**Ex No: 2**

**Date:**

**SIMULATION OF SIMPLE LAN NETWORK USING CISCO PACKET TRACER TOOL AND DEMONSTRATION OF NETWORK TOOLS SUCH AS PING, TCPDUMP, TRACEROUTE, NETSTAT**.

**AIM:**

To simulate a simple LAN and demonstrate the usage of network tools like Ping, TCPdump, Traceroute and Netstat, in Cisco Packet Tracer software.

**THEORY:**

Creating a Local Area Network (LAN) can involve both wired and wireless components.

**1. Required Equipment**

* **Router**: Central device to manage both wired and wireless connections.
* **Ethernet Switch** (optional): Expands the number of Ethernet ports if needed.Hubs can also be used.
* **Ethernet Cables**: For wired connections (Cat5e, Cat6, or higher for better speeds).
* **Wireless Access Point (WAP)**: If the router doesn't have built-in Wi-Fi, or if you need to extend wireless coverage.
* **Network Devices**: PCs, laptops, smartphones, etc., to connect to the network.

**2. Setting Up the Wired LAN**

* **Position Your Router**: Place your router in a central location if possible. This will optimize the wireless coverage and minimize the length of cables for wired devices.
* **Connect to the Internet**: Connect the router to your modem (if separate) using an Ethernet cable. This provides internet access to the network.
* **Wired Device Connections**: Use Ethernet cables to connect your devices (e.g., computers, printers) to the router. If your router has limited Ethernet ports, connect an Ethernet switch to the router, then connect additional devices to the switch.
* **Configuration**: Access the router's web interface by entering the router's IP address in a browser (commonly 192.168.1.1 or 192.168.2.1). Follow the instructions to set up basic network settings like IP addressing (usually DHCP).

**3. Setting Up the Wireless LAN**

* **Configure the Router's Wi-Fi**: If your router has built-in wireless capabilities, configure the wireless network by setting up an SSID (network name) and a secure password (WPA2 or WPA3 encryption).
* **Connect Wireless Devices**: On each wireless device (e.g., laptops, smartphones), search for the SSID and connect using the password you set.
* **Extending Wireless Coverage (Optional)**: If needed, install additional Wireless Access Points (WAPs) connected to the router via Ethernet cables to extend wireless coverage. Ensure WAPs are configured with the same SSID and security settings to allow seamless roaming between them.

**4. Testing the Network :** This can be done wither by pinging from source host to destination host, or by placing the data packet on the source and destination, and check if simulation is successful.

**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 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.

**CONFIGURING THE NETWORK**

* Now assign ip address to each of the PC and laptops and set the subnet mask to 255.255.255.0.
* Under fastethernet tab when you double click on the PC you will able to see fastethernet and under that set IPv4 Address to the 192.168.1.101, 192.168.1.102, 192.168.1.103, 192.168.1.104, 192.168.1.105 and for laptops 192.168.1.106 and 192.168.1.107.

**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.

## *WIRELESS LAN*

* Select the components that are listed on the left bottom corner.
* Select the Home router from the components under wireless devices and place it on the white screen.
* Place the PC’s and laptops from the components and place it on the white screen. For router select wireless router WRT300N.

**CONFIGURING THE NETWORK**

* Configure the static IPs for the end devices with for eg. 11.0.0.2 , 11.0.0.3 and so on and add corresponding subnet mask as 255.0.0.0. etc
* Now in each of the end devices , make sure to power off and remove the LAN port and add “WMP300N” and then power on the devices.
* In the config section of the wireless router , in Wireless 2.4G section , provide the SSID for the wireless router and add the same SSID in the end devices of the network

**TESTING THE NETWORK**

* Use the ping command in the command prompt to check for successful transmission between the two networks.
* If the IP address gets pinged in other system successfully then the network is working successfully.
* Transmission can also be checked by simulating the particular of transfer of data packet from source to destination.

**DEMONSTRATION OF NETWORK TOOLS:**

**PING Command**

The ping command is a very common method for troubleshooting the accessibility of devices.

It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

* Whether a remote host is active or inactive.
* The round-trip delay in communicating with the host.
* Packet loss.

The ping command first sends an echo request packet to an address, and then waits for a reply.

The ping is successful only if:

* the echo request gets to the destination, and
* The destination is able to get an echo reply back to the source within a predetermined time called a timeout. The default value of this timeout is two seconds on Cisco routers.

# **Tracert (traceroute) Command**

1. The trace route command is used to discover the routes that packets actually take when traveling to their destination. The device (for example, a router or a PC) sends out a sequence of User Datagram Protocol (UDP) data grams to an invalid port address at the remote host.
2. Three data grams are sent, each with a Time-To-Live (TTL) field value set to one. The TTL value of 1 causes the datagram to "timeout" as soon as it hits the first router in the path; this router then responds with an ICMP Time Exceeded Message (TEM) indicating that the datagram has expired.
3. Another three UDP messages are now sent, each with the TTL value set to 2, which causes the second router to return ICMP TEMs. This process continues until the packets actually reach the other destination.
4. Since these data grams are trying to access an invalid port at the destination host, ICMP Port Unreachable Messages are returned, indicating an unreachable port; this event signals the Trace route program that it is finished.

**TCPDump (Packet Capturing and Anayzing):**

tcpdump is a powerful command-line network packet analyzer tool used for capturing and inspecting network traffic. It is widely utilized for network troubleshooting, performance analysis, and security testing. In **Cisco Packet Tracer tool**, this capturing and analyzing the packet transfer, with options of filtering traffic based protocols, is possible in the **simulation mode.**

**Key Features**

* Captures and analyzes packets on a specific network interface.
* Supports filtering traffic based on protocols, IP addresses, ports, etc.
* Provides detailed insights into packet headers.

**Netstat (Network Status and Statistics):**

netstat (network statistics) is a command-line tool used for monitoring and troubleshooting network connections and statistics on a system. It provides information about network interfaces, routing tables, and active connections.

**Key Features**

* Displays active TCP/UDP connections.
* Shows listening ports and their associated processes.
* Provides routing table details.
* Offers network interface statistics.

The **commands could be used in CLI** (command Line Interface) of a router/switch:

**Routing Table Check (show ip route):**

* Use on a router to ensure correct routes are learned or configured for packet forwarding.

**TCP Connection Check (show tcp brief):**

* Use to monitor active TCP sessions handled by the device.

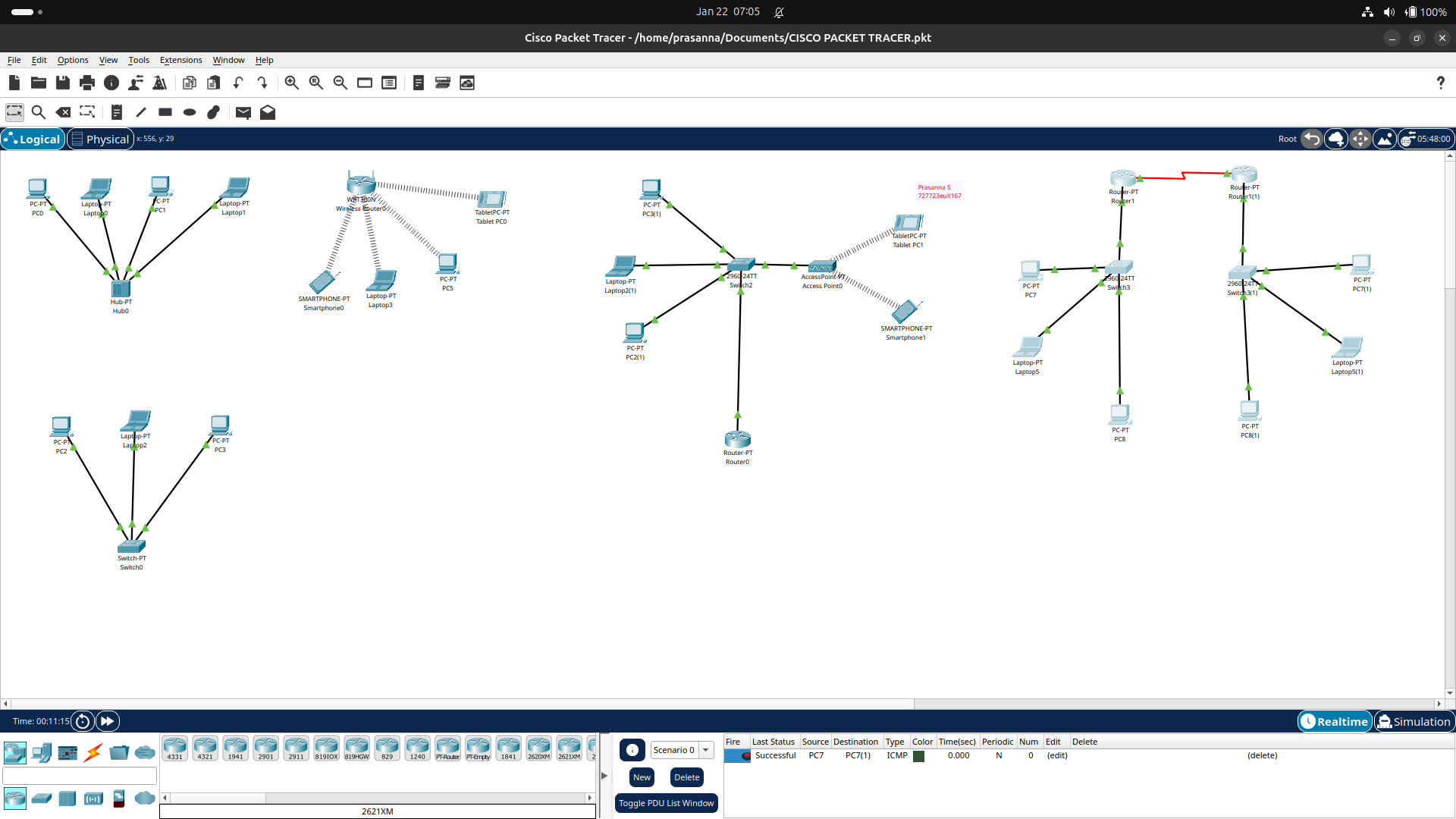
**Interface Status Check (show interfaces):**

* Use on a router or switch to verify the status (up/down) and traffic statistics of interfaces.

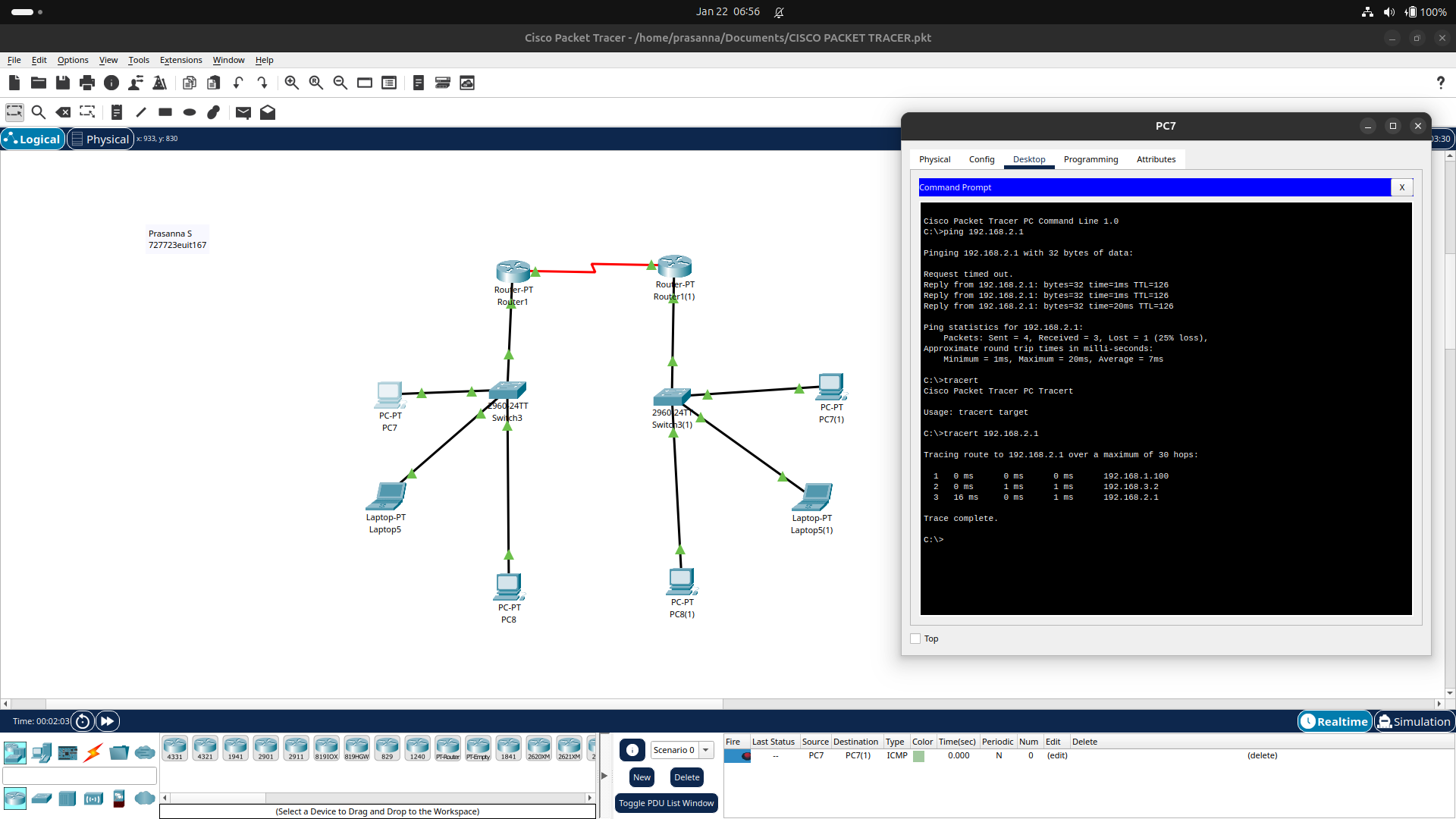
**ARP Table Check (show ip arp):**

* Use on a Layer 3 device to confirm ARP entries for connected devices.

**SIMULATION OUTPUT:**

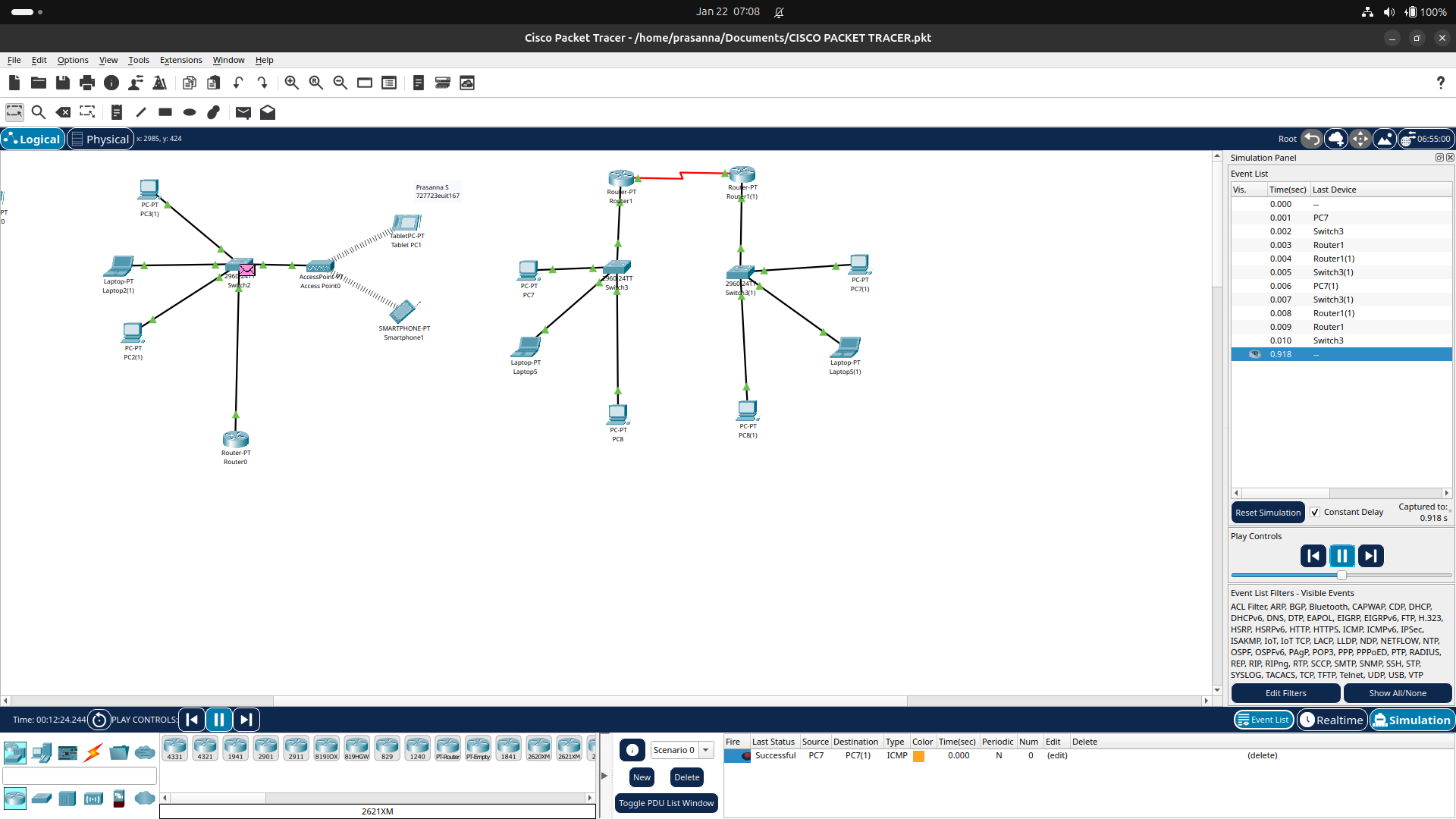


**Ping & tracert commands:**

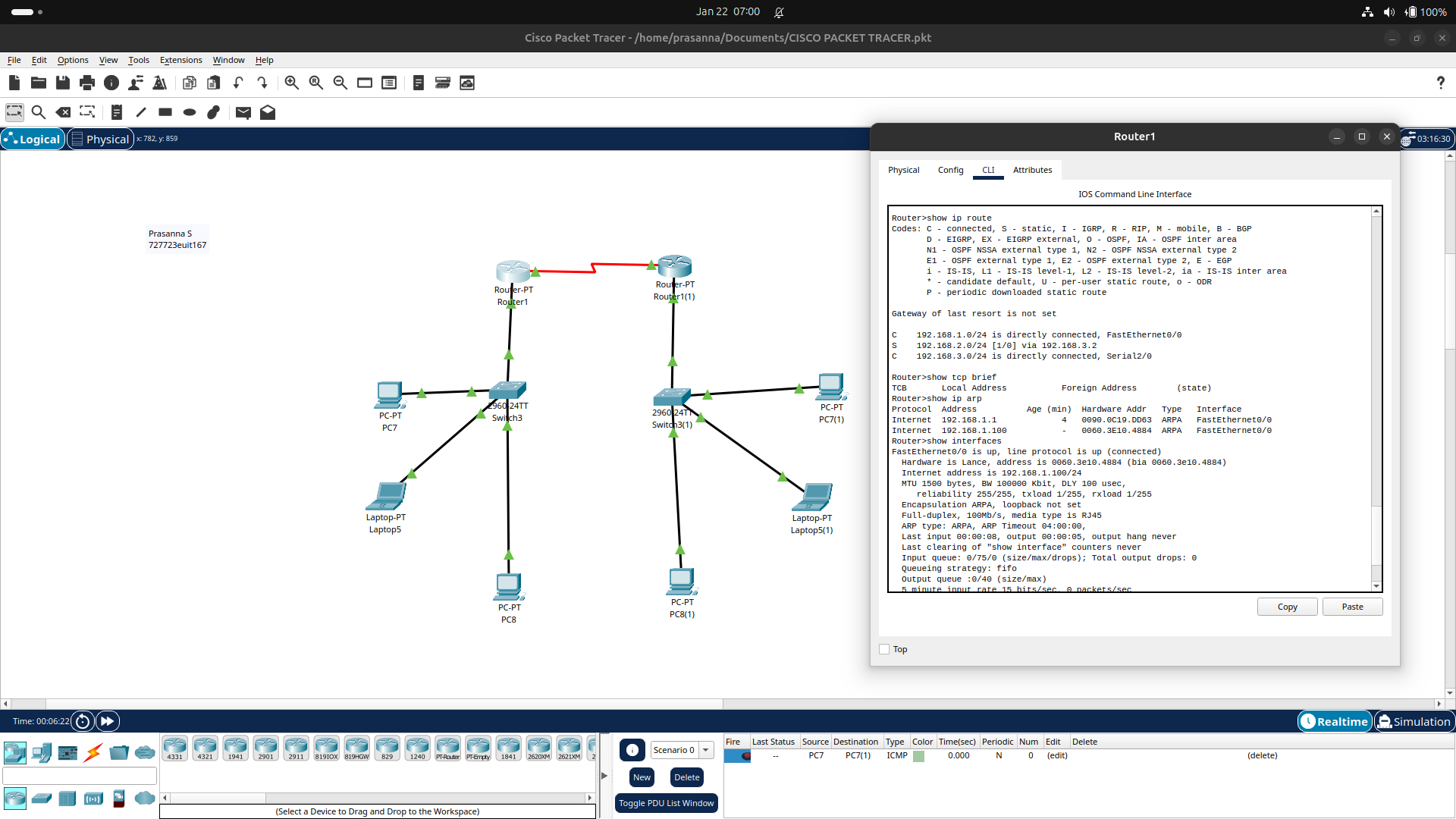


**Packet capturing & Analyzing:**

**­**



**Network status and statistics:**



**RESULT:**

Thus, simple LAN networks, with both wired and wireless communication, were implemented and communication between host devices were established and network tools were tested, among the nodes in the network.