

# Routing Concept

## Contents

<b>Chapter 1: Introduction .....</b>	<b>2</b>
<b>Chapter 2: Concepts .....</b>	<b>3</b>
Why Router? .....	3
<b>Chapter 3: ARP Resolving .....</b>	<b>5</b>
ICMP ECHO REQUEST .....	6
ICMP ECHO REPLY .....	7
<b>Chapter 4: Live Simulation .....</b>	<b>8</b>
Sending the ICMP Echo Request – 8 .....	8
Replying with ICMP Echo Reply - 0 .....	11
Figure 1: GNS3 Topology .....	2
Figure 2: Packet Tracer Topology .....	2
Figure 3: Router ARP Table .....	4
Figure 4: Switch 2 MAC Table .....	4
Figure 5: ARP Request Outbound PDU Details .....	5
Figure 6: ARP Reply Inbound PDU Details .....	5
Figure 7: ICMP Echo Request Diagram Explain .....	6
Figure 8: Wireshark Captured ICMP Echo Request Packet .....	6
Figure 9: ICMP Echo Reply Diagram Explain .....	7
Figure 10: Wireshark Captured ICMP Echo Reply Packet .....	7
Figure 11: Step 01 Ping Process Starts .....	8
Figure 12: Step 02 Ping Process .....	9
Figure 13: Step 03 Ping Process .....	9
Figure 14: Step 04 Ping Process .....	10
Figure 15: Step 05 Ping Process Stops .....	10
Figure 16: Step 06 192.168.1.0 Network's Switch Mac Address Table .....	11
Figure 17: Step 07 Ping Process .....	11
Figure 18: Step 08 Ping Process .....	12
Figure 19: Step 09 Ping Process .....	12
Figure 20: Step 10 Ping Process Successful .....	13
Figure 21: Step 11 192.168.2.0 Network's Switch Mac Address Table .....	13

# Chapter 1: Introduction

Using GNS3 and Packet Tracer to analyze the concept of routing between two different subnets

- Cisco Router 2691
- Two 2960 Switches
- Two Windows PCs

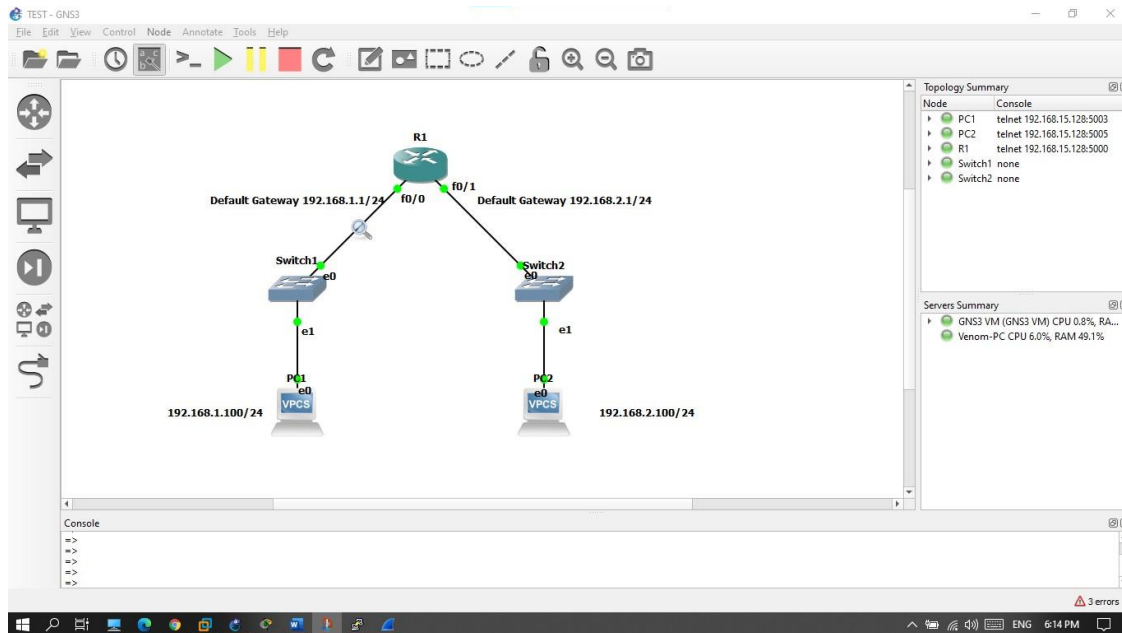


Figure 1: GNS3 Topology

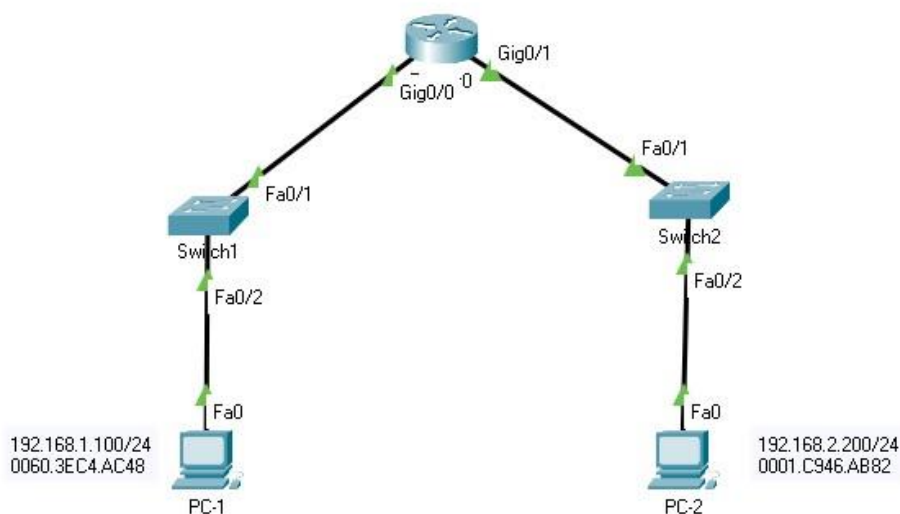


Figure 2: Packet Tracer Topology

## Chapter 2: Concepts

### Why Router?

The router is responsible for the routing of traffic between networks

So basically, to communicate within same network a switch can be used, since it has the layer 2 table to make the forwarding decision.

But in a scenario of two different network. You will need a router to interconnect different network. Router forwarding decision is based on the IP address. that's where the default gateway comes in the role.

When the Router receive a packet. It checks first whether the network is directly connected if its not then it checks the Routing Table.

### ARP RESOLUTION

- A. PC-1 needs to ping PC-2. Where PC-1 doesn't know the route to it. Therefore, it generates an ARP Request to find default gateway mac address. B. It sends the frame to Switch1.
  - a. If the source mac address doesn't exist in MAC address table. Then it will add the port and mac address in the table.
  - b. For every 5mins it refreshes the table if the port changes with different device.
- C. After getting the mac address of default gateway. It generates a ping packet. And it keeps the destination IP address has pc 2 and destination mac address has router.
- D. Since PC-1 can't reach the 192.168.2.100 directly. It will send the packet to the Default Gateway.

### ROUTING

1. The data packet generated by the PC-1 should access the default gateway of the router.
  - a. Example - The PC must have connectivity to the router Default Gateway Ip address.
2. Switch1 will send the ICMP Request to the Router
3. Router interfaces must be assigned with the IP address which means the default gateway to represent the network.
4. Where router has the Routing table with the information of Port and the network

PORTS	NETWORK
Fa0/0	192.168.1.1
Fa0/1	192.168.2.1

5. Router will make sure whenever it sees a packet to be sent for 192.168.2.100 it will forward it from the F0/1.
6. Before that the Router will send ARP request to identify the mac address of the devices within the network. And store them in the ARP table.

ARP Table for Router0

IP Address	Hardware Address	Interface
192.168.1.1	00E0.F7A2.7501	GigabitEthernet0/0
192.168.1.100	0060.3EC4.AC48	GigabitEthernet0/0
192.168.2.1	00E0.F7A2.7502	GigabitEthernet0/1
192.168.2.100	0001.C946.AB82	GigabitEthernet0/1

Figure 3: Router ARP Table

7. Now it will send to the Switch2 and if the destination mac address isn't in the ARP table. Then the switch will flood it and find the destination mac address and the port of the PC-2.

MAC Table for Switch2

VLAN	Mac Address	Port
1	0001.C946.AB82	FastEthernet0/2
1	00E0.F7A2.7502	FastEthernet0/1

Figure 4: Switch 2 MAC Table

8. And it forwards the packet to the destination mac address to the correct port which is PC-2.

## Chapter 3: ARP Resolving

The green packet represents the ARP packet. Where the target IP address will be Default Gateway and the target mac address will be filled with zeros.

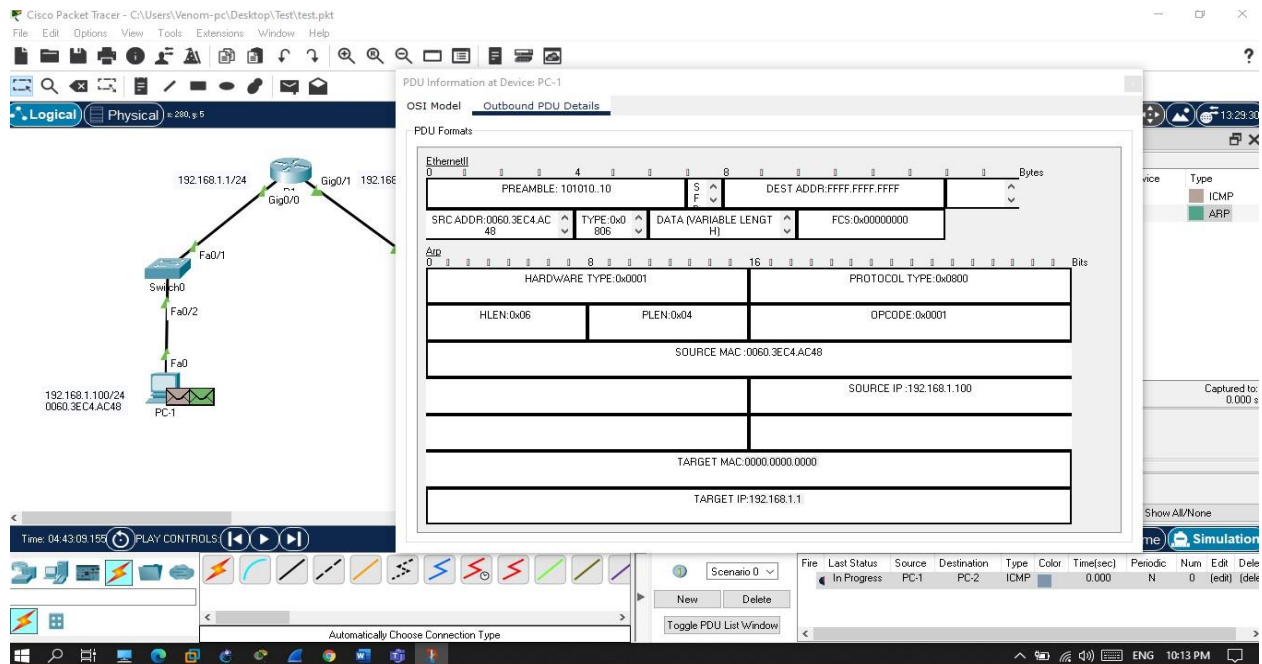


Figure 5: ARP Request Outbound PDU Details

After the reply of ARP packet, the Target Mac Address will be filled with the Routers MAC ADDRESS

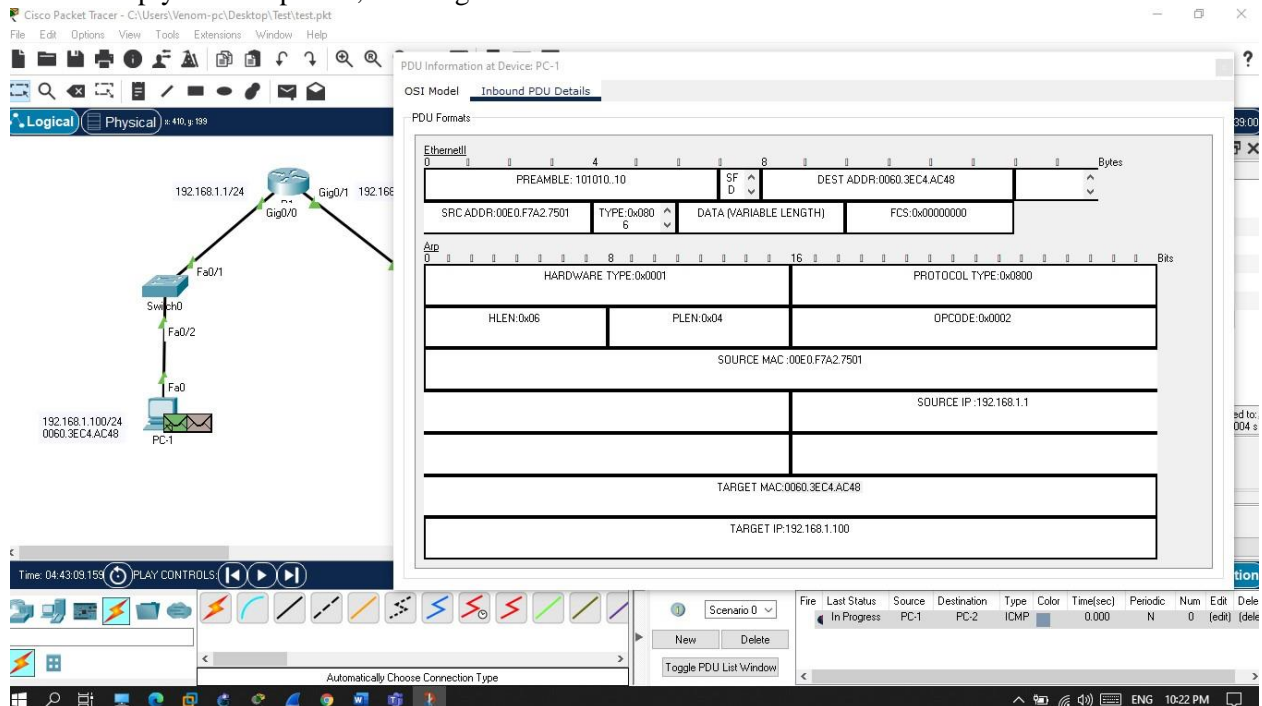


Figure 6: ARP Reply Inbound PDU Details

# ICMP ECHO REQUEST

Every time the packet goes through router, then the TTL value will be decremented by -1

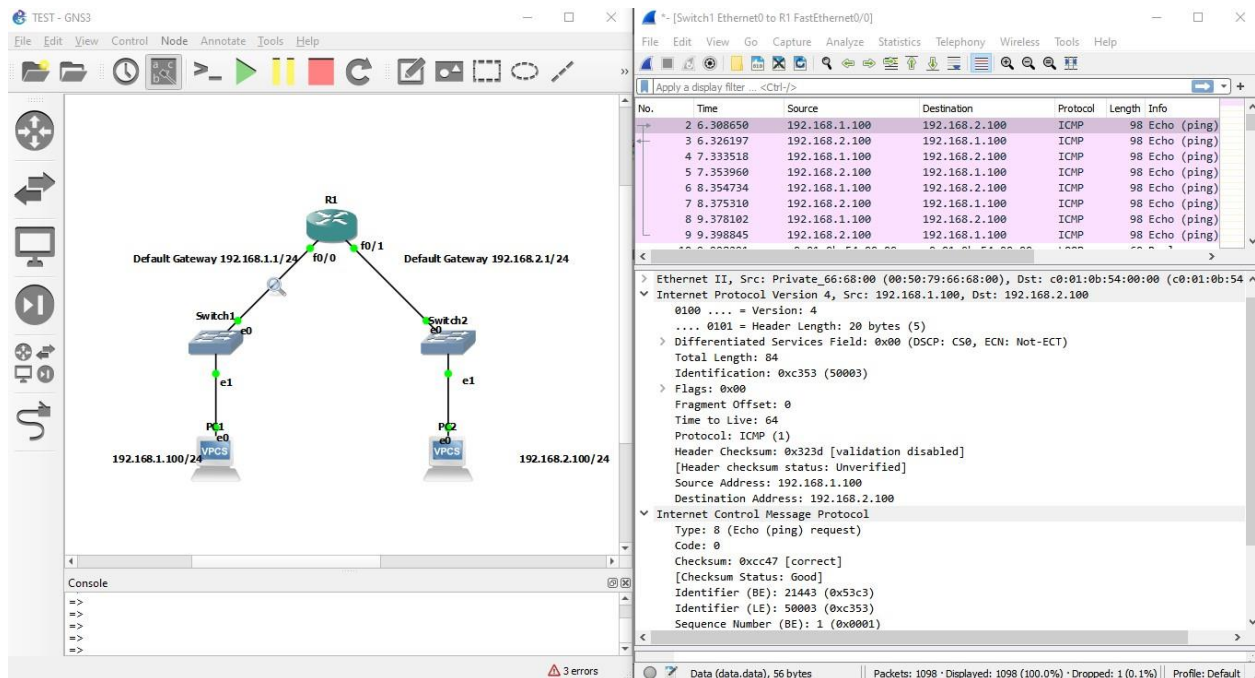
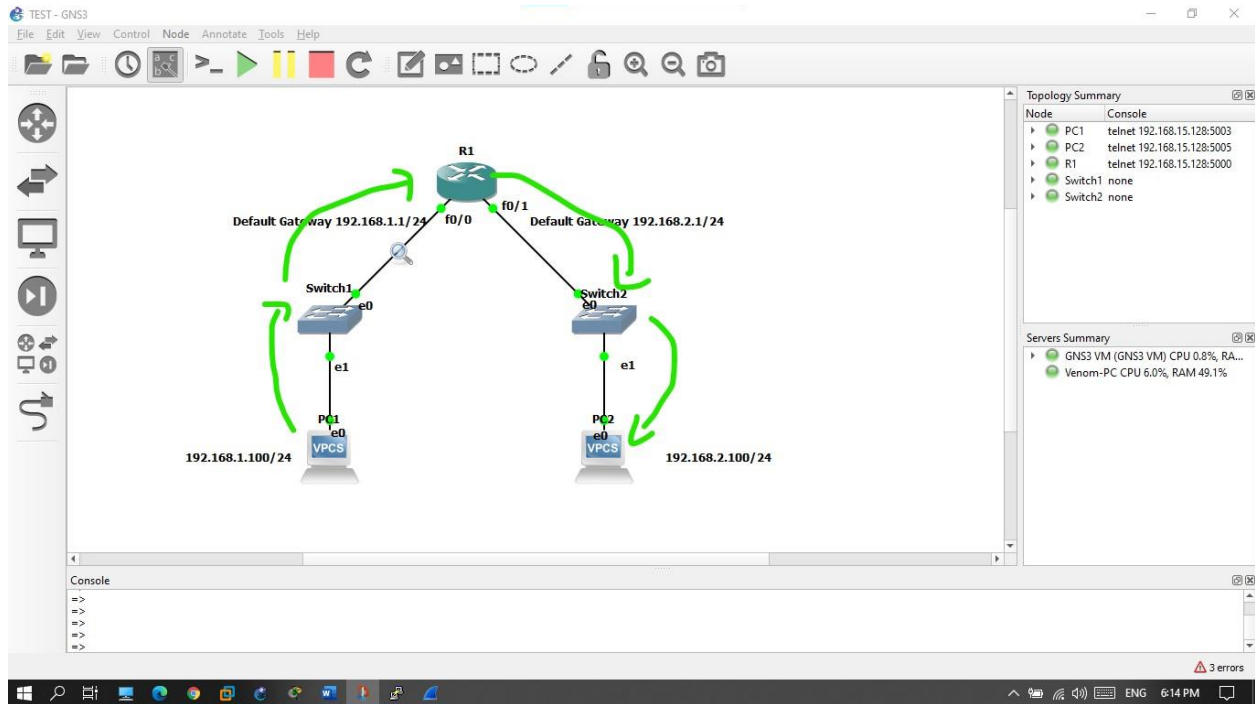


Figure 8: Wireshark Captured ICMP Echo Request Packet

## ICMP ECHO REPLY

Every time the packet goes through router, then the TTL value will be decremented by -1

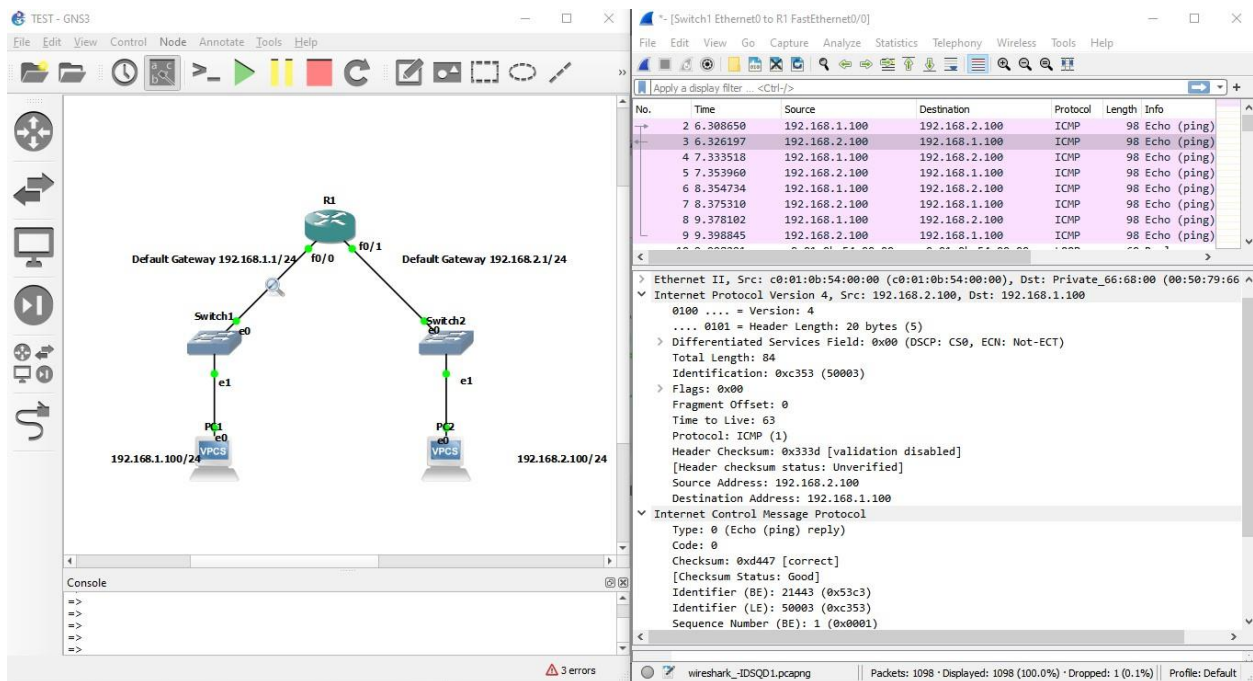
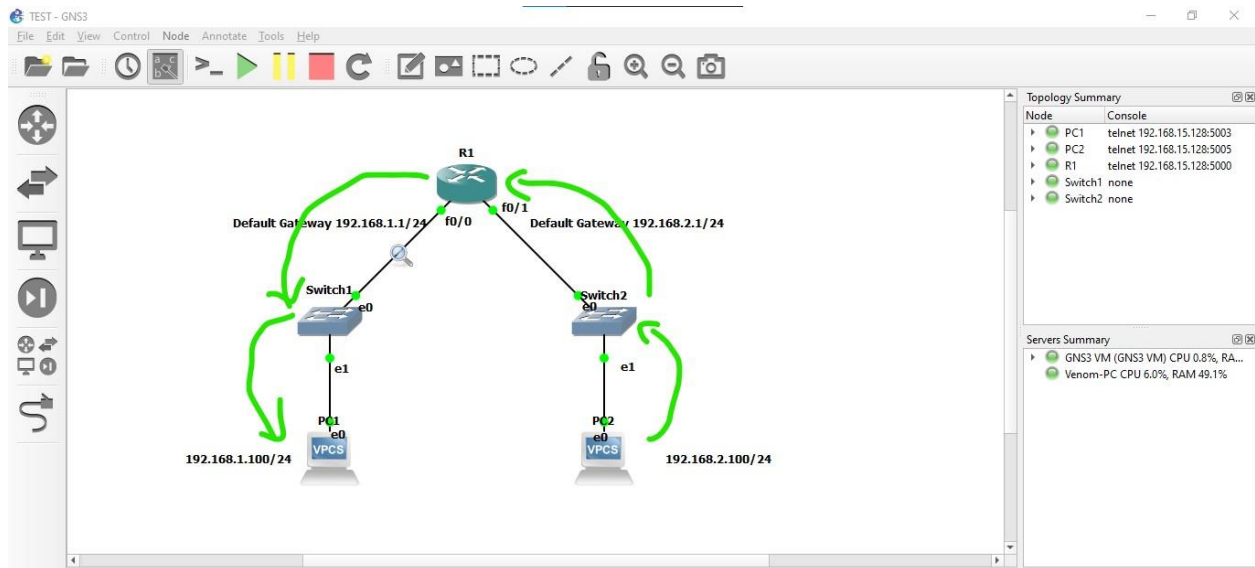


Figure 10: Wireshark Captured ICMP Echo Reply Packet



## Chapter 4: Live Simulation

### Sending the ICMP Echo Request – 8

This explains the process of each layer in **OSI Model**.

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a central router connected to two switches, which are in turn connected to two PCs (PC0 and PC1). The router's GigabitEthernet0/0 interface is connected to Switch0's GigabitEthernet0/1 interface. Switch0's FastEthernet0/20 interface is connected to PC0's FastEthernet0 interface. The router's GigabitEthernet0/1 interface is connected to Switch1's GigabitEthernet0/1 interface. Switch1's FastEthernet0/20 interface is connected to PC1's FastEthernet0 interface.

The main window shows the 'PDU Information at Device: PC0' dialog box. The 'OSI Model' tab is selected, displaying the 'Outbound PDU Details' for an ICMP Echo Request. The source is PC0 and the destination is 192.168.2.100. The 'In Layers' and 'Out Layers' sections show the layers involved in the process:

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 192.168.1.100, Dest. IP: 192.168.2.100 ICMP Message Type: 8
Layer2	Layer2: Ethernet II Header 0060.35C4.AC48 >> 00E0.F7A2.7501
Layer1	Layer1: Port(s): FastEthernet0

Below the layers, a list of steps explains the process:

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address 192.168.2.100 is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

The 'Simulation Panel' on the right shows the 'Event List' with a single event at 0.000 seconds, triggered by PC0, of type ICMP. The 'Play Controls' section shows the simulation is running in 'Realtime' mode.

Figure 11: Step 01 Ping Process Starts

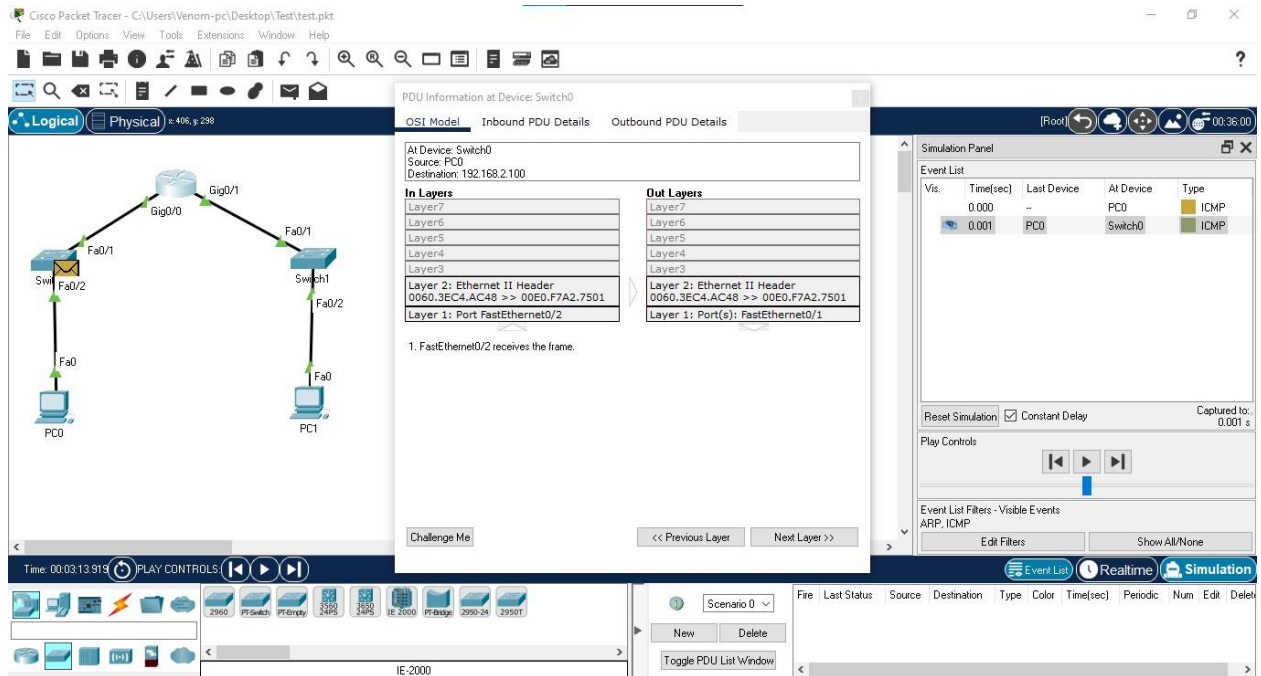


Figure 12: Step 02 Ping Process

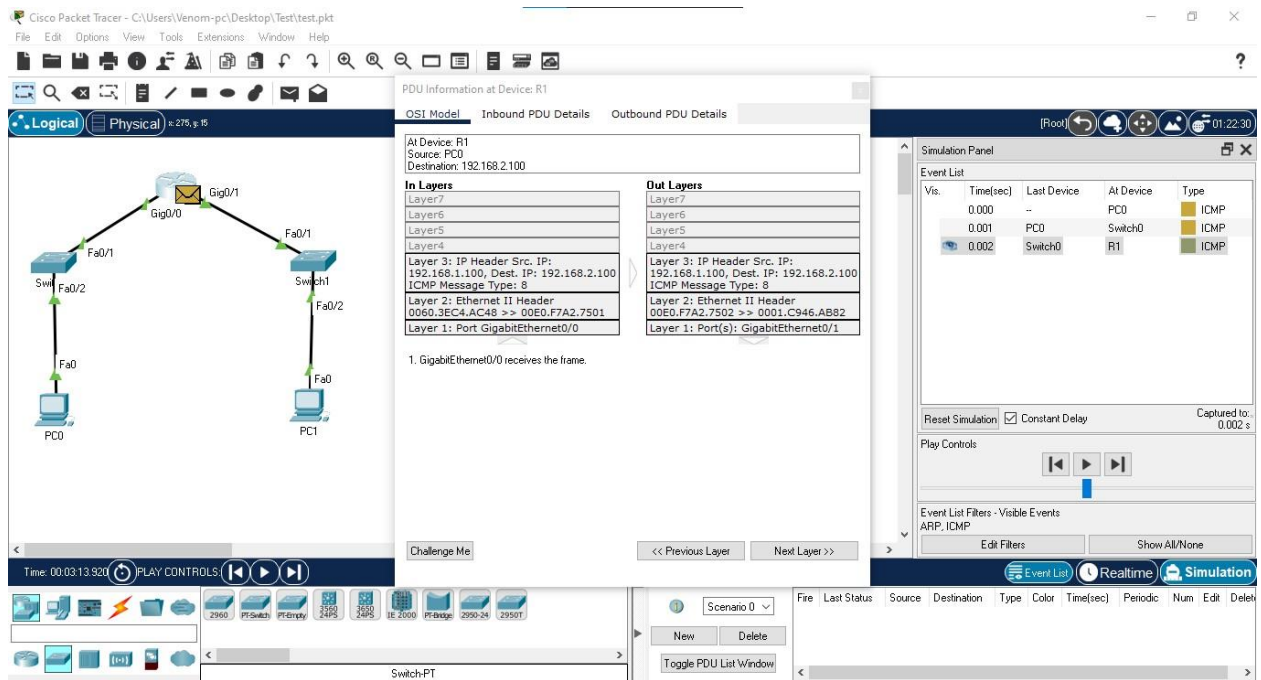


Figure 13: Step 03 Ping Process

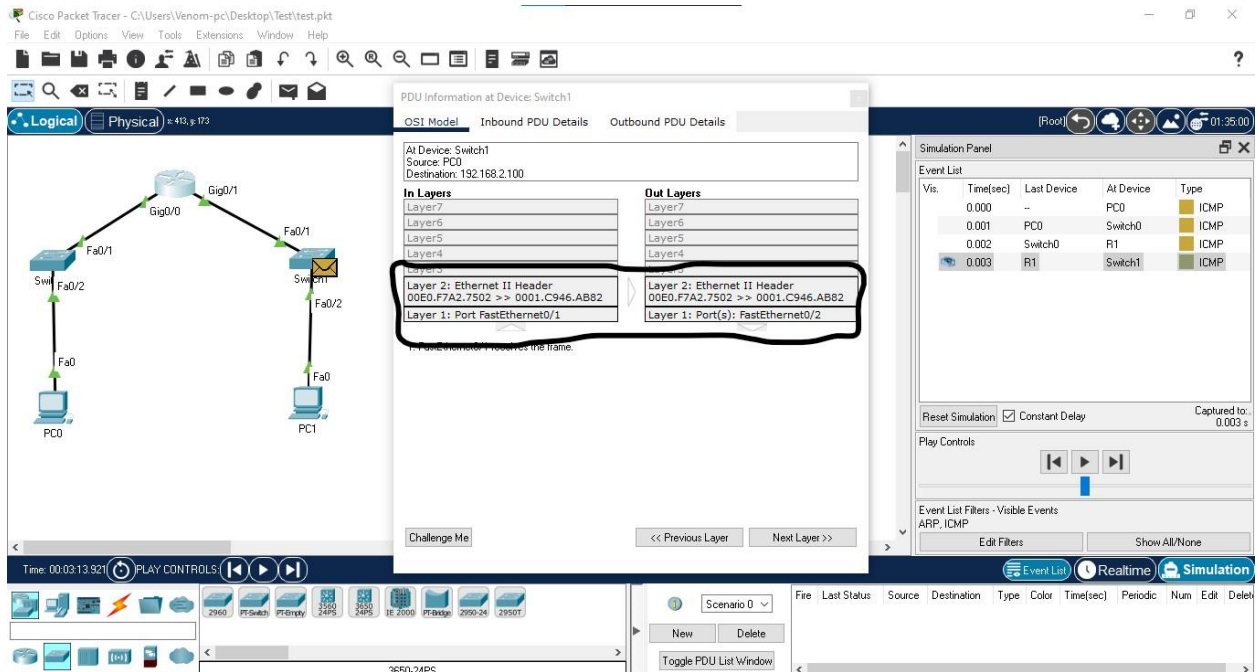


Figure 14: Step 04 Ping Process

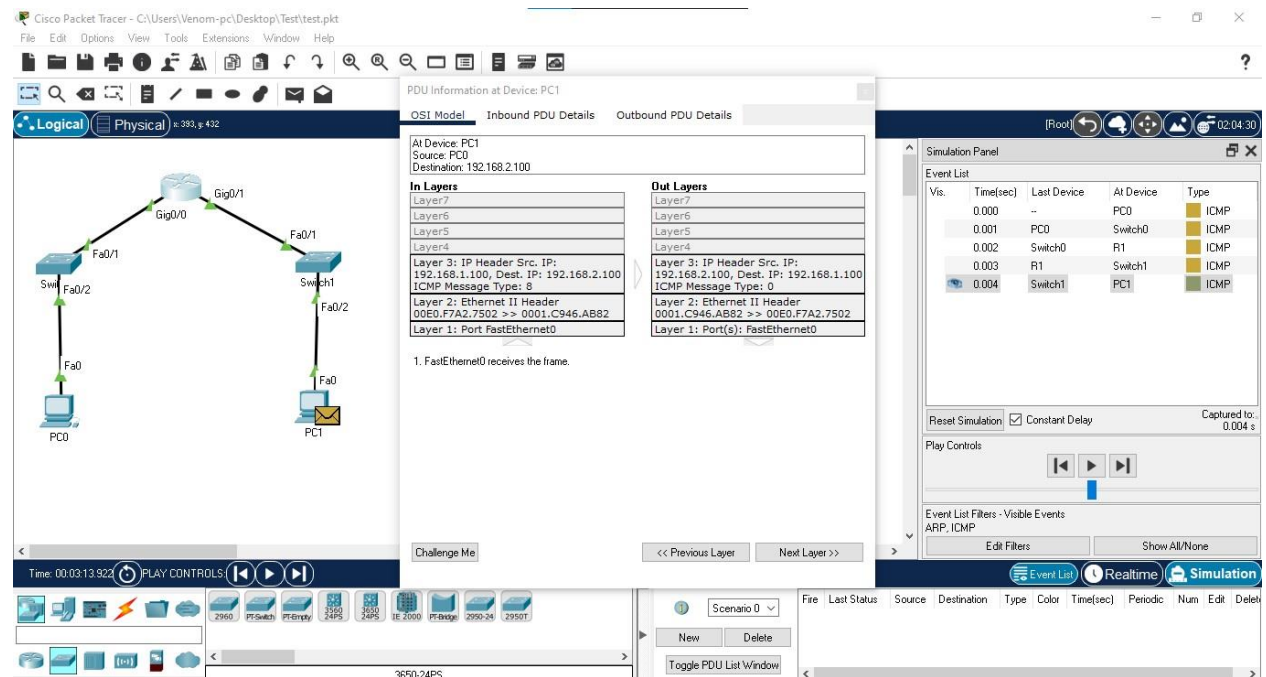


Figure 15: Step 05 Ping Process Stops

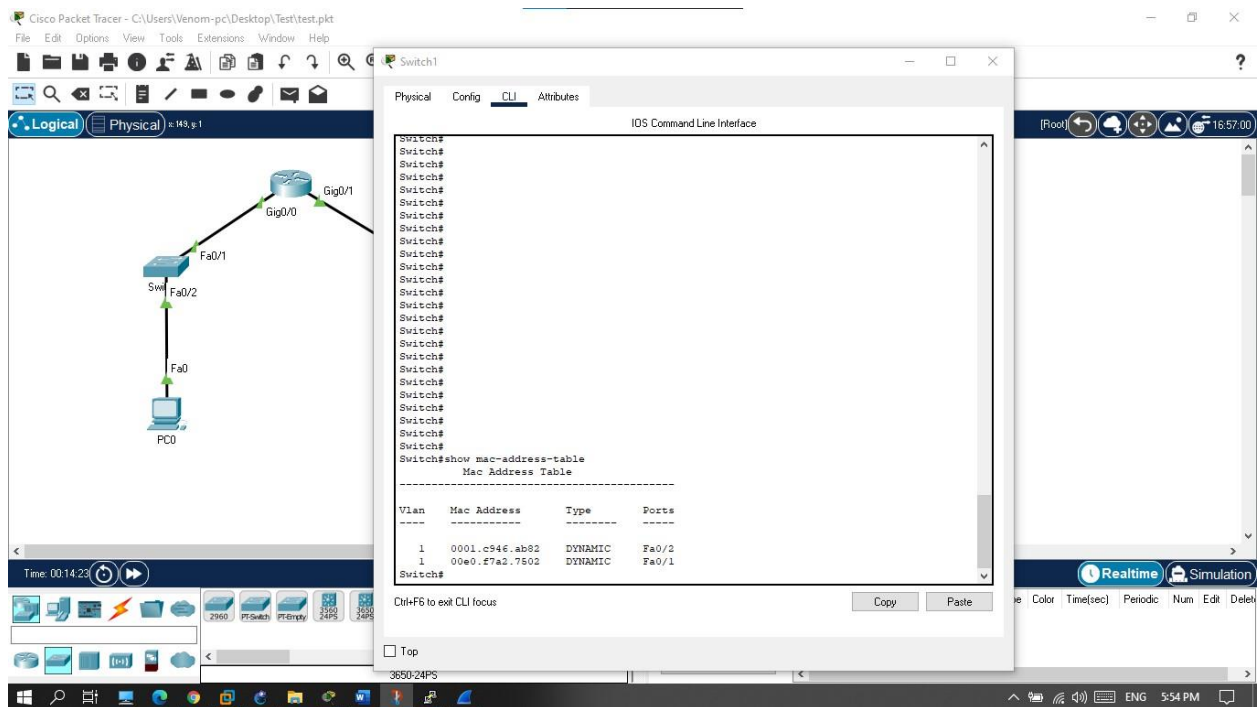


Figure 16: Step 06 192.168.1.0 Network's Switch Mac Address Table

## Replying with ICMP Echo Reply - 0

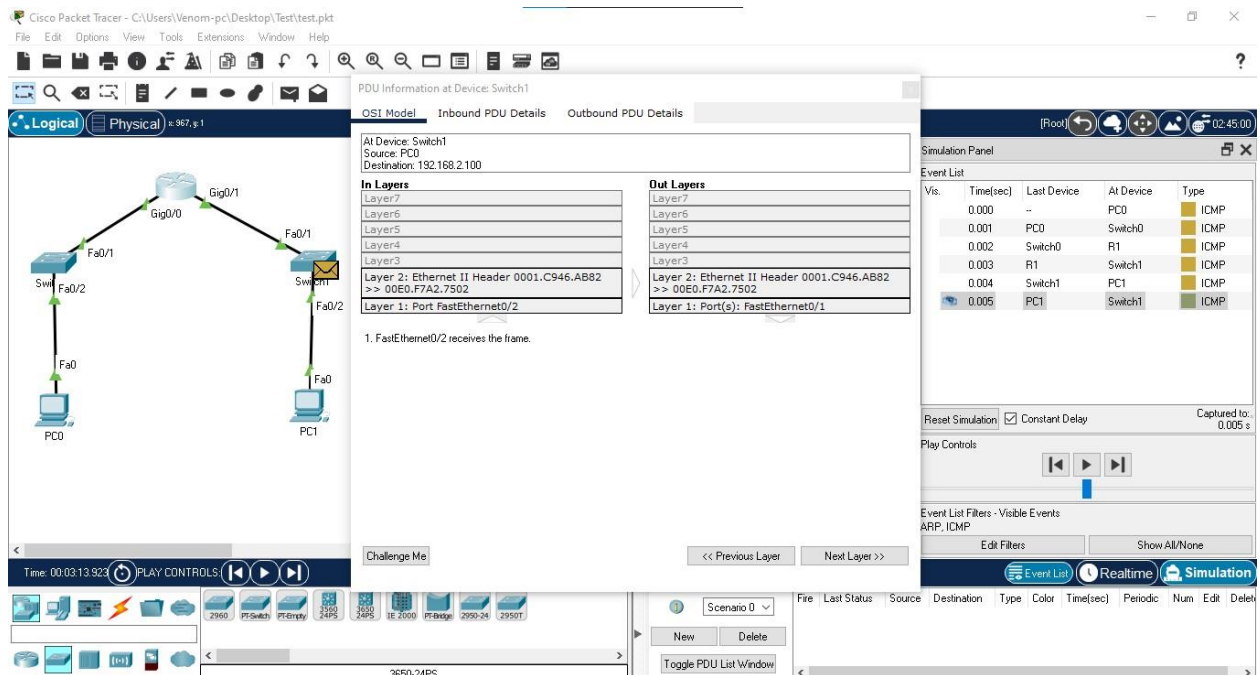


Figure 17: Step 07 Ping Process

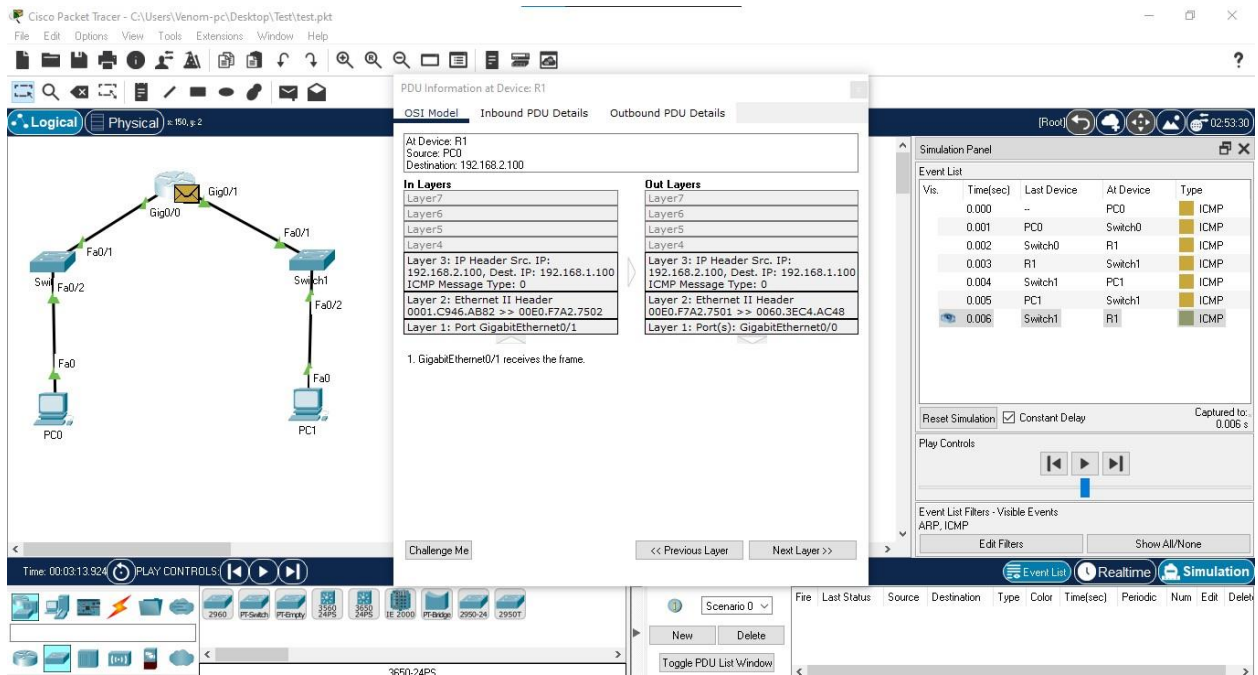


Figure 18: Step 08 Ping Process

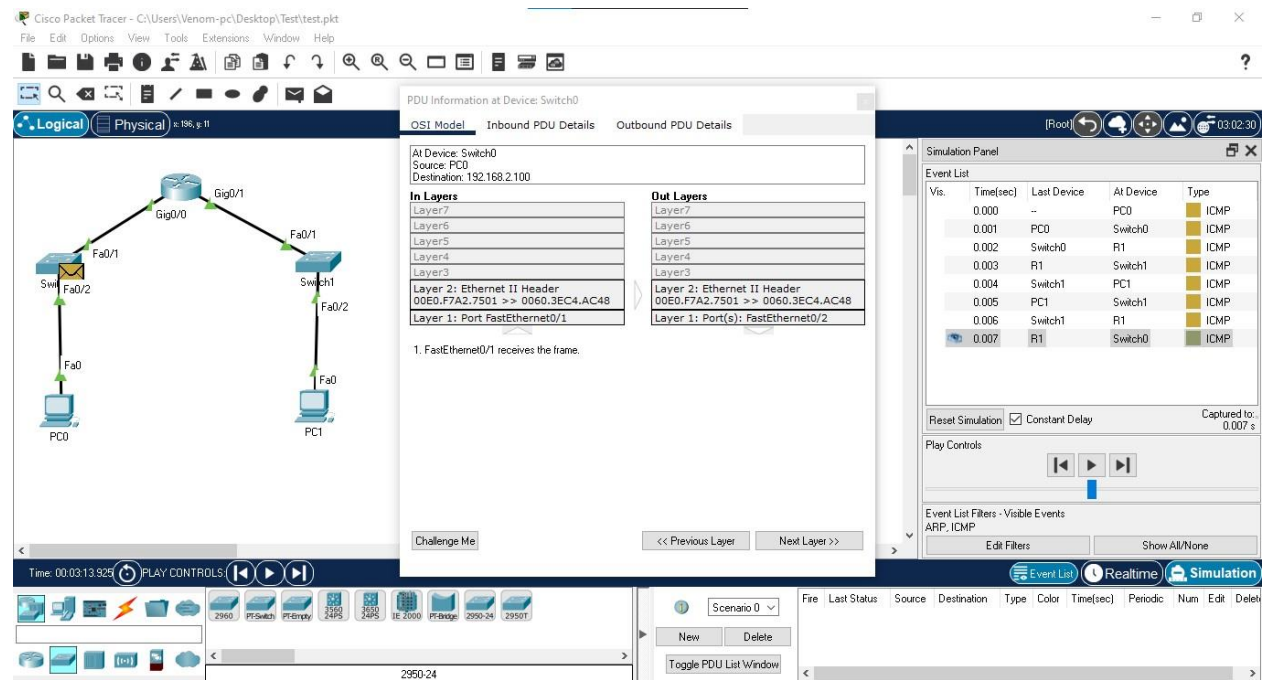


Figure 19: Step 09 Ping Process



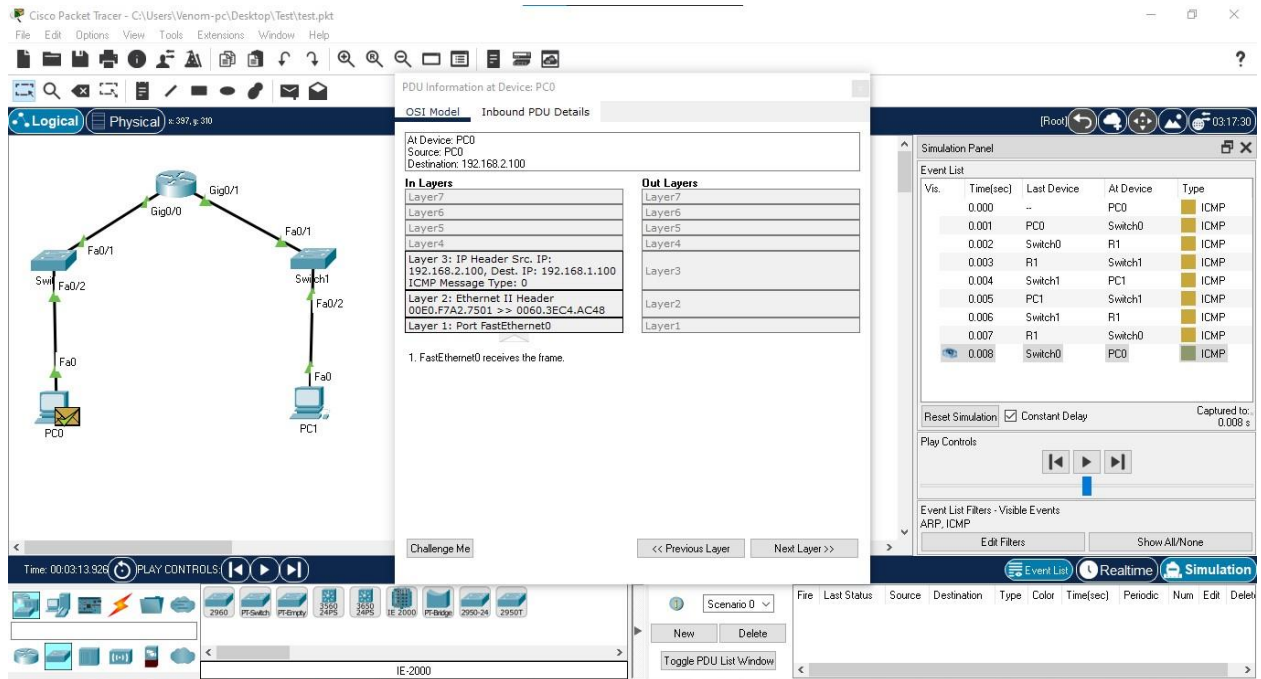


Figure 20: Step 10 Ping Process Successful

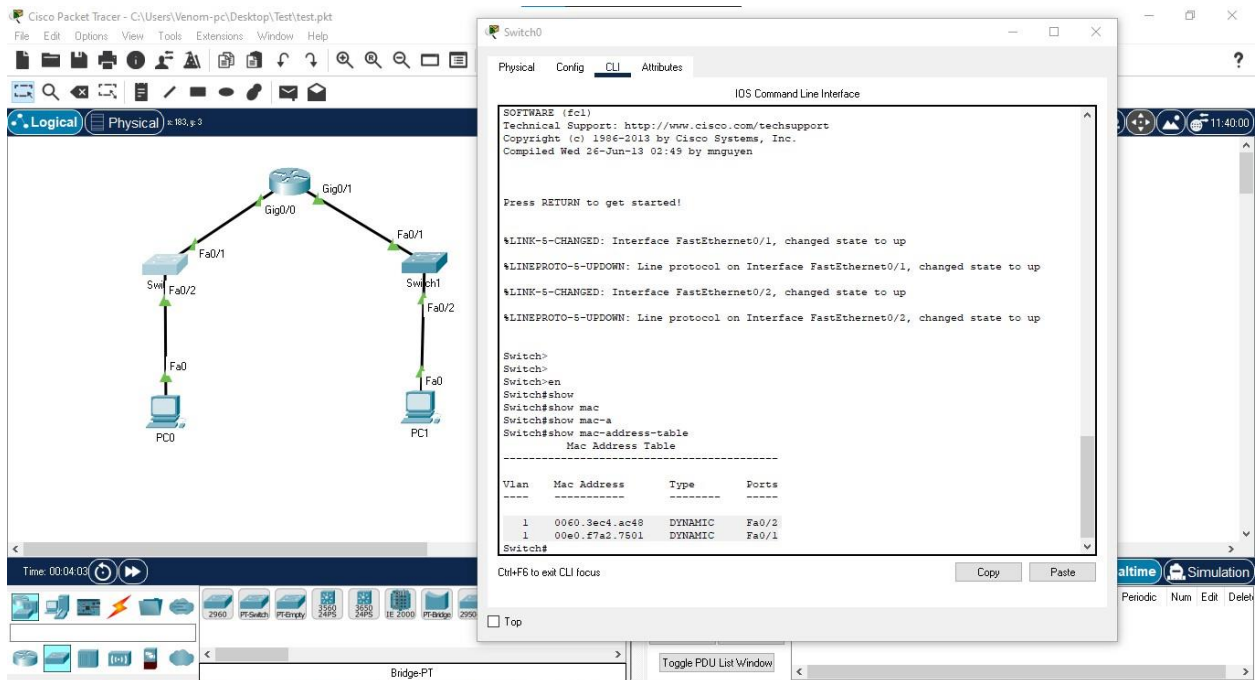


Figure 21: Step 11 192.168.2.0 Network's Switch Mac Address Table