Practical 2 – Computer Networks Lab

Name: Neeraj Belsare

Roll No.: 79

Batch: A4

PRN: 202101040133

Title:

Cisco Packet Tracer

Aim:

Using Cisco packet tracer design different network topologies and Subnet.

Theory:

Network topology refers to the arrangement or configuration of various elements (such as nodes, links, and data transmission devices) in a computer network. The choice of network topology depends on factors like the network's size, purpose, scalability, and fault tolerance.

Physical topology provides an overview of the arrangement of the physical network devices. Logical topology defines the way data transfers in the physical topology. Both are necessary as the network’s overall performance, security, and scalability depend on them.

The **five** most common types of network topologies are:

Bus Topology: In a bus topology, all devices share a common communication channel, making it a simple and cost-effective choice for smaller networks, as devices are daisy-chained along a central cable. However, it's susceptible to cable failures, and its scalability is limited, leading to performance degradation with an increased number of devices.

Star Topology: In a star topology, each device connects directly to a central hub or switch, providing ease of installation and management. This configuration offers robustness, as a failure of one cable or device does not disrupt the entire network, but it relies heavily on the central hub, which, if it fails, can lead to network-wide issues.

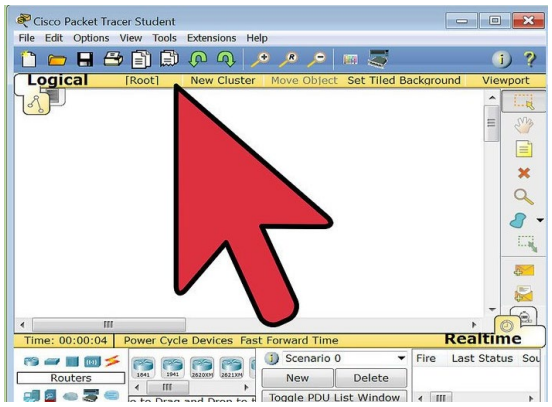
Ring Topology: Ring topology connects devices in a closed loop, with data circulating in one direction. This arrangement ensures predictable performance and uniform data transmission, while cable faults can be easily identified. However, a single device or cable failure can disrupt the entire network, and expansion or modification can be complex.

Mesh Topology: Mesh topology offers high reliability through multiple direct connections between every device, ensuring redundancy and fault tolerance. While it excels in robustness, it's complex to install, and maintain, and costly due to extensive cabling and configuration requirements.

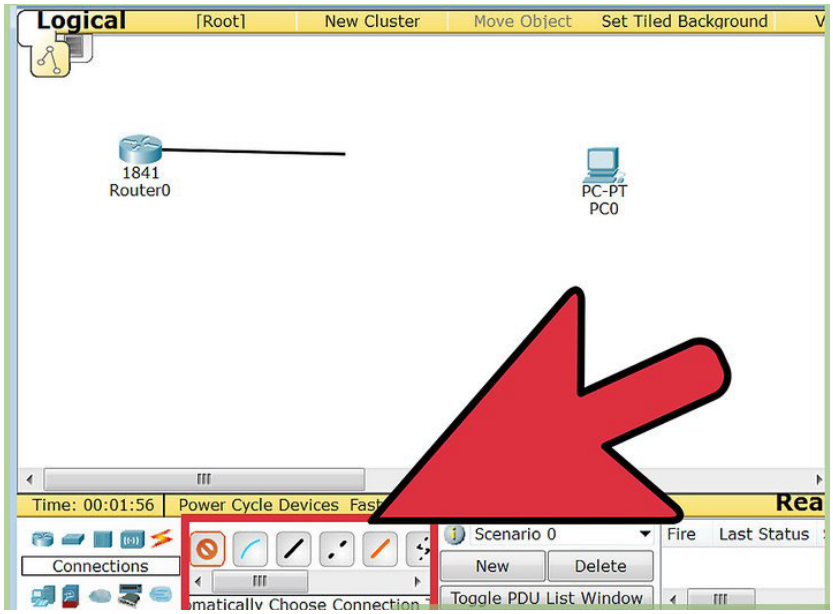
Hybrid Topology: Hybrid topology combines different topology types to balance strengths and weaknesses, offering customization and flexibility for specific network needs. However, its complexity in design and management can be a challenge, potentially driving up costs.

Procedure/code:

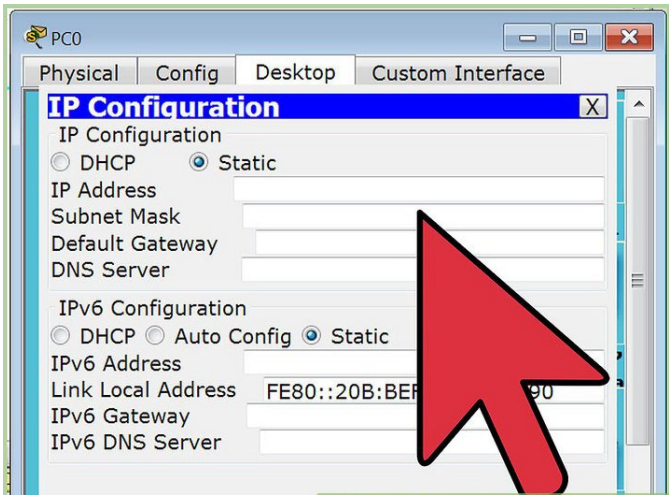
Step 1: Open your Network Topology. Once you've opened your Network Topology on Cisco Packet Tracer, access your network and identify the components of your network, for example; Servers, Routers, End Devices, etc.



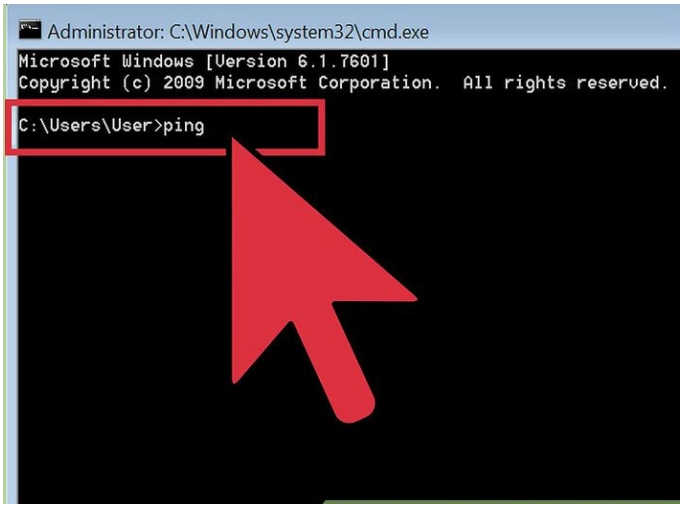
2. **Step 2:** Complete the cabling. Access the cables section and connect completely and correctly the cables between the network in order to ensure connectivity between the devices in the network using the connections table given.



3. Step 3: Configure the IP addresses on the end devices. Using the address table still, correctly and completely configure the IP addresses on all end devices. This can be done by accessing the desktop platform on each device and locating the IP configuration section. The reason for doing this is to enable the devices to be on the right network.

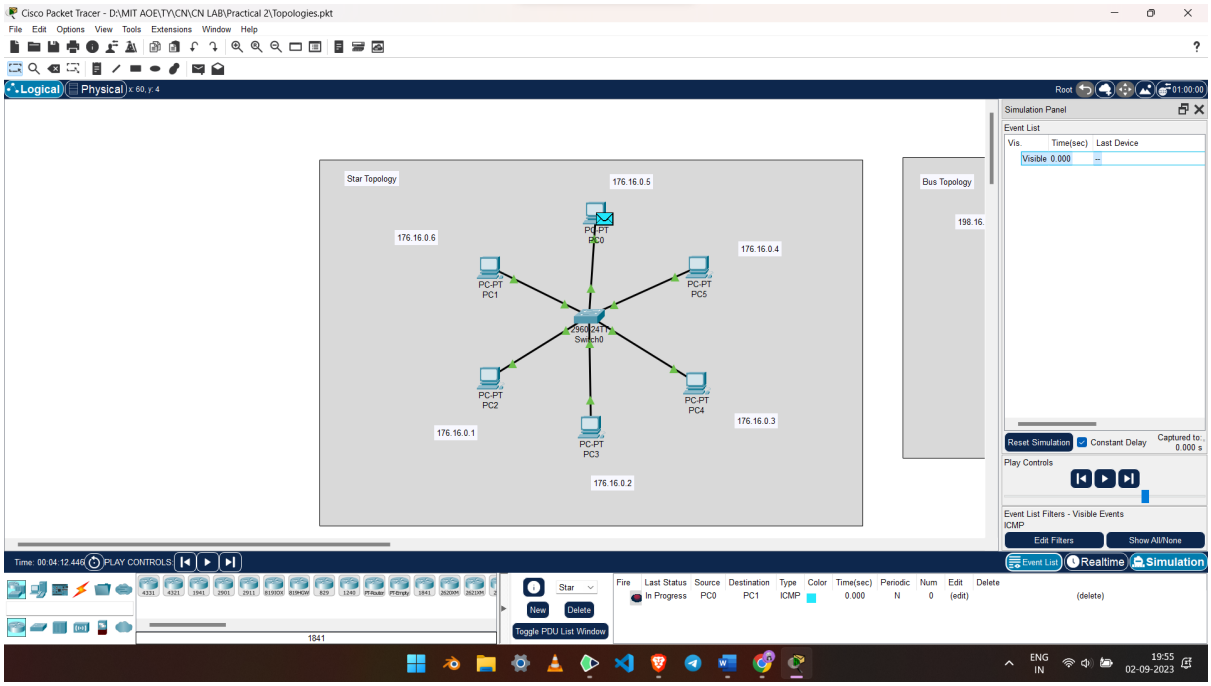


4. Step 4: Test connectivity. After configuring the addresses, you will have to test connectivity by opening a command prompt window on the end devices and try pinging the address on which the network operates. If it gives you a reply, it means your network was configured correctly.

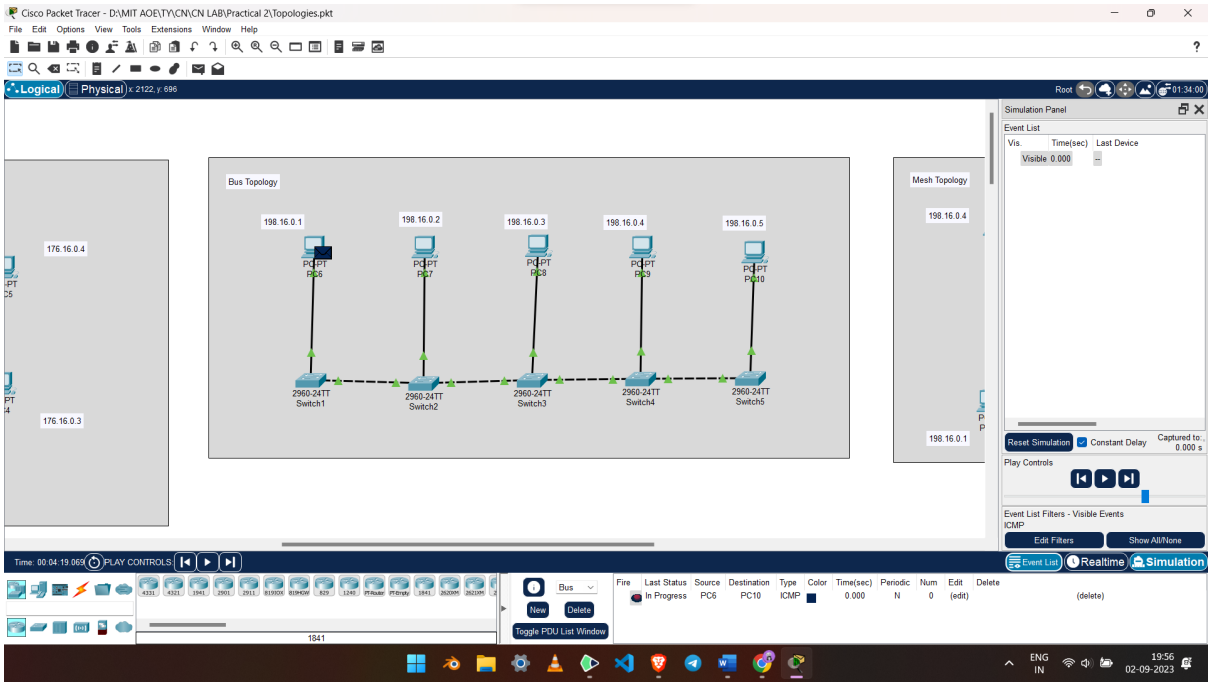


Output:

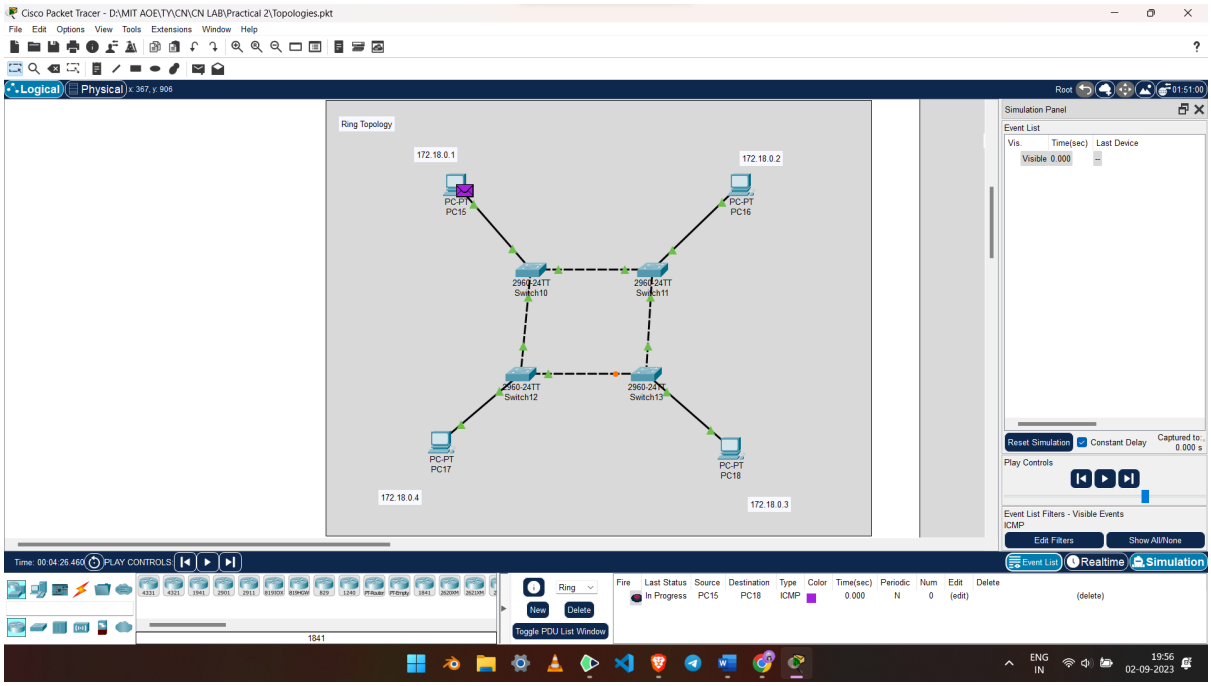
1. Star Topology:



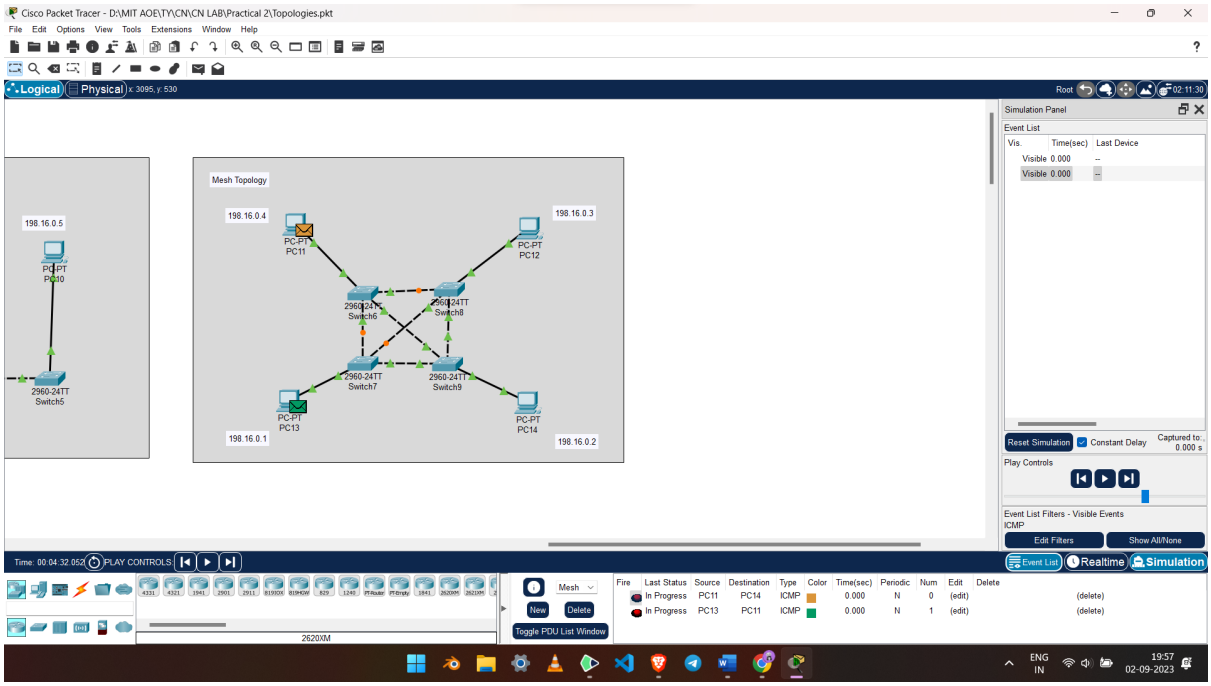
2. Bus Topology:



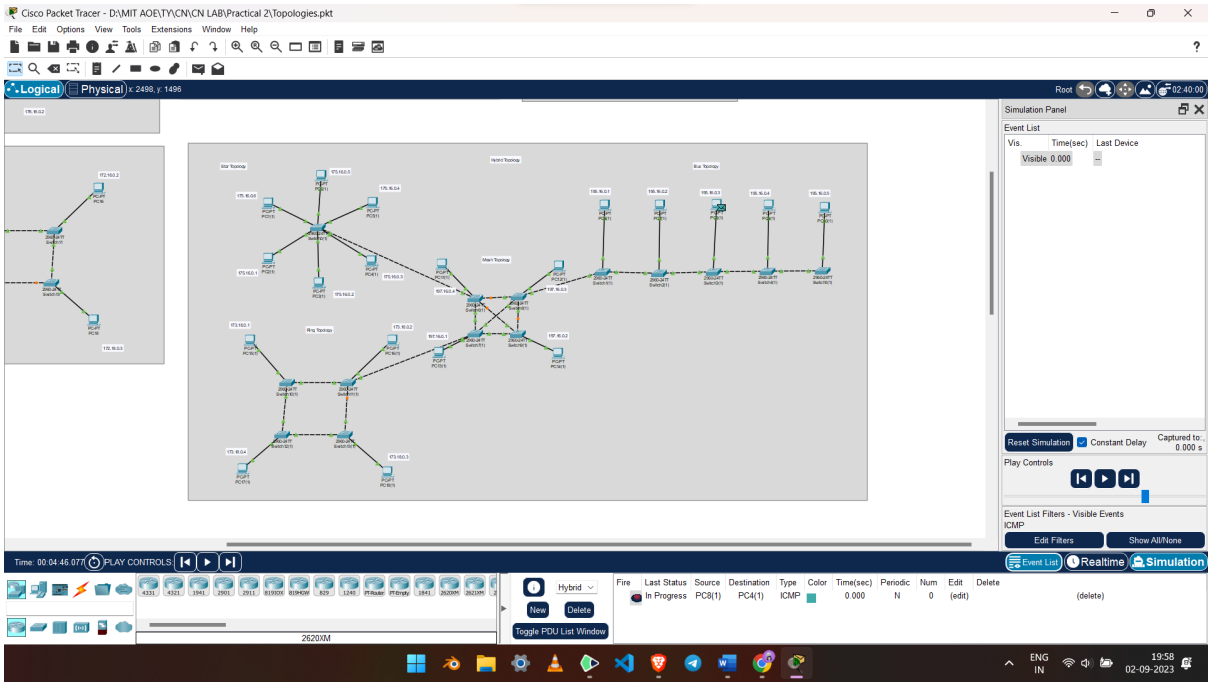
3. Ring Topology:



4. Mesh Topology:



5. Hybrid Topology:



Conclusion:

In conclusion, the practical simulation of various network topologies in Cisco Packet Tracer provided a clear understanding of their respective advantages and limitations. It emphasized the importance of selecting the right topology based on specific network requirements, scalability needs, and fault tolerance considerations. This hands-on experience is invaluable for network administrators in making informed decisions when designing and managing real-world networks.