**Brief overview of the lab objectives:**

In a Cisco Packet Tracer lab, the objectives typically revolve around understanding and implementing network concepts and configurations. Here’s a brief overview of common lab objectives:

1. Network Design and Topology: Learn how to design and implement network topologies, including configuring routers, switches, and other network devices to form a functional network.
2. IP Addressing and Subnetting: Practice assigning IP addresses to devices, configuring subnets, and ensuring proper communication between devices on the same or different subnets.
3. Basic Device Configuration: Get hands-on experience with configuring network devices, such as setting up interfaces, routing protocols, VLANs, and other essential network services.
4. Routing Protocols: Understand and configure different routing protocols like RIP, OSPF, and EIGRP to enable dynamic routing and efficient network communication.
5. Switching and VLANs: Learn about VLAN creation, configuration, and trunking to segment network traffic and manage broadcast domains effectively.
6. Network Security: Implement security features such as access control lists (ACLs), port security, and secure management protocols to protect the network from unauthorized access and threats.
7. Troubleshooting and Verification: Develop skills to troubleshoot network issues, verify configurations, and ensure that all network components are functioning as intended.
8. WAN Technologies: Explore and configure WAN technologies like PPP, HDLC, and VPNs to connect remote sites and extend the network.

**Steps taken to set up the network:**

● Procedure:

1. Open Packet Tracer:

■ Launch Cisco Packet Tracer on your computer.

■ Familiarize yourself with the interface, including the workspace, device

selection, and tools.

2. Create a Simple Network:

■ Drag two computers (PC-PT) onto the workspace.

■ Drag a switch (Switch-PT) onto the workspace.

■ Connect each computer to the switch using straight-through Ethernet

cables.

3. Configure IP Addresses:

■ Click on the first computer, go to the Desktop tab, and select IP

Configuration.

■ Assign an IP address (e.g., 192.168.1.1) and a subnet mask (e.g.,

255.255.255.0).

■ Click on the second computer, go to the Desktop tab, and select IP

Configuration.

■ Assign an IP address (e.g., 192.168.1.2) and a subnet mask (e.g.,

255.255.255.0).

4. Test Peer-to-Peer Communication:

■ On the first computer, open the Command Prompt from the Desktop tab. ■

Use the ping command to test connectivity to the second computer (e.g.,

ping 192.168.1.2). ● Procedure:

1. Open Packet Tracer:

■ Launch Cisco Packet Tracer on your computer.

■ Familiarize yourself with the interface, including the workspace, device

selection, and tools.

2. Create a Simple Network:

■ Drag two computers (PC-PT) onto the workspace.

■ Drag a switch (Switch-PT) onto the workspace.

■ Connect each computer to the switch using straight-through Ethernet

cables.

3. Configure IP Addresses:

■ Click on the first computer, go to the Desktop tab, and select IP

Configuration.

■ Assign an IP address (e.g., 192.168.1.1) and a subnet mask (e.g.,

255.255.255.0).

■ Click on the second computer, go to the Desktop tab, and select IP

Configuration.

■ Assign an IP address (e.g., 192.168.1.2) and a subnet mask (e.g.,

255.255.255.0).

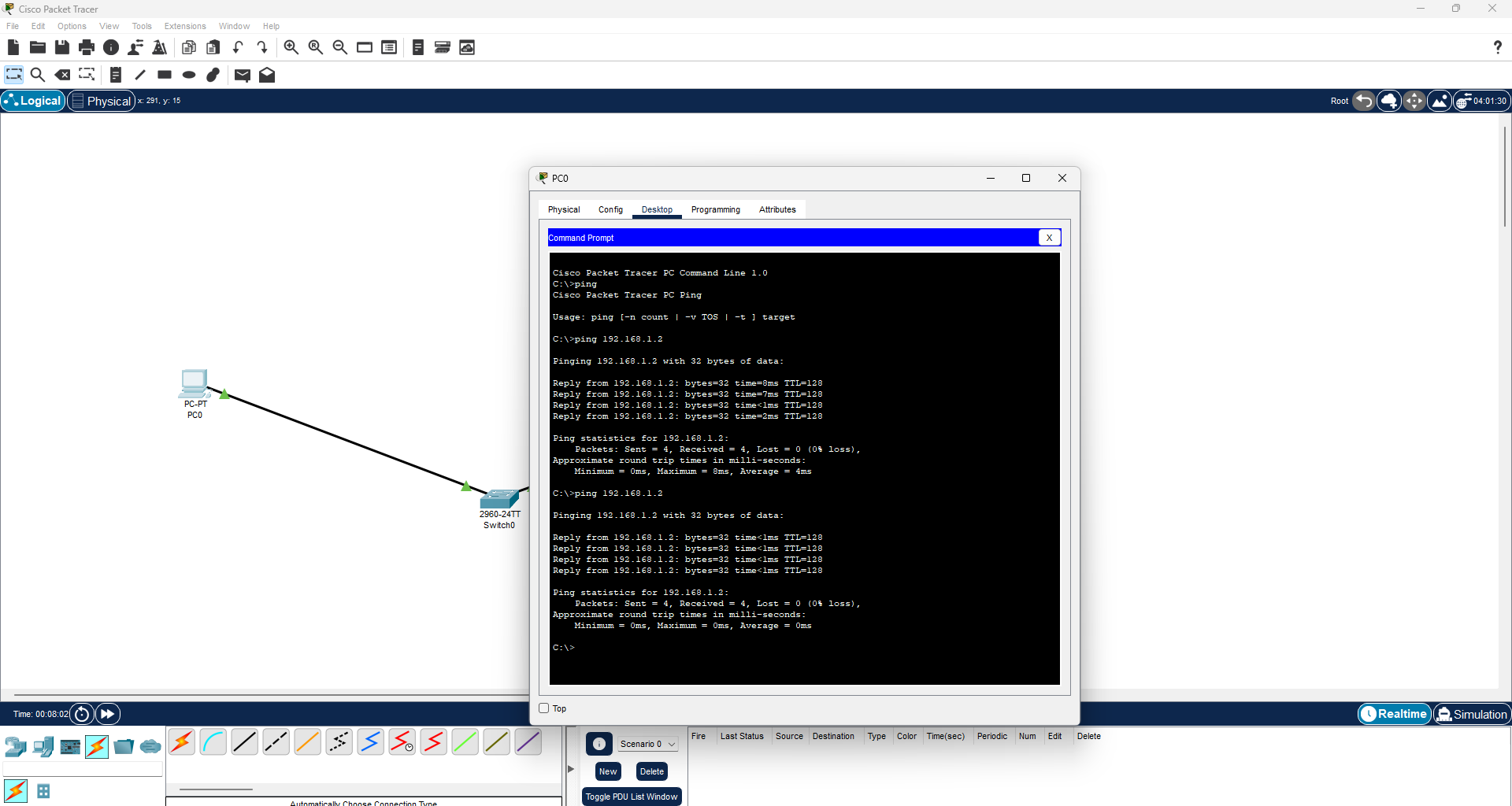
4. Test Peer-to-Peer Communication:

■ On the first computer, open the Command Prompt from the Desktop tab. ■

Use the ping command to test connectivity to the second computer (e.g.,

ping 192.168.1.2).

**Screenshots of configurations and successful ping results**

* ****

**Summary of what you learned from the lab:**

In a Cisco Packet Tracer lab, you typically learn several key concepts and skills essential for managing and troubleshooting networks. Here’s a summary of what you might learn:

1. Network Topology and Design: You gain experience designing and setting up network topologies, including connecting various network devices like routers and switches to form a cohesive network.
2. IP Addressing and Subnetting: You learn how to assign IP addresses correctly, create subnet masks, and segment networks to ensure proper communication and efficient use of IP space.
3. Device Configuration: You become proficient in configuring network devices, including setting up interfaces, routing protocols, VLANs, and other network services essential for network operation.
4. Routing Protocols: You understand and implement various routing protocols (such as RIP, OSPF, and EIGRP), learning how they enable dynamic routing and how to configure them for optimal network performance.
5. Switching and VLANs: You learn to configure VLANs and switch ports, understanding how VLANs help in network segmentation and reducing broadcast traffic within a network.
6. Network Security: You develop skills in applying security measures like ACLs, port security, and secure management practices to protect the network from unauthorized access and potential threats.
7. Troubleshooting and Verification: You practice troubleshooting network issues and verifying configurations using diagnostic tools and commands, which helps in ensuring that the network functions correctly and resolving any problems that arise.
8. WAN Technologies: You explore and configure WAN technologies, including setting up point-to-point protocols, HDLC, and VPNs to connect and manage remote network sites.