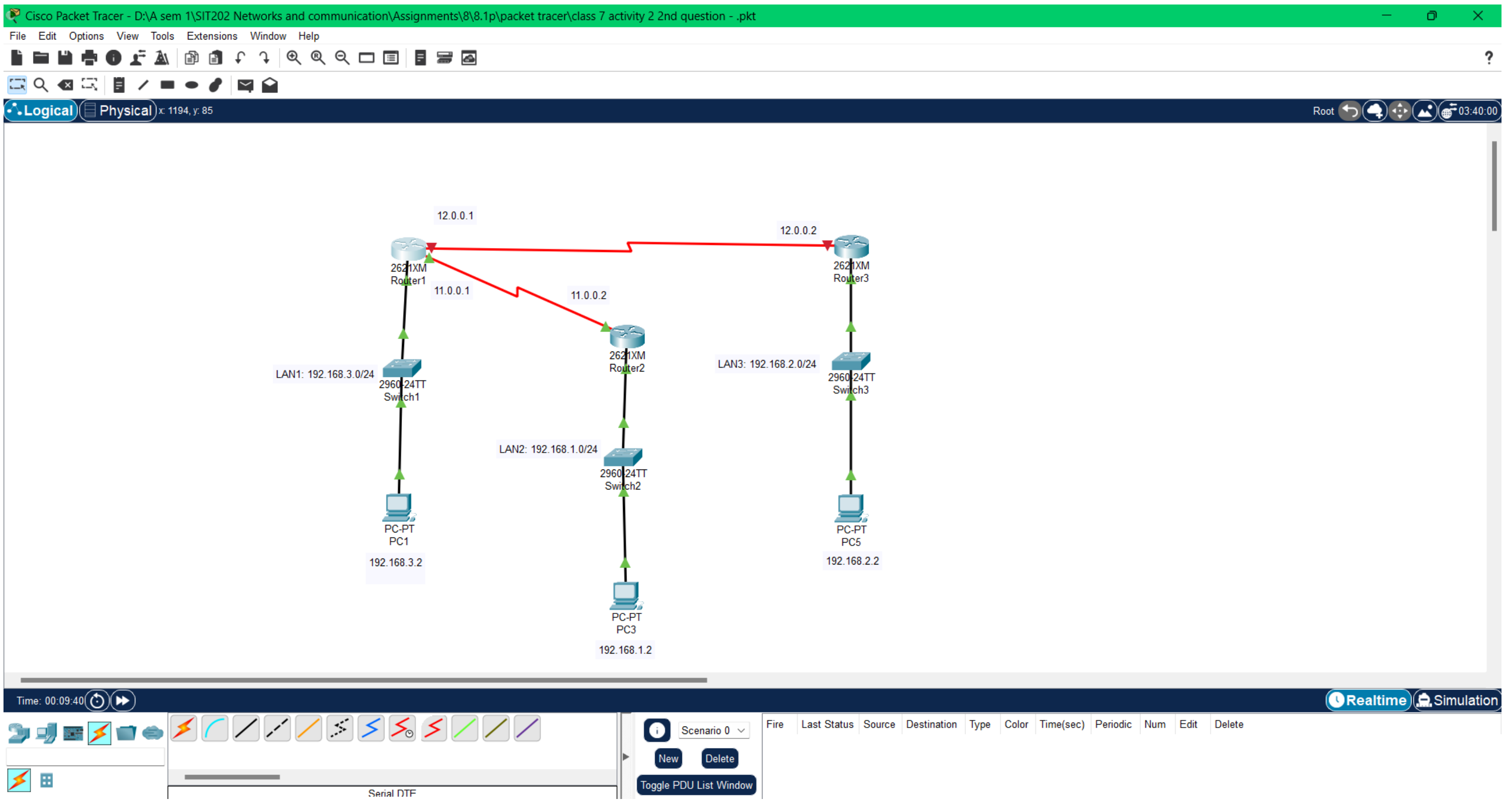
PC1 – PC5


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=16ms TTL=125
Reply from 192.168.2.2: bytes=32 time=17ms TTL=125
Reply from 192.168.2.2: bytes=32 time=2ms TTL=125
Reply from 192.168.2.2: bytes=32 time=3ms TTL=125
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 17ms, Average = 9ms
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
Top

Question 2

First, I'd open up Cisco Packet Tracer and locate Router 1 and Router 3. Then, I'd add a new serial connection between them. This involves selecting the correct interface on each router and establishing the connection.

Next, I'd locate the direct connection between Router 2 and Router 3 and remove it. This ensures that Router 2 is no longer directly connected to Router 3.

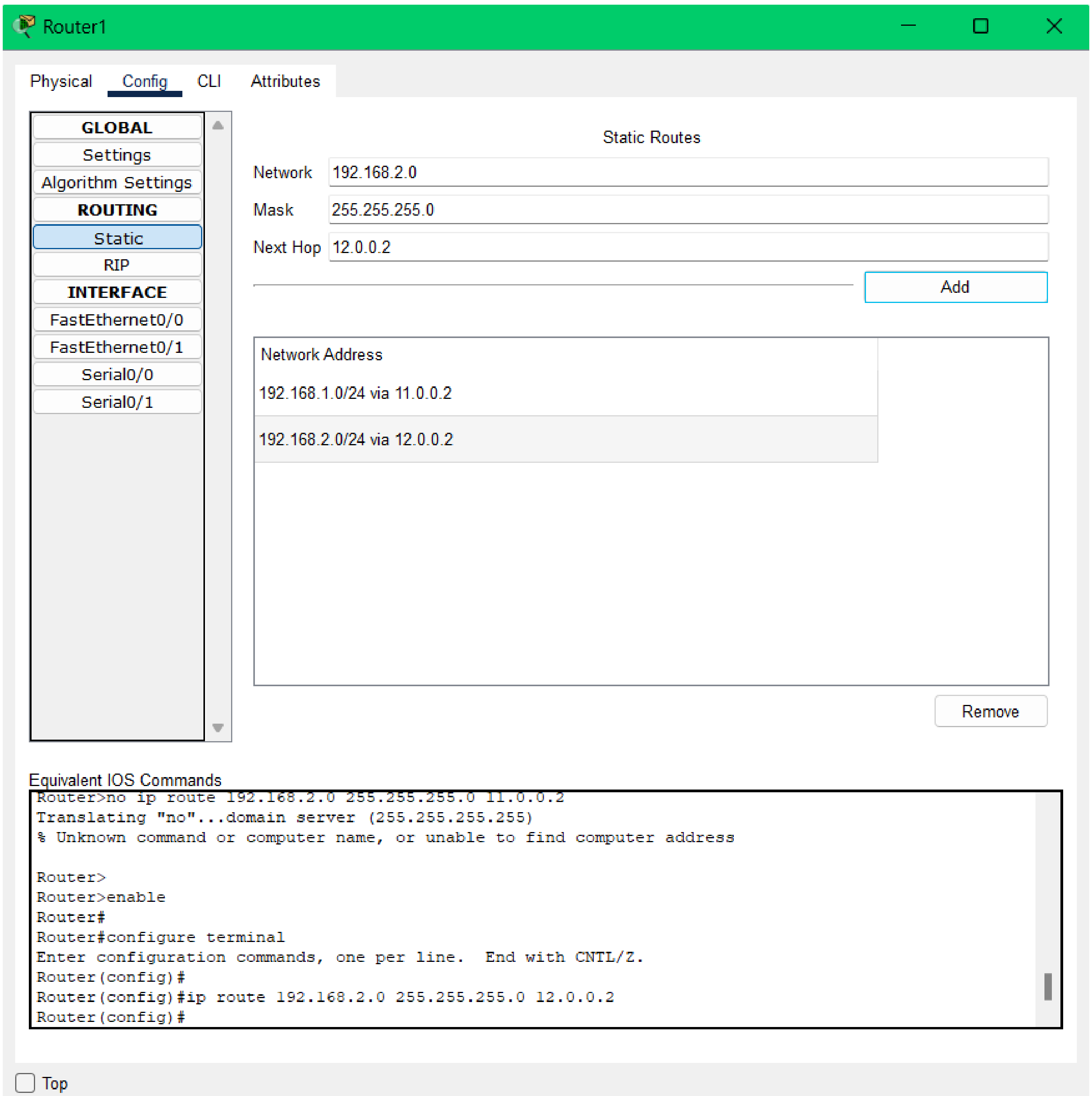


Now that the network topology has changed, I considered how this alteration affects the communication between PC1 and PC5, both of which are in LAN1 (192.168.3.0/24).

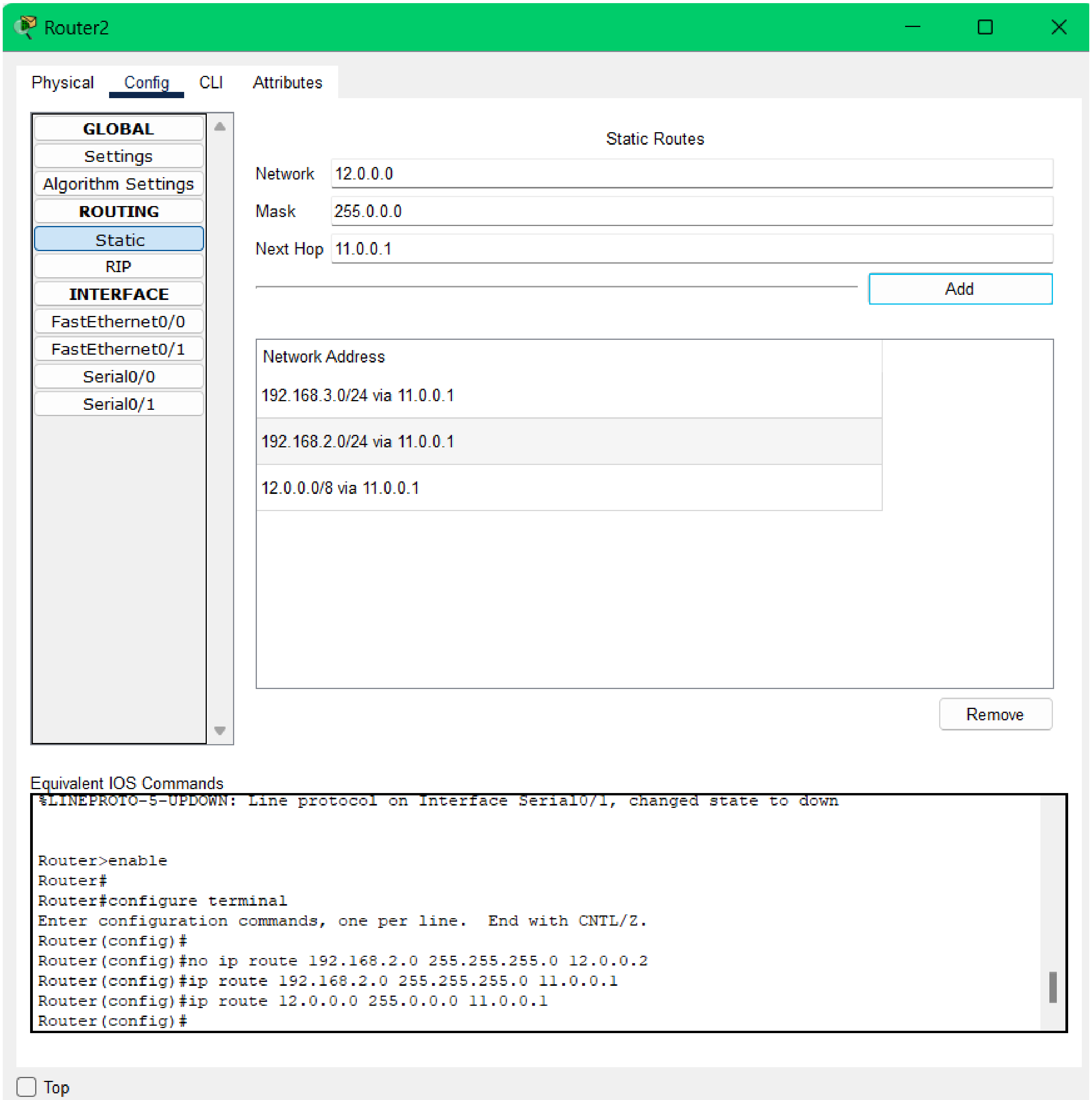
Then identified that the static routes needed to enable communication between PC1 and PC5. Since Router 2 is no longer directly connected to Router 3, I'd likely need to add a static route on Router 2 to instruct it to send traffic destined for LAN1 (192.168.3.0/24) via Router 1.

Then I'd access Router 2's configuration and add the necessary static route pointing towards Router 1 for the LAN1 subnet. Once the route is configured, then saved the changes and ensured they take effect.

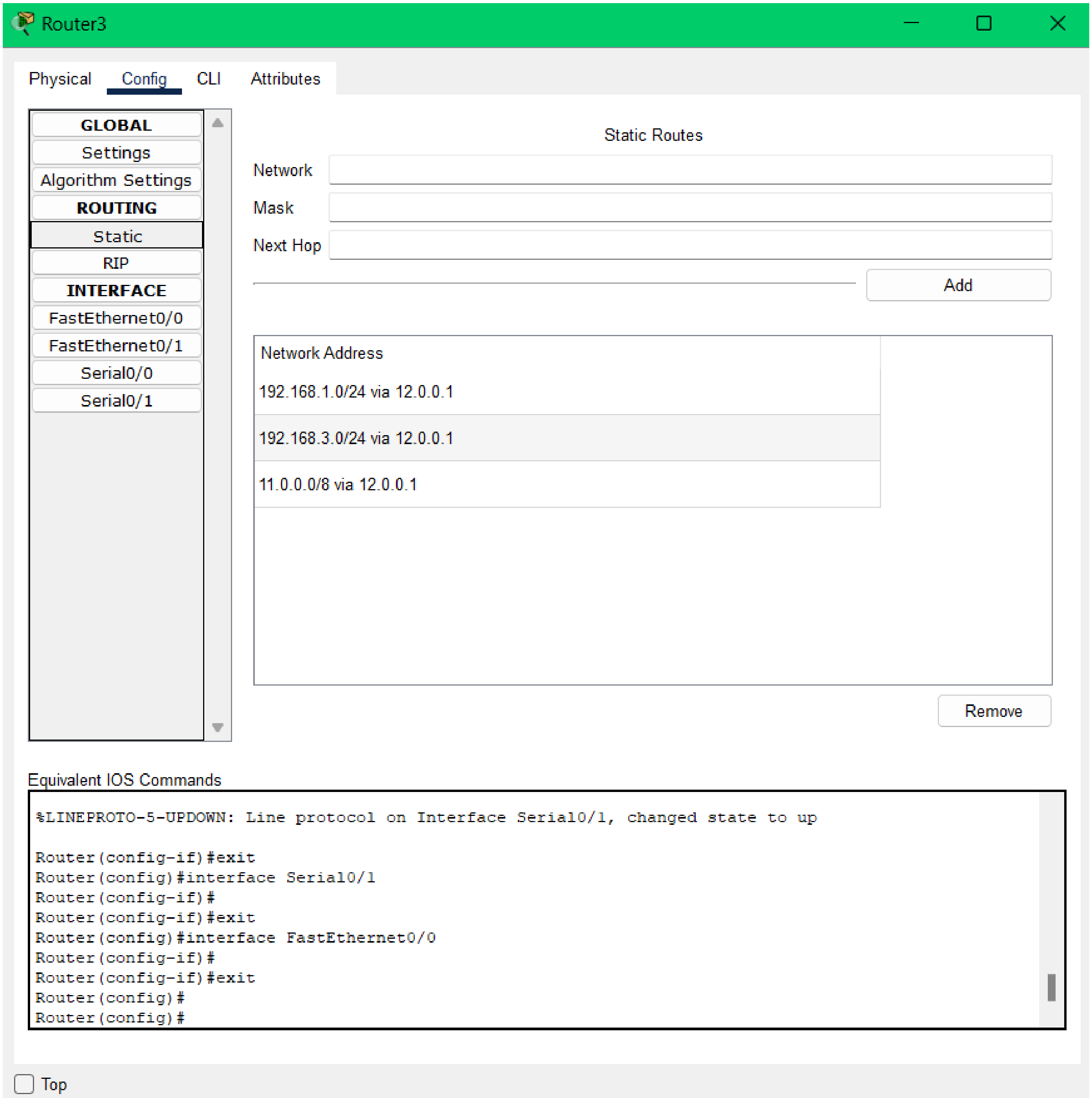
Router 1 static route



Router 2 Static route

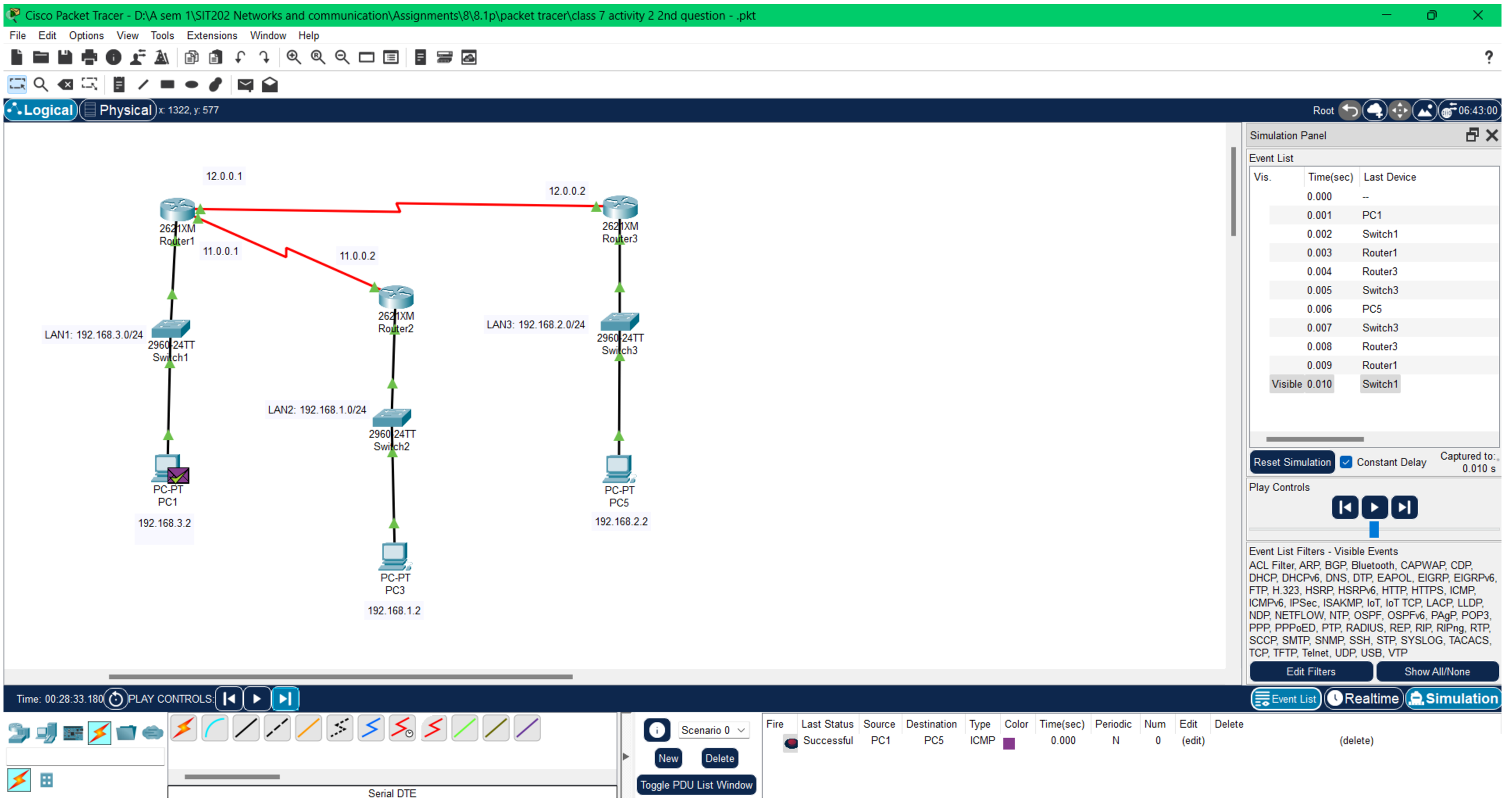


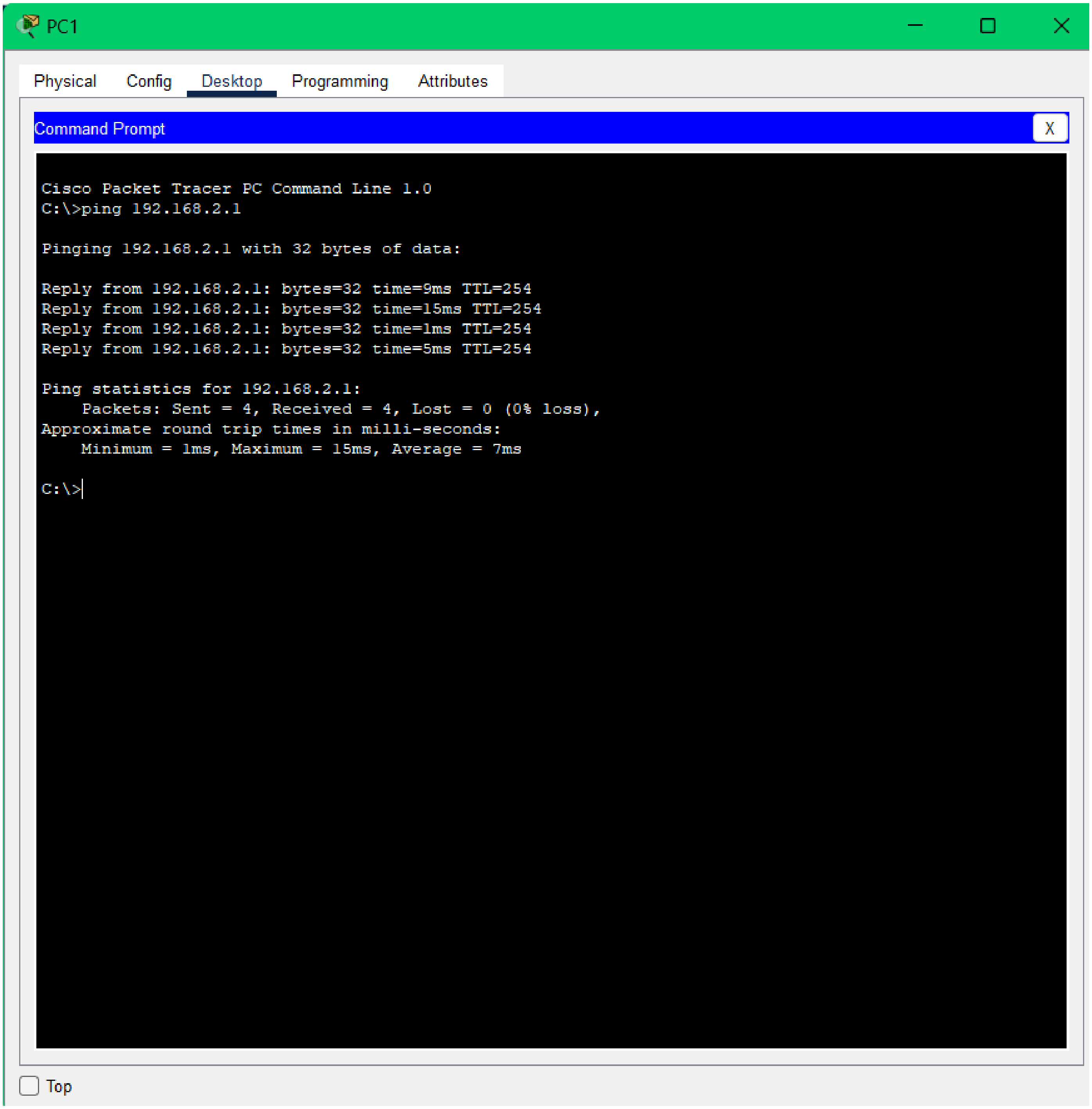
Router 3 static route



Now the router 1 is connected directly to router 3 and 2, the route can be directly to both the routers, like 192.168.1.1 to the router IP 11.0.0.1 and 192.168.2.1 to the router 12.0.0.2. but earlier it was different as shown in the previous question's screenshot.

Finally, I test the network to verify that PC1 can communicate with PC5. Using the PING command and simulations in Cisco Packet Tracer, I confirmed that traffic can flow between the two PCs across the updated network topology. This includes checking for successful ping responses and ensuring that packets are routed correctly through Router 1. If everything works as expected, we'd consider the task successfully completed.




PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=9ms TTL=254
Reply from 192.168.2.1: bytes=32 time=15ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=5ms TTL=254
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 15ms, Average = 7ms
C:\>
Top

Activity 3: Alternative for Static Routing

In Activity 3, we explore alternatives to static routing and discuss modern routing algorithms.

We deliberate on alternatives to manually configuring routing tables each time the network topology changes.

We discuss the latest routing algorithms available and inquire if Cisco Packet Tracer supports any routing algorithms.

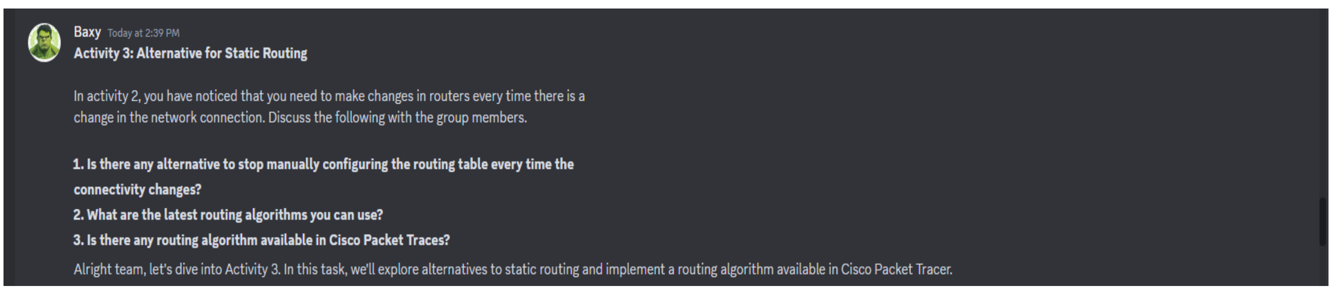
Transitioning back to Cisco Packet Tracer, we implement the network scenario again, this time using the routing algorithm available in the routers.

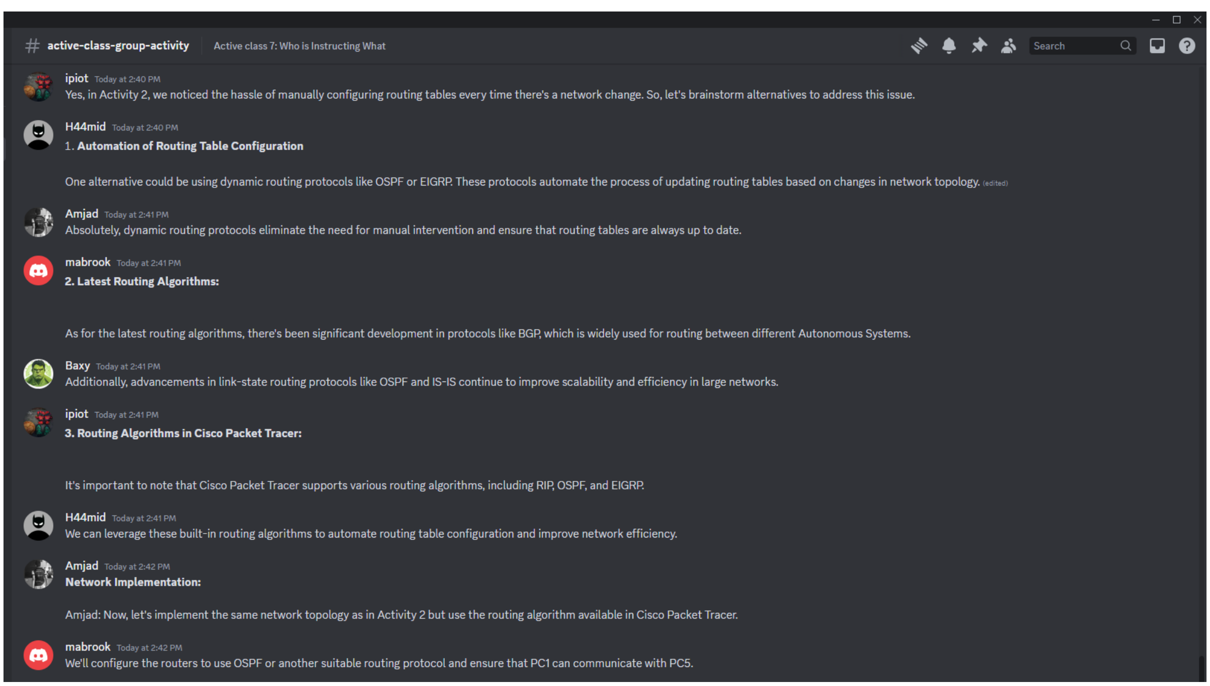
We verify network connections using PING commands on each PC.

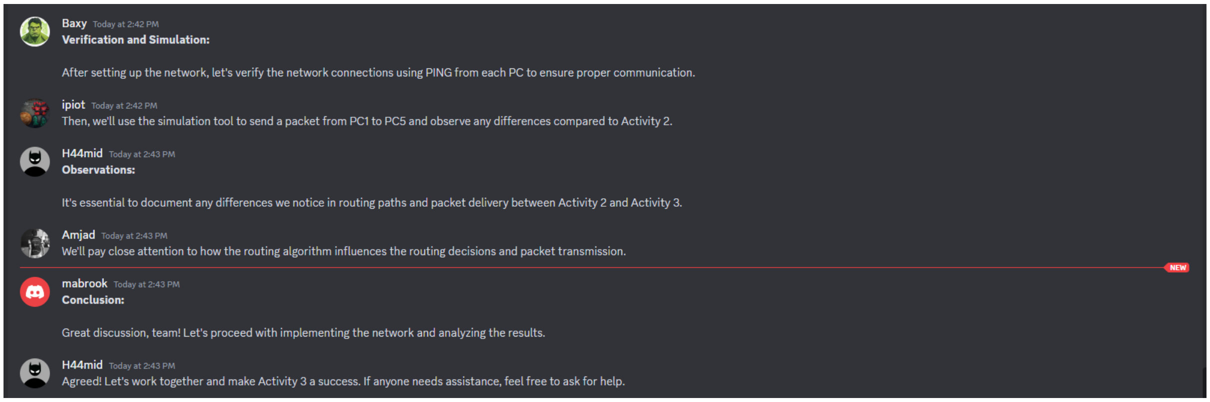
Utilizing the simulation tool, we send a packet from PC1 to PC5, observing any differences compared to the routing in Activity 2.

Finally, we remove the connection between Router 1 and 3 and use the simulation tool to send a packet from PC1 to PC5 without changing any configurations, analyzing the observed behavior.

Discussion







Baxy Today at 2:42 PM
Verification and Simulation:

After setting up the network, let's verify the network connections using PING from each PC to ensure proper communication.

ipiot Today at 2:42 PM
Then, we'll use the simulation tool to send a packet from PC1 to PC5 and observe any differences compared to Activity 2.

H44mid Today at 2:43 PM
Observations:

It's essential to document any differences we notice in routing paths and packet delivery between Activity 2 and Activity 3.

Amjad Today at 2:43 PM
We'll pay close attention to how the routing algorithm influences the routing decisions and packet transmission.

NEW

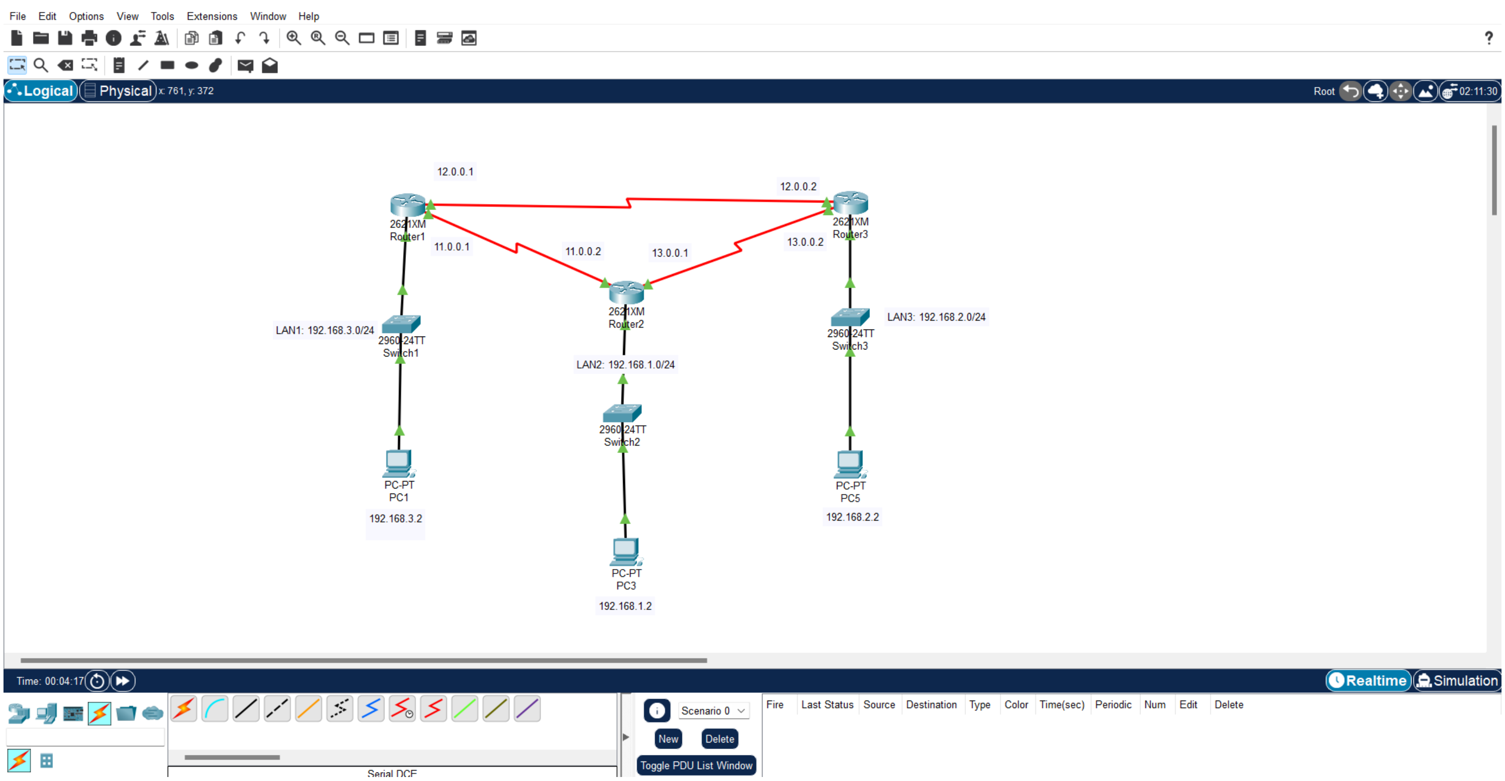
mabrook Today at 2:43 PM
Conclusion:

Great discussion, team! Let's proceed with implementing the network and analyzing the results.

H44mid Today at 2:43 PM
Agreed! Let's work together and make Activity 3 a success. If anyone needs assistance, feel free to ask for help.

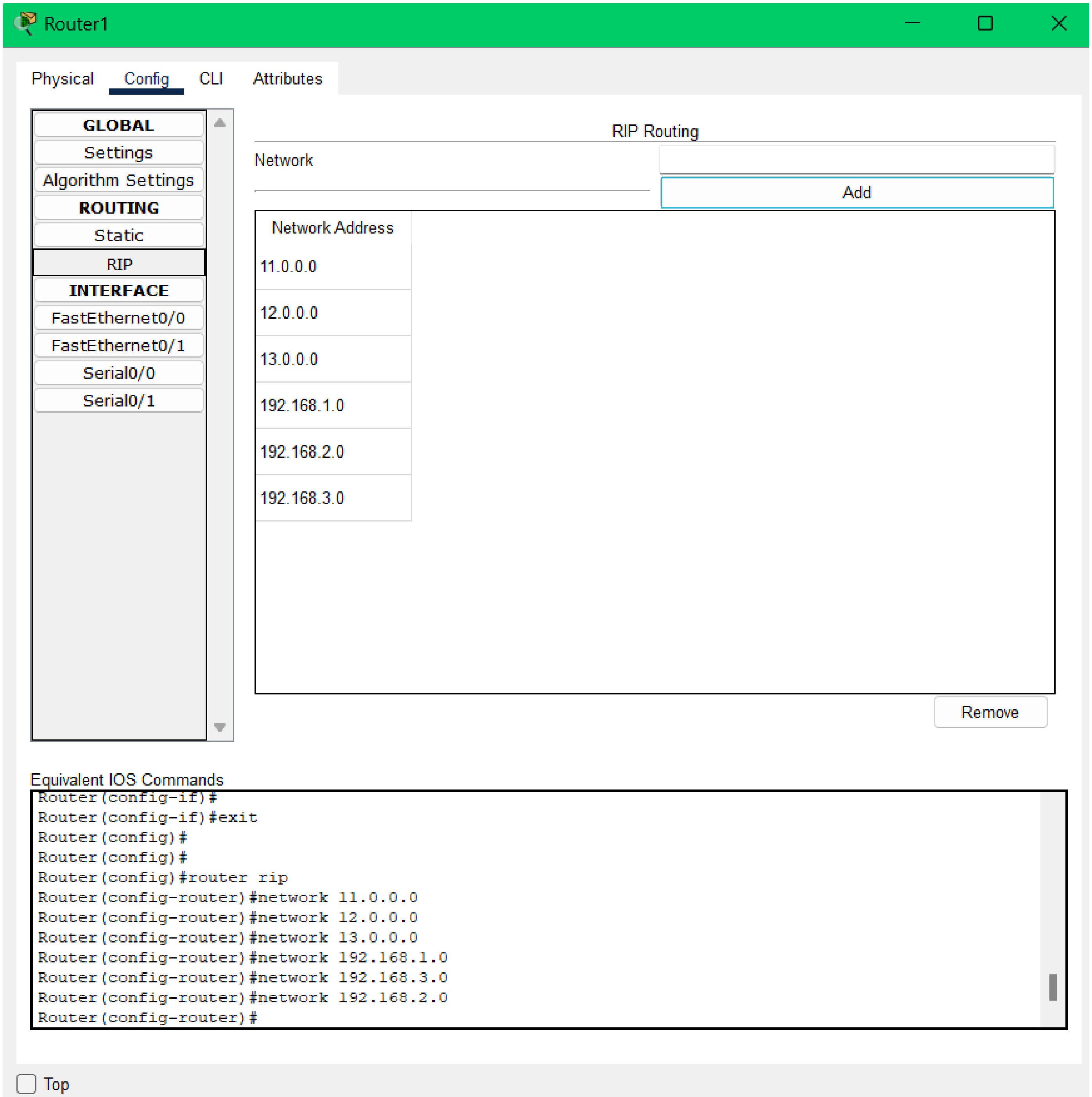
Simulation

Network before configuration of routing protocol

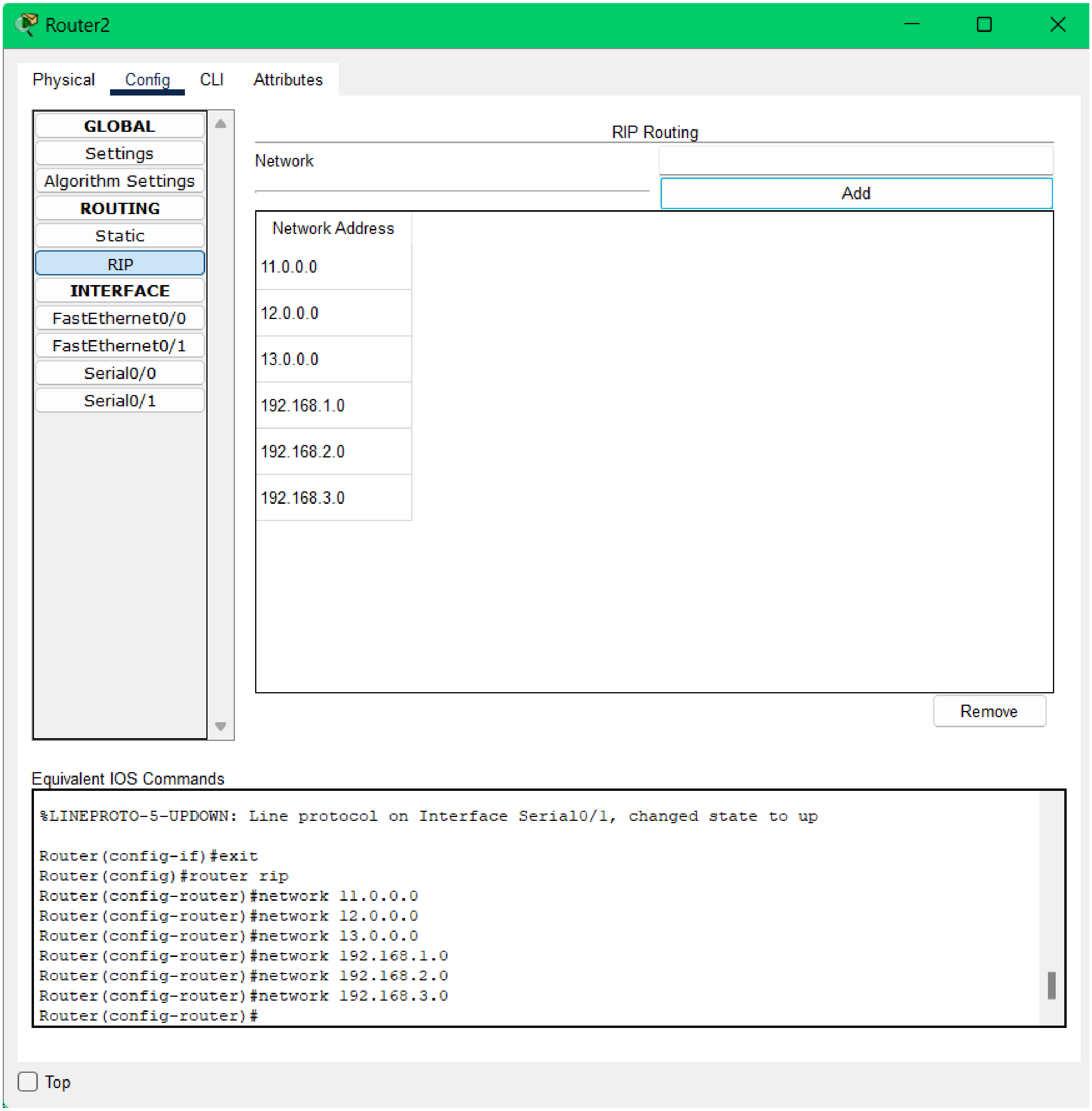


Setting the routers to have Routing Information Protocol enabled

Router 1

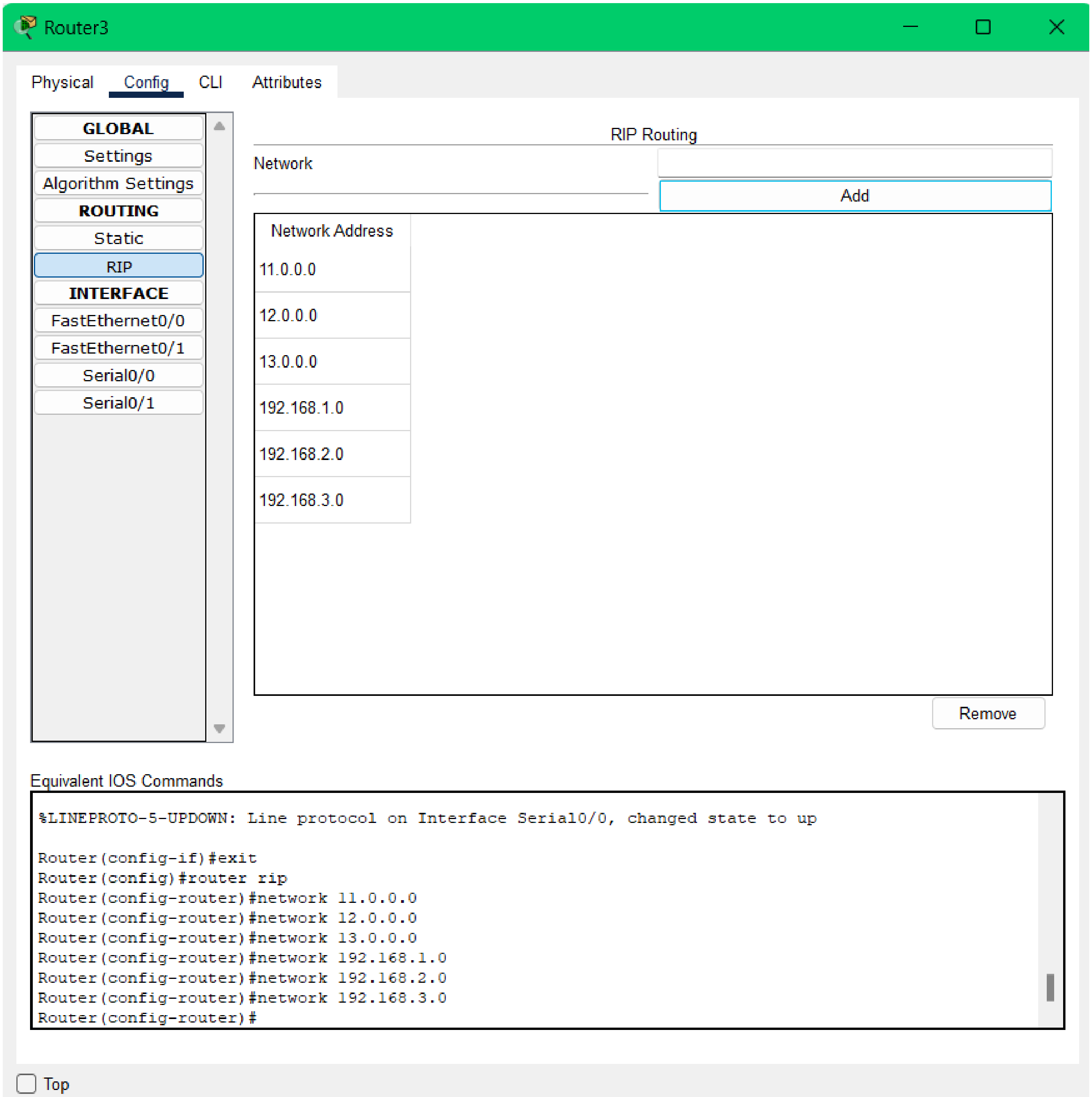


Router 2



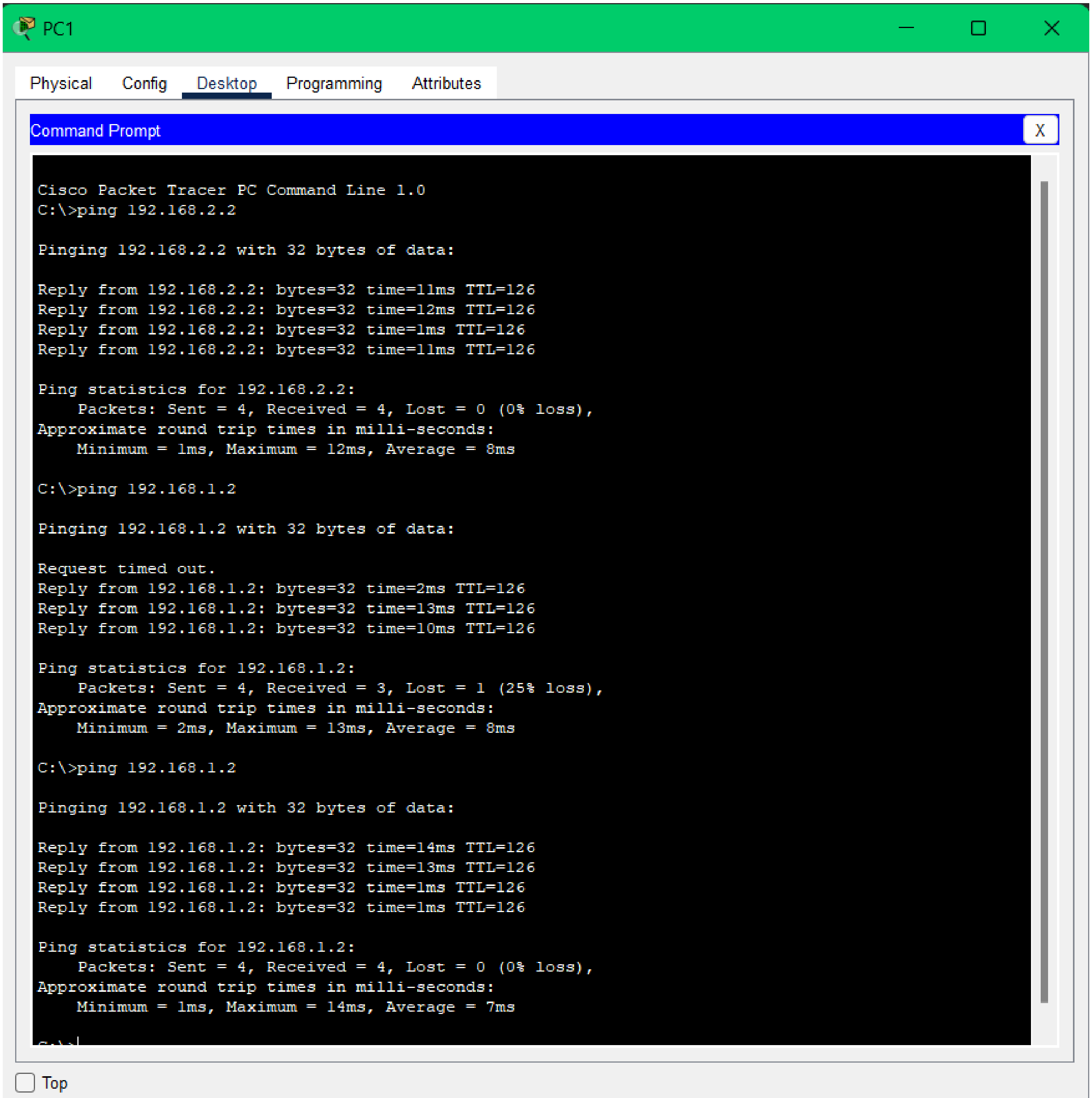
Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0
Serial0/1
RIP Routing
Network
Add
Network Address
11.0.0.0
12.0.0.0
13.0.0.0
192.168.1.0
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
Router(config-router)#network 12.0.0.0
Router(config-router)#network 13.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
Top

Router 3

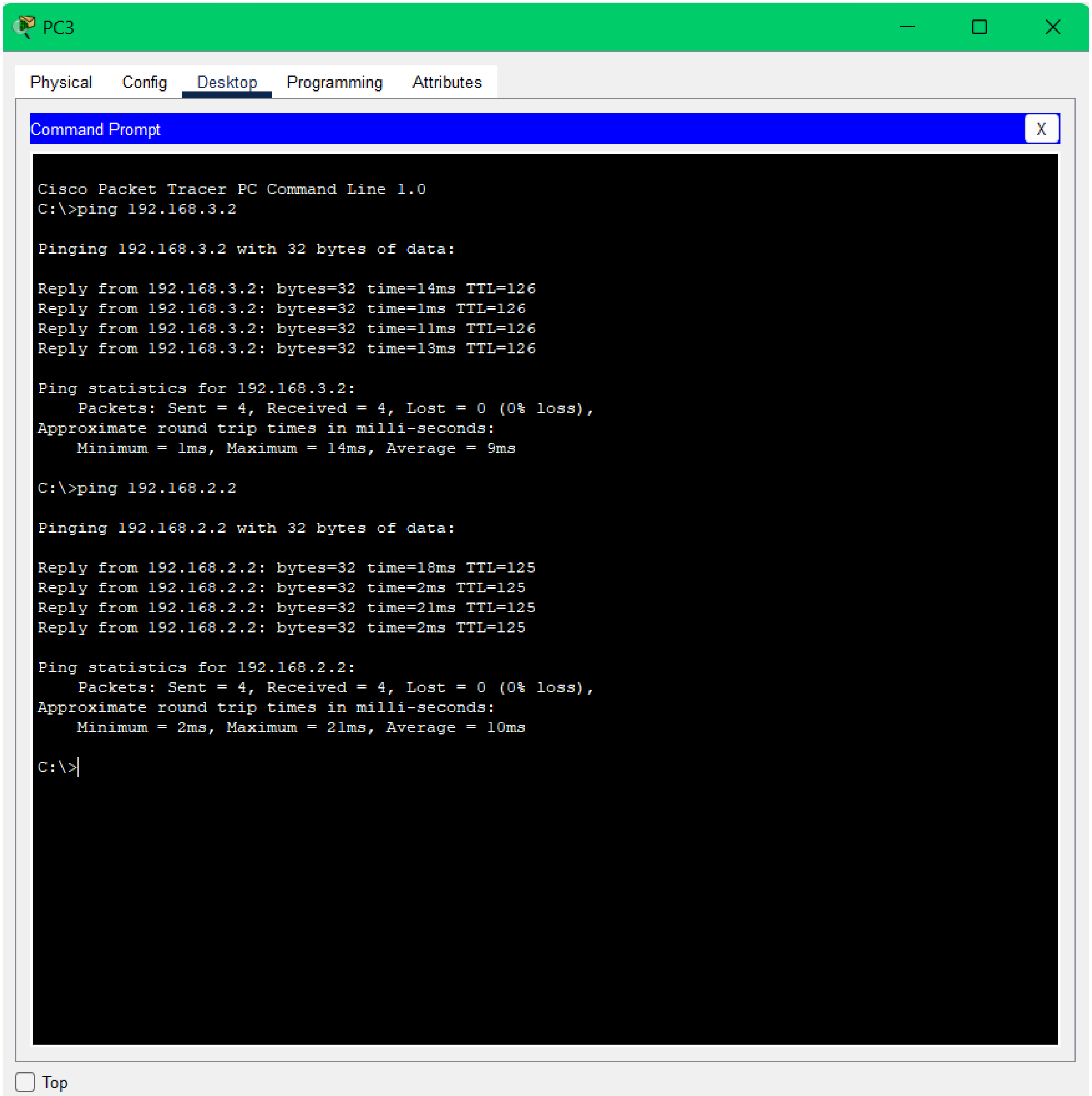

Router3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0
Serial0/1
RIP Routing
Network
Add
Network Address
11.0.0.0
12.0.0.0
13.0.0.0
192.168.1.0
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
Router(config-router)#network 12.0.0.0
Router(config-router)#network 13.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
Top

After enabling the routes using the RIP, we pinged each PCs to confirm that the connection is established properly between the networks after enabling the RIP, making sure the algorithm does its job

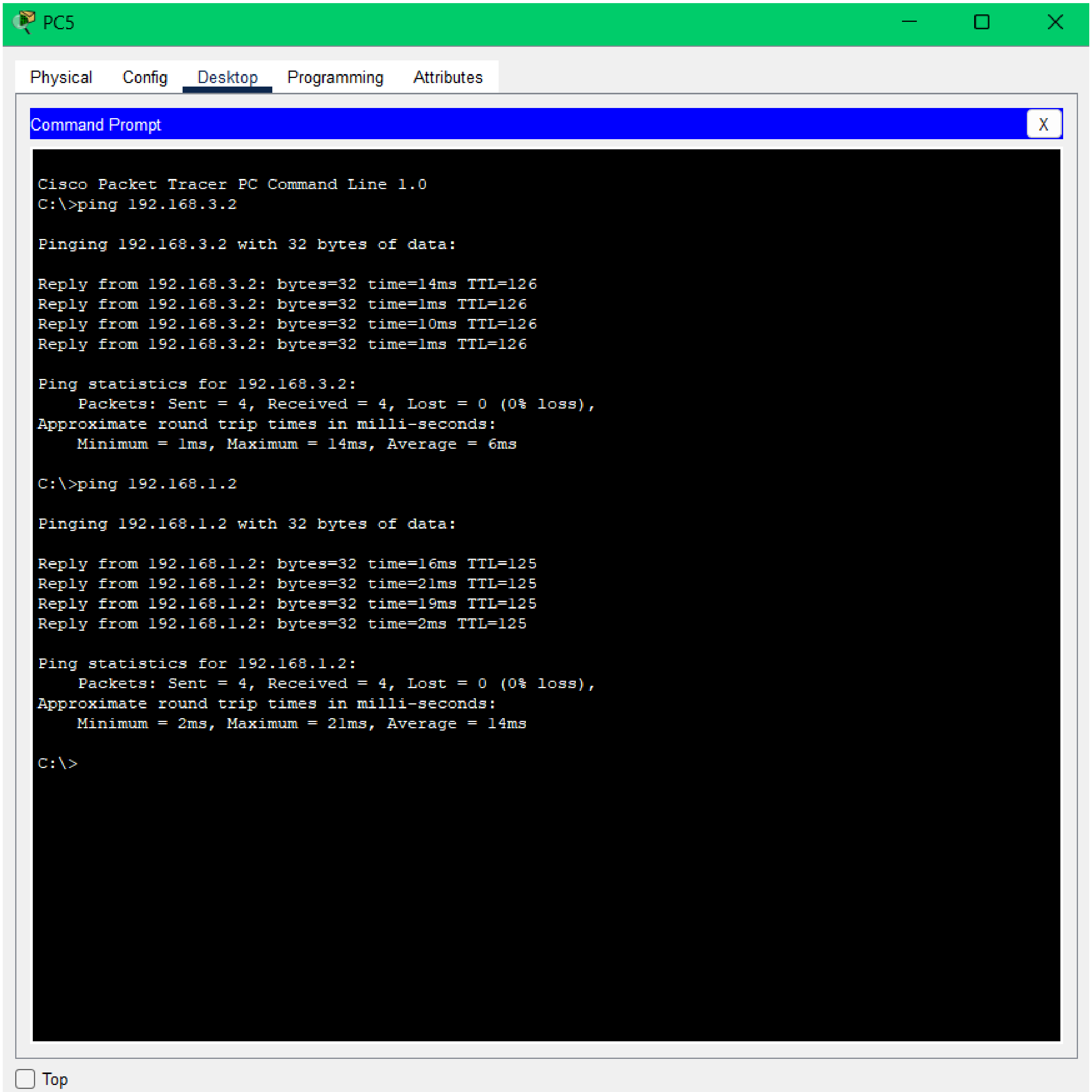
PC1 pinging to others



PC3 pinging to others



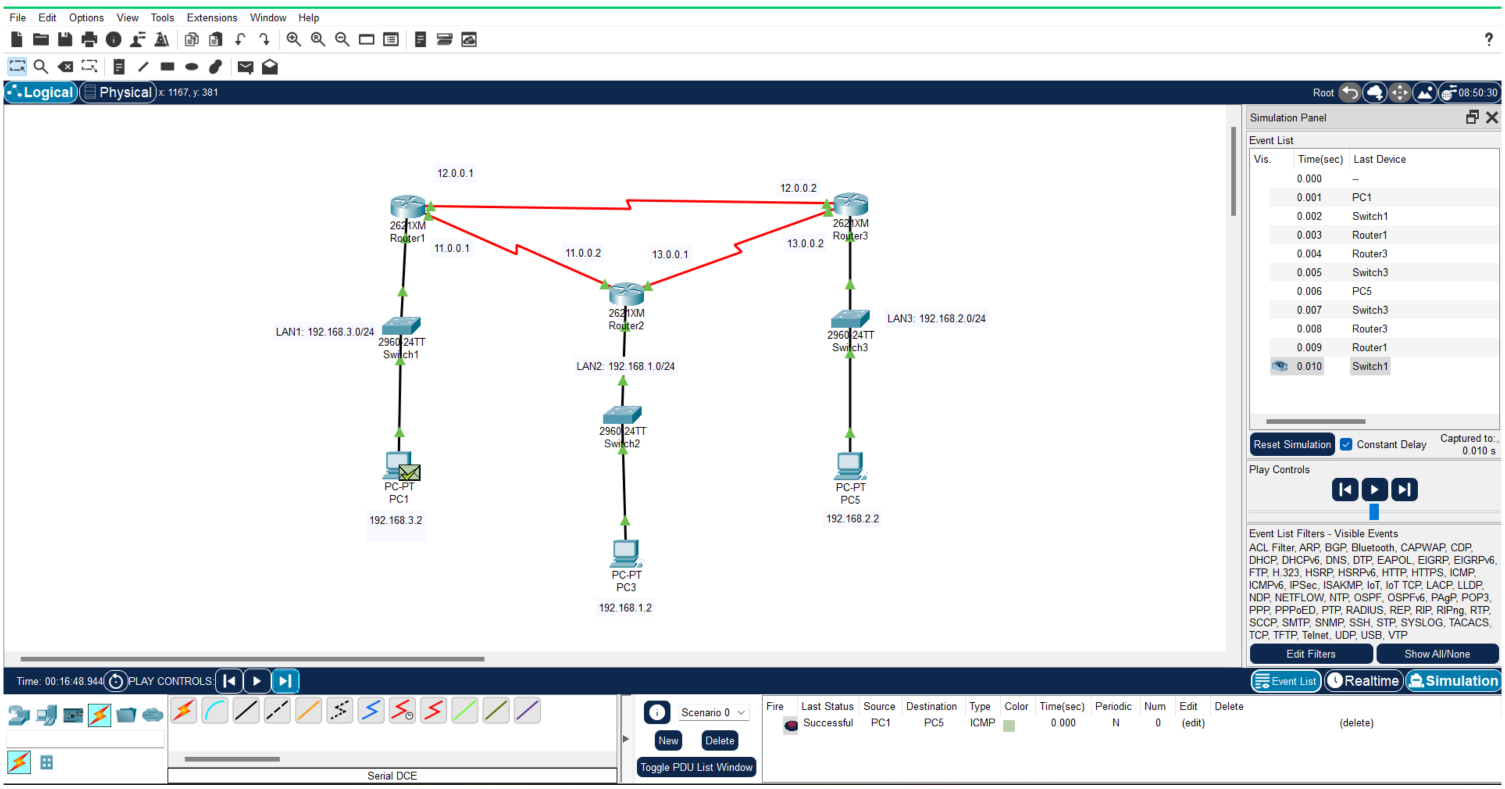
PC5 pinging to others



Use the simulation tool to send a packet from PC1 to PC5. Have you seen any differences compared to the route you have seen in Activity 2? Explain what happened.

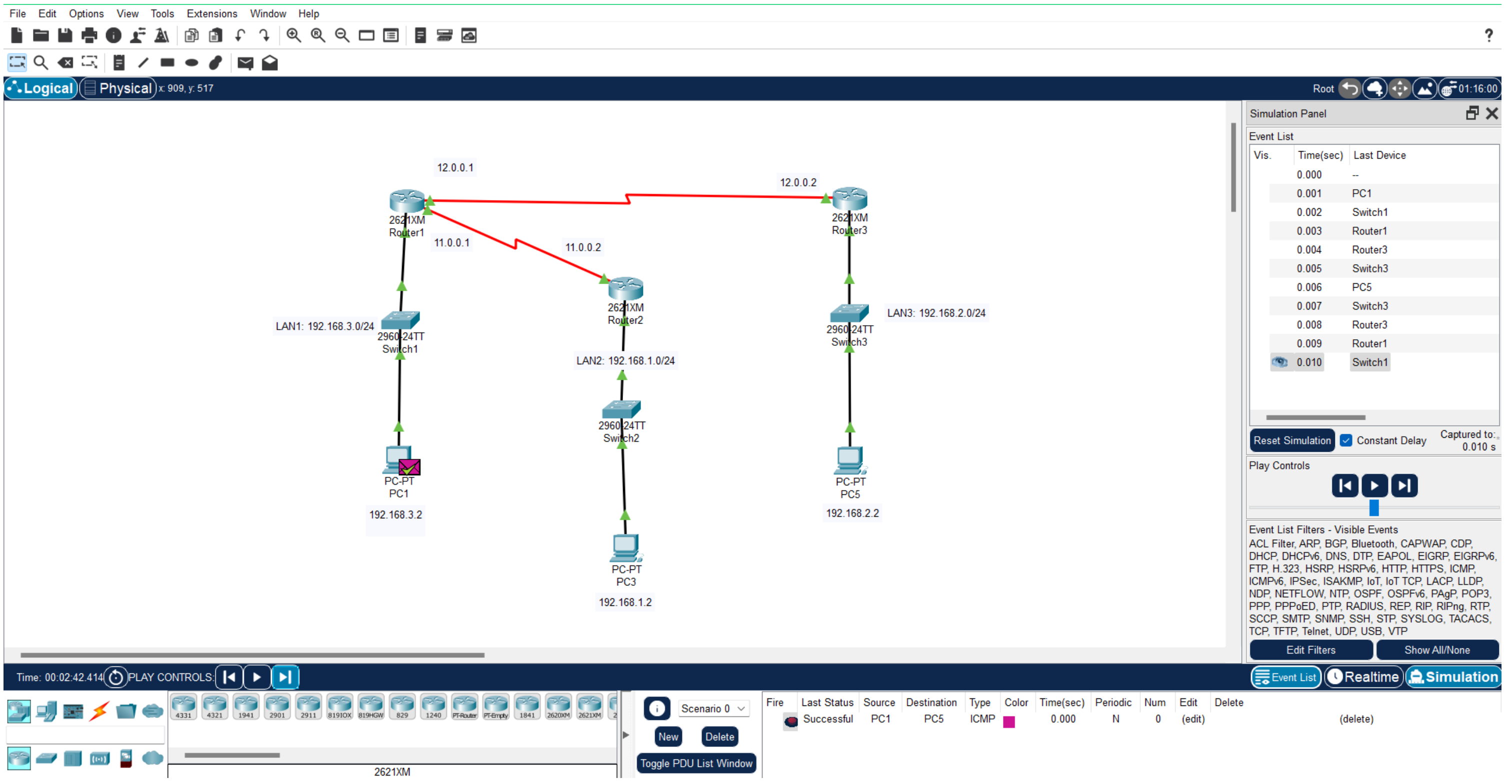
This time the packets were sent by the shortest and best path possible to reach the destination. Earlier in activity 2 it wasn't the case; it only went through the path which was statically configured and didn't choose the best path. Once the RIP is enabled the packet were sent through the 12.0.0.0 route instead of going via 11.0.0.0 and 13.0.0.0 to reach from pc1 to pc5. So, this algorithm has a great benefit to efficiently send the packet source to destination.

The benefit of the Routing Information Protocol (RIP) is that it is easy to configure as it does not require any parameters, unlike other protocols. Additionally, RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination, ensuring network stability.

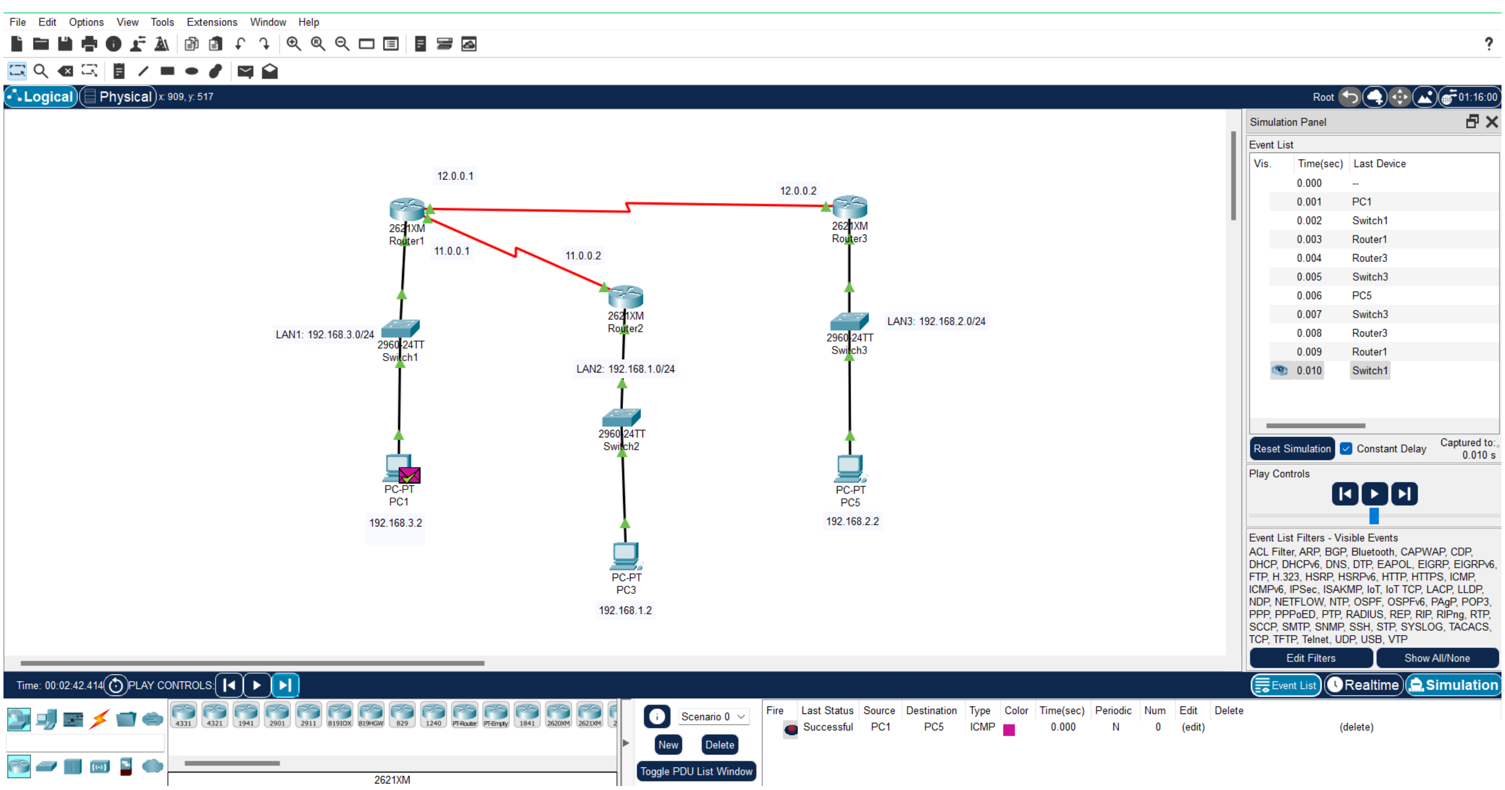


In the right side pane we can see that the path chose by the routers to route the packet was the shortest and best.

Now remove the connection between router 1 and 3 and use the simulation tool to send a packet from PC1 to PC5 without changing any configuration.



The packet still went through the available route instead of getting sent back, because the RIP will look for alternative paths when one is not available. When we first configured the routes, all the routers have the info about the routes to other networks, so when one route becomes unavailable the information of other routes in the router makes the packet to reach the destination without any disturbance.



Active class 8: Internet is full of Network Protocols

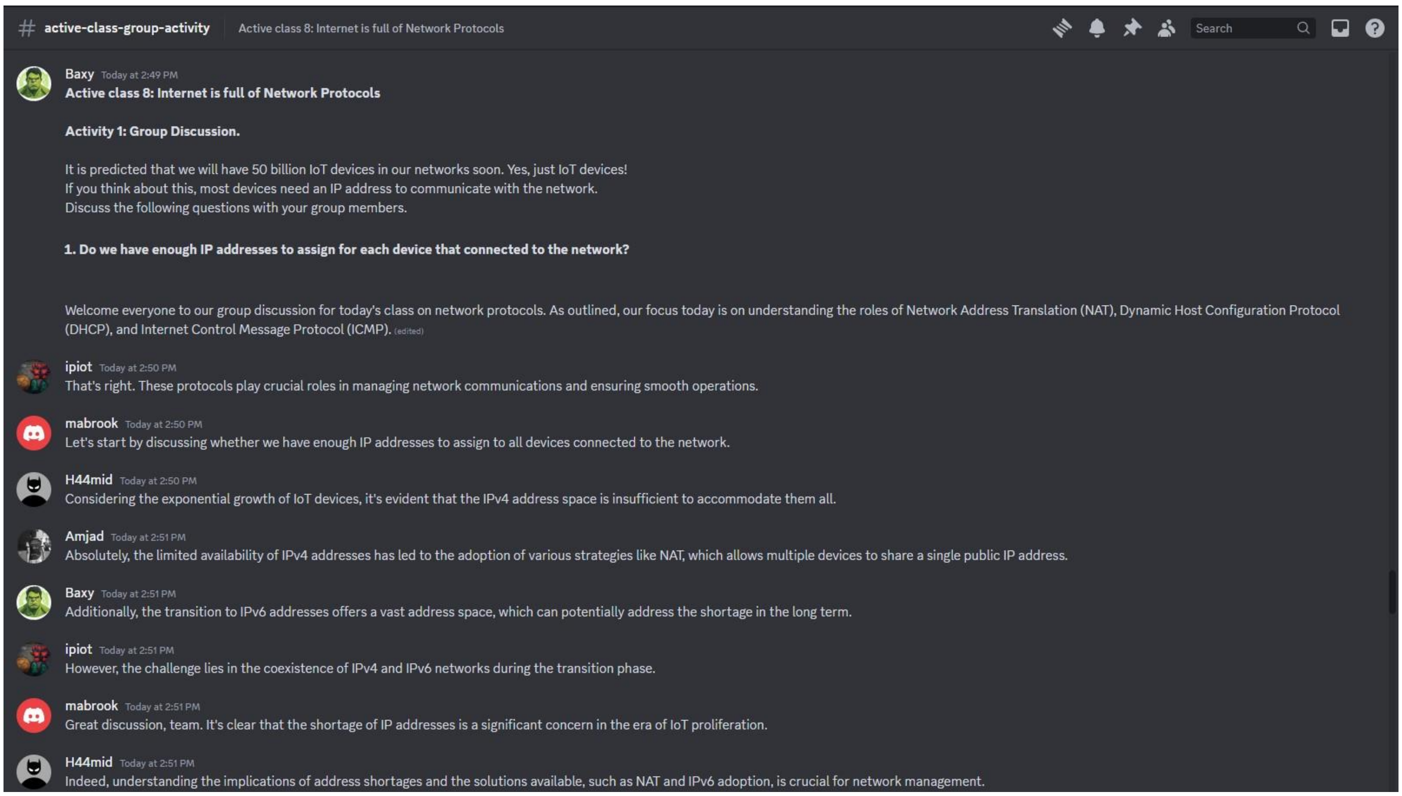
Activity 1: Group Discussion

In this activity, we engage in a group discussion about the challenges posed by the increasing number of IoT devices in networks and potential solutions to address these challenges.

We contemplate whether there are enough IP addresses available to assign to the growing number of devices connected to networks.

We brainstorm possible solutions to conserve the global IP address space amidst the proliferation of IoT devices.

We discuss a protocol that can be used alongside IPv4 to conserve IP addresses, considering the limitations of IPv4's address space.



active-class-group-activity | Active class 8: Internet is full of Network Protocols

Amjad Today at 2:51 PM
Let's keep these insights in mind as we proceed to build our network and analyze the protocols in action.

Baxy Today at 2:51 PM
Absolutely. Let's continue collaborating effectively and make the most out of today's activities.

ipiot Today at 2:52 PM
2. Do we have any solution?

Let's start with the first question. Do we have enough IP addresses to assign for each device connected to the network?

mabrook Today at 2:52 PM
Considering the exponential growth of IoT devices, it's likely that we'll face a shortage of IPv4 addresses soon.

H44mid Today at 2:52 PM
That's true. With the exhaustion of IPv4 addresses, it's becoming increasingly challenging to allocate unique addresses to every device.

Amjad Today at 2:52 PM
So, do we have any solutions to address this issue?

Baxy Today at 2:52 PM
One potential solution is the widespread adoption of IPv6, which offers a significantly larger address space compared to IPv4.

ipiot Today at 2:53 PM
Additionally, implementing NAT allows multiple devices within a private network to share a single public IP address, effectively conserving IPv4 addresses.

mabrook Today at 2:53 PM
DHCP also plays a crucial role in IP address management by dynamically assigning IP addresses to devices when they connect to the network.

Baxy Today at 2:53 PM
3. Explain a protocol that we can use along with IPv4 to conserve the global IP address space?

Alright team, let's delve into the third question for our discussion today. We'll explore protocols that can be used alongside IPv4 to conserve the global IP address space. We'll focus on identifying and explaining protocols that assist in conserving IPv4 addresses, considering the limited address space and increasing demand for IP addresses.

active-class-group-activity | Active class 8: Internet is full of Network Protocols

ipiot Today at 2:53 PM
To start, let's brainstorm protocols that can help conserve IPv4 address space.

mabrook Today at 2:53 PM
One protocol that immediately comes to mind is Network Address Translation (NAT). NAT allows multiple devices within a private network to share a single public IP address.

H44mid Today at 2:53 PM
Absolutely. By using NAT, organizations can significantly reduce the number of public IP addresses required to connect internal devices to the internet.

Amjad Today at 2:53 PM
Another protocol worth mentioning is Classless Inter-Domain Routing (CIDR). CIDR allows more efficient allocation of IP addresses by aggregating multiple smaller IP address blocks into larger blocks.

Baxy Today at 2:53 PM
That's correct. CIDR helps minimize IP address wastage by allowing organizations to request only the number of addresses they need, rather than entire class-based address blocks.

ipiot Today at 2:53 PM
Additionally, Subnetting is another technique that can help conserve IPv4 addresses. By dividing a larger network into smaller subnets, organizations can optimize address allocation based on their specific requirements

Baxy Today at 2:53 PM
Great insights, everyone! NAT, CIDR, and Subnetting are all valuable protocols and techniques that play crucial roles in conserving the limited IPv4 address space. Let's ensure we understand the functionalities of these protocols as we move forward with our practical exercises.

Activity 2: DHCP Role Play and Implementation

Now, we transition to a role-playing exercise to simulate the DHCP process within a local area network (LAN).

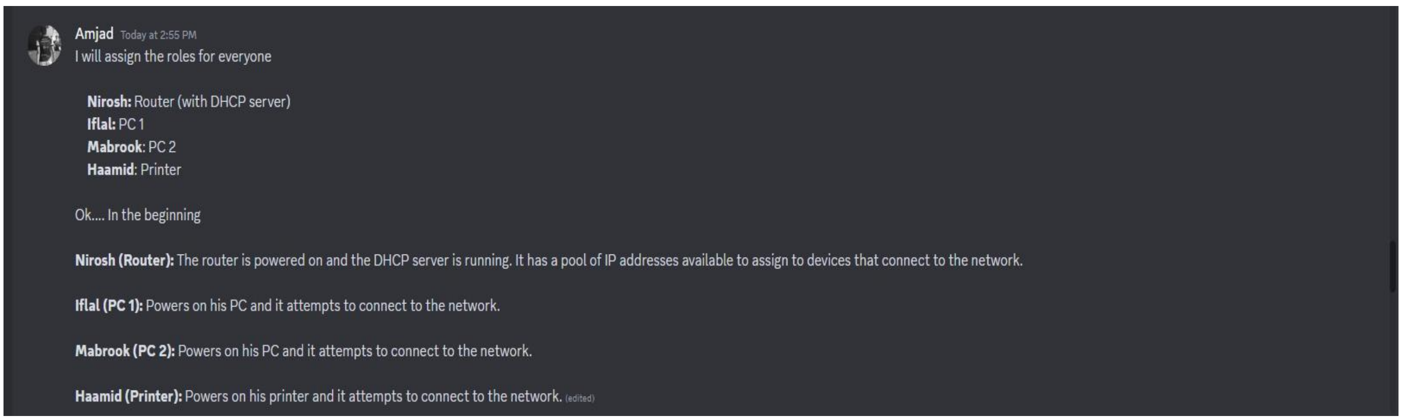
One member assumes the role of a router with a DHCP server, while the rest of us act as host devices attempting to connect to the network.

Each member follows a predefined message sequence to establish connections with the router and receive IP addresses dynamically through DHCP.

We draw a timing diagram to visualize the sequence of messages exchanged between devices during the DHCP process.

Following the role play, we move on to implementing a DHCP server in Cisco Packet Tracer, configuring network pools, default gateway, and IP addresses as per the provided diagram.

We set up the router, configuring interfaces and DHCP settings, and proceed to configure each host with DHCP to obtain IP configurations, verifying connectivity within the network.



Amjad Today at 2:55 PM
I will assign the roles for everyone

Nirosh: Router (with DHCP server)
Iflal: PC 1
Mabrook: PC 2
Haamid: Printer

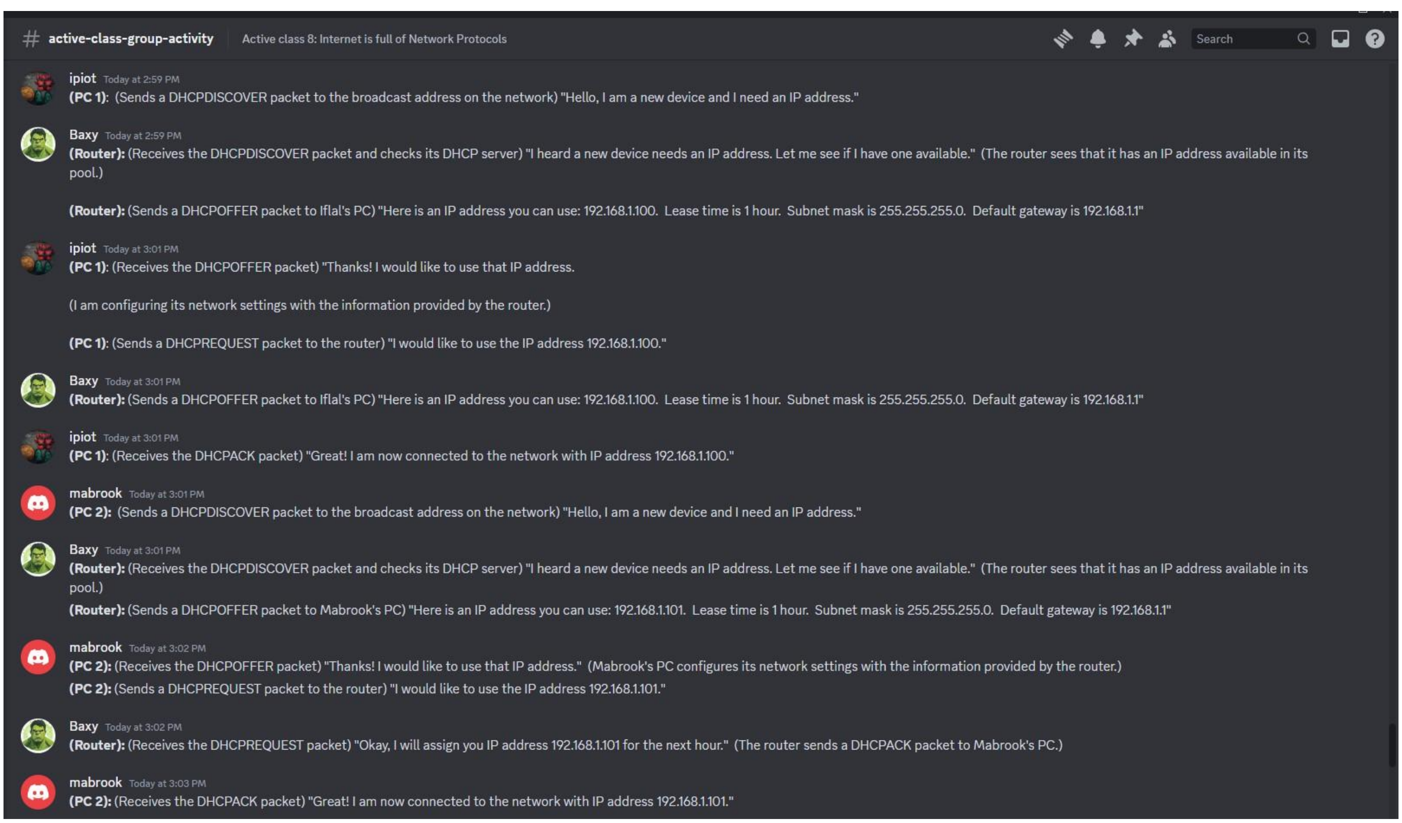
Ok.... In the beginning

Nirosh (Router): The router is powered on and the DHCP server is running. It has a pool of IP addresses available to assign to devices that connect to the network.

Iflal (PC 1): Powers on his PC and it attempts to connect to the network.

Mabrook (PC 2): Powers on his PC and it attempts to connect to the network.

Haamid (Printer): Powers on his printer and it attempts to connect to the network. (edited)



active-class-group-activity | Active class 8: Internet is full of Network Protocols

ipiot Today at 2:59 PM
(PC 1): (Sends a DHCPDISCOVER packet to the broadcast address on the network) "Hello, I am a new device and I need an IP address."

Baxy Today at 2:59 PM
(Router): (Receives the DHCPDISCOVER packet and checks its DHCP server) "I heard a new device needs an IP address. Let me see if I have one available." (The router sees that it has an IP address available in its pool.)

(Router): (Sends a DHCPOFFER packet to Iflal's PC) "Here is an IP address you can use: 192.168.1.100. Lease time is 1 hour. Subnet mask is 255.255.255.0. Default gateway is 192.168.1.1"

ipiot Today at 3:01 PM
(PC 1): (Receives the DHCPOFFER packet) "Thanks! I would like to use that IP address.

(I am configuring its network settings with the information provided by the router.)

(PC 1): (Sends a DHCPREQUEST packet to the router) "I would like to use the IP address 192.168.1.100."

Baxy Today at 3:01 PM
(Router): (Sends a DHCPOFFER packet to Iflal's PC) "Here is an IP address you can use: 192.168.1.100. Lease time is 1 hour. Subnet mask is 255.255.255.0. Default gateway is 192.168.1.1"

ipiot Today at 3:01 PM
(PC 1): (Receives the DHCPACK packet) "Great! I am now connected to the network with IP address 192.168.1.100."

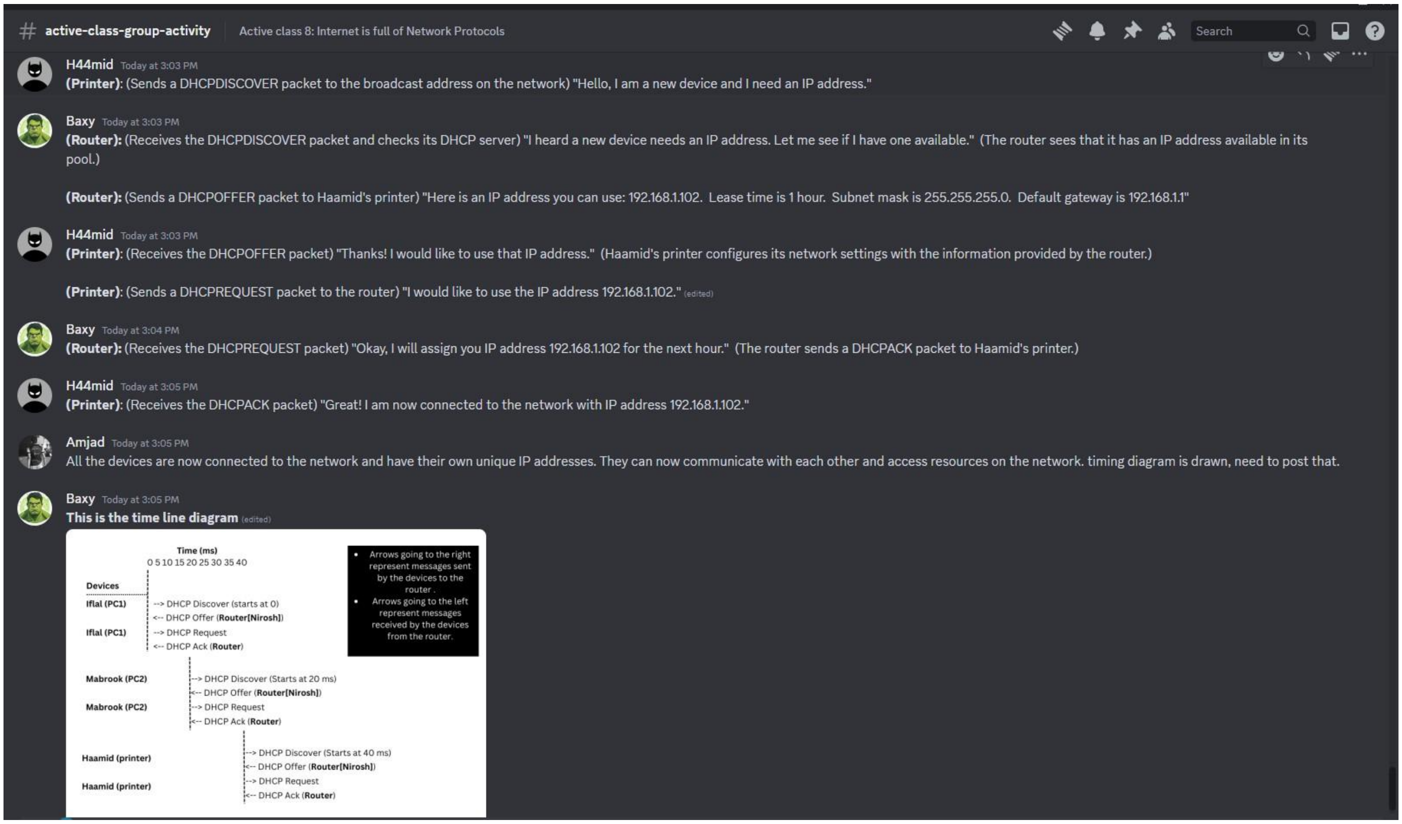
mabrook Today at 3:01 PM
(PC 2): (Sends a DHCPDISCOVER packet to the broadcast address on the network) "Hello, I am a new device and I need an IP address."

Baxy Today at 3:01 PM
(Router): (Receives the DHCPDISCOVER packet and checks its DHCP server) "I heard a new device needs an IP address. Let me see if I have one available." (The router sees that it has an IP address available in its pool.)
(Router): (Sends a DHCPOFFER packet to Mabrook's PC) "Here is an IP address you can use: 192.168.1.101. Lease time is 1 hour. Subnet mask is 255.255.255.0. Default gateway is 192.168.1.1"

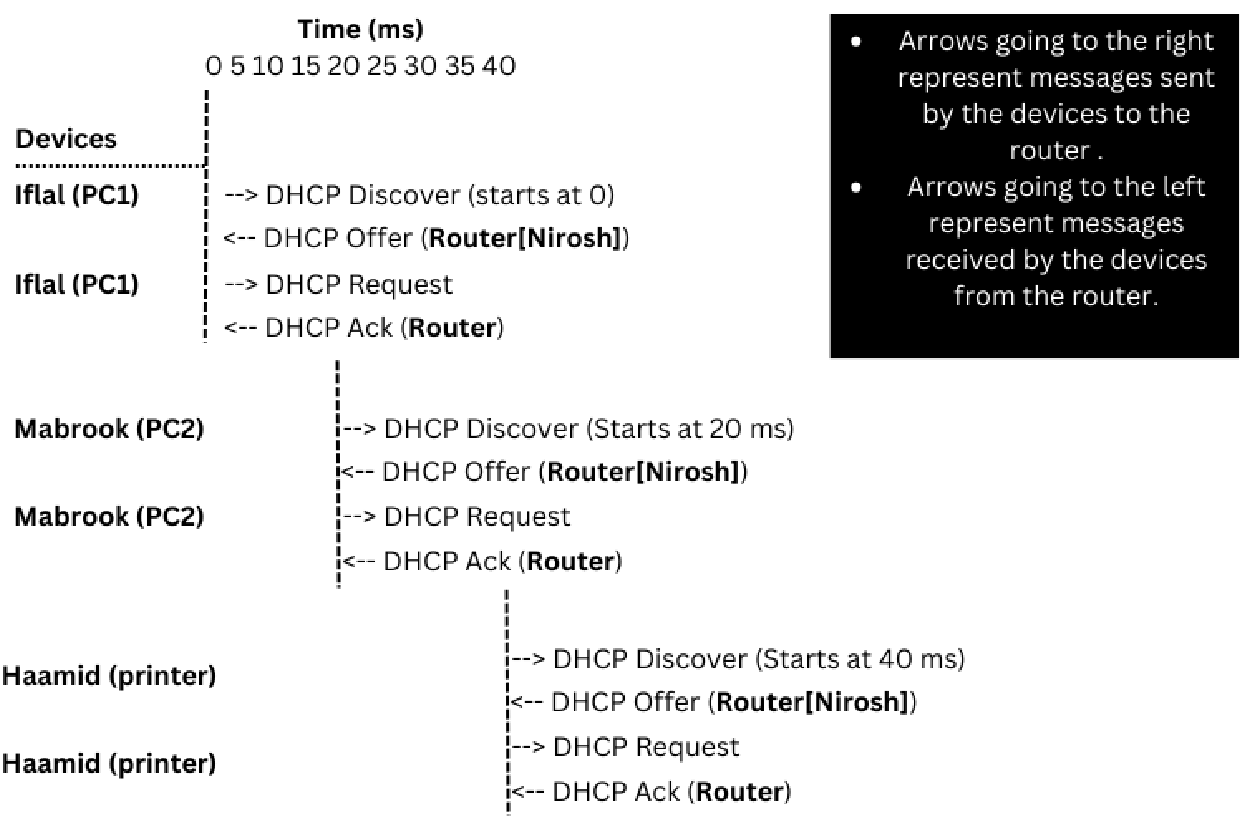
mabrook Today at 3:02 PM
(PC 2): (Receives the DHCPOFFER packet) "Thanks! I would like to use that IP address." (Mabrook's PC configures its network settings with the information provided by the router.)
(PC 2): (Sends a DHCPREQUEST packet to the router) "I would like to use the IP address 192.168.1.101."

Baxy Today at 3:02 PM
(Router): (Receives the DHCPREQUEST packet) "Okay, I will assign you IP address 192.168.1.101 for the next hour." (The router sends a DHCPACK packet to Mabrook's PC.)

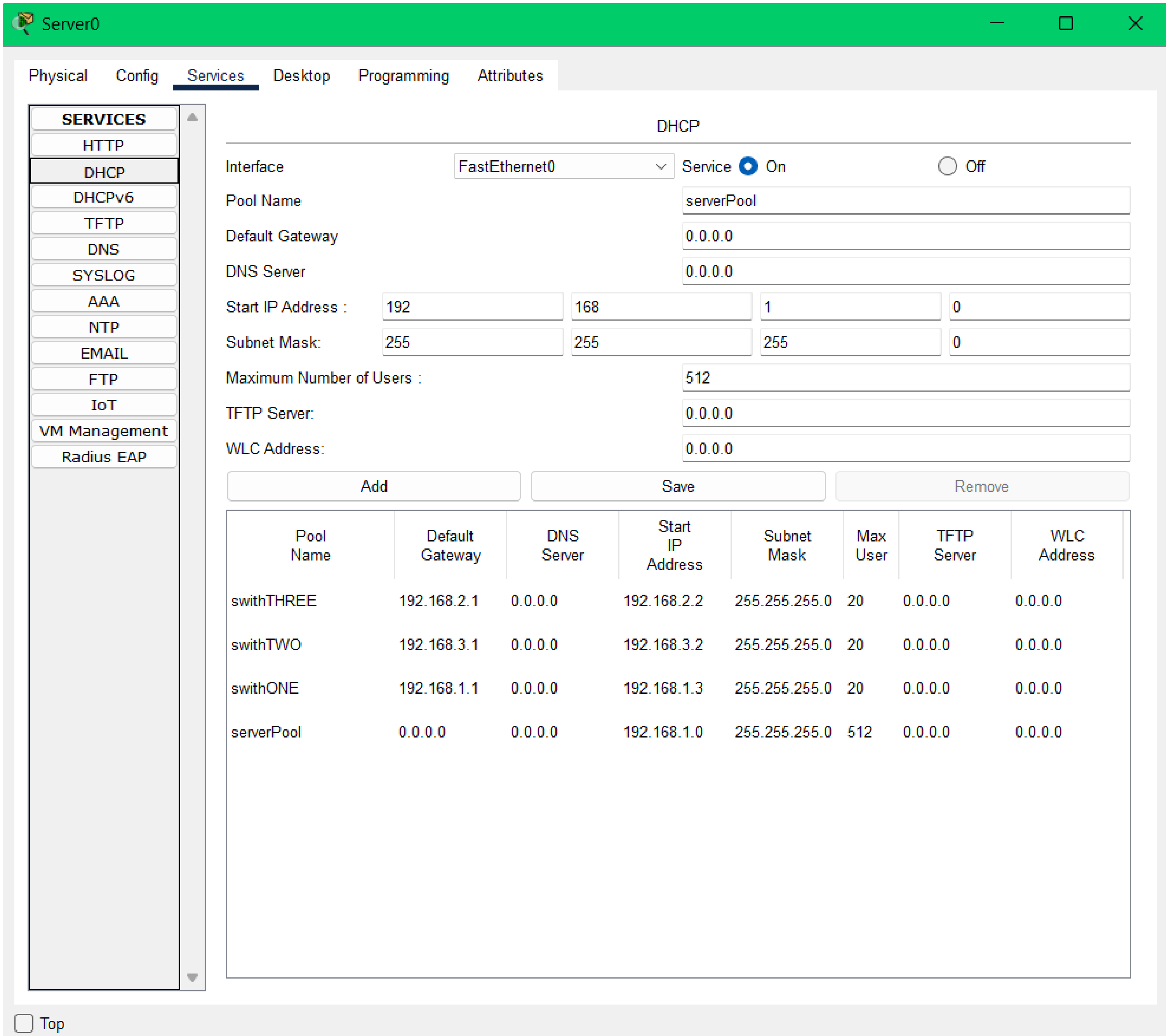
mabrook Today at 3:03 PM
(PC 2): (Receives the DHCPACK packet) "Great! I am now connected to the network with IP address 192.168.1.101."



Time line diagram

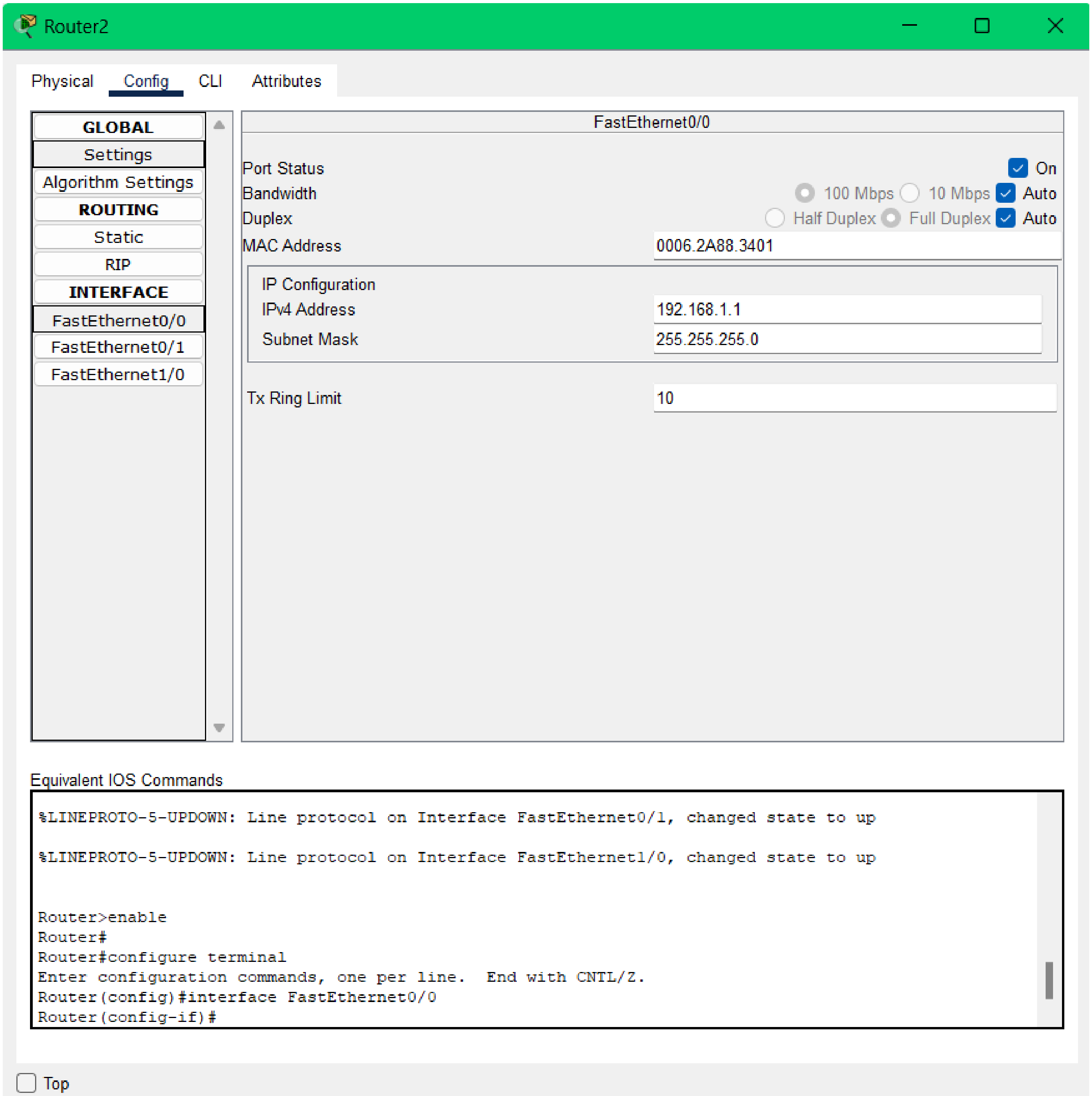


DHCP server config and pooling

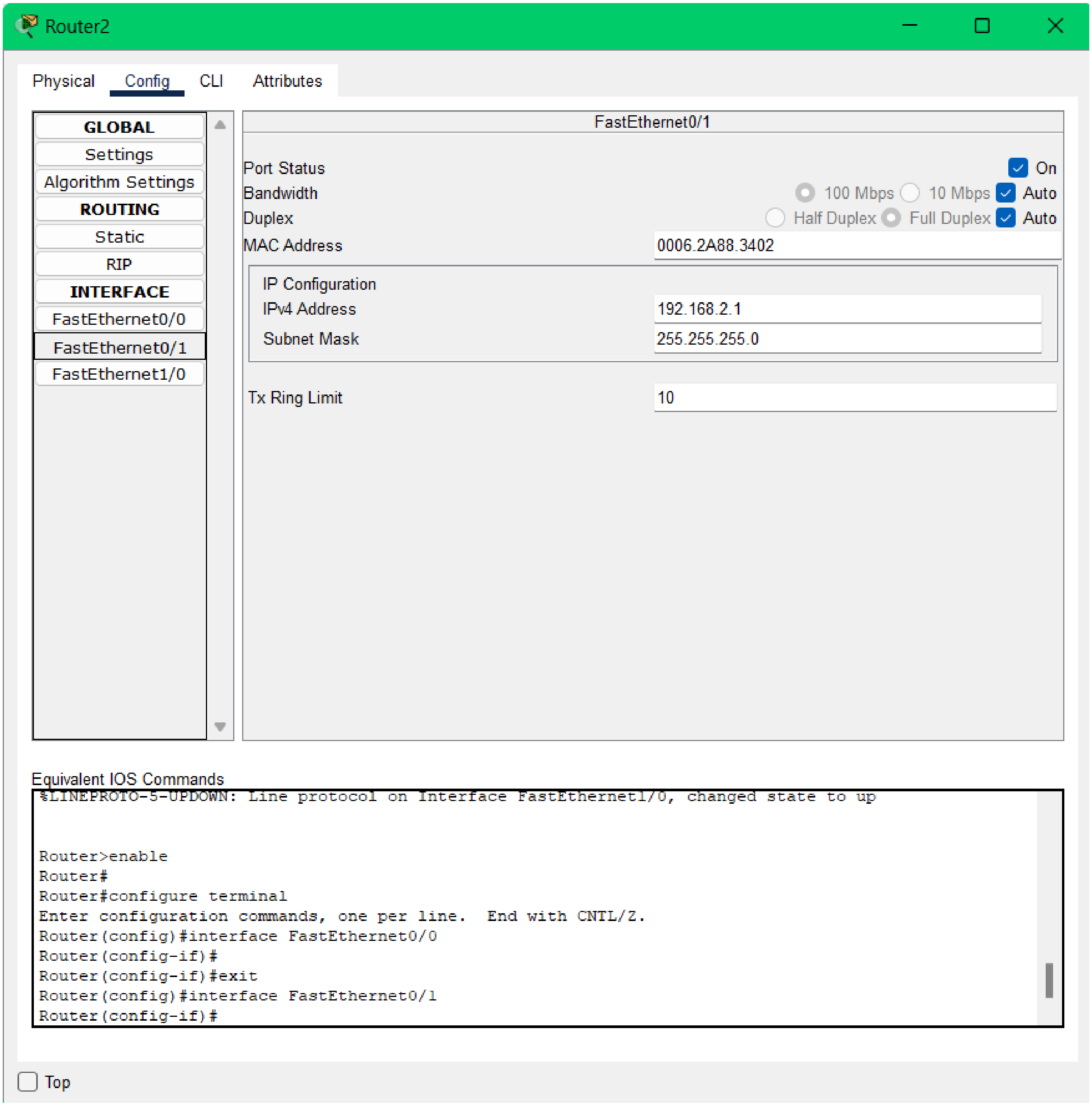


Then I configured the router's ports

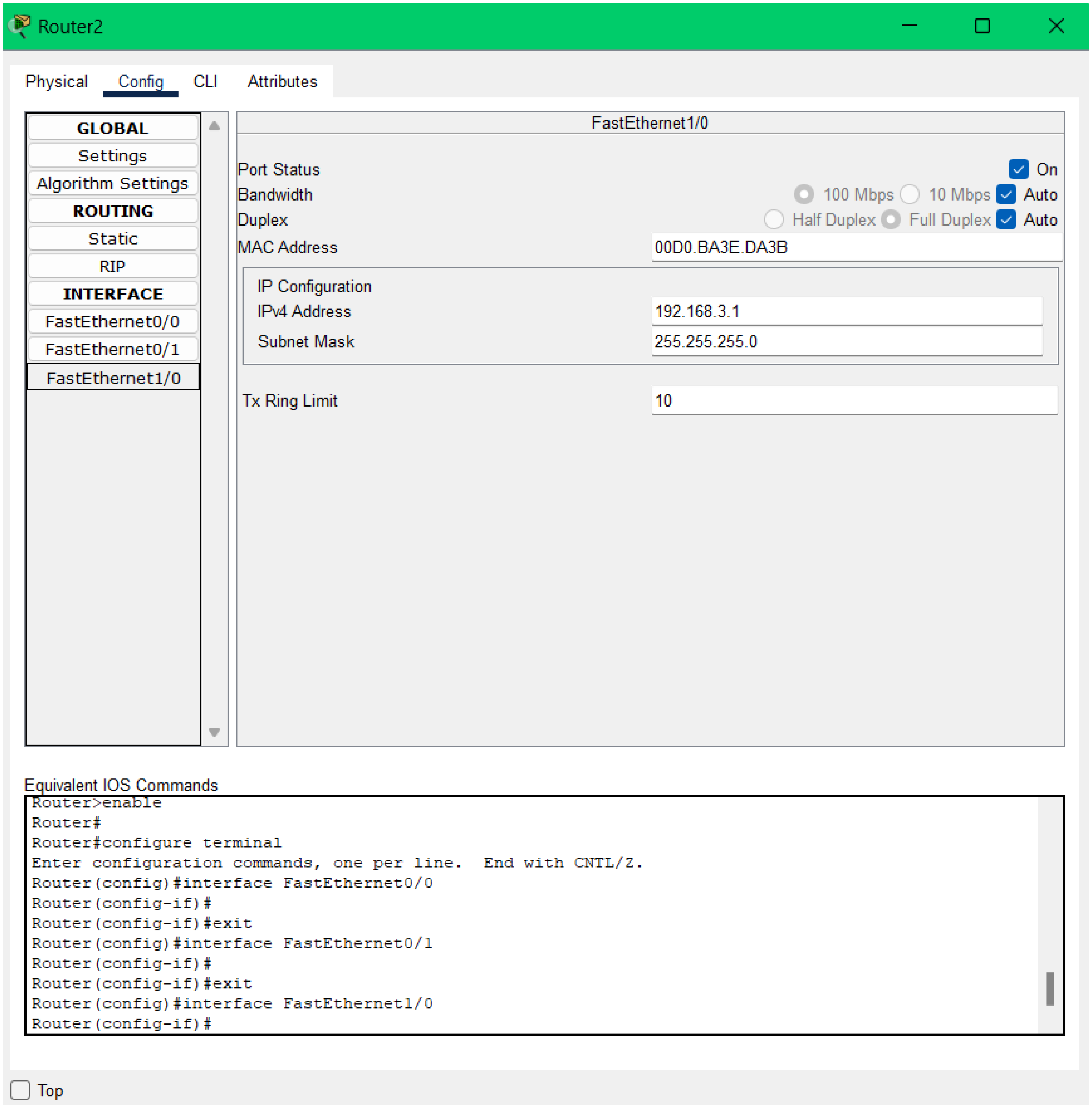
FastEthernet 0/0



FastEthernet 0/1

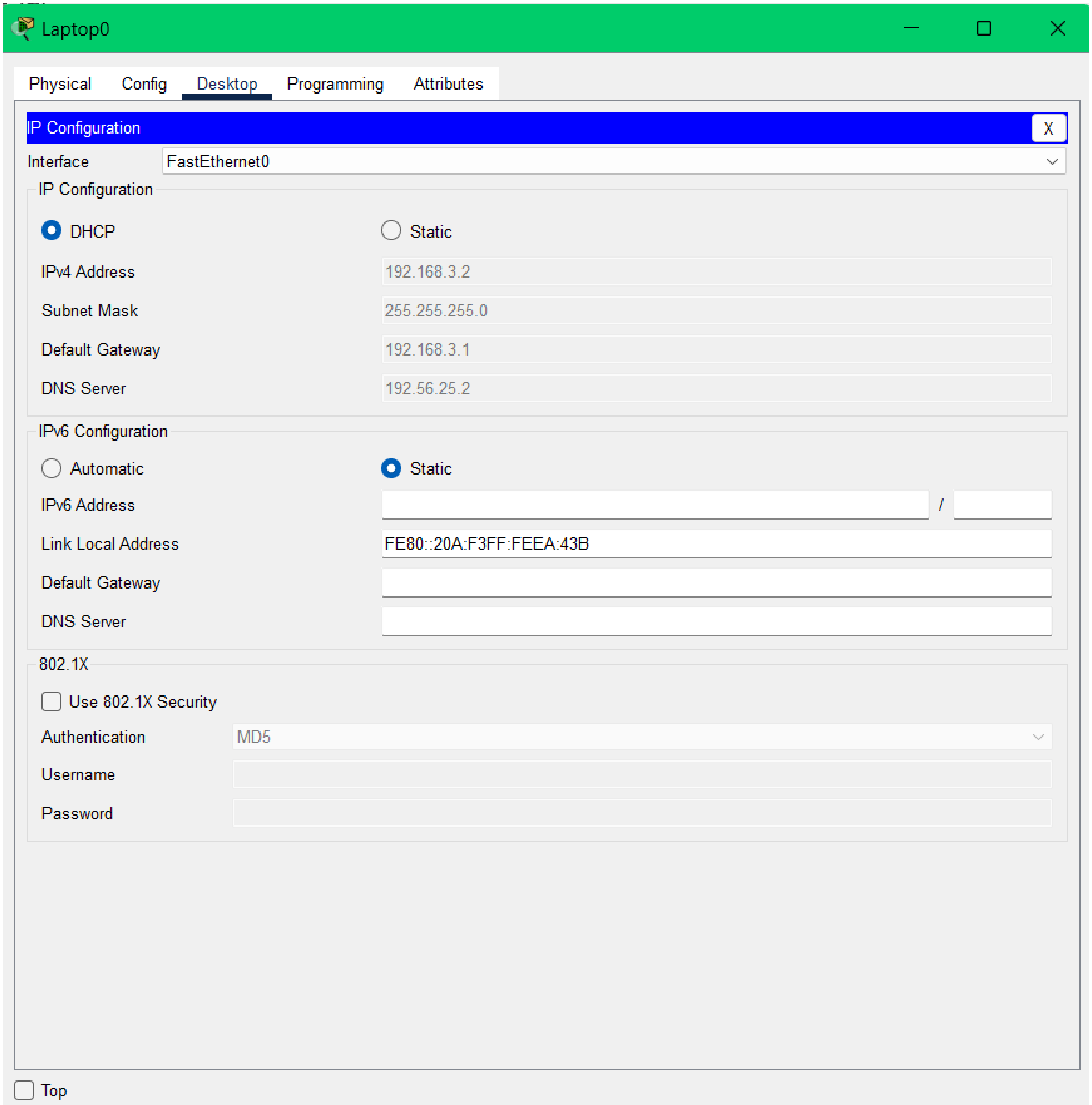


FastEthernet 1/0

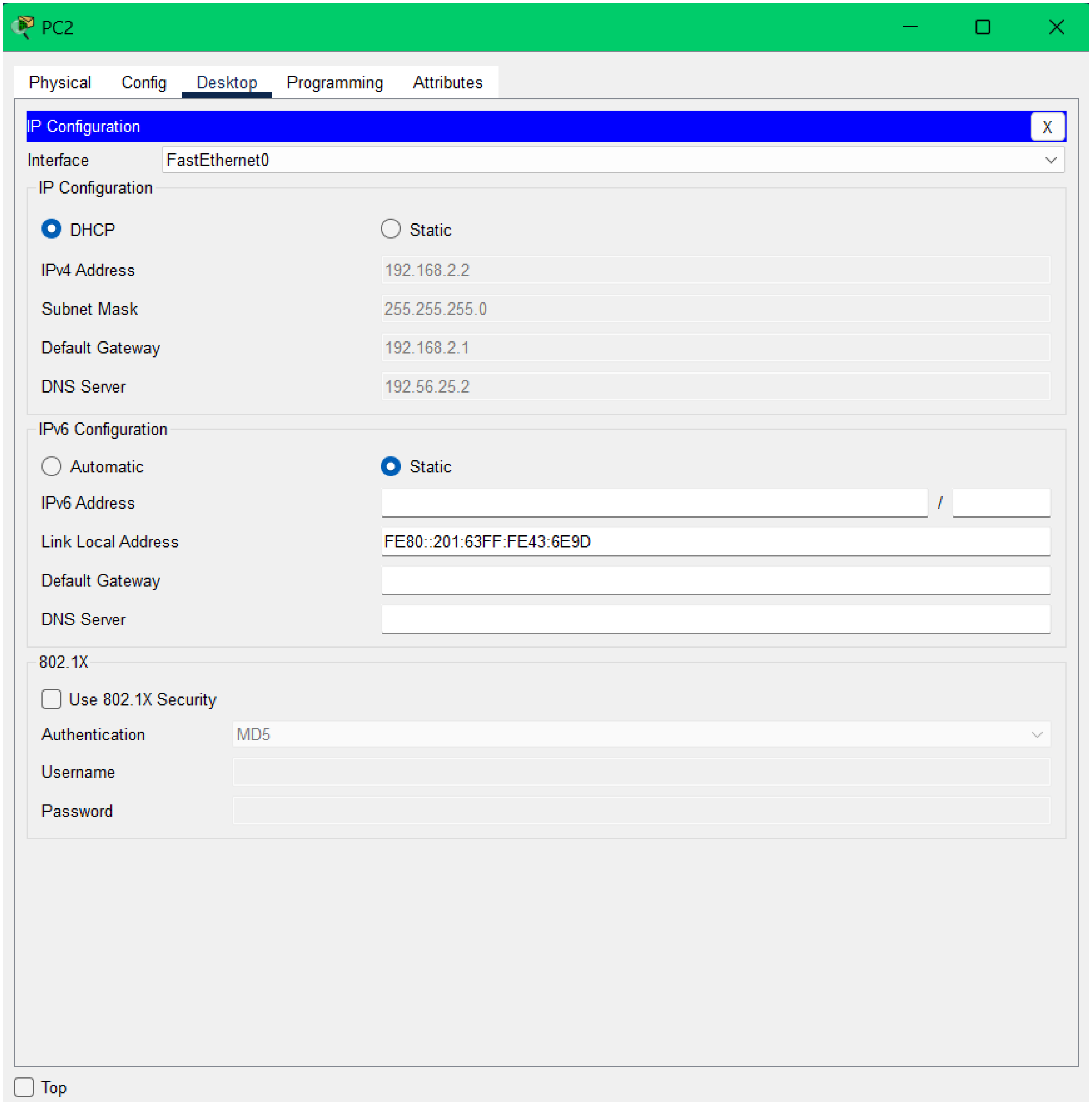


When I requested the ip addresses for each device, the ip addresses were allocated just like how I asked them

Laptop 2 in Lan 3’s DHCP IP address

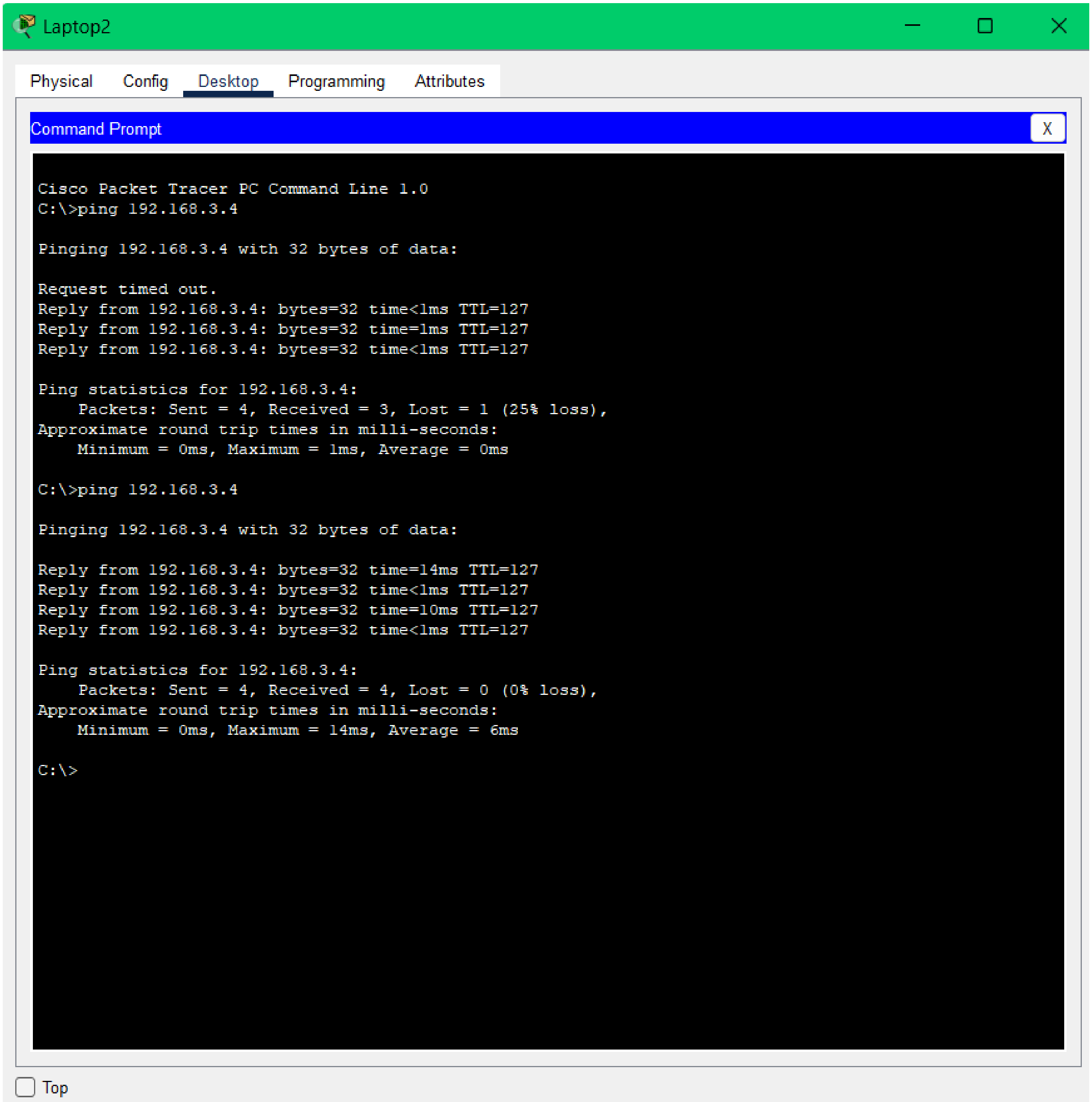


PC2 in LAN 2's DHCP IP address

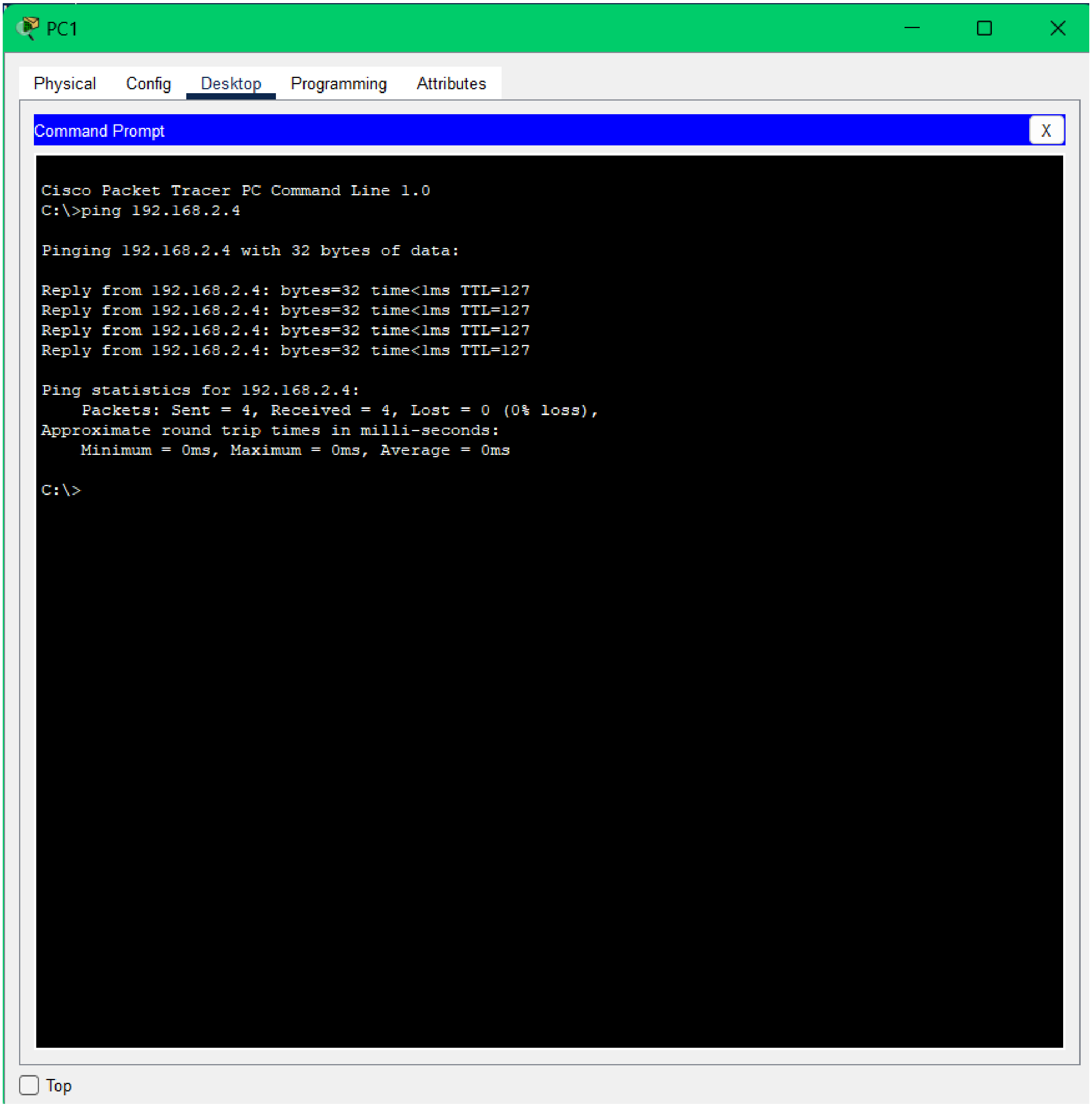


Then I pinged from lan2 to lan3 to make sure that the connection between the hosts are working

LAN2 – LAN3



LAN3 – LAN2


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4
Pinging 192.168.2.4 with 32 bytes of data:
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Reply from 192.168.2.4: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.2.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

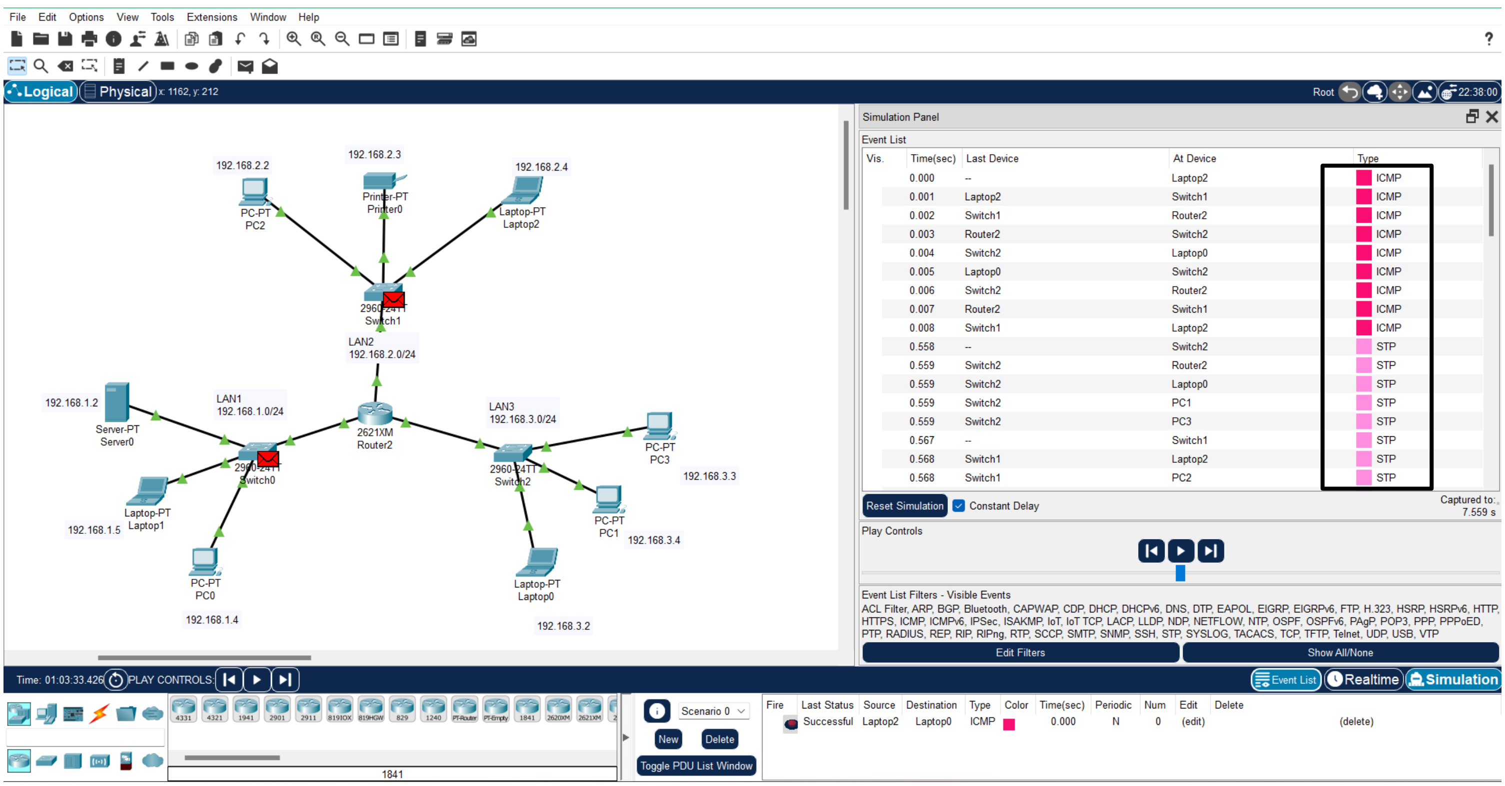
Activity 3: ICMP Exploration

In this activity, we use Cisco Packet Tracer's simulation tool to explore ICMP (Internet Control Message Protocol) within the network implemented in Activity 2.

We utilize the Simulation mode to send a simple packet from one host in LAN1 to another host in LAN2, paying attention to the types of messages passed.

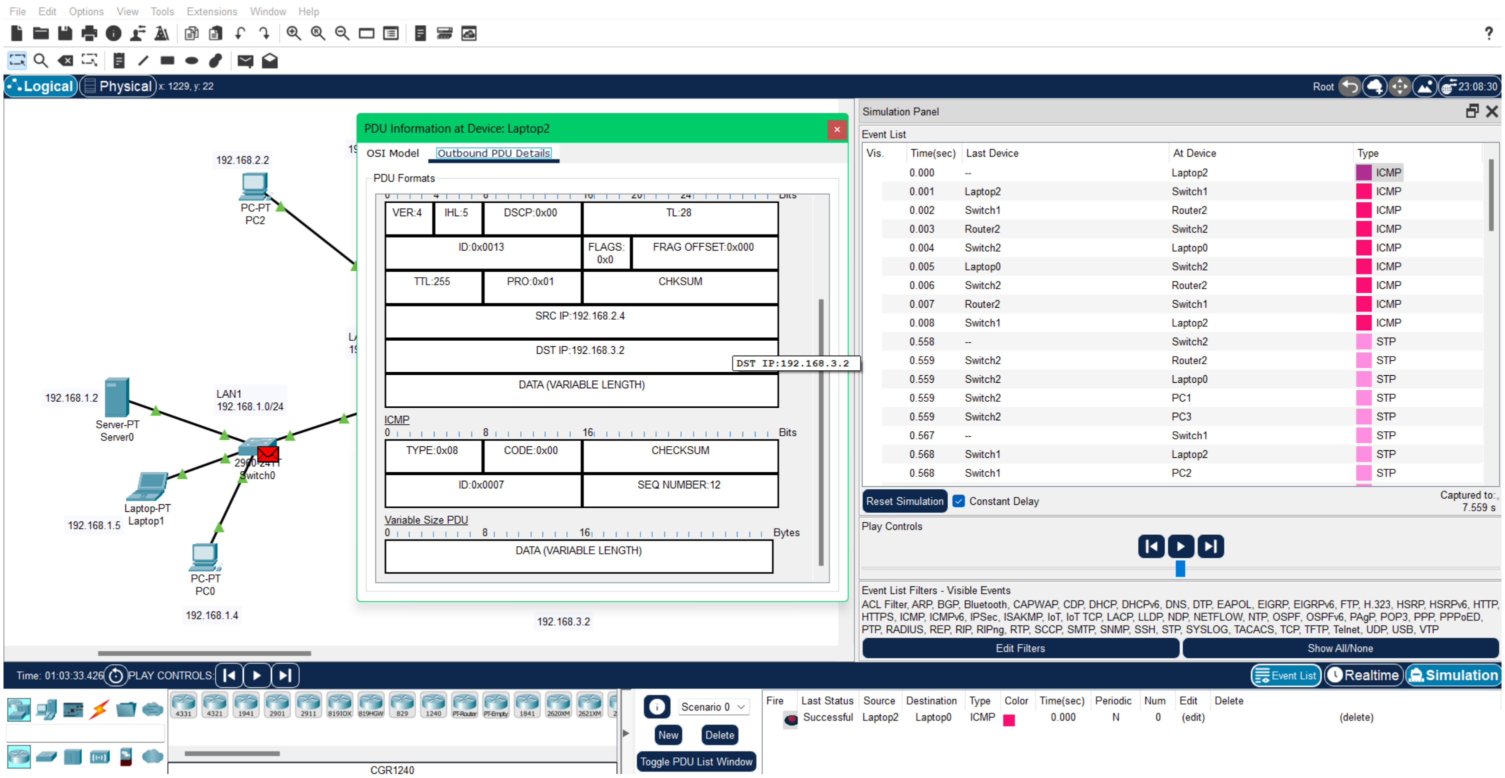
By examining packet details, we analyze the information found in "outbound PDU details," gaining insights into the ICMP message format and identifying message types and codes.

We compare ICMP messages generated during a ping operation with those during a traceroute operation, noting any differences in message structure and content.



In the above image the simulation of a packet being sent from a laptop in LAN2 to the laptop in LAN3. There are ICMP packets being transferred.

Then the packet details panel is analyzed to explore more about the ICMP packets in the previous simulation



The outbound PDU details window in Cisco Packet Tracer provides information about the Protocol Data Units (PDUs) leaving a device on a network.

The information displayed in the outbound PDU details window includes:

- Time (sec): The time that the PDU left the device.
- Last Device: The last device that the PDU passed through before reaching Laptop2.
- Layer - This section shows the OSI model layers involved in the communication. You can expand or collapse this section by clicking on the + or - symbol next to it.

PDU Details: This section shows details of the PDU headers, broken up by header type and the individual fields within each header. You can expand or collapse this section by clicking on the + or - symbol next to it.

we can see that at 0.001 seconds, an ICMP PDU left Laptop2 headed for Switch1. The ICMP PDU has a source IP address of 192.168.2.2 and a destination IP address of 192.168.3.2.

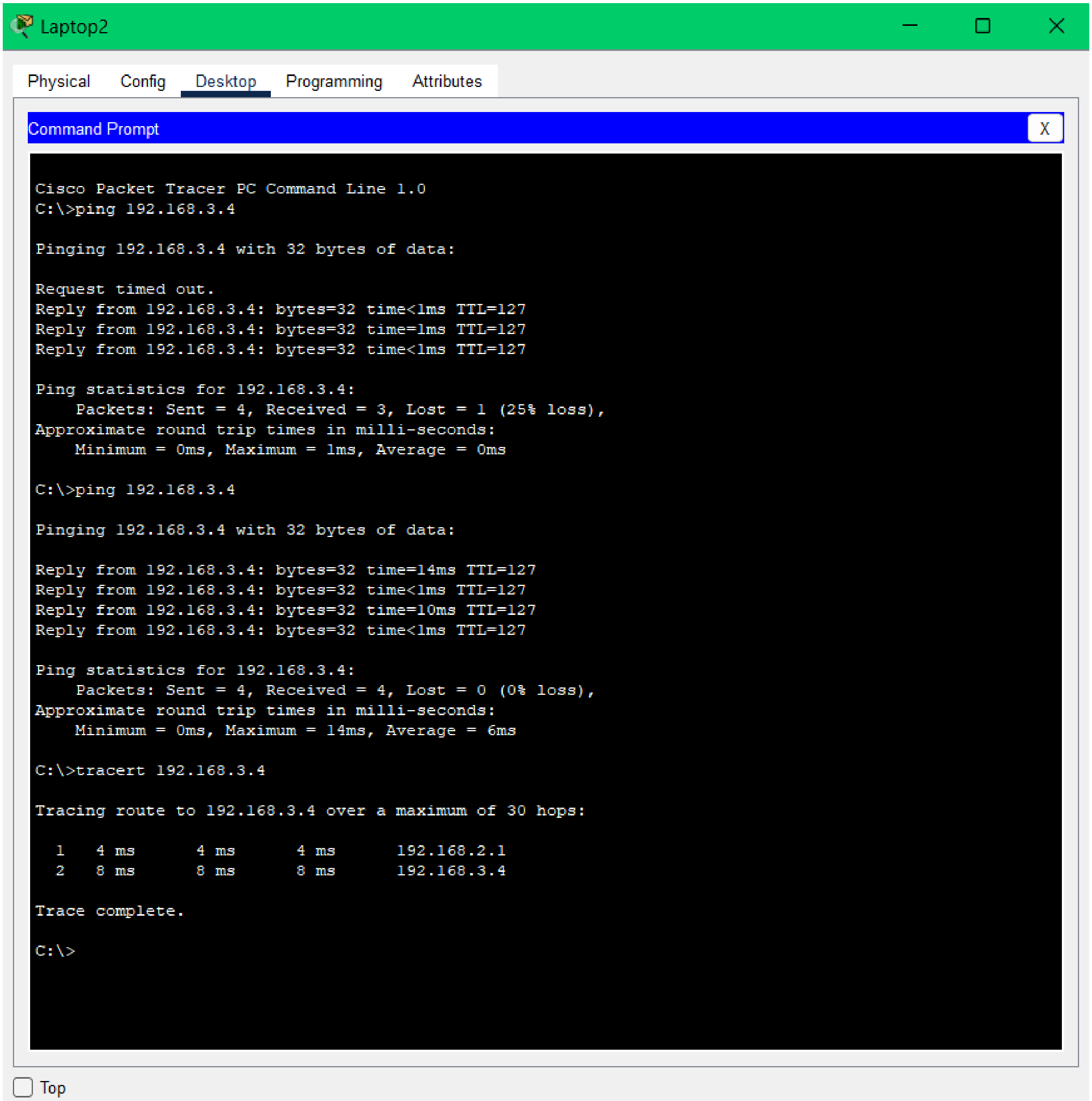
Based on the ICMP message format in this screenshot, I can identify the following details:

- Type: 0x08 (Echo Request)
- Code: 0x00

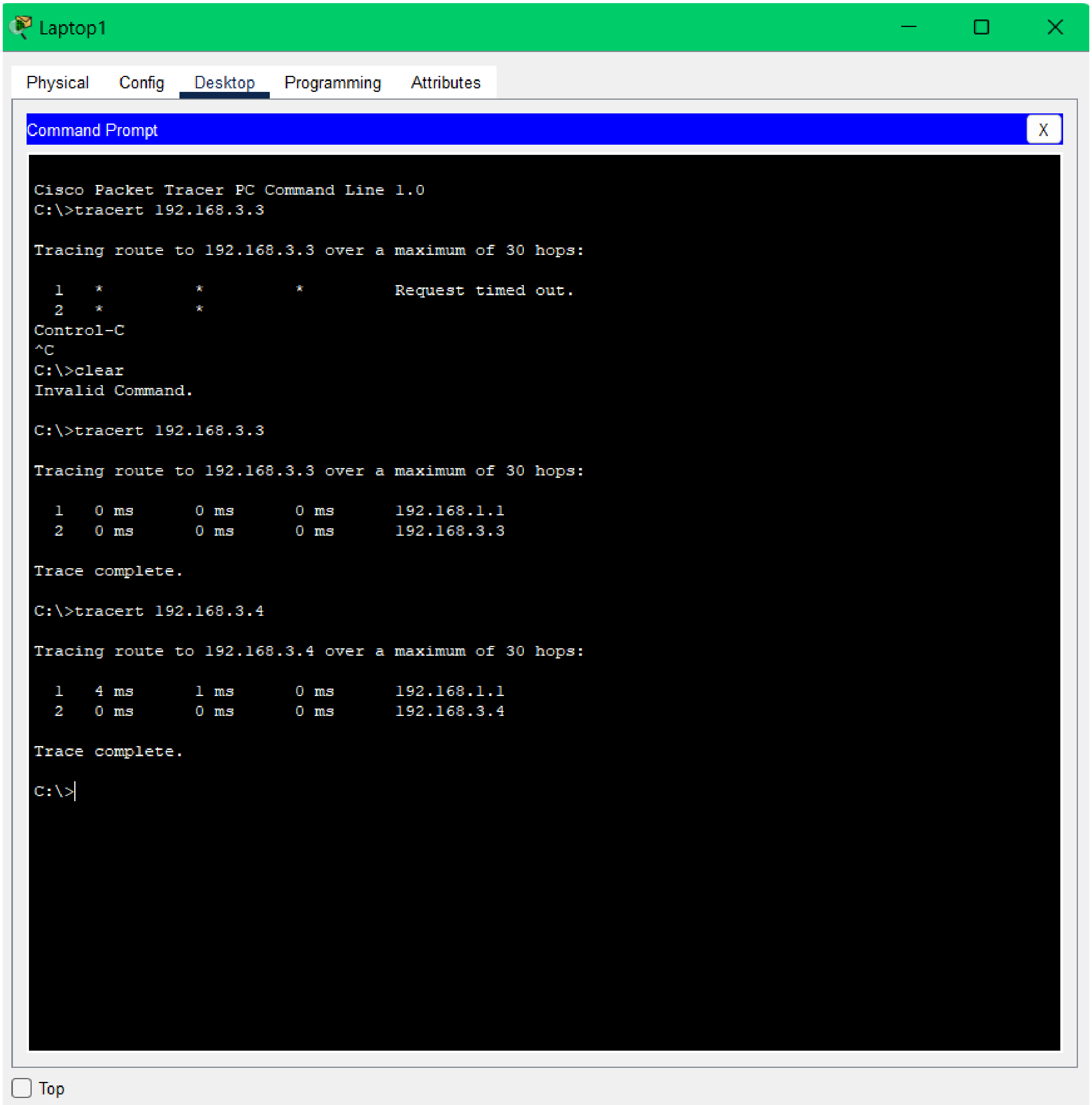
An ICMP Echo Request message, also known as a ping, is sent by a source to check if a destination host is reachable. A code of 0x00 is typically used for echo requests.

We can see that the ICMP message also has an ID of 0x0007 and a sequence number of 12. These fields are used to identify specific echo requests and replies.

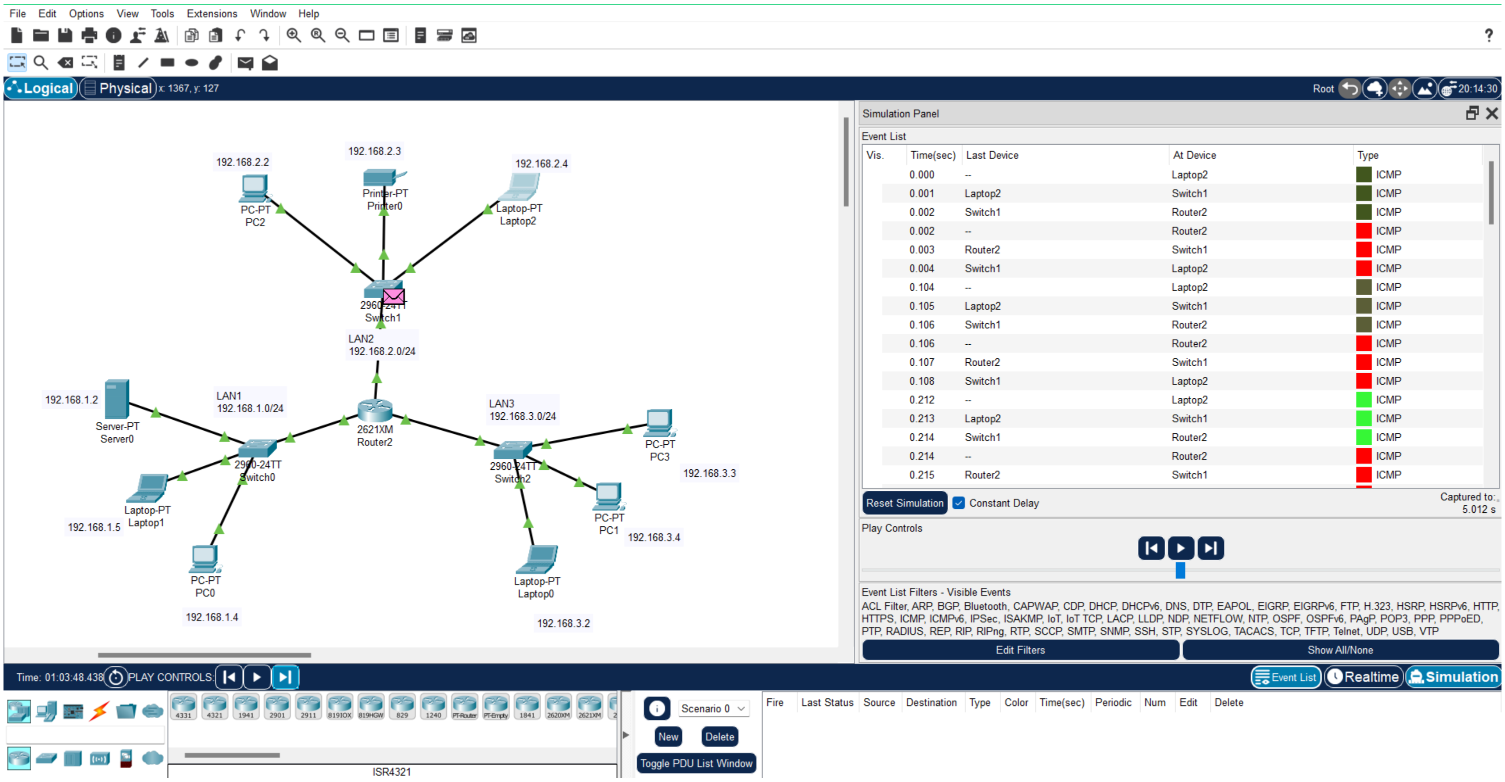
Now I use the tracert command to trace the route between the lan2’s laptop and lan3’s PC

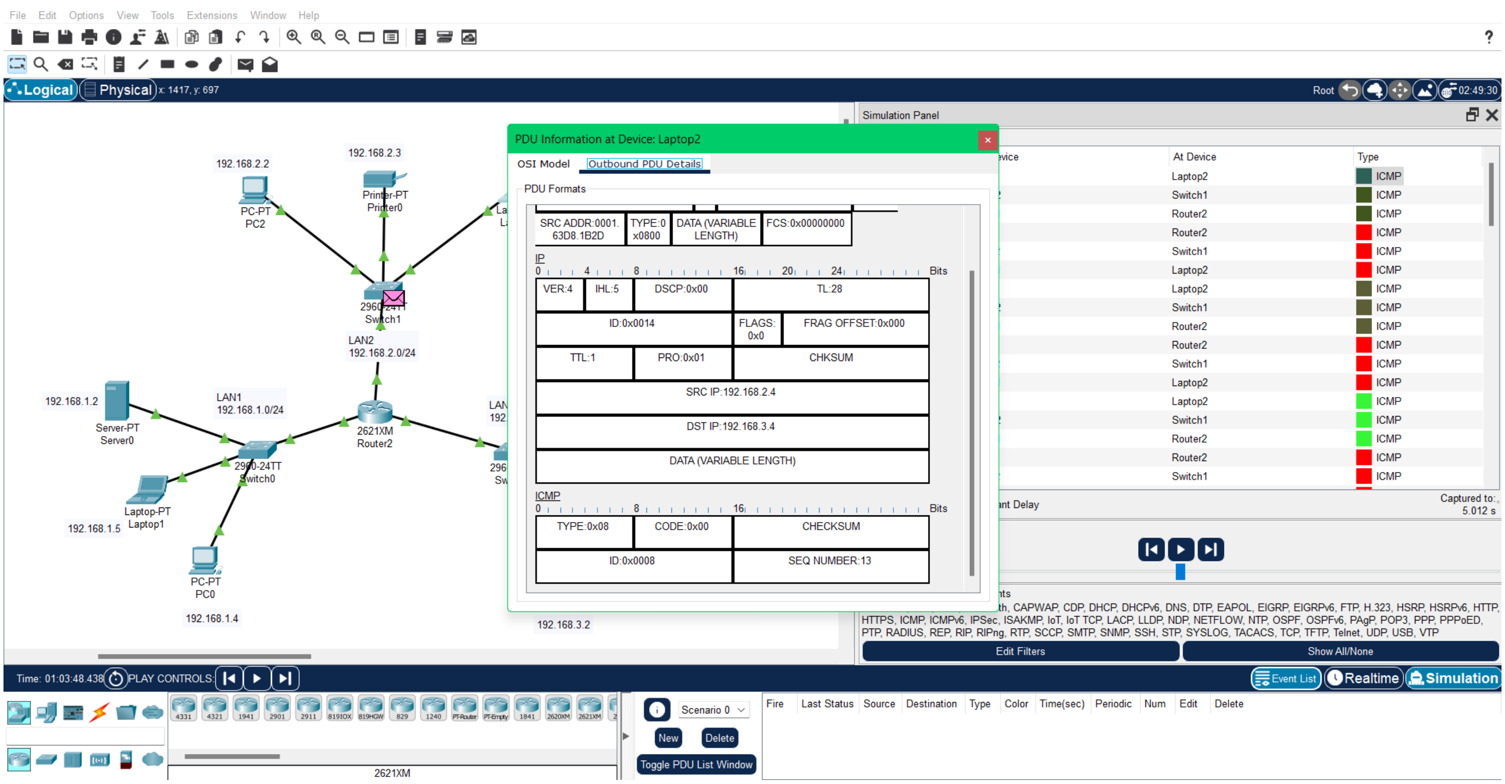



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127
Reply from 192.168.3.4: bytes=32 time=1ms TTL=127
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=14ms TTL=127
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127
Reply from 192.168.3.4: bytes=32 time=10ms TTL=127
Reply from 192.168.3.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 6ms

C:\>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1   4 ms      4 ms      4 ms      192.168.2.1
  2   8 ms      8 ms      8 ms      192.168.3.4

Trace complete.

C:\>
```


Laptop1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:
1 * * * Request timed out.
2 * *
Control-C
^C
C:\>clear
Invalid Command.
C:\>tracert 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.1.1
2 0 ms 0 ms 0 ms 192.168.3.3
Trace complete.
C:\>tracert 192.168.3.4
Tracing route to 192.168.3.4 over a maximum of 30 hops:
1 4 ms 1 ms 0 ms 192.168.1.1
2 0 ms 0 ms 0 ms 192.168.3.4
Trace complete.
C:\>
Top

The simulation for the trace route





ICMP messages in Ping:

ICMP Echo Request (Type: 0x08, Code: 0x00) - Sent by Host A to query if Host B is reachable.

ICMP Echo Reply (Type: 0x00, Code: 0x00) - Sent by Host B in response to an Echo Request from Host A, indicating reachability.

ICMP messages in Traceroute:

ICMP Time Exceeded (Type: 11, Code: 0) - Sent by a router along the path to Host B when the Time To Live (TTL) field in the IP header reaches zero. Each router decrements the TTL by 1 as it forwards the packet. When the TTL hits 0, the router sends an ICMP Time Exceeded message back to Host A.

While both ping and traceroute use ICMP messages, they use different message types:

Ping uses Echo Request/Reply messages to test reachability between two hosts.

Traceroute uses Time Exceeded messages to identify the routers along the path to a destination by exceeding the TTL on packets.

In summary, the ICMP message used by traceroute (Time Exceeded) differs from the ICMP messages used by ping (Echo Request/Reply).