**Ex No: 6**

**Date:**

**SIMULATION OF NETWORK LAYER PROTOCOLS**

1. **IMPLEMENTATION OF IPv4 AND IPv6 ADDRESSING PROTOCOLS**

**AIM:**

To build simple LANs, perform basic configurations for routers and switches, and implement IPv4 and IPv6 addressing schemes.

**THEORY:**

**IPv4 (Internet Protocol version 4)** is the most widely used version of the IP protocol, providing 32-bit addresses and supporting approximately 4.3 billion unique IP addresses. It uses a hierarchical addressing scheme consisting of a network address and a host address, separated by subnet masks to define network boundaries.

**IPv6 (Internet Protocol version 6)**, on the other hand, was introduced to address the limitations of IPv4, offering a 128-bit address space, which provides a virtually limitless number of unique addresses. IPv6 also introduces improvements such as simplified header structures, improved security features, and better support for mobile networks. In this experiment, both addressing schemes are configured in a simple LAN, demonstrating how devices can communicate within the network and how these protocols coexist. IPv4 addresses are usually assigned using DHCP, while IPv6 uses **stateless address autoconfiguration (SLAAC)** or DHCPv6 for automatic address assignment. The setup allows for understanding how both protocols function, highlighting the importance of transitioning from IPv4 to IPv6 due to the growing demand for IP addresses in modern networks.

**IPv4 (Internet Protocol Version 4)**

* Format: IPv4 addresses are 32-bit numeric values, typically written in dotted-decimal notation (e.g., 192.168.1.1).
* Structure: It consists of four octets (8 bits each) separated by periods, with each octet ranging from 0 to 255.
* Address Space: IPv4 supports approximately 4.3 billion unique addresses.
* Example: 192.0.2.1
* Limitations: Due to rapid internet growth, IPv4 faces address exhaustion despite techniques like NAT (Network Address Translation).

**IPv6 (Internet Protocol Version 6)**

* Format: IPv6 addresses are 128-bit values, typically written in hexadecimal notation, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
* Structure: It consists of eight groups of four hexadecimal digits, with leading zeros in groups often omitted for simplicity.
* Address Space: IPv6 provides a vast address space (approximately 340 undecillion addresses), effectively solving the exhaustion problem.
* Example: 2001:db8::ff00:42:8329 (using :: to compress consecutive zeros).
* Enhancements: IPv6 offers improved security, multicast addressing, simplified header structure, and better support for mobile devices.
* An IPv6 (normal) address has the format y:y:y:y:y:y:y:y, where *y* is called a *segment* and can be any hexadecimal value between 0 and FFFF. The segments are separated by colons, not periods. An IPv6 normal address must have eight segments; however, a short form notation can be used in the TS4500 management GUI for segments that are zero, or those that have leading zeros.
* The following are examples of valid IPv6 (normal) addresses:2001:db8:3333:4444:5555:6666:7777:8888
* 2001:db8:3333:4444:CCCC:DDDD:EEEE:FFFF
* :: (implies all 8 segments are zero)
* 2001:db8:: (implies that the last six segments are zero)
* ::1234:5678 (implies that the first six segments are zero)
* 2001:db8::1234:5678 (implies that the middle four segments are zero)
* 2001:0db8:0001:0000:0000:0ab9:C0A8:0102 (This can be compressed to eliminate leading zeros, as follows: 2001:db8:1::ab9:C0A8:102 )

**PROCEDURE:**

## WIRED LAN

* 1. First, we will download Cisco Packet Tracer from netacad.com (latest version).
  2. After downloading we will open it and now in this window, we see there are multiple small windows where we can select component and create our own particular computer network.
  3. Select the components that are listed on the left bottom corner.
  4. Select the 2950T switch and 2 routers from the components and place it on the white screen.
  5. Place the PC’s and laptops from the components and place it on the white screen.
  6. Now select the wire from the connections and select copper straight through wire and connect fastethernet from PC to the switch.
  7. Select serial connecter for router to router connection.

**CONFIGURING THE NETWORK**

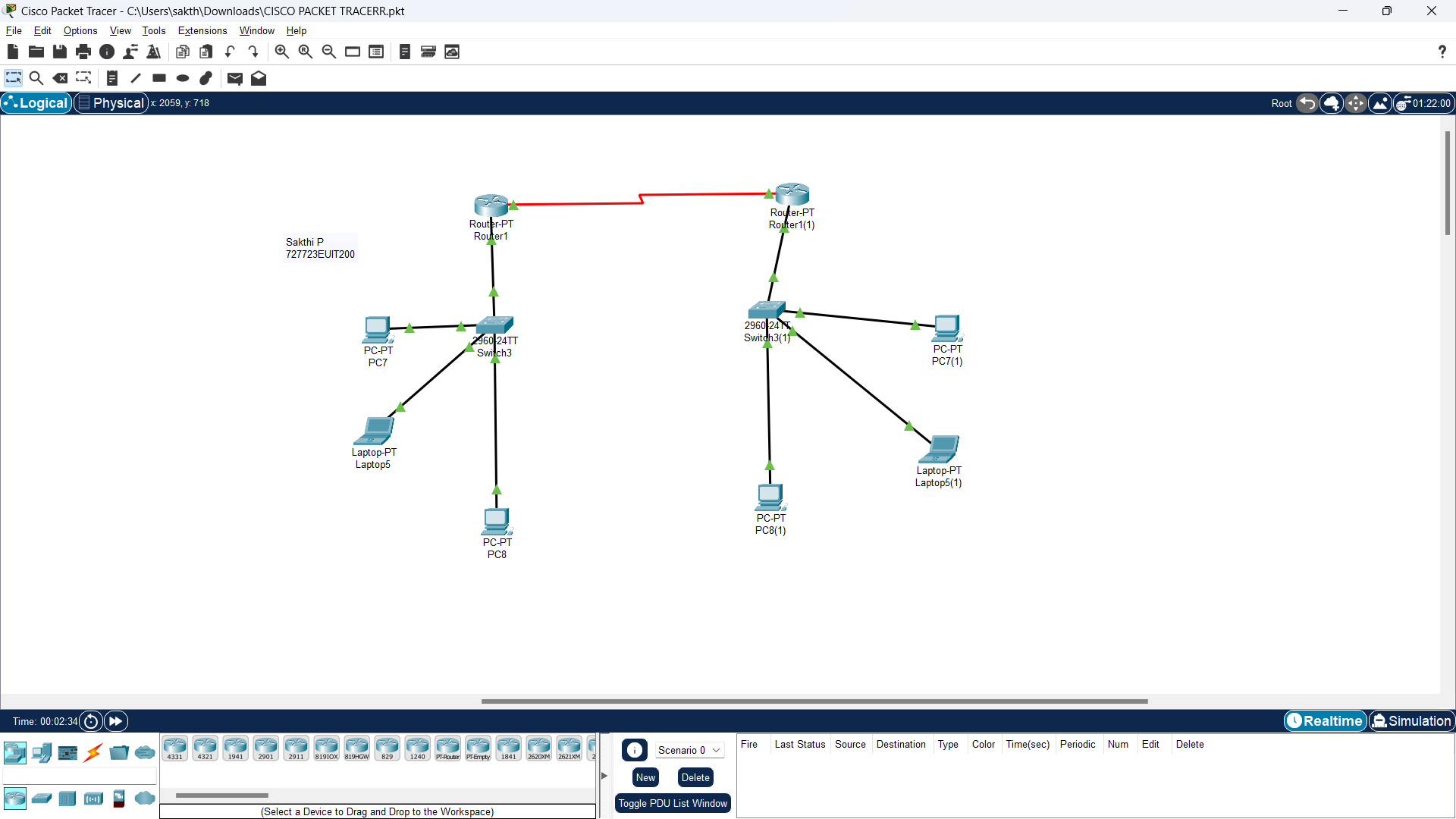
* Now assign ip address to each of the PC and laptops based on IPv4 or IPv6 formats.
* Under fastethernet tab when you double click on the PC you will able to see fastethernet and under that set IPv4 or IPv6 Address.

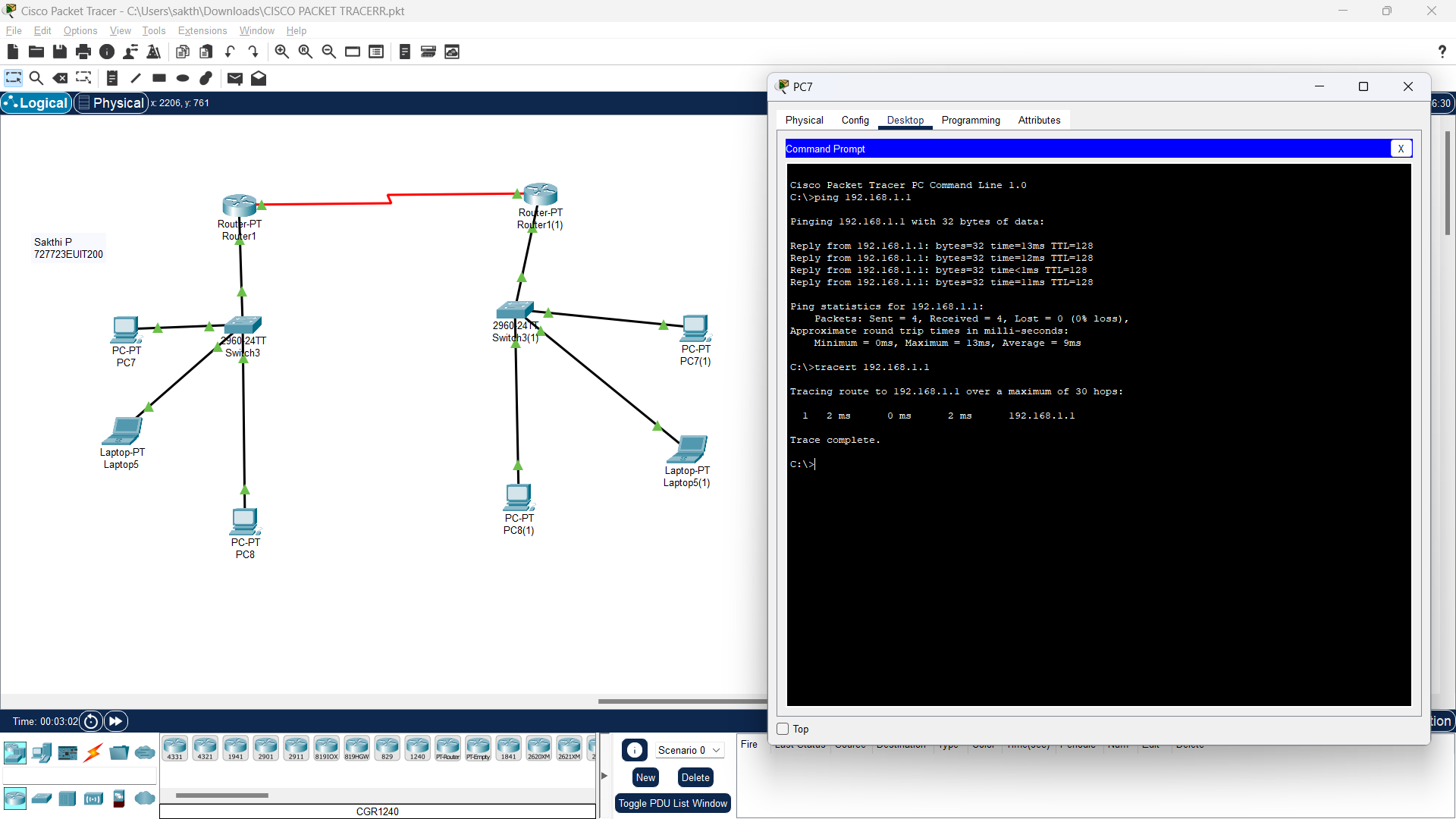
**TESTING THE NETWORK**

* Choose the device you want to test and double click on that and under desktop you will see the command prompt option
* Click on that and type the command ping “host ip”(the ip of any other device in the network).
* The data packets are successfully sent from the source to destination.

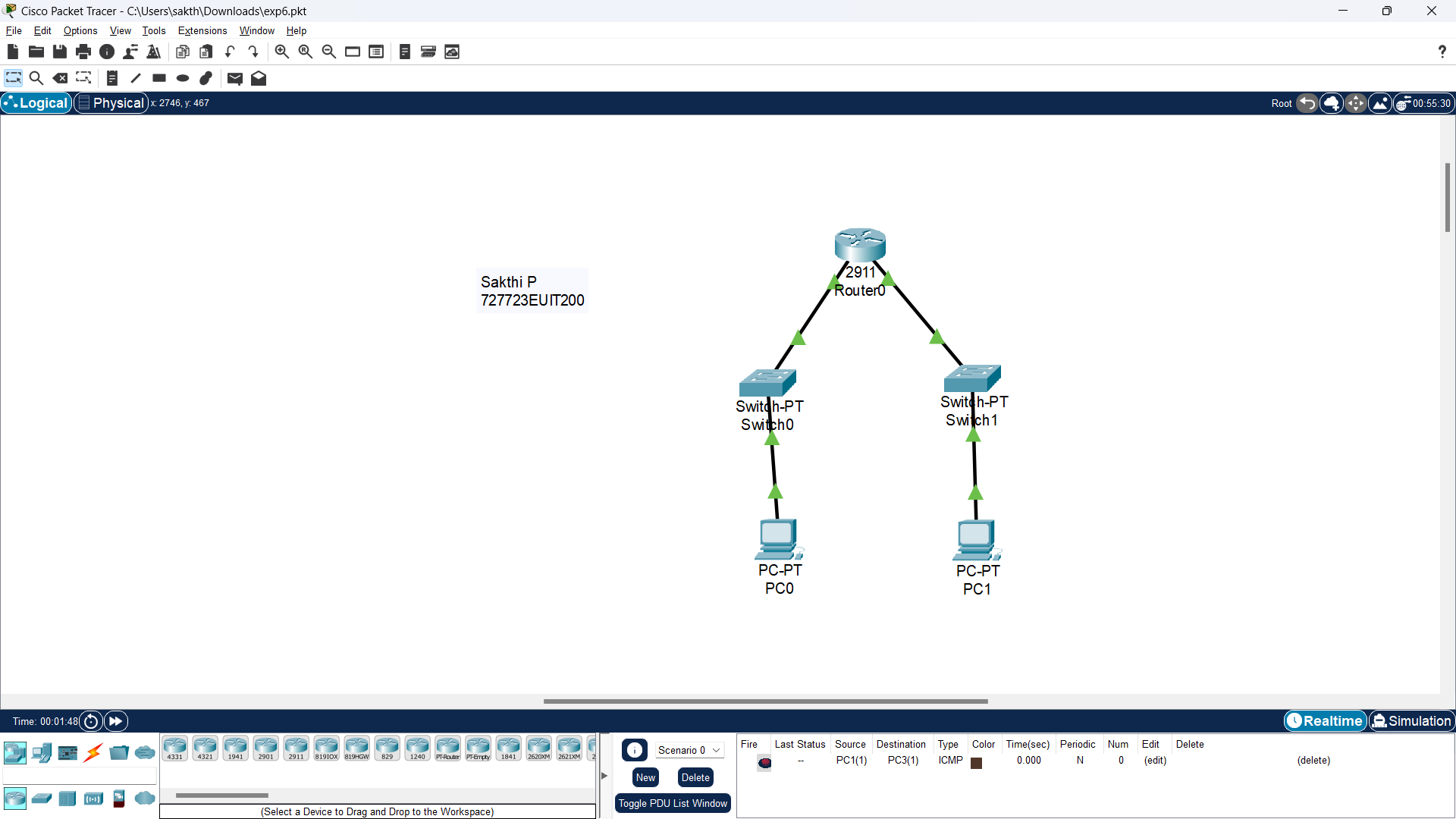
**SIMULATION OUTPUT:**

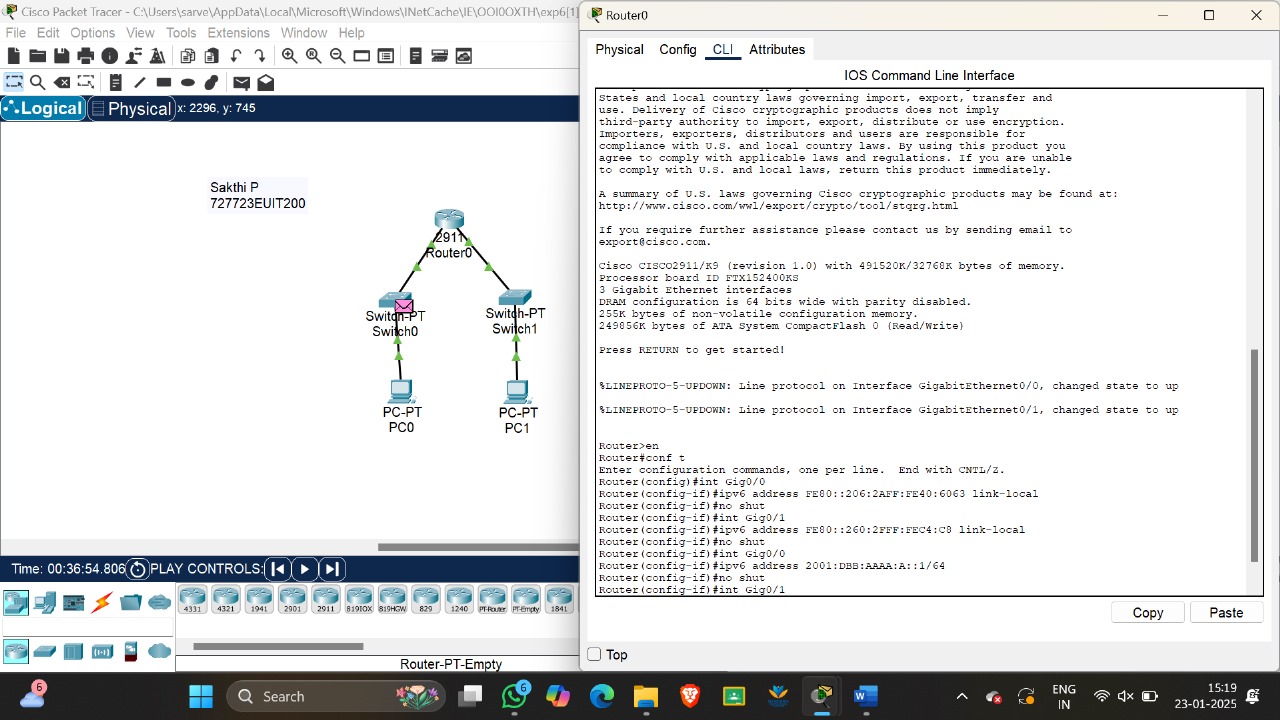
**IPv4:**

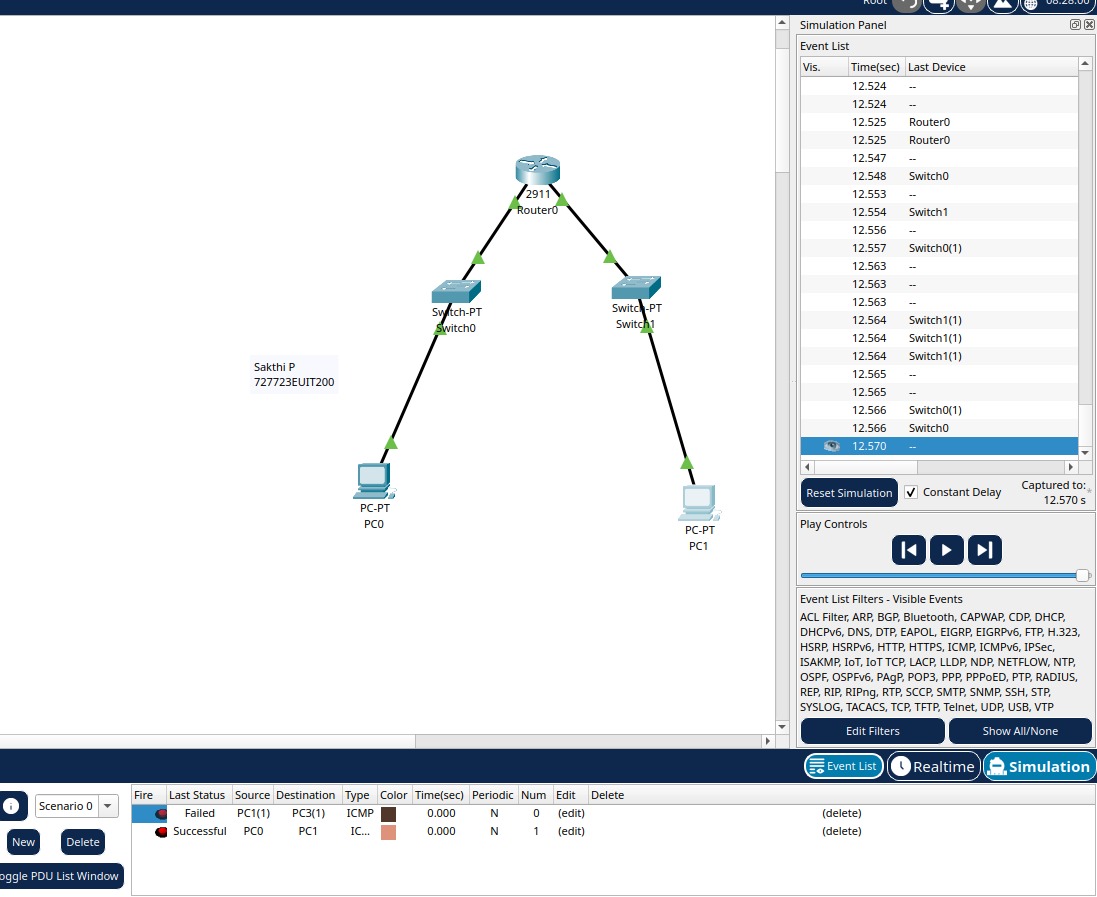




**IPv6:**



****



**RESULT:**

Thus, simple LAN networks, were implemented, where all the nodes were configured with both IPv4 and IPv6 addressing and communication between nodes was tested, in the Cisco Packet Tracer Simulation environment.

1. **IMPLEMENTATION OF INTERNET CONTROL MESSAGE PROTOCOL (ICMP)**

**Aim:**

The aim of this experiment is to understand and implement the Internet Control Message Protocol (ICMP) in a network using Cisco Packet Tracer. The experiment will involve configuring devices to send and receive ICMP messages (such as ping requests and replies), which are used for diagnosing network connectivity and ensuring communication between devices on a network.

**Theory:**

The Internet Control Message Protocol (ICMP) is an integral part of the Internet Protocol Suite (TCP/IP) used by routers, network devices, and hosts to send error messages and operational information. ICMP is primarily used for diagnostic tools like ping and traceroute, and it helps to verify the connectivity and status of network devices.

1. ICMP Overview:
   * ICMP is designed to send error messages such as "Destination Unreachable," "Time Exceeded," and "Echo Request/Echo Reply."
   * It operates at the Network Layer (Layer 3) of the OSI model.
   * The most common ICMP message is the Echo Request and Echo Reply, which are used in the ping operation to check if a device is reachable over the network.
2. ICMP Structure:
   * ICMP packets contain a type, code, checksum, and data.
     + Type: Specifies the type of message (e.g., Echo Request = 8, Echo Reply = 0).
     + Code: Provides additional information related to the type (e.g., Destination Unreachable code = 3).
     + Checksum: Ensures integrity of the packet.
     + Data: Usually includes additional information like the time elapsed in Echo Request and Echo Reply.
3. Common Uses:
   * Ping: A tool to send an Echo Request and receive an Echo Reply to check whether a host is reachable and measure the round-trip time.
   * Traceroute: A diagnostic tool that uses ICMP to determine the route packets take to reach a destination.

**Procedure:**

The procedure for implementing ICMP using Cisco Packet Tracer will involve setting up two or more devices (routers, switches, and PCs) in a network and then using ICMP-based diagnostic tools like ping to check connectivity.

**Step-by-Step Process in Cisco Packet Tracer**

1. Launch Cisco Packet Tracer:
   * Open Cisco Packet Tracer.
2. Create Network Topology:
   * Add Devices: Place the following devices on the workspace:
     + 2 PCs (PC0 and PC1)
     + 1 Switch
     + 1 Router
     + Cables: Use appropriate cables to connect the devices (Ethernet cables for connections between the router and PCs through the switch).
3. Configure IP Addresses for PCs:
   * Select PC0 and go to Desktop > IP Configuration.
     + Assign an IP address to PC0. For example:
       - IP Address: 192.168.1.1
       - Subnet Mask: 255.255.255.0
     + Repeat the process for PC1, assigning:
       - IP Address: 192.168.1.2
       - Subnet Mask: 255.255.255.0
     + Both PCs should be in the same IP subnet for communication to be possible.
4. Configure Router's Interfaces:
   * Select the Router and go to the CLI (Command Line Interface).
   * Configure the router’s interfaces to ensure the PCs can communicate via the router:

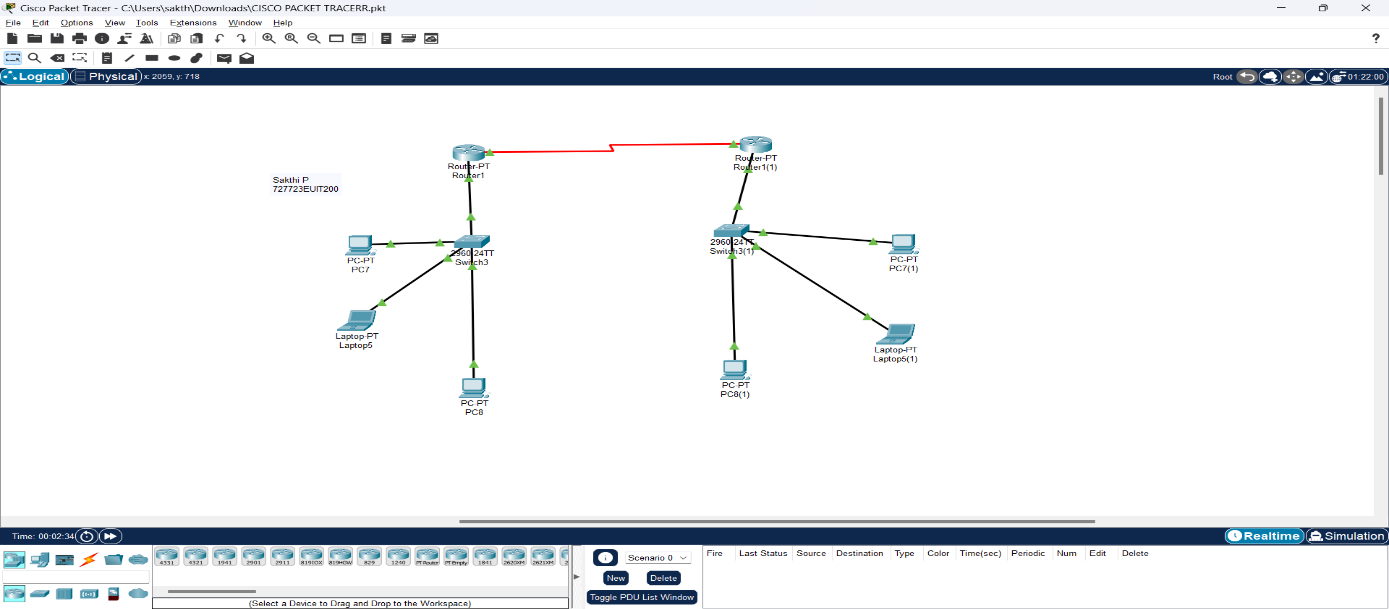
For example, configure the router's GigabitEthernet interface that is connected to the switch:

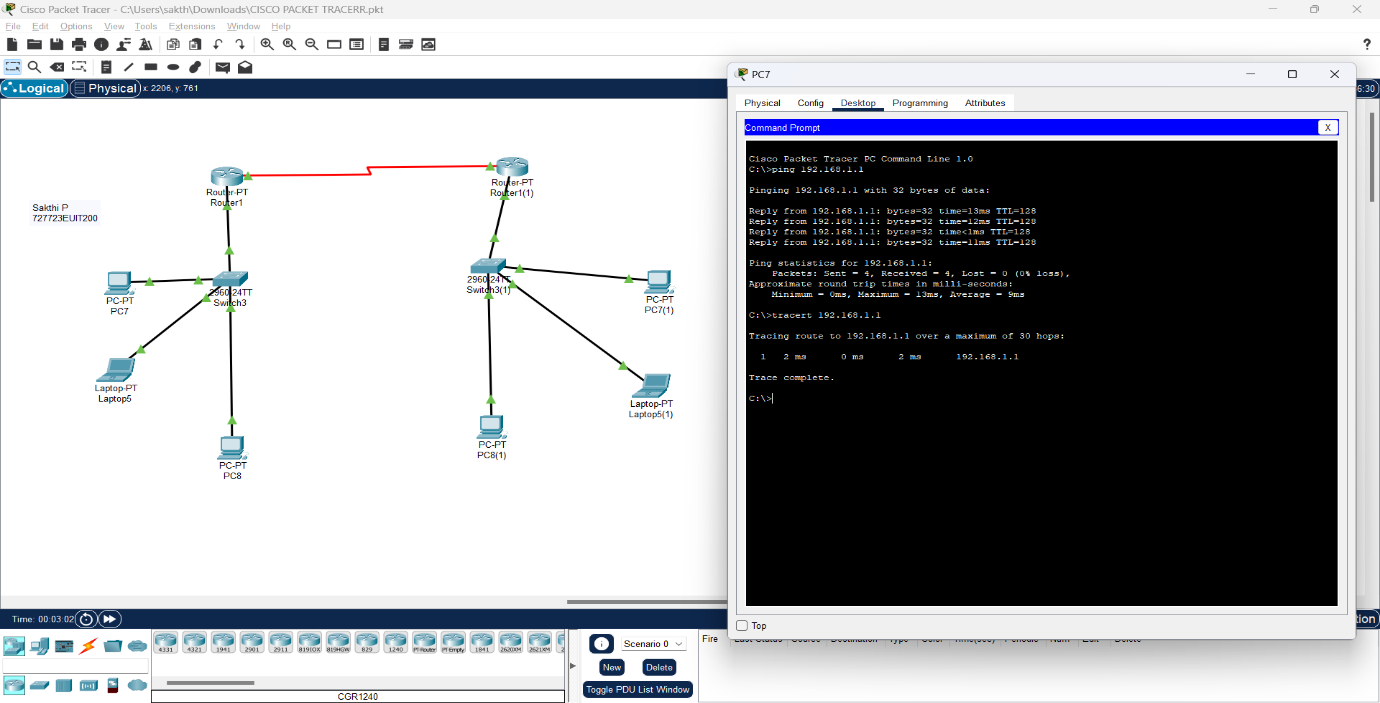
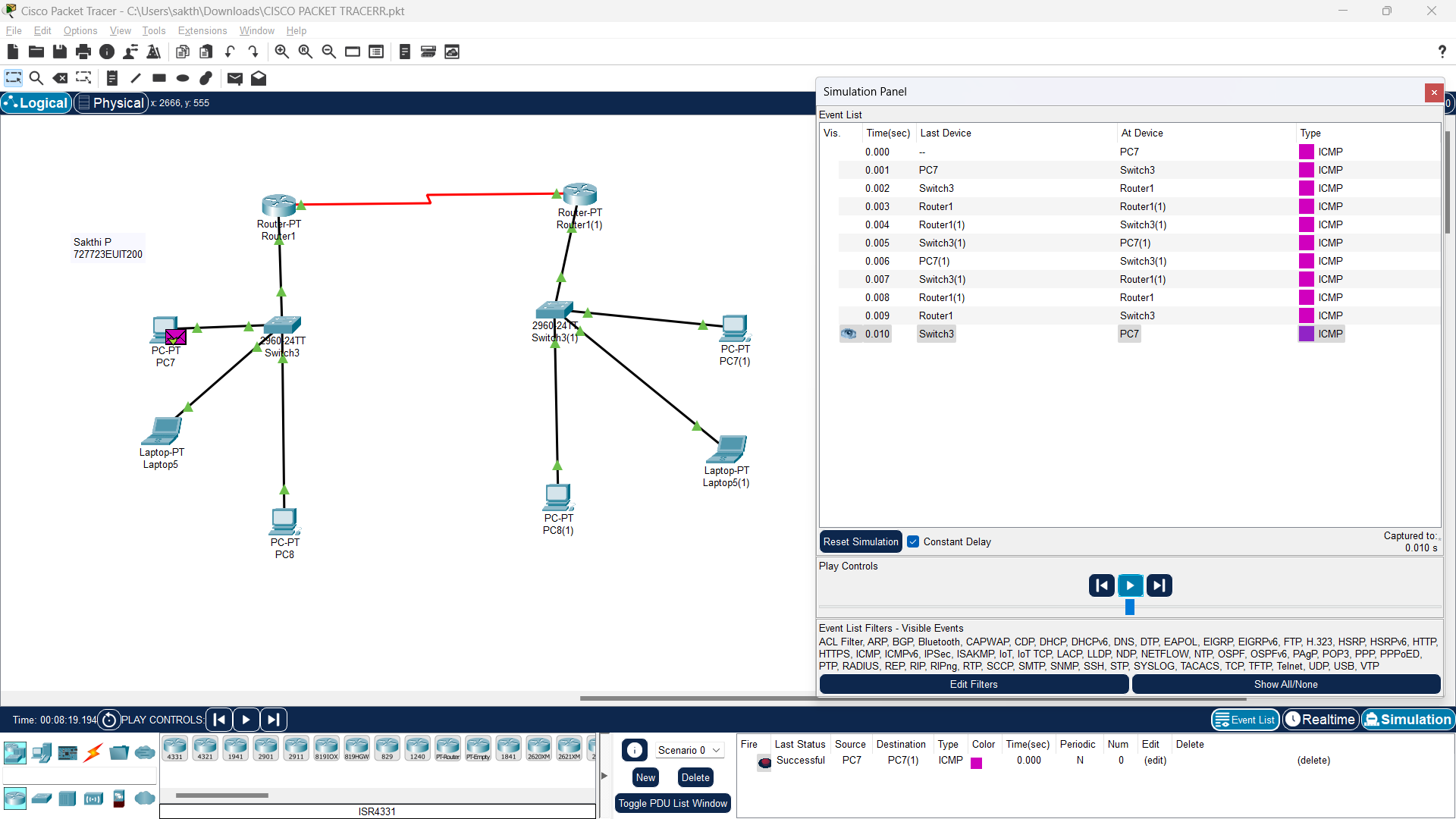
* + - Router> enable
    - Router# configure terminal
    - Router(config)# interface gigabitEthernet0/0
    - Router(config-if)# ip address 192.168.1.254 255.255.255.0
    - Router(config-if)# no shutdown
    - Router(config-if)# exit

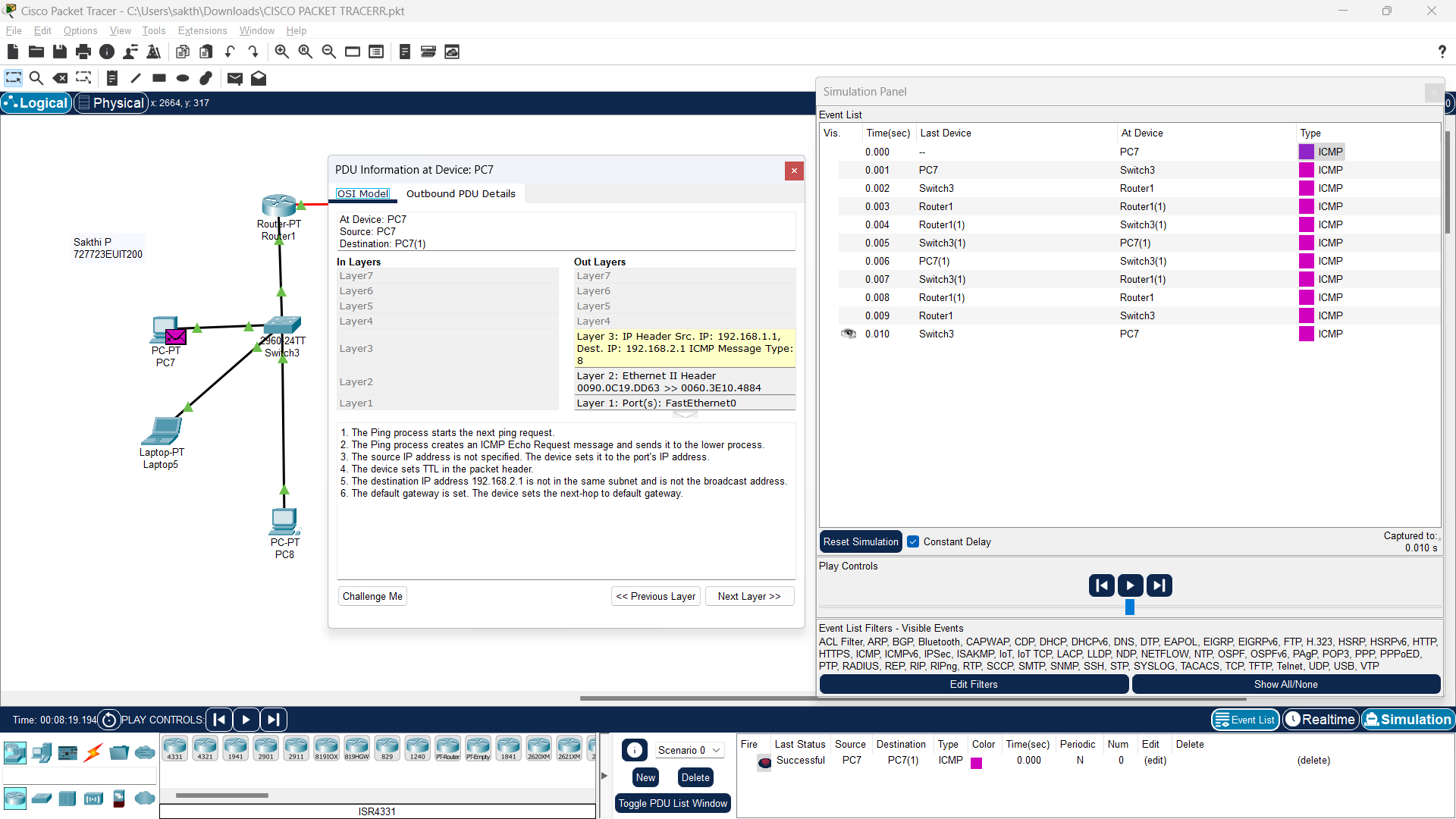
1. Connect the Devices:
   * Use the Copper Straight-Through Cable to connect:
     + PC0 to the switch.
     + PC1 to the switch.
     + Router’s GigabitEthernet0/0 interface to the switch.
   * Make sure the devices are connected to the correct interfaces on the router and switch.
2. Enable Routing:
   * If there is more than one subnet or if routing between different networks is needed, enable routing on the router. However, for this experiment, a simple network in the same subnet (192.168.1.0/24) does not need routing.
3. Ping Test:
   * On PC0, open the Command Prompt (Desktop > Command Prompt).
   * Type the following command to send an ICMP Echo Request to PC1:
   * ping 192.168.1.2
   * PC0 will send an ICMP Echo Request, and PC1 will respond with an Echo Reply if the devices are connected correctly.
4. Observe ICMP Results:
   * If the ping is successful, you will see a message like:
   * Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
   * This confirms that ICMP is functioning and the devices can communicate on the network.
5. Troubleshooting:
   * If the ping fails, ensure:
     + All devices are connected correctly.
     + The IP configuration is correct.
     + The router interface is up and properly configured.
     + The firewall on the PCs (if applicable) allows ICMP traffic.
   * You can check the ping status by looking at the LED indicators in Cisco Packet Tracer or using the ping tool from PC1 to PC0 for further verification.
6. Further Testing with Traceroute:

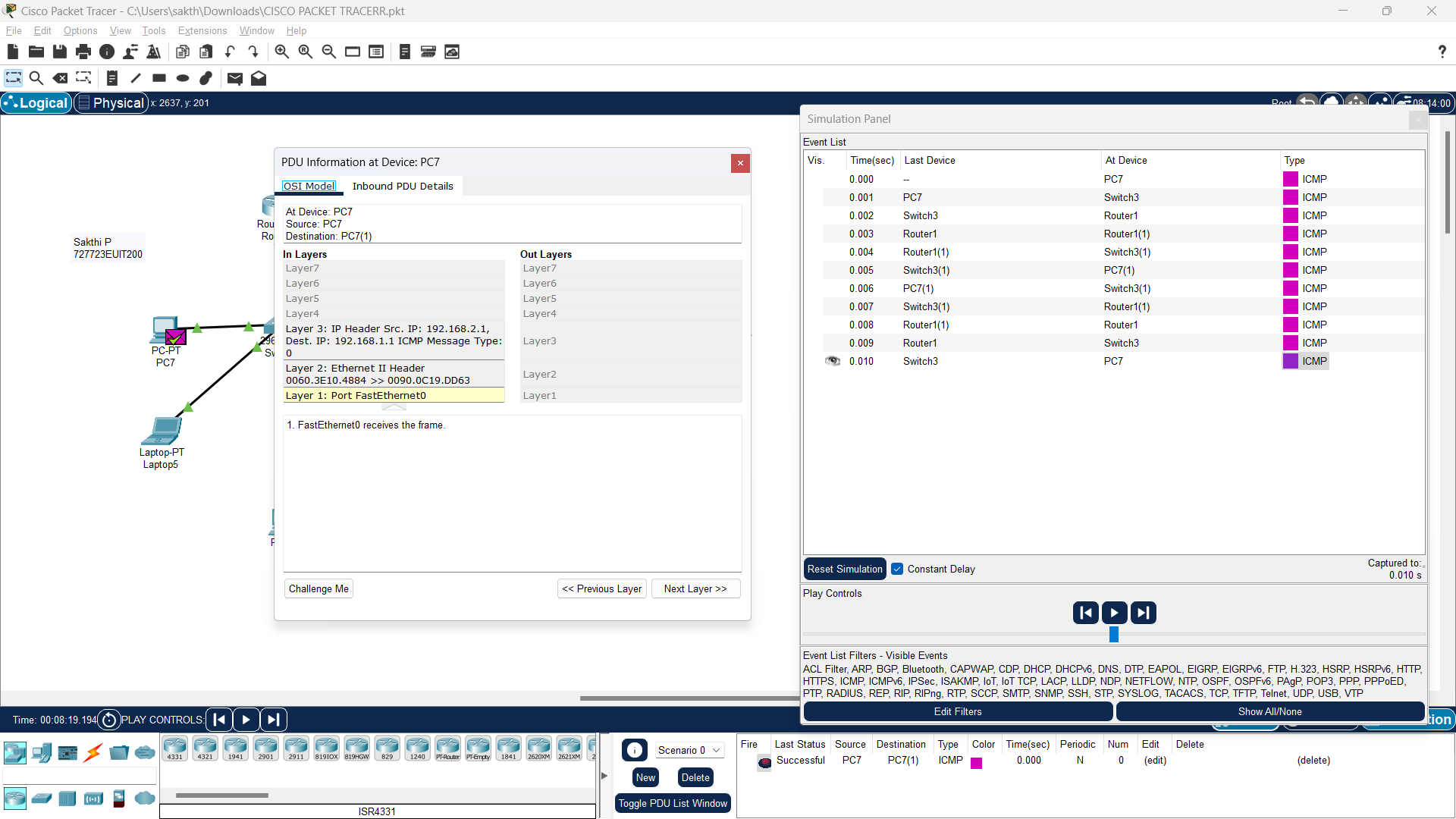
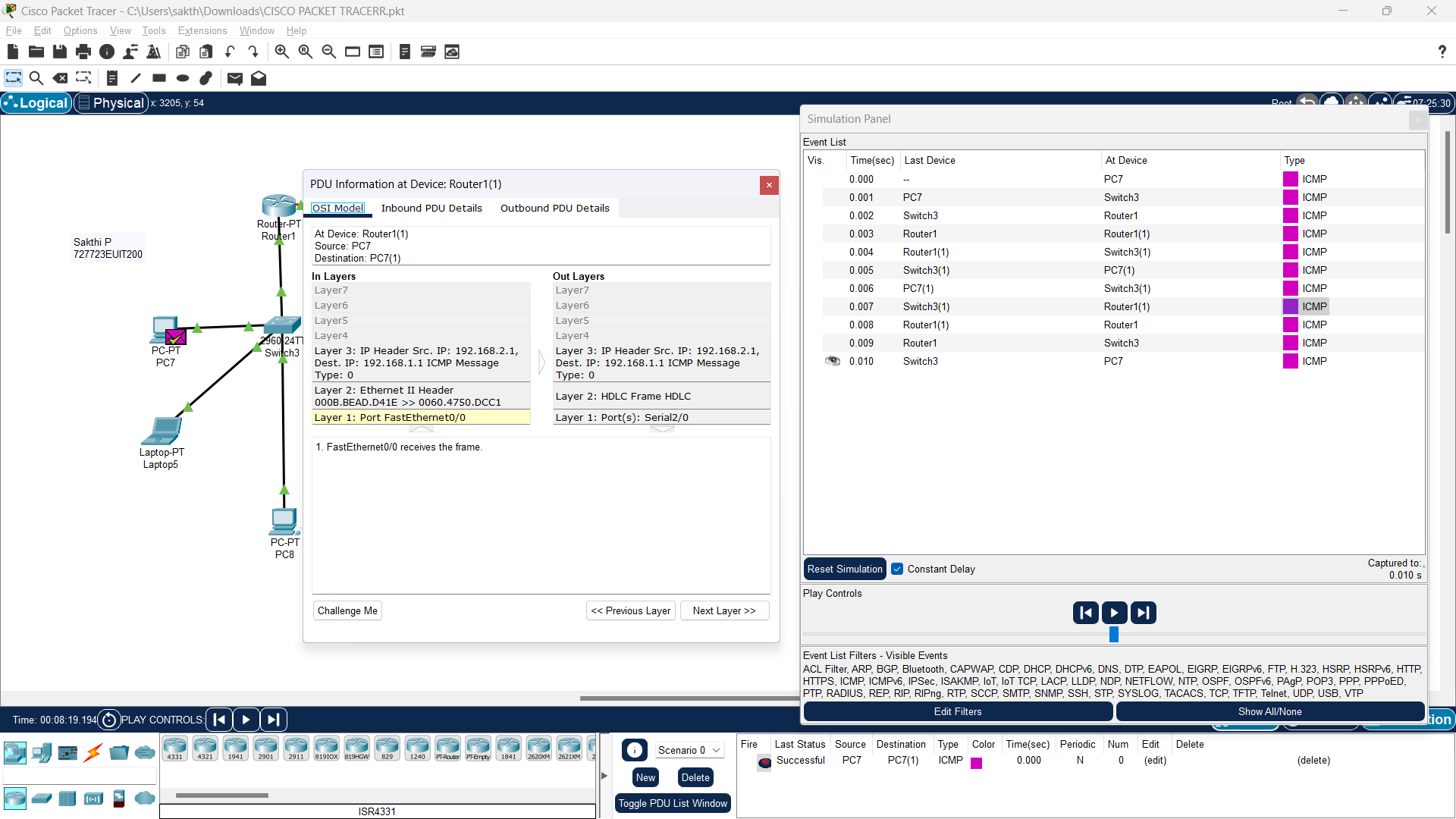
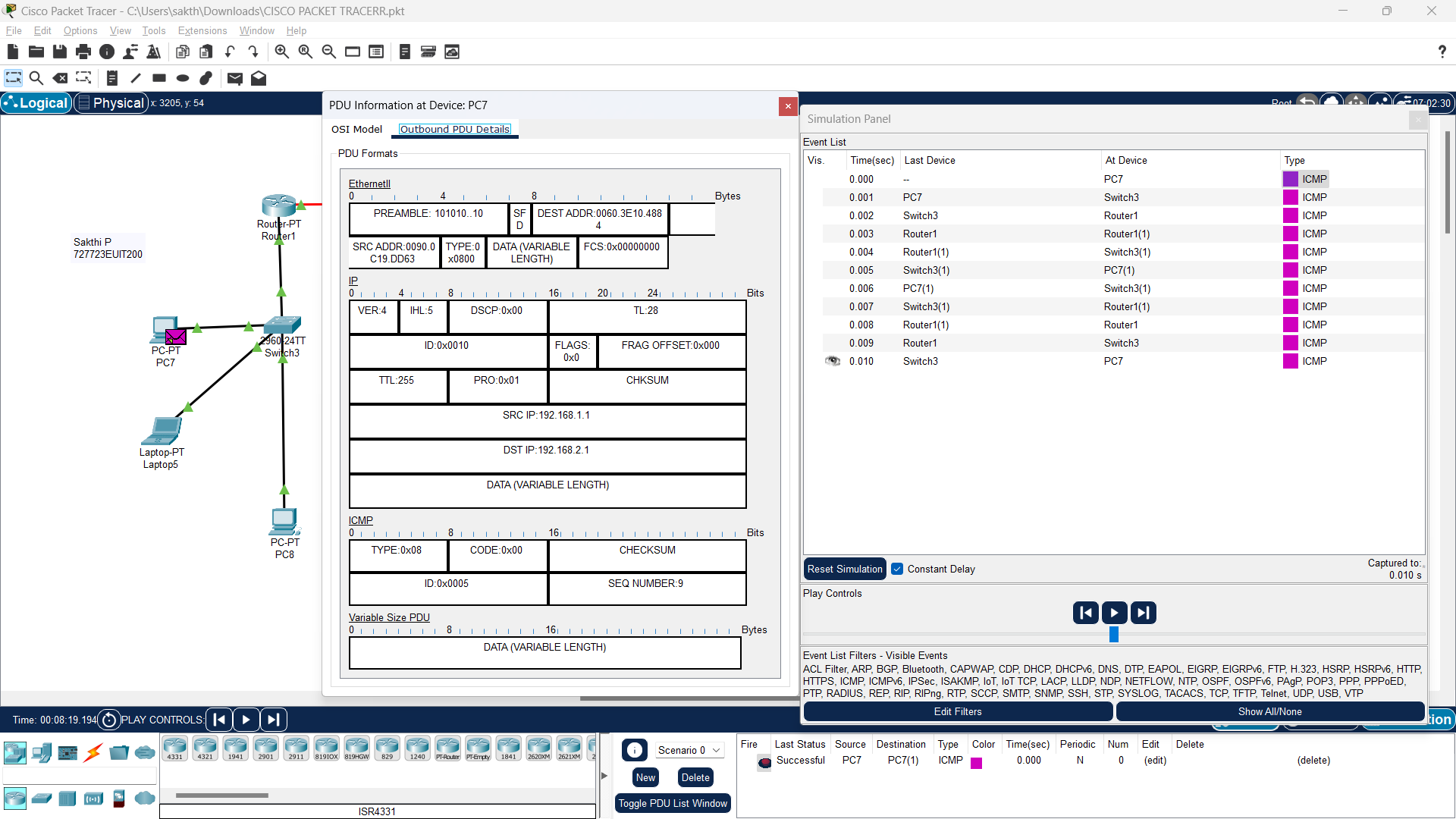
* To extend the experiment, you can use the Traceroute tool to trace the path packets take to reach the destination, verifying the network's routing path.
* On PC0, open Desktop > Command Prompt and type:
* tracert 192.168.1.2
* This will show the hops taken by the packet, giving you insights into the route used by ICMP messages.

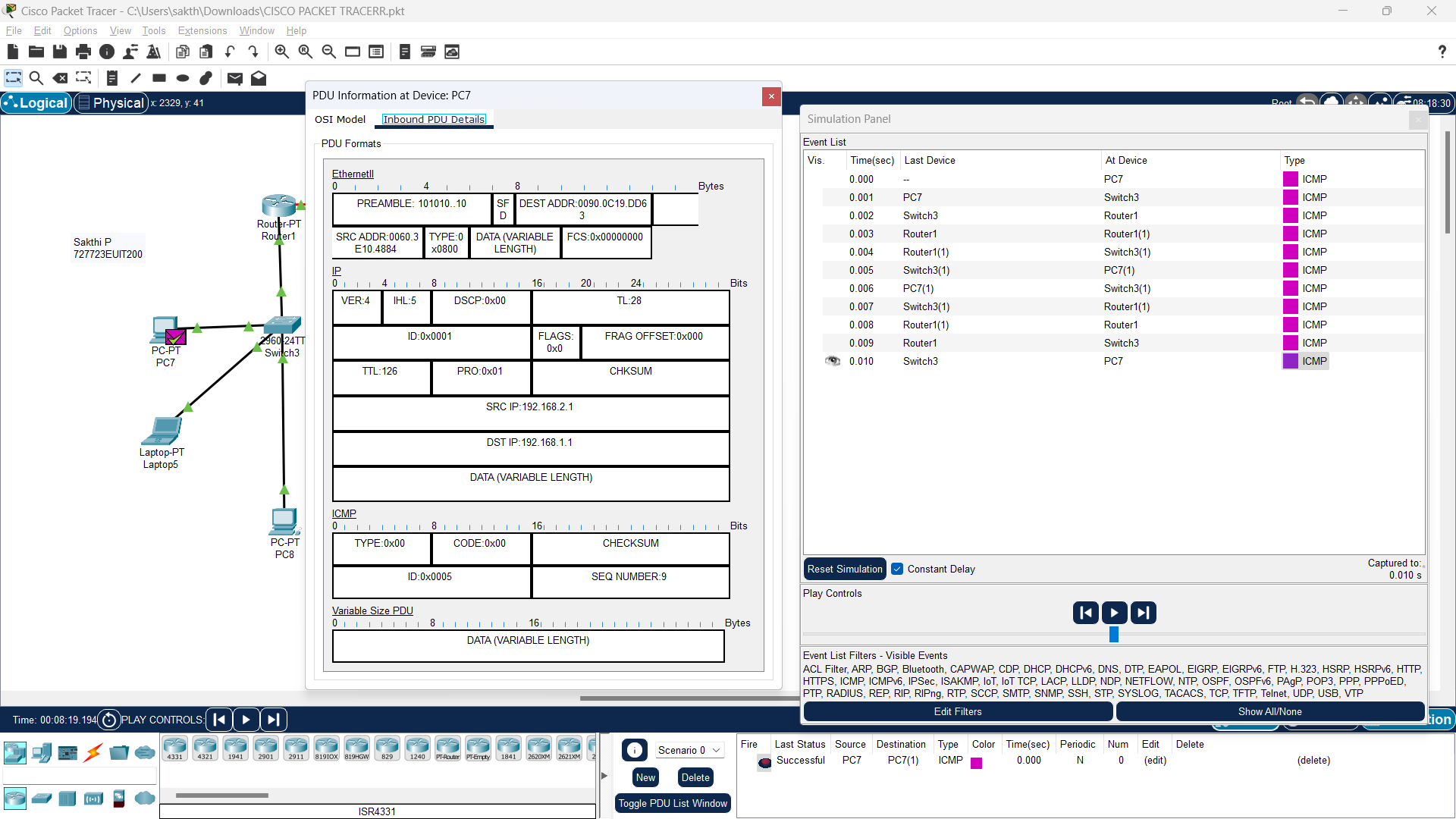
**SIMULATION SCREENSHOTS:**









**Result:**

This experiment demonstrates the implementation of ICMP in a simple Local Area Network (LAN) to check the connectivity between devices, using ping and traceroute tools, effectively diagnose network problems and results were verified successfully