**Computer Networks LAB-1: Introduction to Packet Tracer, Peer-to-Peer Communication, Study of Cables and its Colour Codes**

**Objective**:

* To familiarize students with Cisco Packet Tracer.
* To set up a peer-to-peer (P2P) communication network.
* To study different types of network cables and their color codes.
* To document the observations and save the configuration file in a GitHub repository.

**Requirements**:

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission.

**Instructions:**

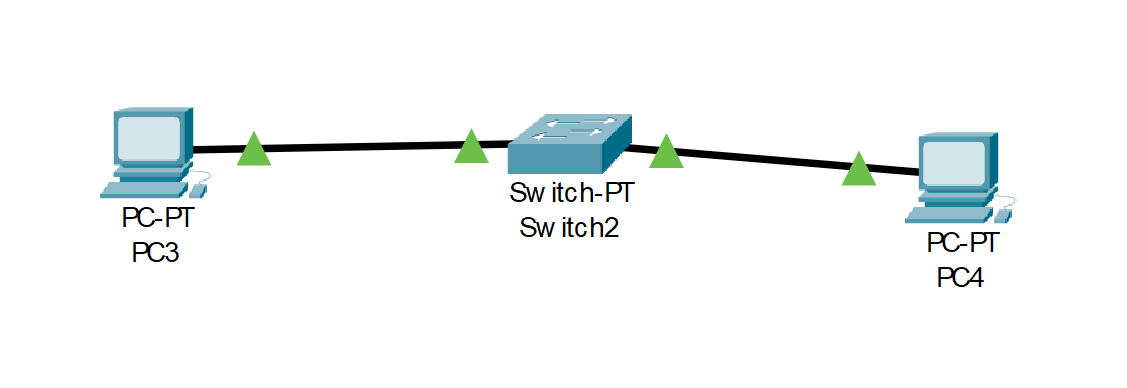
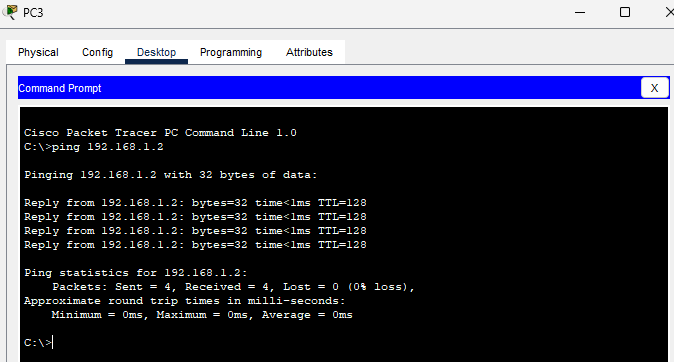
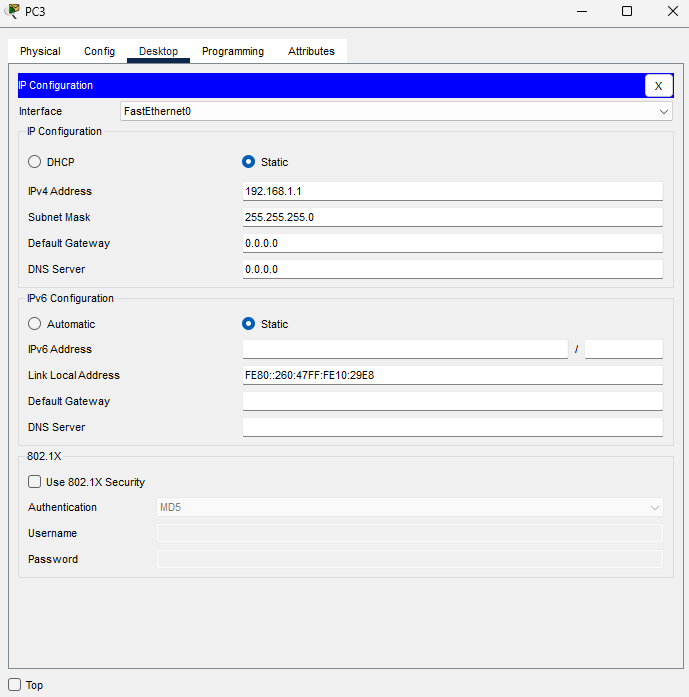
**Part 1: Introduction to Packet Tracer**

* Ensure you have Cisco Packet Tracer installed on your computer. If not, download it from the Cisco Networking Academy website.
* Open Packet Tracer and explore the user interface. Familiarize yourself with different tools and components available in the software.

**Part 2: Peer-to-Peer Communication Setup**

* Open Packet Tracer and create a new network.
* Add two PCs to the workspace.
* Use a copper straight-through cable to connect the FastEthernet0 port of PC0 to the FastEthernet0 port of PC1.
* Assign IP addresses to both PCs:
* PC0: IP address: 192.168.1.1, Subnet Mask: 255.255.255.0
* PC1: IP address: 192.168.1.2, Subnet Mask: 255.255.255.0
* Open the command prompt on PC0 and ping PC1 using the command ping 192.168.1.2.
* Take a screenshot of the successful ping results.

**Results:**



**Study of Network Cables and Color Codes**

**Types of Network Cables in Computer Networking**

1. **Copper Cables**
   * **Straight-Through Cable**
     + Purpose: Used to connect different types of devices, such as a computer to a switch or a switch to a router.
     + Structure: The wiring is consistent on both ends of the cable, meaning Pin 1 is connected to Pin 1, Pin 2 to Pin 2, and so on.
     + Common Use: Connecting a computer to a network device like a hub, switch, or router.
   * **Crossover Cable**
     + Purpose: Used to connect similar devices directly, such as connecting two computers or two switches without a hub or switch.
     + Structure: The wiring is crossed on the ends of the cable, where Pin 1 is connected to Pin 3 and Pin 2 to Pin 6.
     + Common Use: Connecting two similar network devices directly, such as PC-to-PC or switch-to-switch.
   * **Shielded Twisted Pair (STP) Cable**
     + Purpose: Provides more protection against electromagnetic interference (EMI) and crosstalk.
     + Structure: Similar to UTP but with an additional shielding layer.
     + Common Use: Environments with high EMI, such as industrial settings or places with many electronic devices.
   * **Unshielded Twisted Pair (UTP) Cable**
     + Purpose: The most common type of copper cable used in networks, without additional shielding.
     + Structure: Consists of pairs of wires twisted together.
     + Common Use: General network cabling, including both straight-through and crossover cables.
2. **Fiber Optic Cables**
   * **Single-Mode Fiber (SMF)**
     + Purpose: Used for long-distance communication, typically in telecom networks.
     + Structure: Uses a single strand of glass fiber to carry data via light waves.
     + Common Use: Long-distance data transmission, such as between buildings or across cities.
   * **Multi-Mode Fiber (MMF)**
     + Purpose: Used for shorter distances, like within a building or between buildings on the same campus.
     + Structure: Uses multiple light paths to carry data, allowing for more data to be transmitted over shorter distances.
     + Common Use: Data centers, LAN backbones, and other short-distance applications.

**Standard Color Codes for Copper Straight-Through and Crossover Cables**

**Straight-Through Cable (TIA/EIA-568-B Standard):**

* Pin 1: White/Orange
* Pin 2: Orange
* Pin 3: White/Green
* Pin 4: Blue
* Pin 5: White/Blue
* Pin 6: Green
* Pin 7: White/Brown
* Pin 8: Brown

**Crossover Cable:**

* **End 1 (TIA/EIA-568-B Standard):**
  + Pin 1: White/Orange
  + Pin 2: Orange
  + Pin 3: White/Green
  + Pin 4: Blue
  + Pin 5: White/Blue
  + Pin 6: Green
  + Pin 7: White/Brown
  + Pin 8: Brown
* **End 2 (TIA/EIA-568-A Standard):**
  + Pin 1: White/Green
  + Pin 2: Green
  + Pin 3: White/Orange
  + Pin 4: Blue
  + Pin 5: White/Blue
  + Pin 6: Orange
  + Pin 7: White/Brown
  + Pin 8: Brown

**Purpose and Use Cases of Each Type of Cable**

1. **Straight-Through Cable:**
   * Purpose: Primarily used for connecting different types of devices within a network.
   * Use Cases: Connecting computers to switches, switches to routers, or computers to hubs.
2. **Crossover Cable:**
   * Purpose: Enables direct communication between two similar devices without an intermediary device.
   * Use Cases: Directly connecting two computers, two switches, or two routers for data transfer.
3. **Fiber Optic Cables:**
   * **Single-Mode Fiber (SMF):**
     + Purpose: For high-speed, long-distance data transmission.
     + Use Cases: Telecommunications, connecting different buildings within a campus, or connecting cities.
   * **Multi-Mode Fiber (MMF):**
     + Purpose: For high-speed data transmission over shorter distances.
     + Use Cases: Data centers, LAN backbones, and other applications where high bandwidth over shorter distances is required.

**Computer Networks – LAB 2: Implementation of Network Topologies**

**Objective:**

* To explore and implement various network topologies using Cisco Packet Tracer.
* To understand the use of different network cables and their appropriate connections.
* To assign IP addresses and test connectivity within each topology.
* To document the setup and save the Packet Tracer files for future reference.

**Requirements:**

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission

**Procedure:**

1. Open Packet Tracer:

* Launch Cisco Packet Tracer on your computer.

2. Implement a Bus Topology:

* Drag three computers onto the workspace.
* Connect them using a single backbone cable (Coaxial Cable).

3. Implement a Star Topology:

* Drag three computers and a switch onto the workspace.
* Connect each computer to the switch using straight-through Ethernet

cables.

4. Implement a Ring Topology:

* Drag three computers onto the workspace.
* Connect them in a circular manner using crossover cables.

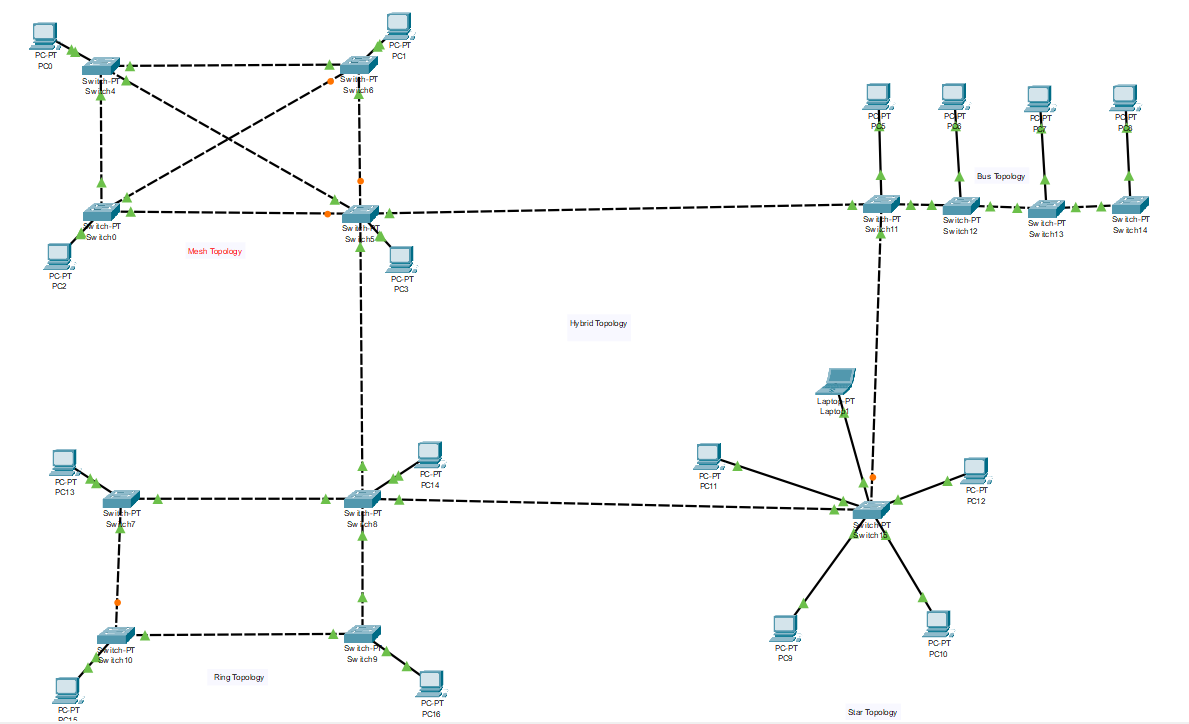
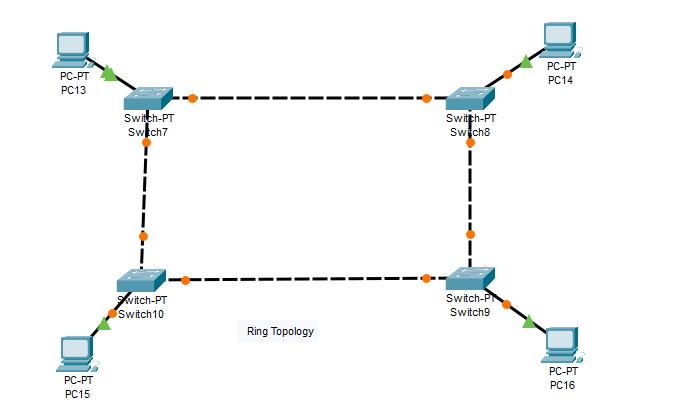
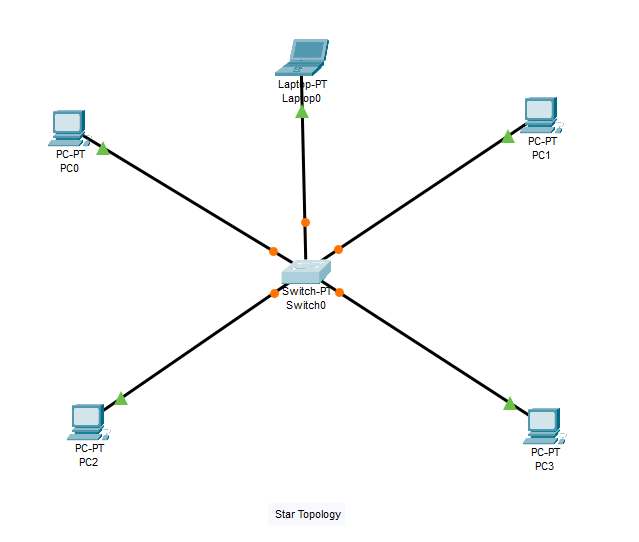
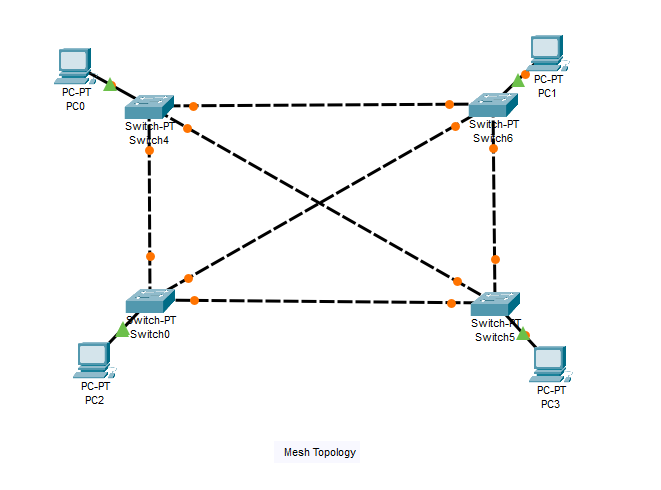
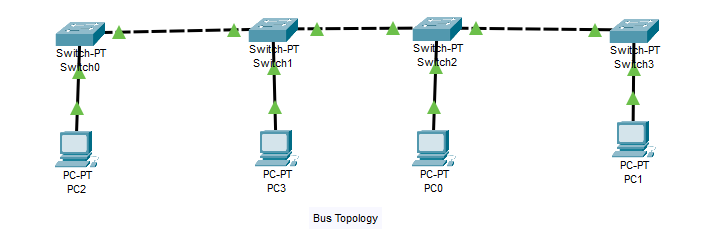
5. Implement a Mesh Topology:

* Drag three computers onto the workspace.
* Connect each computer to every other computer using crossover cables.

6. Test Connectivity:

* For each topology, assign IP addresses to the computers.
* Use the ping command to test connectivity between all computers.

**Results:**



**Computer Networks – LAB 3: Router Configuration (Creating Passwords, Configuring Interfaces)**

**Objective:**

* To configure a router and PCs using Cisco Packet Tracer.
* To establish network connectivity between two PCs through a router.
* To assign IP addresses and configure router interfaces for communication.
* To simulate and verify data transfer between PCs using Packet Tracer.

**Requirements:**

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission

**Procedure:**

Step 1: Configuring Router1

1. Select the router and open CLI.

2. Press ENTER to start configuring Router1.

3. Activate privileged mode:

* Type enable

4. Access the configuration menu:

* Type config t (configure terminal)

5. Configure interfaces of Router1:

* FastEthernet0/0:
  + Type interface FastEthernet0/0
  + Configure with the IP address 192.168.10.1 and Subnet mask 255.255.255.0
* FastEthernet0/1:
  + Type interface FastEthernet0/1
* Configure with the IP address 192.168.20.1 and Subnet mask 255.255.255.0

6. Finish configuration:

* Type no shutdown to activate the interfaces

Step 2: Configuring PCs

1. Assign IP addresses to each PC:

PC0:

Go to the desktop, select IP Configuration, and assign the following:

* IP address: 192.168.10.2
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.10.1

PC1:

Go to the desktop, select IP Configuration, and assign the following:

* IP address: 192.168.20.2
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.20.1

Step 3: Connecting PCs with Router

1. Connect the devices using copper straight-through cables:

* Connect FastEthernet0 port of PC0 to FastEthernet0/0 port of Router1
* Connect FastEthernet0 port of PC1 to FastEthernet0/1 port of Router1

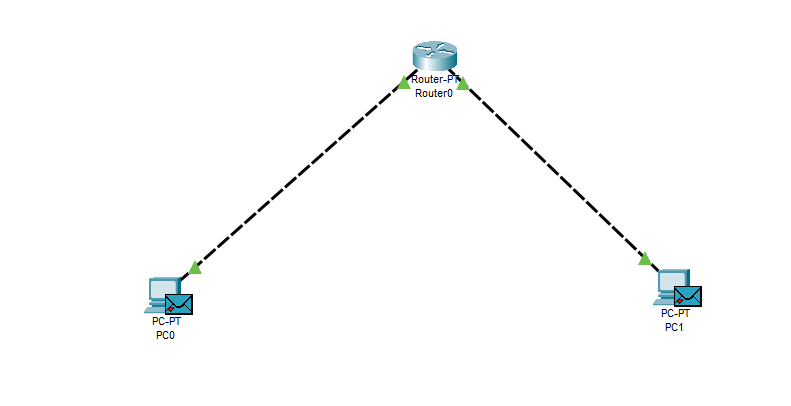
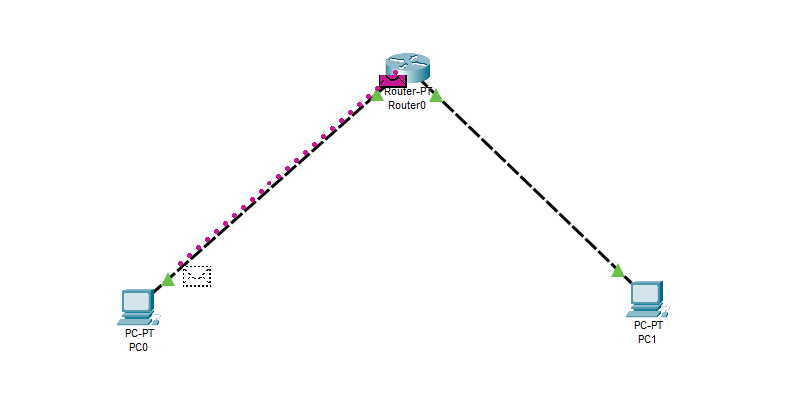
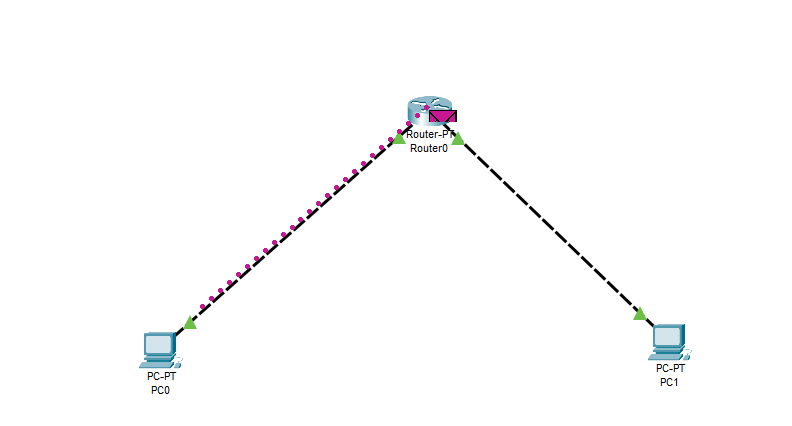
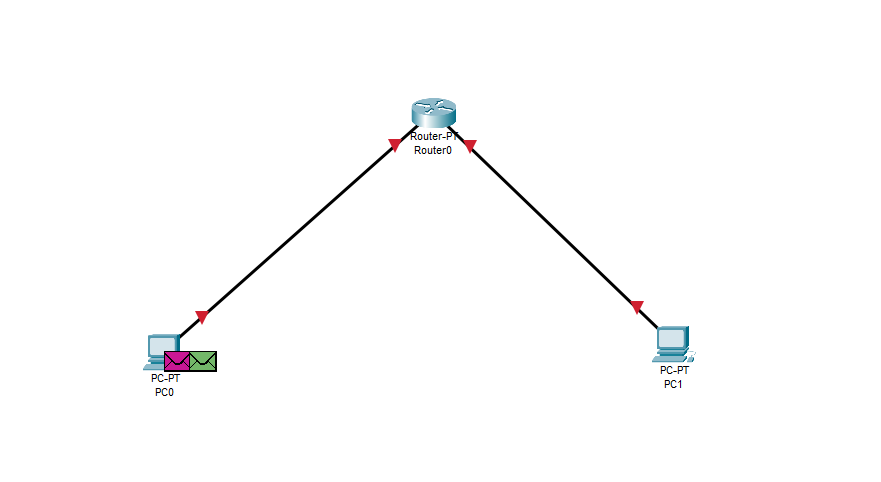
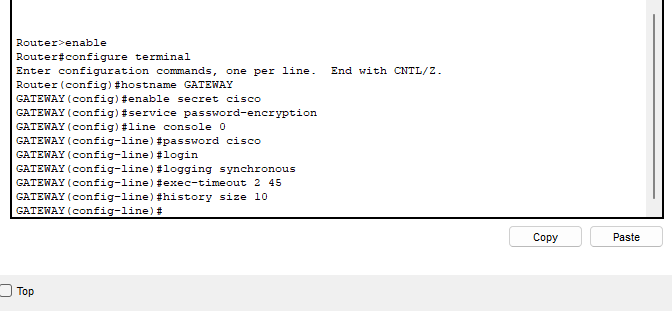
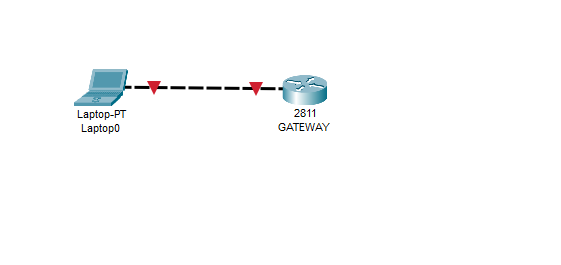
**Simulation of Designed Network Topology**

Sending a PDU from PC0 to PC1

1. Open the simulation mode in Packet Tracer.

2. Send a PDU from PC0 to PC1:

○ Observe the packet traveling from PC0 to the router and then to PC1.

**Results:** 

**Summary of Lab Learnings:**

In this lab, we successfully configured a basic network using Cisco Packet Tracer, involving a router and two PCs. The key learnings include:

1. **Router Configuration:** We learned how to access and configure router interfaces using the CLI, including assigning IP addresses and activating the interfaces.
2. **PC Configuration:** We practiced setting up the IP configuration on PCs, including assigning IP addresses, subnet masks, and default gateways, ensuring proper communication within the network.
3. **Cable Selection and Connectivity:** We explored the use of copper straight-through cables to connect PCs to the router, reinforcing the importance of selecting the correct cable type for different connections.
4. **Network Topology Simulation:** We tested network connectivity by sending a PDU from one PC to another, demonstrating the router's ability to route traffic between different network segments.

**Computer Networks – LAB 4: Addressing and Subnetting (VLSM) with Cisco Packet Tracer**

**Objective:**

* To configure a network using Variable Length Subnet Masking (VLSM) to optimize IP address utilization.
* To design and implement subnets of different sizes based on network requirements.
* To configure routers and PCs with the appropriate IP addresses and subnet masks.
* To simulate and verify end-to-end connectivity within the network using Cisco Packet Tracer.

**Requirements:**

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission

**Procedure:**

Network Design and Subnetting:

1. Design the network topology:

* Determine the IP address requirements for each subnet.
* Calculate the subnet addresses using VLSM.

Step 1: Subnetting the Network

1. Identify the major network address:

* Example: 192.168.0.0/24

2. Determine the number of subnets and their sizes:

* Subnet 1 (e.g., 50 hosts): Network Address: 192.168.0.0/26 (Subnet Mask: 255.255.255.192)
* Subnet 2 (e.g., 30 hosts): Network Address: 192.168.0.64/27 (Subnet Mask: 255.255.255.224)
* Subnet 3 (e.g., 10 hosts): Network Address: 192.168.0.96/28 (Subnet Mask: 255.255.255.240)
* Subnet 4 (e.g., 5 hosts): Network Address: 192.168.0.112/29 (Subnet Mask: 255.255.255.248)

Step 2: Configuring Router1

1. Select the router and open CLI.

2. Press ENTER to start configuring Router1.

3. Activate privileged mode:

* Type enable

4. Access the configuration menu:

* Type config t (configure terminal)

5. Configure interfaces of Router1:

○ FastEthernet0/0:

* Type interface FastEthernet0/0
* Configure with the IP address 192.168.0.1 and Subnet mask 255.255.255.192

○ FastEthernet0/1:

* Type interface FastEthernet0/1
* Configure with the IP address 192.168.0.65 and Subnet mask 255.255.255.224

6. Finish configuration:

* Type no shutdown to activate the interfaces

Step 3: Configuring PCs

1. Assign IP addresses to each PC:

○ PC0:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.0.2

■ Subnet Mask: 255.255.255.192

■ Default Gateway: 192.168.0.1

○ PC1:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.0.66

■ Subnet Mask: 255.255.255.224

■ Default Gateway: 192.168.0.65

Step 4: Connecting PCs with Router

1. Connect the devices using copper straight-through cables:

* Connect FastEthernet0 port of PC0 to FastEthernet0/0 port of Router1
* Connect FastEthernet0 port of PC1 to FastEthernet0/1 port of Router1

Configuration Tables

Simulation of Designed Network Topology

Sending a PDU from PC0 to PC1

1. Open the simulation mode in Packet Tracer.

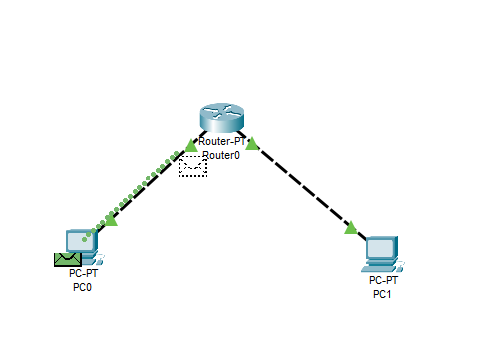
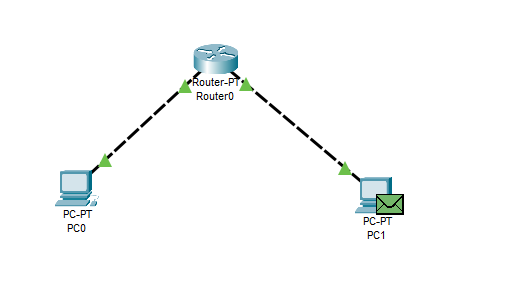
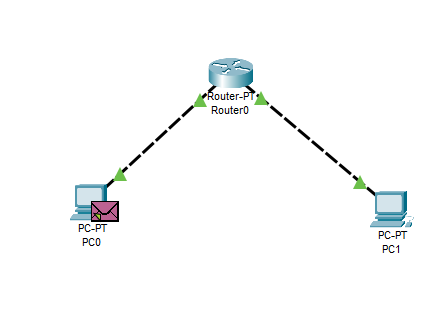
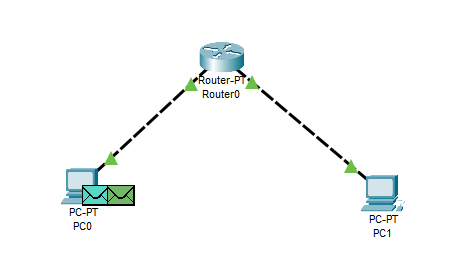
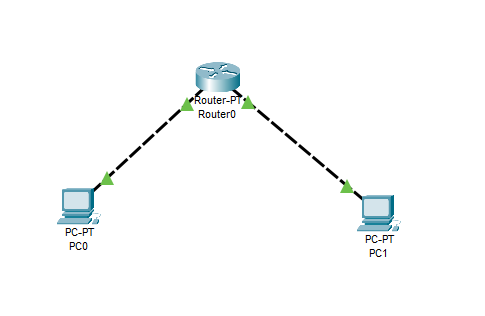
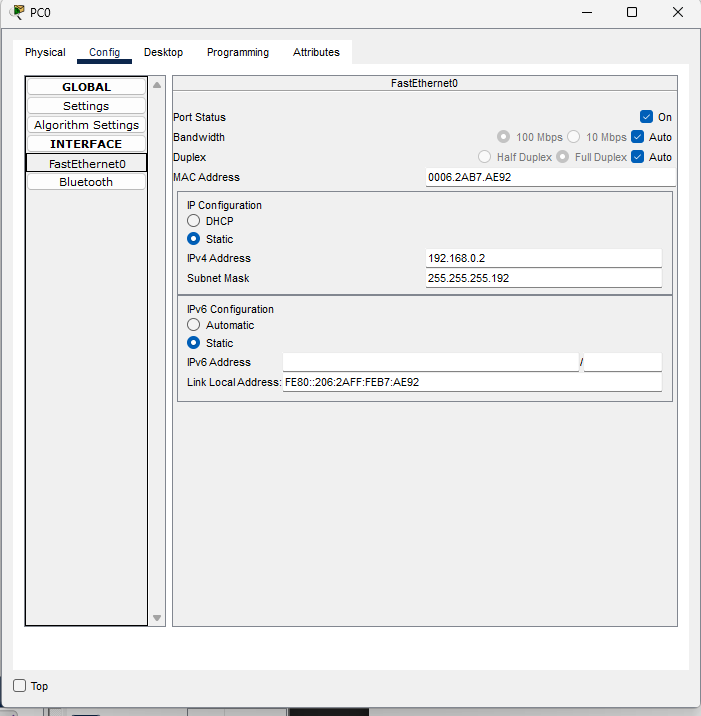
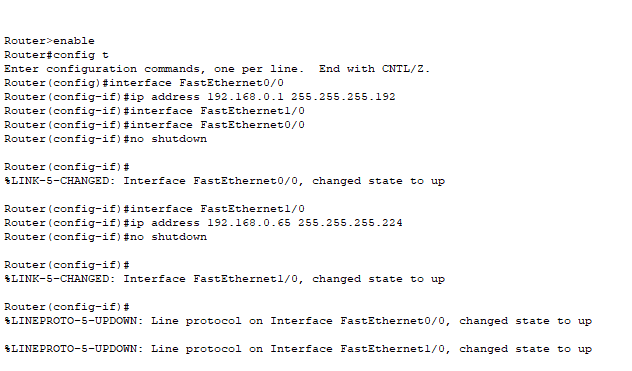
2. Send a PDU from PC0 to PC1:

* Observe the packet traveling from PC0 to the router and then to PC1.

Acknowledgment from PC1 to PC0

1. Observe the acknowledgment packet:

* Ensure that the acknowledgment packet travels back from PC1 to PC0, confirming successful communication.

**Results:** 

**Conclusions:**

In this experiment, we successfully demonstrated the use of Variable Length Subnet Masking (VLSM) to create an efficient network design by optimizing IP address allocation. By configuring routers and PCs with appropriate IP addresses and subnet masks, we established a functional network topology with subnets of varying sizes tailored to specific requirements. The simulation in Cisco Packet Tracer verified that the network was correctly configured, enabling smooth and successful communication between devices. This exercise reinforced the importance of VLSM in managing IP address space efficiently, particularly in networks with diverse size requirements.

**Computer Networks – LAB 5: Static and Default Routing**

**Objective:**

* To configure static and default routing on routers using Cisco Packet Tracer.
* To establish communication between different network segments through proper routing configurations.
* To test and verify successful data transfer and connectivity between PCs in different subnets using the configured routes.

**Requirements:**

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission

**Procedure:**

Network Design:

* Router1 connected to Router2.
* PC0 connected to Router1.
* PC1 connected to Router2.

Step 1: Configure Network Addresses

1. Determine IP address scheme:

* Router1 to Router2 link: 192.168.1.0/30
* PC0 Network: 192.168.10.0/24
* PC1 Network: 192.168.20.0/24

Step 2: Configuring Router1

1. Select Router1 and open CLI.

2. Press ENTER to start configuring Router1.

3. Activate privileged mode:

* Type enable

4. Access the configuration menu:

* Type config t (configure terminal)

5. Configure interfaces of Router1:

○ FastEthernet0/0 (connected to PC0):

* Type interface FastEthernet0/0
* Configure with the IP address 192.168.10.1 and Subnet mask 255.255.255.0

○ Serial0/0/0 (connected to Router2):

* Type interface Serial0/0/0
* Configure with the IP address 192.168.1.1 and Subnet mask 255.255.255.252

6. Activate interfaces:

* Type no shutdown

Step 3: Configuring Router2

1. Select Router2 and open CLI.

2. Press ENTER to start configuring Router2.

3. Activate privileged mode:

○ Type enable

4. Access the configuration menu:

○ Type config t (configure terminal)

5. Configure interfaces of Router2:

○ FastEthernet0/0 (connected to PC1):

■ Type interface FastEthernet0/0

■ Configure with the IP address 192.168.20.1 and Subnet mask 255.255.255.0

○ Serial0/0/0 (connected to Router1):

■ Type interface Serial0/0/0

■ Configure with the IP address 192.168.1.2 and Subnet mask 255.255.255.252

6. Activate interfaces:

* Type no shutdown

Step 4: Configuring PCs

1. Assign IP addresses to each PC:

○ PC0:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.10.2

■ Subnet Mask: 255.255.255.0

■ Default Gateway: 192.168.10.1

○ PC1:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.20.2

■ Subnet Mask: 255.255.255.0

■ Default Gateway: 192.168.20.1

Step 5: Static Routing Configuration

1. Configure static routes on Router1:

○ Access Router1 CLI and type the following commands:

■ ip route 192.168.20.0 255.255.255.0 192.168.1.2

2. Configure static routes on Router2:

○ Access Router2 CLI and type the following commands:

■ ip route 192.168.10.0 255.255.255.0 192.168.1.1

Step 6: Default Routing Configuration

1. Configure default route on Router1 (if Router1 needs to send packets to networks

outside its knowledge):

○ ip route 0.0.0.0 0.0.0.0 192.168.1.2

2. Configure default route on Router2 (if Router2 needs to send packets to networks

outside its knowledge):

○ ip route 0.0.0.0 0.0.0.0 192.168.1.1

Step 7: Verify Connectivity

1. Test the connectivity by pinging from PC0 to PC1:

○ Open the command prompt on PC0.

○ Type ping 192.168.20.2 and observe the response.

2. Test the connectivity by pinging from PC1 to PC0:

○ Open the command prompt on PC1.

○ Type ping 192.168.10.2 and observe the response.

Simulation of Designed Network Topology

Sending a PDU from PC0 to PC1

1. Open the simulation mode in Packet Tracer.

2. Send a PDU from PC0 to PC1:

○ Observe the packet traveling from PC0 to Router1, then Router2, and finally to

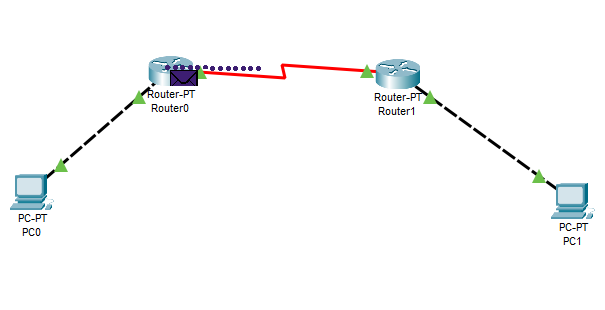
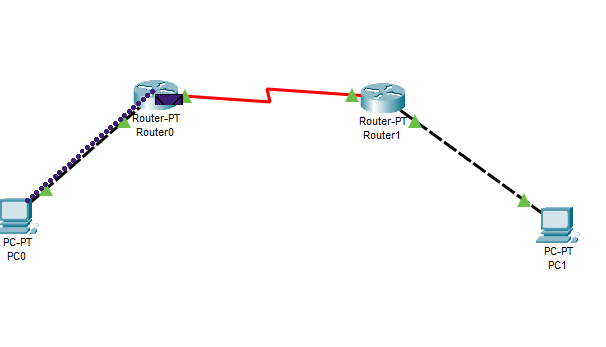
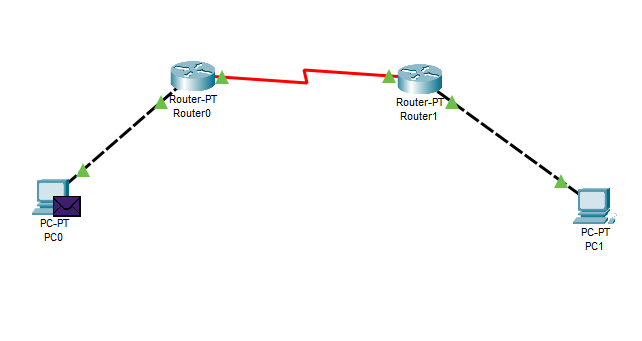
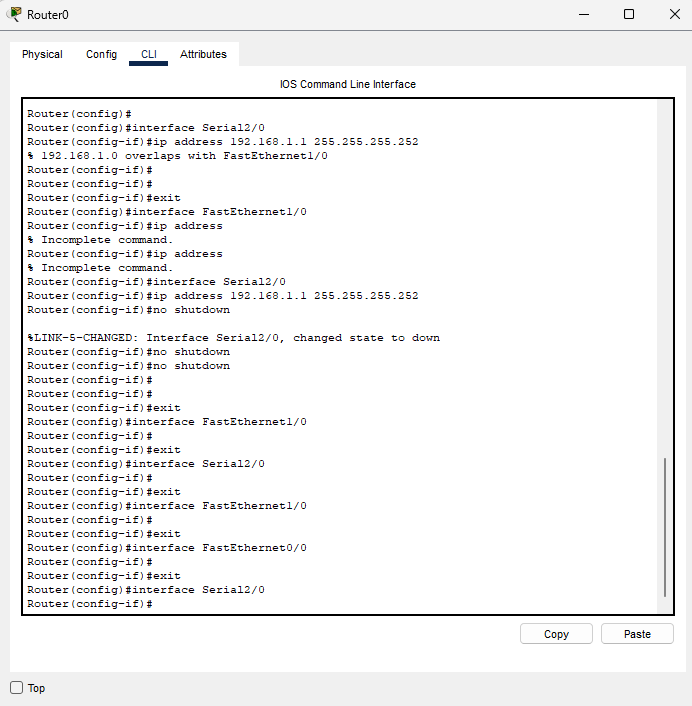
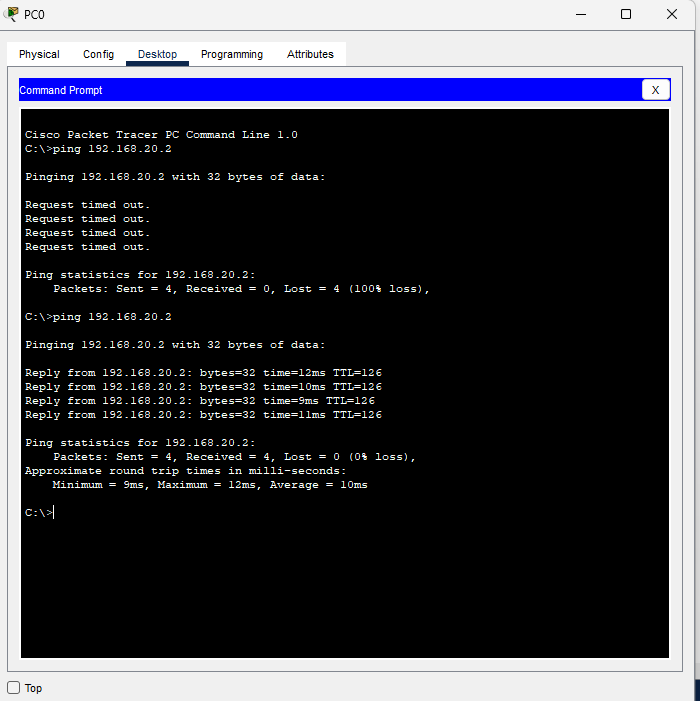
PC1.

Acknowledgment from PC1 to PC0

1. Observe the acknowledgment packet:

○ Ensure that the acknowledgment packet travels back from PC1 to PC0, confirming successful communication.

**Results:**



**Conclusion:**

In this experiment, we successfully configured static and default routing on routers to facilitate communication between different network segments. By setting up a network with multiple routers and PCs, we demonstrated how static and default routes ensure that data packets are correctly routed to their destination networks. The successful ping tests between the PCs confirmed the accurate configuration of routing tables, allowing for seamless data transfer across the network. This exercise highlighted the importance of static and default routing in managing network traffic efficiently and ensuring connectivity between devices on separate subnets.

**Computer Networks – LAB 6: NAT Configuration**

**Objective:**

* To configure Network Address Translation (NAT) on a router using Cisco Packet Tracer.
* To enable internal network devices with private IP addresses to communicate with external networks using a public IP address.
* To verify successful NAT configuration by testing connectivity between internal PCs and an external network.

**Requirements:**

* Cisco Packet Tracer software.
* A GitHub account and a repository for lab assignments.
* Access to Google Classroom for submission

**Procedure:**

**Network Design:**

● Router1 connected to the ISP Router.

● PC0 connected to Router1.

● PC1 connected to Router1.

Step 1: Configure Network Addresses

1. Determine IP address scheme:

○ Inside network (LAN): 192.168.10.0/24

○ Outside network (ISP): 200.0.0.0/30

Step 2: Configuring Router1

1. Select Router1 and open CLI.

2. Press ENTER to start configuring Router1.

3. Activate privileged mode:

○ Type enable

4. Access the configuration menu:

○ Type config t (configure terminal)

5. Configure interfaces of Router1:

○ FastEthernet0/0 (connected to LAN):

■ Type interface FastEthernet0/0

■ Configure with the IP address 192.168.10.1 and Subnet mask 255.255.255.0

○ Serial0/0/0 (connected to ISP Router):

■ Type interface Serial0/0/0

■ Configure with the IP address 200.0.0.1 and Subnet mask 255.255.255.252

6. Activate interfaces:

○ Type no shutdown

Step 3: Configuring ISP Router

1. Select the ISP Router and open CLI.

2. Press ENTER to start configuring the ISP Router.

3. Activate privileged mode:

○ Type enable

4. Access the configuration menu:

○ Type config t (configure terminal)

5. Configure interfaces of the ISP Router:

○ Serial0/0/0 (connected to Router1):

■ Type interface Serial0/0/0

■ Configure with the IP address 200.0.0.2 and Subnet mask 255.255.255.252

6. Activate interfaces:

○ Type no shutdown

ISP Router Command Line Interface:

Step 4: Configuring PCs

1. Assign IP addresses to each PC:

○ PC0:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.10.2

■ Subnet Mask: 255.255.255.0

■ Default Gateway: 192.168.10.1

○ PC1:

■ Go to the desktop, select IP Configuration, and assign the following:

■ IP address: 192.168.10.3

■ Subnet Mask: 255.255.255.0

■ Default Gateway: 192.168.10.1

Step 5: Configuring NAT on Router1

1. Define the inside and outside interfaces:

○ Access Router1 CLI and type the following commands:

■ interface FastEthernet0/0

■ ip nat inside

■ exit

■ interface Serial0/0/0

■ ip nat outside

■ exit

2. Configure a standard access list to permit the internal network:

○ access-list 1 permit 192.168.10.0 0.0.0.255

3. Configure NAT overload (PAT) for the internal network:

○ ip nat inside source list 1 interface Serial0/0/0 overload

Router1 NAT Configuration Commands:

Step 6: Verify NAT Configuration

1. Test the connectivity by pinging from PC0 to the ISP Router:

○ Open the command prompt on PC0.

○ Type ping 200.0.0.2 and observe the response.

2. Check NAT translation table on Router1:

○ On Router1 CLI, type show ip nat translations to see the NAT entries.

Step 7: Verify External Connectivity

1. Test external connectivity by pinging a public IP (simulated):

○ On PC0, type ping 8.8.8.8 (replace with an actual reachable IP in Packet

Tracer).

○ On PC1, type ping 8.8.8.8.

Configuration Tables

Simulation of Designed Network Topology

Sending a PDU from PC0 to an External Network

1. Open the simulation mode in Packet Tracer.

2. Send a PDU from PC0 to a simulated external IP (e.g., 8.8.8.8):

○ Observe the packet traveling from PC0 to Router1, NAT translation occurring,

then to the ISP Router and the external network.

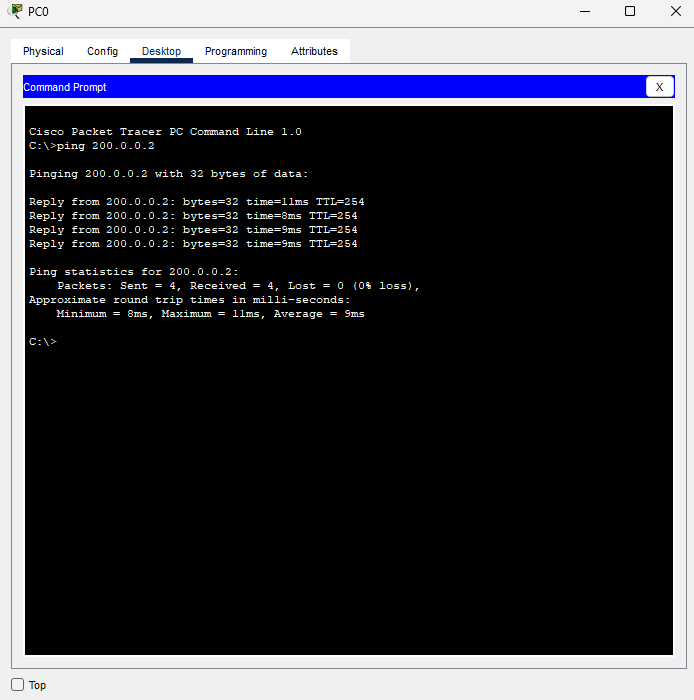
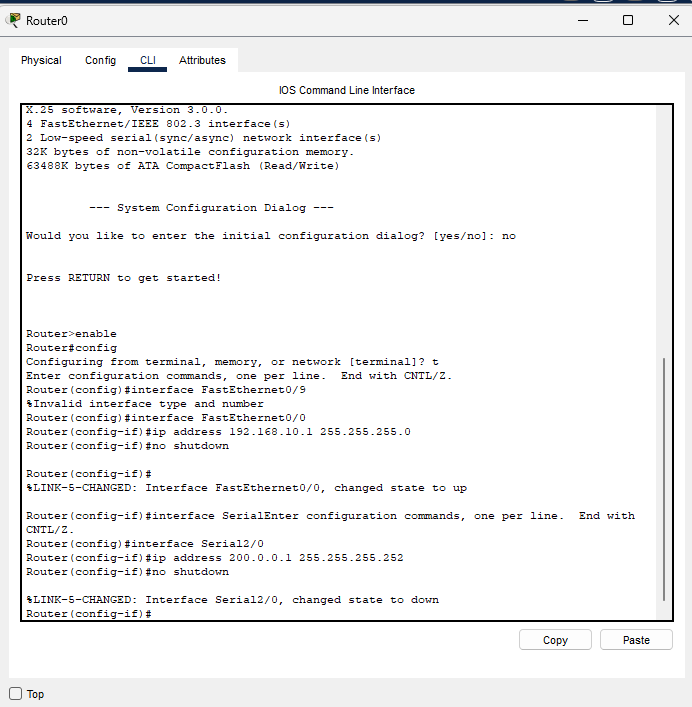
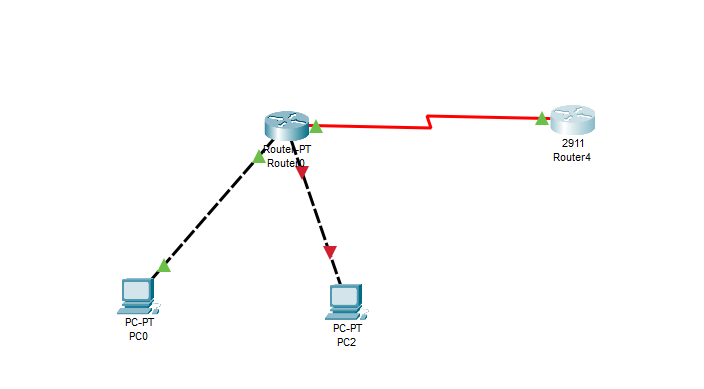
Acknowledgment from External Network to PC0

1. Observe the acknowledgment packet:

○ Ensure that the acknowledgment packet travels back from the external network to

PC0, confirming successful NAT configuration and communication.

**Results:**



**Conclusion:**

In this experiment, we successfully implemented Network Address Translation (NAT) on a router to allow internal network devices to access external networks. By configuring NAT, we translated private IP addresses from the local network into a public IP address, enabling communication with the internet. The successful ping tests and observations of the NAT translation table confirmed that NAT was correctly configured, allowing for seamless communication between the internal and external networks. This exercise highlighted the essential role of NAT in modern networking, ensuring both security and efficient use of public IP addresses.

**GitHub Link (for all lab exp.):**

Made by **R.R. DHARUN RAAGAV (RA2211003050088)**