COMPUTER NETWORKS

LAB-1: Introduction to Packet Tracer, Peer-to-Peer Communication, Study of Cables and its Color Codes.

Objective:

- Acquaint knowledge with Cisco Packet Tracer software.
- Establish a peer-to-peer (P2P) communication network.
- Examine various types of network cables and their color codes.
- Record observations and save the configuration in a GitHub repository.

Requirements:

- Software: Cisco Packet Tracer.
- Account: GitHub account with a repository for lab assignments.
- Submission Platform: Google Classroom.

Instructions:

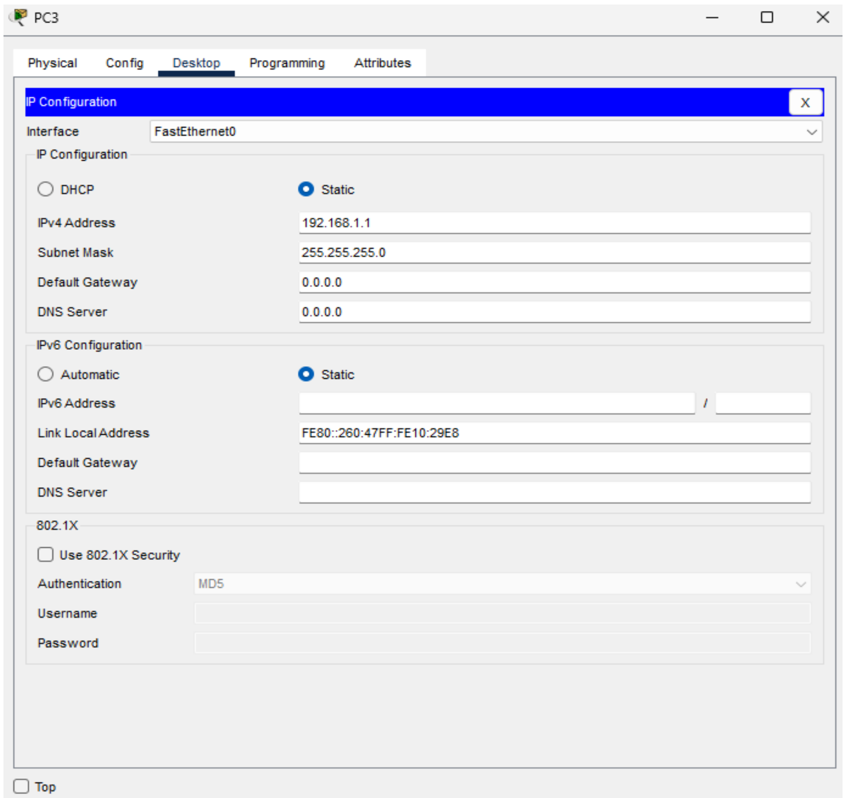
Part 1: Getting Started with Packet Tracer

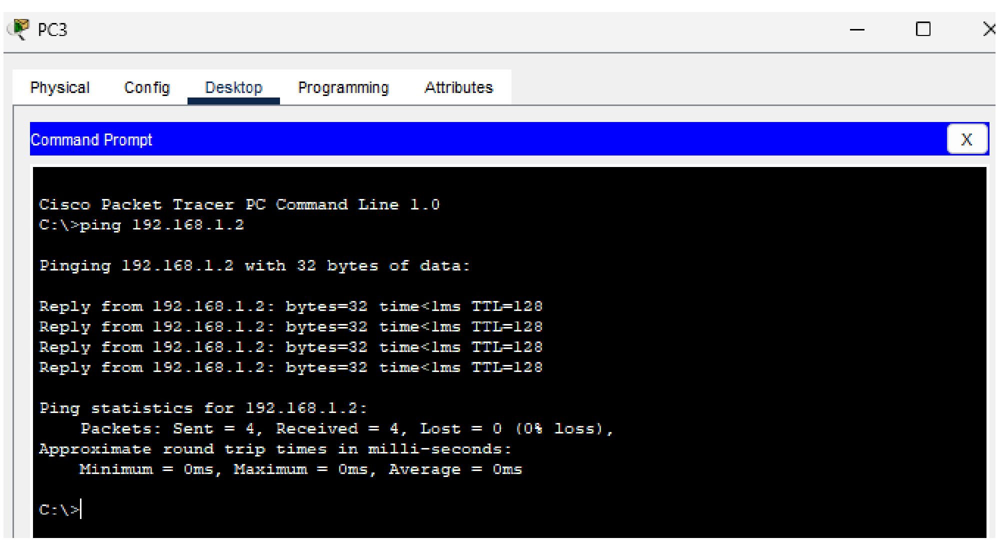
- Confirm Cisco Packet Tracer is installed on your device. If not, download it from the Cisco Networking Academy website.
- Launch Packet Tracer and explore the interface. Familiarize yourself with the tools and components provided in the software.

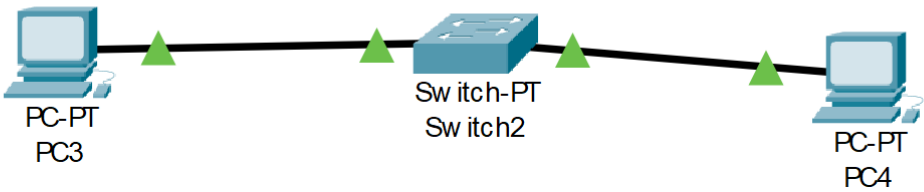
Part 2: Setting Up Peer-to-Peer Communication

- Open Packet Tracer and create a new network configuration.
- Add two PCs to the workspace.
- Connect PC0 and PC1 using a copper straight-through cable by linking their FastEthernet0 ports.
- Assign the following IP addresses and subnet masks:
  For PC0: IP address: 192.168.1.1, Subnet Mask: 255.255.255.0
  For PC1: IP address: 192.168.1.2, Subnet Mask: 255.255.255.0
- On PC0, open the command prompt and test the connection by pinging PC1 with the command: ping 192.168.1.2.
- Capture a screenshot showing the successful ping result.

Result:


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::260:47FF:FE10:29E8
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>



Study of Network Cables and Color Codes

Types of Network Cables in Computer Networking:

1. Copper Cables

- Straight-Through Cable
  - Function: Used to link different types of devices, like connecting a computer to a switch or a switch to a router.
  - Configuration: Both ends of the cable have the same wiring sequence, meaning that Pin 1 on one end is connected to Pin 1 on the other, Pin 2 to Pin 2, and so on.
  - Typical Use: Commonly used for connecting a computer to network devices such as hubs, switches, or routers.
- Crossover Cable
  - Function: Enables direct connection between similar devices, such as two computers or two switches, without using an intermediary device like a hub or switch.
  - Configuration: The wiring is "crossed" at the ends; for example, Pin 1 is connected to Pin 3, and Pin 2 to Pin 6.
  - Typical Use: Often used for PC-to-PC or switch-to-switch direct connections.
- Shielded Twisted Pair (STP) Cable
  - Function: Offers extra protection against electromagnetic interference (EMI) and signal interference from nearby cables.
  - Configuration: Similar in structure to Unshielded Twisted Pair (UTP), but with added shielding around the twisted wire pairs.
  - Typical Use: Best suited for environments with high EMI, such as industrial areas or locations with many electronic devices.

- Unshielded Twisted Pair (UTP) Cable
  - Function: The most common type of copper cable used in networking, lacking the additional protective shielding.
  - Configuration: Consists of multiple pairs of wires twisted together to reduce interference.
  - Typical Use: Widely used in general networking scenarios, including for both straight-through and crossover connections.

2. Fiber Optic Cables

- Single-Mode Fiber (SMF)
  - Function: Designed for long-distance communication, often used in telecom networks.
  - Configuration: Utilizes a single strand of glass fiber to transmit data using light waves.
  - Typical Use: Ideal for long-distance data transmission, such as between different buildings or across cities.
- Multi-Mode Fiber (MMF)
  - Function: Suitable for shorter distances, such as within the same building or between nearby buildings.
  - Configuration: Uses multiple paths for light transmission, allowing for more data transfer over shorter distances.
  - Typical Use: Commonly found in data centers and used for LAN backbones or other short-distance network applications.

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

1. **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
2. **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

Conclusion:
This exercise demonstrated the successful setup of a peer-to-peer network using Cisco Packet Tracer, validating connectivity between two PCs. The configuration and testing of IP addresses and subnet masks confirmed proper network communication. Understanding the various types of network cables and their configurations is crucial for designing efficient and reliable network infrastructures. Each cable type serves distinct purposes, from long-distance fiber optics to versatile copper cables, ensuring optimal performance based on specific network needs.

LAB 2: Implementation of Network Topologies

Objective:

- Learn and set up different network topologies using Cisco Packet Tracer.
- Understand how to use various types of network cables and their proper connections.
- Assign IP addresses to devices and test their connectivity.
- Save the setup files for future reference.

Requirements:

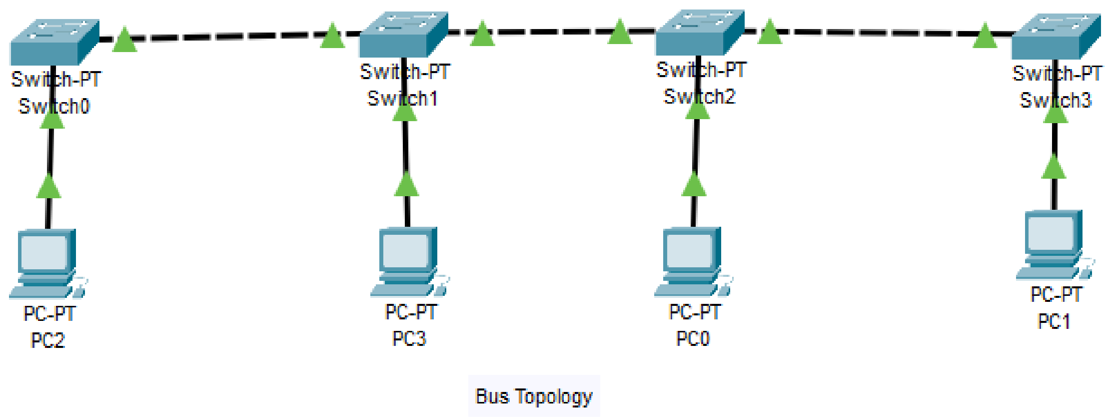
- Cisco Packet Tracer software installed.
- A GitHub account with a repository to store your lab assignments.
- Access to Google Classroom for submitting your work.

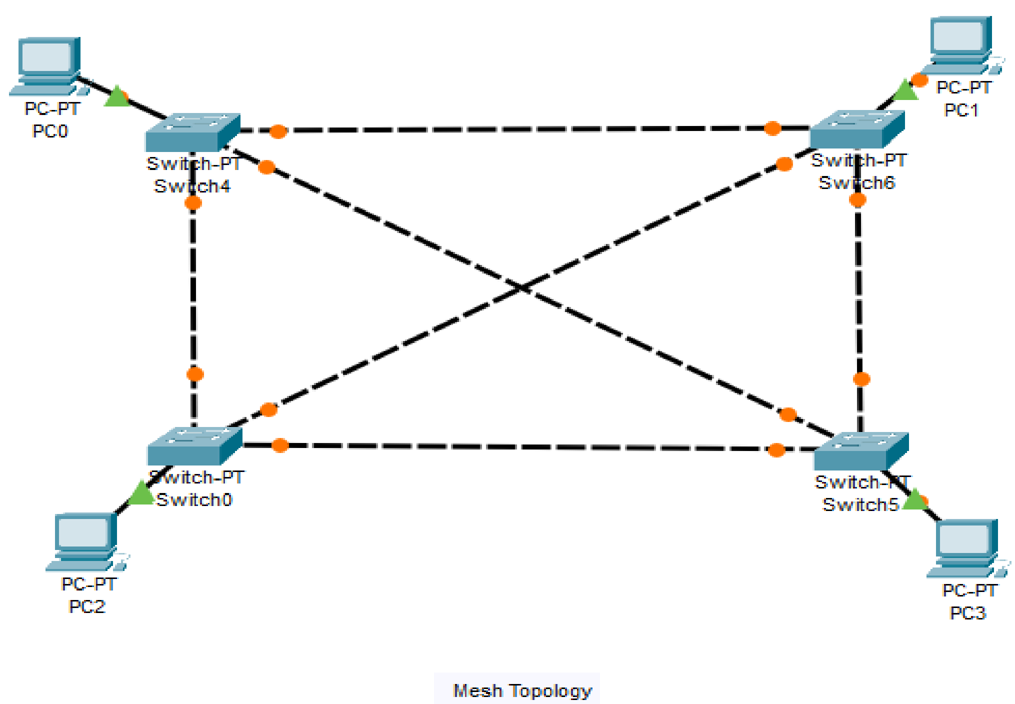
Steps:

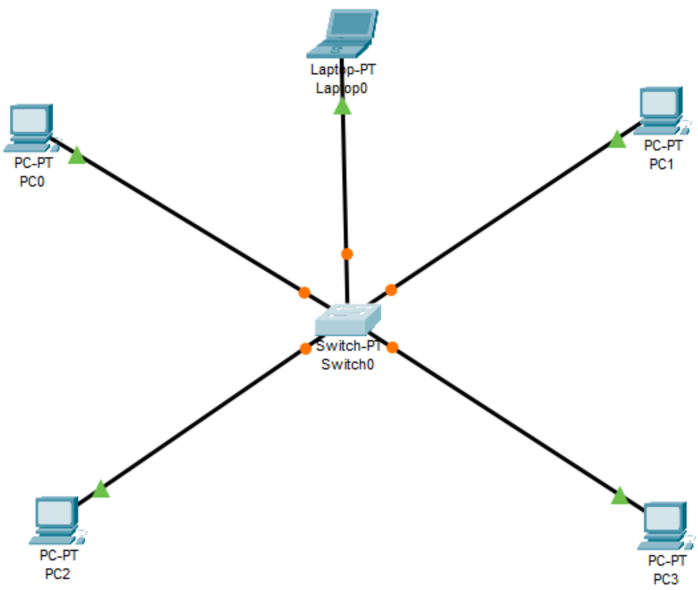
1. **Launch Cisco Packet Tracer:**
   - Open Cisco Packet Tracer on your computer.
2. **Create a Bus Topology:**
   - Place three computers on the workspace.
   - Connect them using a single backbone cable (Coaxial Cable).
3. **Create a Star Topology:**
   - Place three computers and a switch on the workspace.
   - Use straight-through Ethernet cables to connect each computer to the switch.
4. **Create a Ring Topology:**
   - Place three computers on the workspace.
   - Connect the computers in a circle using crossover cables.
5. **Create a Mesh Topology:**
   - Place three computers on the workspace.
   - Connect each computer to every other computer using crossover cables.
6. **Test the Network:**
   - Assign IP addresses to the computers in each topology.

- Use the ping command to check if the computers can communicate with each other.

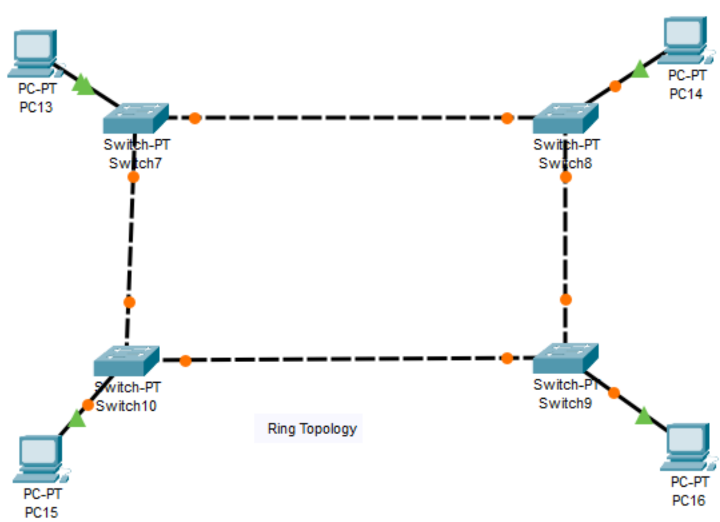
Result:



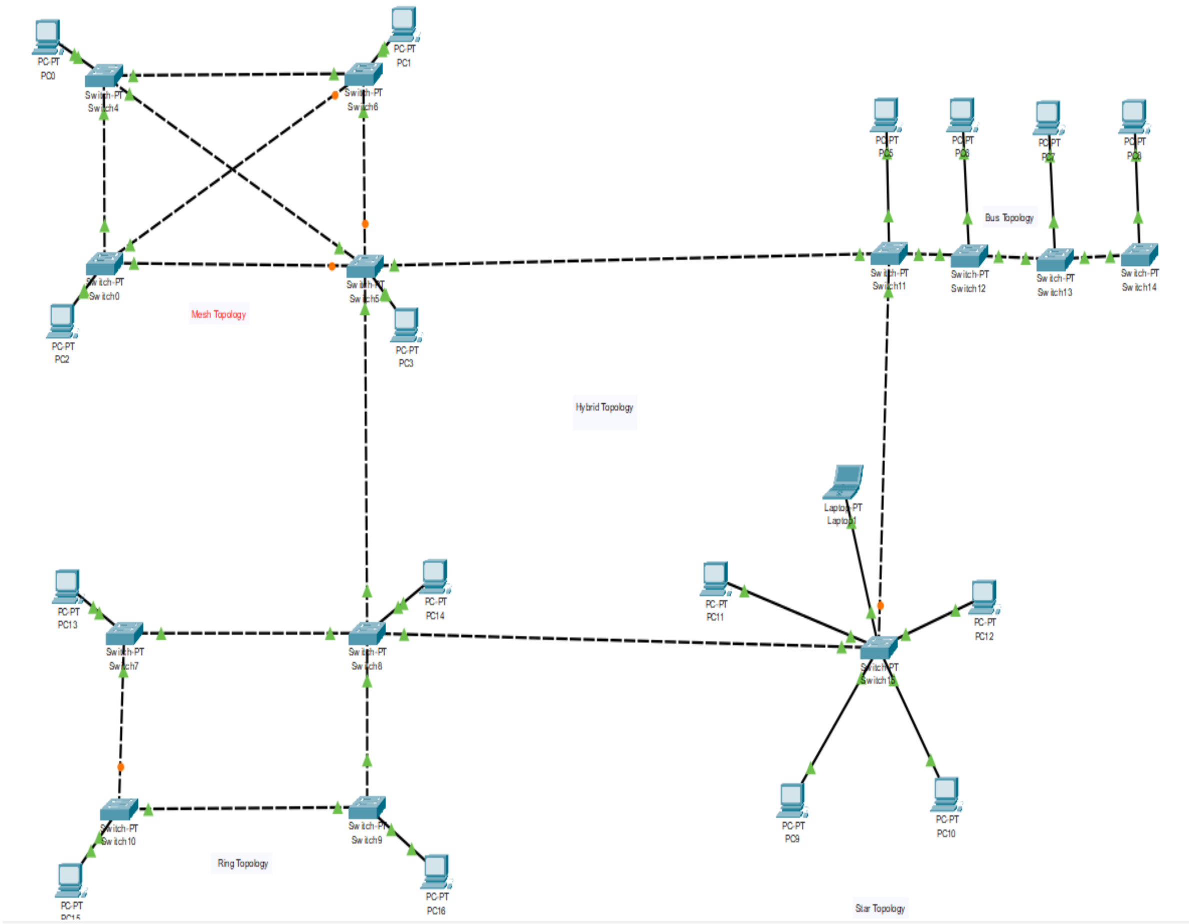




Star Topology



Ring Topology



Conclusion:

In conclusion, this exercise demonstrates the practical implementation of various network topologies using Cisco Packet Tracer, enhancing our understanding of network design and cable usage. By configuring IP addresses and testing connectivity, we ensure the functionality of each topology. Documenting and saving these setups will aid in future reference and analysis. This hands-on experience is crucial for mastering network management and troubleshooting.

LAB 3: Router Configuration (Creating Passwords, Configuring Interfaces)

Objective:

- Set up a router and PCs in Cisco Packet Tracer.
- Create a network connection between two PCs via a router.
- Assign IP addresses and configure router interfaces for communication.
- Simulate and verify data transfer between PCs.

Requirements:

- Cisco Packet Tracer software.
- GitHub account with a repository for lab assignments.
- Access to Google Classroom for submissions.

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: Configure PCs

- For **PC0**:
    a. Go to Desktop > IP Configuration.
    b. Assign the following:
        - IP Address: 192.168.10.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.10.1
- For **PC1**:
    c. Go to Desktop > IP Configuration.
    d. Assign the following:
        - IP Address: 192.168.20.2
        - Subnet Mask: 255.255.255.0
        - Default Gateway: 192.168.20.1

Step 3: Connect PCs to Router

- Use copper straight-through cables:
    - Connect PC0's FastEthernet port to Router1's FastEthernet0/0.
    - Connect PC1's FastEthernet port to Router1's FastEthernet0/1.

Simulation: Verify Data Transfer

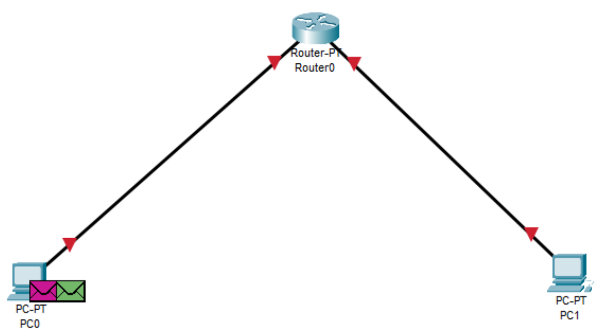
- Switch to simulation mode in Cisco Packet Tracer.
- Send a PDU (data packet) from PC0 to PC1.
- Observe the packet traveling through the router to reach PC1.

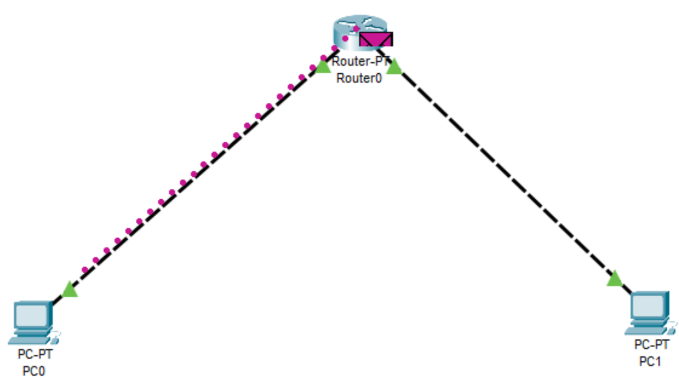
Result:

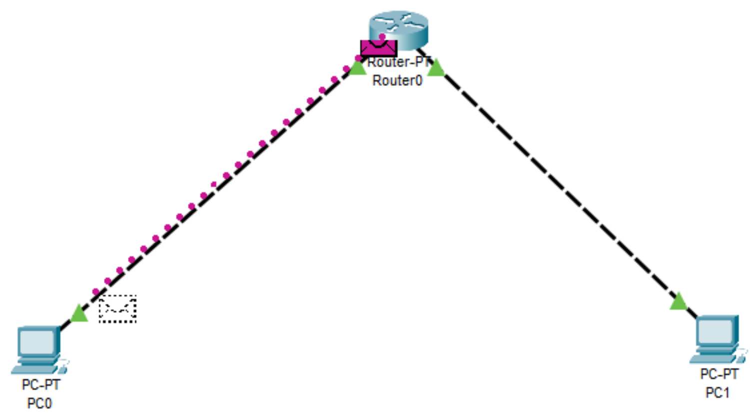
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname GATEWAY
GATEWAY(config)#enable secret cisco
GATEWAY(config)#service password-encryption
GATEWAY(config)#line console 0
GATEWAY(config-line)#password cisco
GATEWAY(config-line)#login
GATEWAY(config-line)#logging synchronous
GATEWAY(config-line)#exec-timeout 2 45
GATEWAY(config-line)#history size 10
GATEWAY(config-line)#
```

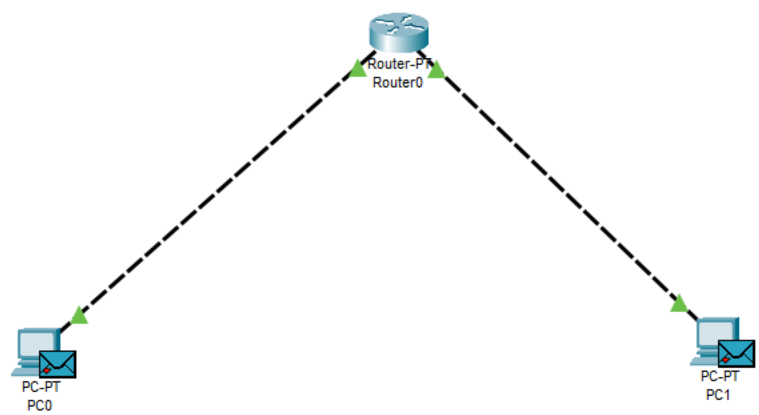
Copy Paste

Top









Conclusion:

In conclusion, this lab effectively demonstrated the configuration of a router and PCs in Cisco Packet Tracer. By assigning IP addresses and setting up interfaces, connectivity was established between two PCs through the router. The simulation confirmed successful data transfer between the devices, verifying proper network setup and configuration. This exercise highlights the importance of accurate configuration and testing in network design.

LAB 4: Addressing and Subnetting (VLSM) with Cisco Packet Tracer.

Objective:

- Configure a network using Variable Length Subnet Masking (VLSM) to optimize IP addresses.
- Create subnets of different sizes based on network requirements.
- Set up routers and PCs with correct IP addresses and subnet masks.
- Test end-to-end connectivity using Cisco Packet Tracer.

Requirements:

- Cisco Packet Tracer software.
- A GitHub repository for lab work.
- Access to Google Classroom for submission.

Procedure:

Step 1: Network Design and Subnetting

- **Design the Network Topology:**
  - Determine how many subnets you need and their sizes.
  - Use VLSM to calculate subnet addresses.
- **Example Subnetting**:
  - Start with the network address: 192.168.0.0/24
  - Break it down into smaller subnets:
    - Subnet 1 (50 hosts): Network Address: 192.168.0.0/26, Subnet Mask: 255.255.255.192
    - Subnet 2 (30 hosts): Network Address: 192.168.0.64/27, Subnet Mask: 255.255.255.224
    - Subnet 3 (10 hosts): Network Address: 192.168.0.96/28, Subnet Mask: 255.255.255.240

        - Subnet 4 (5 hosts): Network Address: 192.168.0.112/29, Subnet Mask: 255.255.255.248

Step 2: Router Configuration

- **Open Router CLI**:
    - Select Router1 and open the Command Line Interface (CLI).
    - Press Enter to start.
- **Enter Privileged Mode**:
    - Type: enable.
- **Enter Global Configuration Mode**:
    - Type: config t (for "configure terminal").
- **Configure Router Interfaces**:
    - For FastEthernet0/0:
        - Type interface FastEthernet0/0.
        - Set the IP address to 192.168.0.1 with a subnet mask of 255.255.255.192.
    - For FastEthernet0/1:
        - Type interface FastEthernet0/1.
        - Set the IP address to 192.168.0.65 with a subnet mask of 255.255.255.224.
- **Activate the Interfaces**:
    - Type no shutdown for both interfaces.

Step 3: PC Configuration

- **PC0 Setup**:
    - Go to Desktop > IP Configuration.
    - Set:
        - IP address: 192.168.0.2
        - Subnet Mask: 255.255.255.192
        - Default Gateway: 192.168.0.1
- **PC1 Setup**:
    - Go to Desktop > IP Configuration.
    - Set:

        - IP address: 192.168.0.66
        - Subnet Mask: 255.255.255.224
        - Default Gateway: 192.168.0.65

Step 4: Connecting Devices

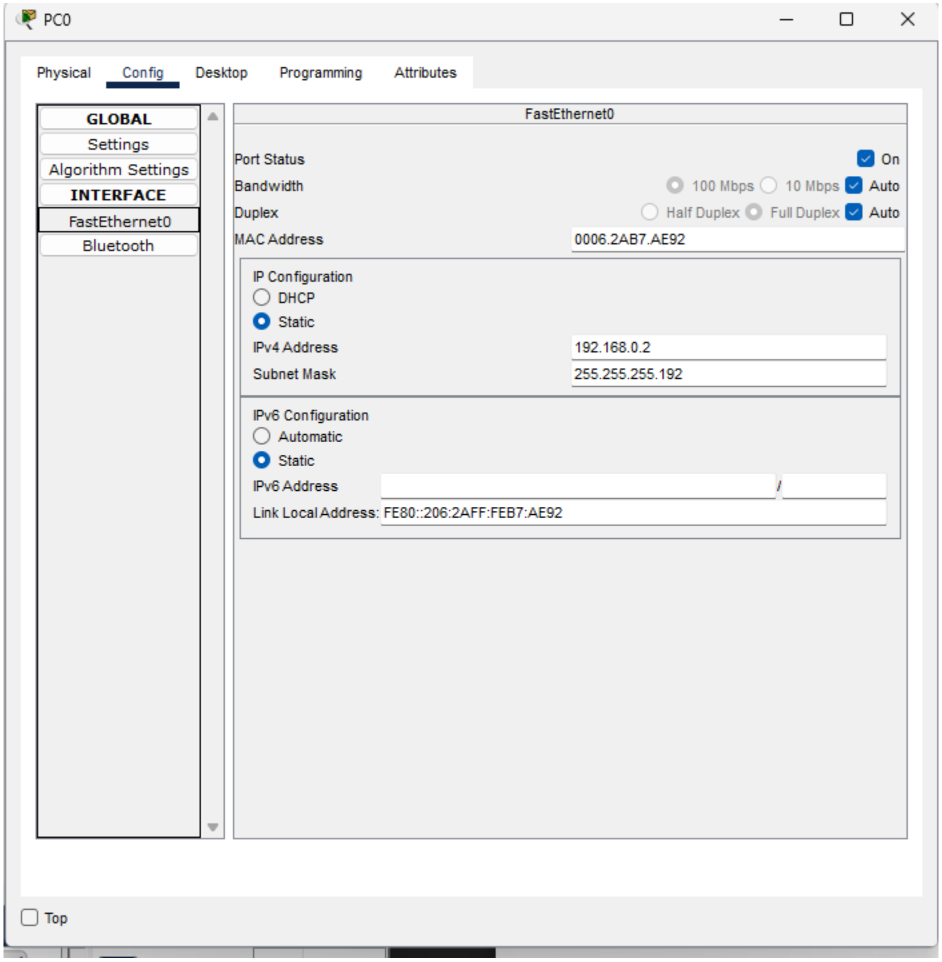
- **Connect PCs to Router**:
    - Use Copper Straight-through Cables.
    - Connect:
        - PC0's FastEthernet0 port to Router1's FastEthernet0/0 port.
        - PC1's FastEthernet0 port to Router1's FastEthernet0/1 port.

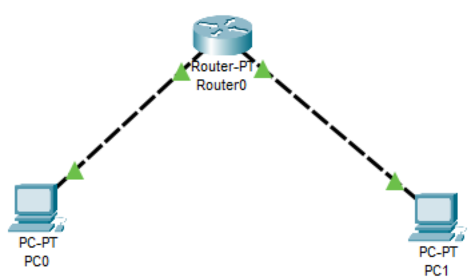
Step 5: Simulating and Testing Network

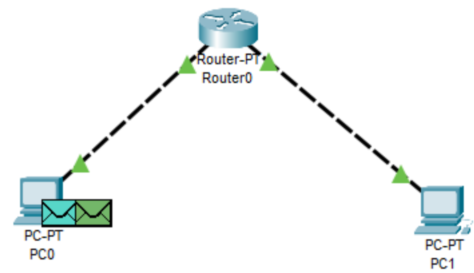
- Switch to Simulation Mode in Packet Tracer.
- Send a Test Packet (PDU) from PC0 to PC1:
    - Observe the packet traveling from PC0 to the router and then to PC1.
- Check Acknowledgment:
    - Watch for an acknowledgment packet returning from PC1 to PC0, confirming the communication was successful.

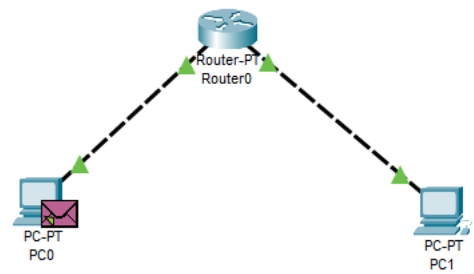
Result:

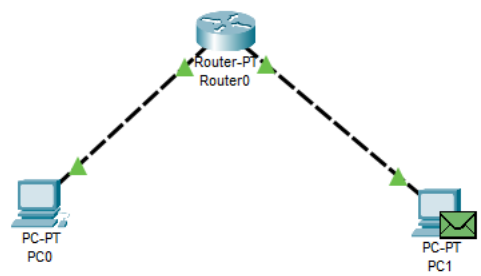
```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.192
Router(config-if)#interface FastEthernet1/0
Router(config-if)#interface FastEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.0.65 255.255.255.224
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
```

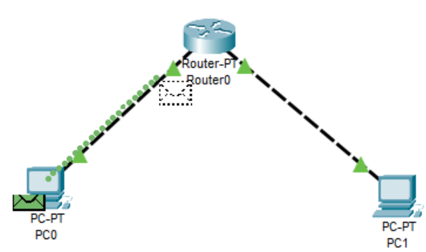

PC0
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0006.2AB7.AE92
IP Configuration
DHCP
Static
IPv4 Address
192.168.0.2
Subnet Mask
255.255.255.192
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address:
FE80::206:2AFF:FEB7:AE92
Top


Router-PT
Router0
PC-PT
PC0
PC-PT
PC1


Router-PT
Router0
PC-PT
PC0
PC-PT
PC1


Router-PT
Router0
PC-PT
PC0
PC-PT
PC1


Router-PT
Router0
PC-PT
PC0
PC-PT
PC1


Router-PT
Router0
PC-PT
PC0
PC-PT
PC1

Conclusion:

In conclusion, the network was successfully designed and configured using Variable Length Subnet Masking (VLSM) to optimize IP address utilization. Router and PC settings were precisely configured to ensure proper subnet segmentation and connectivity. The end-to-end communication between devices was verified through simulation in Cisco Packet Tracer, confirming the network's functionality. This exercise demonstrated effective subnetting and network configuration skills essential for managing complex network environments.

LAB 5: Static and Default Routing

Objective:

- Configure static and default routing on routers using Cisco Packet Tracer.
- Enable communication between different network segments by setting up proper routing.
- Test and verify connectivity between PCs in different subnets.

Requirements:

- Cisco Packet Tracer software.
- A GitHub account for lab assignments.
- Access to Google Classroom for submission.

Network Design:

- Router1 connected to Router2.
- PC0 connected to Router1.
- PC1 connected to Router2.

Procedure:

Step 1: IP Addressing

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

Step 2: Configure Router1

- Open **Router1's CLI** and start configuration.
- Enter privileged mode:
  - Command: enable
- Access configuration mode:
  - Command: config t
- Configure Router1's interfaces:

- **FastEthernet0/0 (connected to PC0)**:

IP: 192.168.10.1
Subnet Mask: 255.255.255.0

- **Serial0/0/0 (connected to Router2)**:

IP: 192.168.1.1
Subnet Mask: 255.255.255.252

- Activate the interfaces:
  - Command: no shutdown.

Step 3: Configure Router2

- Open Router2's CLI and start configuration.
- Enter privileged mode:
  - Command: enable
- Access configuration mode:
  - Command: config t
- Configure Router2's interfaces:
  - FastEthernet0/0 (connected to PC1):

IP: 192.168.20.1
Subnet Mask: 255.255.255.0

- Serial0/0/0 (connected to Router1):

IP: 192.168.1.2
Subnet Mask: 255.255255.252

7. Activate the interfaces:
   - Command: no shutdown

Step 4: Configure PCs

- **PC0 Configuration**:
  - IP Address: 192.168.10.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.10.1
- **PC1 Configuration**:
  - IP Address: 192.168.20.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.20.1

Step 5: Configure Static Routes

- **Router1**:
  - Command: ip route 192.168.20.0 255.255.255.0 192.168.1.2

- **Router2**:
    - Command: ip route 192.168.10.0 255.255.255.0 192.168.1.1

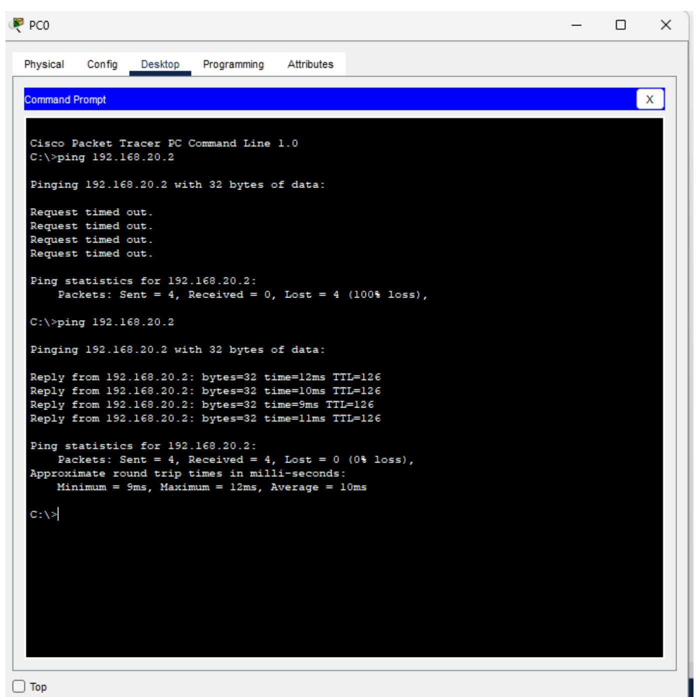
Step 6: Configure Default Routes

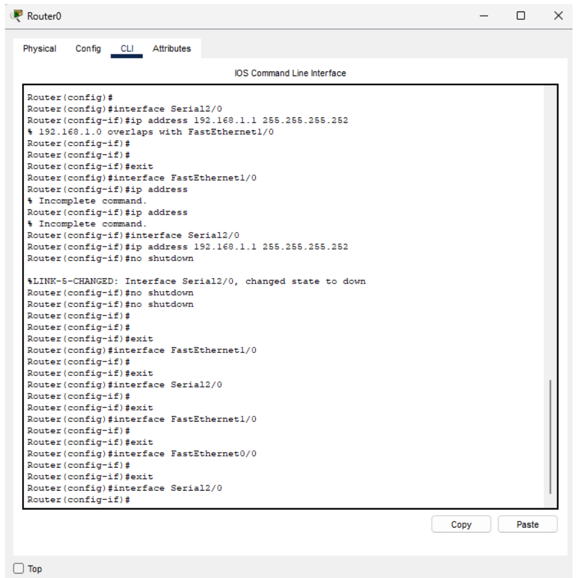
- **Router1**:
    - Command: ip route 0.0.0.0 0.0.0.0 192.168.1.2
- **Router2**:
    - Command: ip route 0.0.0.0 0.0.0.0 192.168.1.1

Step 7: Verify Connectivity

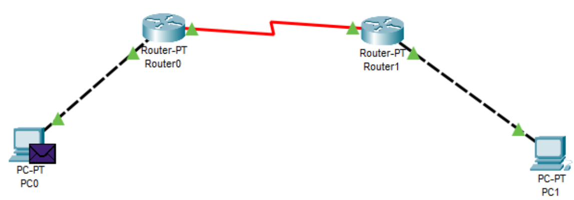
- Ping test:
    - From PC0, ping PC1 (IP: 192.168.20.2).
    - From PC1, ping PC0 (IP: 192.168.10.2).
- Simulate communication:
    - Use Packet Tracer's simulation mode to send a PDU from PC0 to PC1 and observe the path through both routers.
    - Ensure the acknowledgment packet returns from PC1 to PC0 for successful communication.

Results:

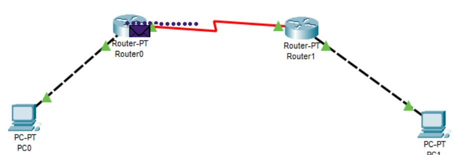




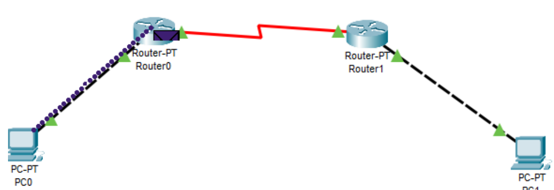
Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config)#
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
% 192.168.1.0 overlaps with FastEthernet1/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address
% Incomplete command.
Router(config-if)#ip address
% Incomplete command.
Router(config-if)#interface Serial2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
Router(config-if)#no shutdown
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#
Copy
Paste
Top



Router-PT
Router0
Router-PT
Router1
PC-PT
PC0
PC-PT
PC1



Router-PT
Router0
Router-PT
Router1
PC-PT
PC0
PC-PT
PC1



Router-PT
Router0
Router-PT
Router1
PC-PT
PC0
PC-PT
PC1

Conclusion:

In conclusion, this lab successfully demonstrated the configuration of static and default routing between two routers using Cisco Packet Tracer. By establishing appropriate IP addressing and routing protocols, seamless communication between PCs in different subnets was achieved. The implementation and verification steps confirmed that the routing setup was correctly executed, facilitating efficient data transfer across the network. This exercise underscores the importance of precise routing configurations in ensuring effective network connectivity.

LAB 6: NAT Configuration

Objective

- Configure Network Address Translation (NAT) on a router using Cisco Packet Tracer.
- Allow internal devices with private IP addresses to communicate with external networks using a public IP.
- Verify NAT configuration by testing connectivity between internal PCs and an external network.

Requirements

- Cisco Packet Tracer software.
- GitHub account and repository for lab submissions.
- Google Classroom access for assignment submission.

Network Design

- Router1 connected to an ISP router.
- PC0 and PC1 connected to Router1.

Procedure:

Step 1: Configure Network Addresses

1. **IP address scheme:**
   - Internal network (LAN): 192.168.10.0/24
   - External network (ISP): 200.0.0.0/30

Step 2: Configure Router1

1. **Open Router1's CLI:**
   - Press ENTER to start.
   - Type: enable to enter privileged mode.

    - Type config t to go to the configuration mode.
2. **Configure Router1 interfaces:**
   - **FastEthernet0/0** (LAN):
     - Type interface FastEthernet0/0
     - Set the IP: ip address 192.168.10.1 255.255.255.0
   - **Serial0/0/0** (connected to ISP):
     - Type interface Serial0/0/0
     - Set the IP: ip address 200.0.0.1 255.255.255.252
3. **Activate interfaces:**
   - Type no shutdown for both interfaces.

Step 3: Configure the ISP Router

1. **Open ISP Router's CLI:**
    - Press ENTER and type enable.
    - Type config t to configure the router.
2. **Configure ISP Router interface:**
    - **Serial0/0/0** (connected to Router1):
      - Type interface Serial0/0/0
      - Set the IP: ip address 200.0.0.2 255.255.255.252
3. **Activate interface:**
    - Type no shutdown.

Step 4: Configure PCs

1. **PC0:**
    - Set IP: 192.168.10.2
    - Subnet Mask: 255.255.255.0
    - Gateway: 192.168.10.1
2. **PC1:**
    - Set IP: 192.168.10.3
    - Subnet Mask: 255.255.255.0
    - Gateway: 192.168.10.1

Step 5: Configure NAT on Router1

1. **Define inside and outside interfaces:**
   - On Router1’s CLI, type:
     - interface FastEthernet0/0
     - ip nat inside
     - exit
     - interface Serial0/0/0
     - ip nat outside
     - exit
2. **Create an access list for the internal network:**
   - Type: access-list 1 permit 192.168.10.0 0.0.0.255
3. **Configure NAT overload (PAT):**
   - Type: ip nat inside source list 1 interface Serial0/0/0 overload

Step 6: Verify NAT Configuration

1. **Test connectivity:**
   - On PC0, open the command prompt and type ping 200.0.0.2 (ISP router IP).
2. **Check NAT translation:**
   - On Router1 CLI, type show ip nat translations to view the NAT table.

Step 7: Verify External Connectivity

1. **Ping an external IP:**
   - On PC0 and PC1, type ping 8.8.8.8 (or any reachable IP in Packet Tracer).

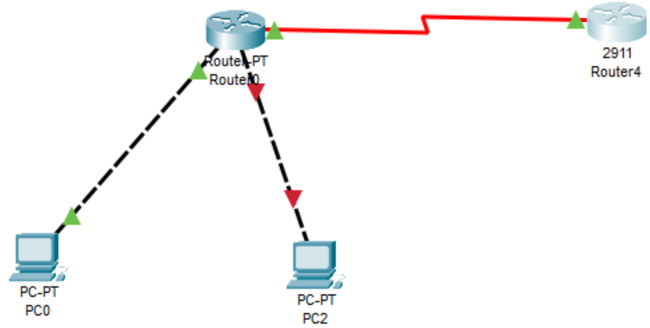
Step 8: Simulation in Packet Tracer

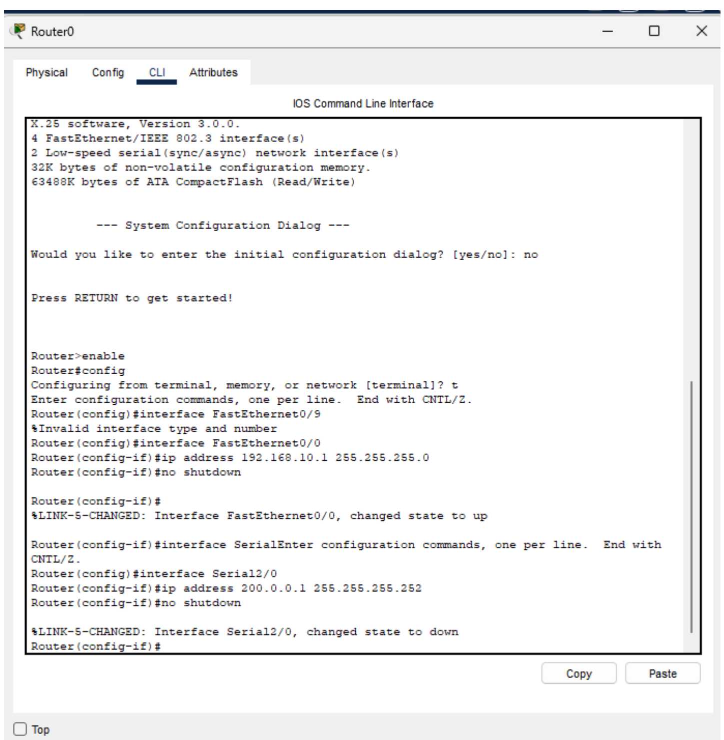
1. **Simulation mode:**
   - In Packet Tracer, switch to simulation mode and send a packet from PC0 to a simulated external IP (e.g., 8.8.8.8).
   - Observe the packet as it passes through Router1, undergoes NAT translation, and reaches the external network.

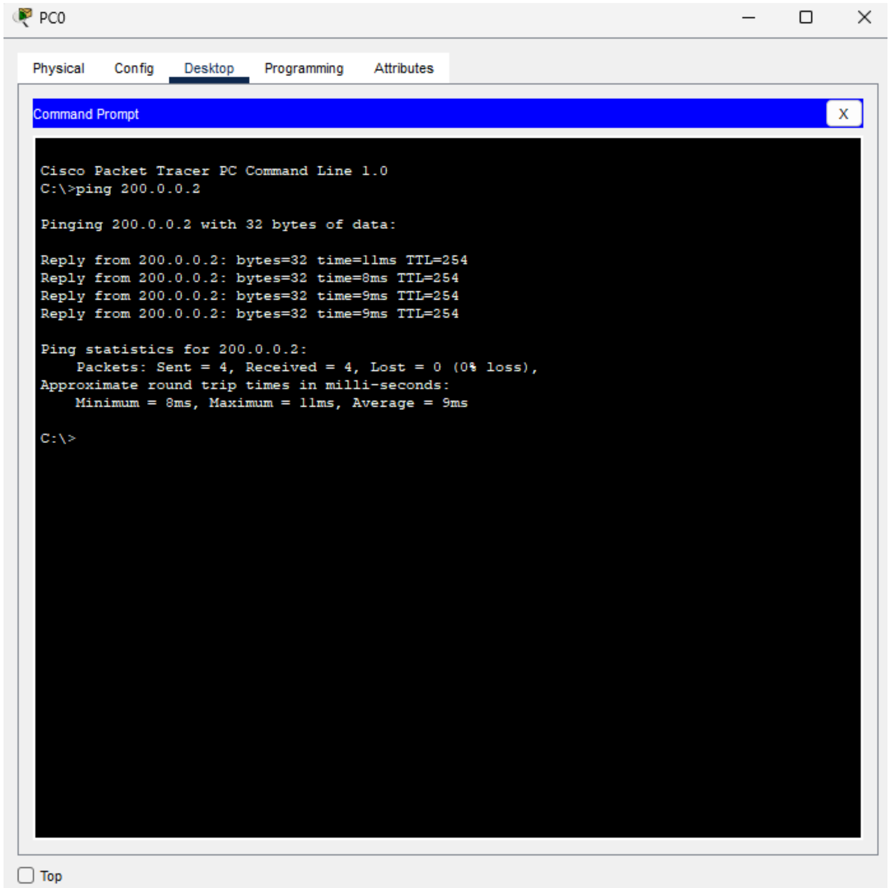
2. Acknowledgment:

- Watch the acknowledgment packet return to PC0, confirming successful communication via NAT.

Result:







Conclusion:

In this lab exercise, Network Address Translation (NAT) was successfully configured on Router1, allowing internal devices with private IP addresses to access external networks via a public IP. The configuration involved setting up Router1 and the ISP Router with the correct IP addresses and configuring PCs with appropriate network settings. NAT was implemented on Router1, defining inside and outside interfaces, creating an access list, and enabling NAT overload. The successful verification through pings and NAT translation observation in simulation mode confirms the effective facilitation of communication between private and public networks.