Lab no: 1 **Date: 2025/ 10 /02**

Understanding of Network Equipment, Wiring in Details (CAT6 UTP EIA/TIA 568A/B Straight and Cross-Over Wiring and Testing)

Objectives:

- Learn about networking devices and tools, such as repeaters, hubs, switches, routers, crimping tools, UTP and fiber cables, connectors, patch panels, cable organizers, racks, and LAN testers, as well as CAT6 wiring standards and RJ-45 connectors.
- Understand the color-coding rules for UTP cables.
- Make straight-through and crossover cables and check their connectivity using a LAN tester.

➢ **Understanding Networking Equipment:**

1. **Repeaters:**
   A repeater is a networking device that helps to amplify and regenerate signals to increase the reach of a network. Also operating at the physical layer of the OSI, repeaters help overcome distance-related limitations by strengthening the strength and quality of the signal. This will ensure efficient and safe communication. Repeater has two ports, so cannot be used to connect for more than two devices.

2. **Hubs:**
   A hub is a multi-port repeater. It is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.
   Drawbacks: Hubs do not filter traffic, which means all connected devices receive the same data, leading to inefficient bandwidth usage.

3. **Switch's:**
   The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address. A switch is more intelligent than an Ethernet Hub. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

4. **Bridge:**
   A network bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is called network bridging. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge.

5. **Routers:**
   The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. It uses the routing protocol to transfer the data across a network. Furthermore, it is more expensive than other networking devices like switches and hubs.

6. **Gate ways:**
   A gateway is a computer on a network that provides the interface between two applications or networks that use different protocols. They are also used to provide a connection to the Internet. A gateway in a network converts information from one protocol to another and then transfers it over the web. They are more complex than routers, performing protocol conversions to enable communication between systems using different networking protocols, such as TCP/IP and AppleTalk.

➢ **Understanding the Color-Coding Standard of UTP Cable:**

The color-coding standard for Unshielded Twisted Pair (UTP) cables is based on four pairs of wires, each with a solid color and a white-striped wire of the same color:

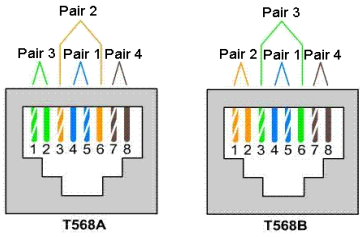
- **Blue:** The first pair
- **Orange:** The second pair
- **Green:** The third pair
- **Brown:** The fourth pair

Color-Coding Rules:

1. Striped wires go in odd-numbered pins, and solid-colored wires go in even-numbered pins.
2. The main difference between T568A and T568B is the order of the green and orange wire pairs.
3. In T568A, the green pair starts first (pins 1 and 2), while in T568B, the orange pair starts first.
4. The blue and brown wire pairs (pins 4, 5, 7, and 8) stay the same in both standards.

Wiring Patterns:

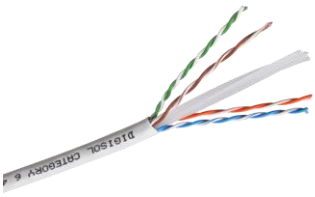
1. T568A Standard: Starts with green (pin 1: green-white, pin 2: green). 2. T568B Standard: Starts with orange (pin 1: orange-white, pin 2: orange)



- **Creating Straight and Crossover Cables and Verifying Connectivity:**

Apparatus:

- UTP CAT6 cable (1 meter or more), RJ-45 connectors, crimper tool, LAN tester.



CAT6 cable

RJ-45 connectors

crimper tool

LAN tester

Steps for Creating a Straight Cable:

1. **Strip the Cable Jacket:**
   - Use a cable stripper to remove about 1.2 inches of the outer jacket, revealing the twisted pairs inside.
   - If using a CAT6 cable, carefully trim the plastic spine if present.

2. **Untwist and Align the Wires:**
   - Separate and untwist the four pairs of wires.
   - Arrange the wires according to the T568A or T568B color-coding standard as needed.

3. **Trim the Wires:**
   - Once the wires are aligned, cut them evenly, leaving about 0.5 inches extending from the cable jacket.

4. **Insert Wires into the RJ-45 Connector:**
   - Carefully insert the wires into the RJ-45 connector, ensuring each wire is in its correct slot.
   - Make sure the wires are fully pushed to the end of the connector for proper contact.

5. **Crimp the Connector**:
   - Insert the connector into the crimping tool and squeeze firmly to secure the wires in place.

6. **Repeat for the Other End**:
   - Follow the same process to attach a connector to the other end of the cable, completing the straight-through cable assembly.

7. **Test the Cable**:
   - Use a LAN cable tester to check the connectivity of each pin. The tester will ensure that the cable has been properly terminated on both ends and is functioning correctly.

- **Steps for Creating a Crossover Cable:**

1. **Cut and Strip:**
   Cut the Ethernet cable to the required length. Strip about 1 inch of the outer jacket to expose the internal wires.
2. **Arrange the Wires:**
   - On one end, arrange the wires in the T568A standard (green/white, green, orange/white, blue, blue/white, orange, brown/white, brown).
   - On the other end, arrange the wires in the T568B standard (orange/white, orange, green/white, blue, blue/white, green, brown/white, brown).

3. **Trim and Insert the Wires:**
   Align the wires evenly and trim them to the same length. Insert the wires into the RJ45 connectors, ensuring they remain in the correct order.

4. **Crimp the Connectors:**
   Use a crimping tool to press the connectors onto the wires securely.

Testing:

- **Connect to LAN Tester:**
  Plug one end of the crossover cable into the TX (Transmit) port and the other end into the RX (Receive) port of the LAN tester.

- **Turn on the Tester:**
  Power on the tester to start the testing process.

- **Verify Connections:**
  Check the tester's lights or display to confirm the pin mapping. For a crossover cable:
  - Pin 1 on one end should connect to Pin 3 on the other.
  - Pin 2 should connect to Pin 6.

- **Check for Errors:**
  Ensure there are no faults like open circuits, short circuits, or incorrect wiring.

Lab no: 3 **Date: 2025/ 10 /04**

Overview of IP Addressing and Subnetting.

Objective(s):

- To gain theoretical knowledge of IPv4 addressing and subnetting.

IP Address:

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. While IP addresses are binary numbers, they are typically expressed in decimal form (for IPv4) or hexadecimal form (for IPv6) to facilitate easier human readability.

Terminologies:

- **IPv4 Address:** A 32-bit address that uniquely identifies a device on a network, typically represented in dotted decimal notation (e.g., 192.168.1.1).
- **Host Address:** Refers to the IP address assigned to a specific device (host) within a network.
- **Network:** A collection of devices (hosts) sharing a common starting portion in their IP addresses, usually identified by a network address**.**
- **Broadcast Address**: A special 32-bit address used to send data to all hosts within a specific network or subnet; it is reserved and cannot be assigned to any individual host.
- **Subnet:** A smaller subdivision of a network, where devices within the subnet share a common portion of their IP addresses**.**
- **Subnetting:** The method of dividing a larger network into smaller, more manageable subnets.
- **Subnet Mask**: A 32-bit mask used to define the boundary between the network portion and the host portion of an IP address, indicating which bits are used for the network and which for the host.

IPv4 Representation:

An IPv4 address is a unique identifier for a device on a network, represented as a 32-bit number divided into four 8-bit segments (octets). Each octet is expressed as a decimal number ranging from 0 to 255, and the four octets are separated by periods (dots).
For example, 192.168.1.1 is an IPv4 address.

- 32-bit: 4 octets × 8 bits = 32 bits.
- Each octet can represent 256 values (0-255), so the total possible IPv4 addresses are 4.3 billion.

Subnet mask:

A subnet mask is a 32-bit number used in IP networking to divide an IP address into a network and host portion. It helps determine which part of the IP address identifies the network and which part identifies the specific device (host) on that network. Common default subnet masks include:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

IP Address Classes:

As show in figure we teach how the ip addresses are classified and when they are used.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	A Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

IPv4 subnetting:
Subnetting is the process of taking a network and splitting it into smaller networks, known as subnets. It's used to free up more public IPv4 addresses and segment networks for security and easier management.

Exercise:

Address Class Identification:
1. 119.18.45.0 - Class A
2. 230.230.45.58 - Class D
3. 199.200.15.0 - Class C
4. 10.250.1.1 - Class A
5. 249.240.80.78 - Class E
6. 126.8.156.0 - Class A
7. 199.155.77.56 - Class C
8. 192.14.2.0 - Class C
9. 177.100.18.4 - Class B
10. 148.17.9.1 - Class B
11. 117.89.56.45 - Class A
12. 193.42.1.1 - Class C
13. 150.10.15.0 - Class B
14. 215.45.45.0 - Class C
15. 220.200.23.1 - Class C

Default Subnet Masks, Network Address and Broadcast Address

Write the correct default subnet mask, network address and broadcast address for each of the following addresses:

IP Address Network	Default Subnet Mask	Address Broadcast	Address
189.210.50.1	255.255.0.0	189.210.0.0	189.210.255.255
223.23.223.109	255.255.255.0	223.23.223.0	223.23.223.255
10.10.250.1	255.0.0.0	10.0.0.0	10.255.255.255
126.123.23.1	255.255.0.0	126.123.0.0	126.123.255.255
223.69.230.250	255.255.255.0	223.69.230.0	223.69.230.255
192.12.35.105	255.255.255.0	192.12.35.0	192.12.35.255
77.251.200.51	255.0.0.0	77.0.0.0	77.255.255.255
191.249.234.191	255.255.0.0	191.249.0.0	191.249.255.255
119.18.45.0	255.0.0.0	119.0.0.0	119.255.255.255
134.125.34.9	255.255.0.0	134.125.0.0	134.125.255.255
220.90.130.45	255.255.255.0	220.90.130.0	220.90.130.255
125.125.250.1	255.0.0.0	125.0.0.0	125.255.255.255
193.100.77.8	255.255.255.0	193.100.77.0	193.100.77.255
88.45.65.35	255.0.0.0	88.0.0.0	88.255.255.255
177.100.18.4	255.255.0.0	177.100.0.0	177.100.255.255

Conclusion:

This lab provided a foundational understanding of IPv4 addressing and subnetting. It covers key terminologies, classifications of IP addresses, and the significance of subnetting for effective network management.

Lab no: 4 **Date: 2025/11/07**

Connecting the computers in a Local Area Network (LAN)

Objectives:

- To connect multiple computers in a Local Area Network (LAN)**.**

Apparatus (Software):

- Windows Operating System on all participating computers.
- Administrator privileges for configuration**.**

On the host computer:

Follow these steps to share the internet connection:

Step:1: Log on to the host computer as Administrator or as Owner.
Step:2: Click Start, and then click Control Panel.
Step:3: Click Network and Internet Connections.
Step:4: Click Network Connections.
Step:5: Right-click the connection that you use to connect to the Internet.
For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up/other network available.
Step:6: Click Properties.
Step:7: Click the Advanced tab.
Step:8: Under Internet Connection Sharing, select the Allow other network users to connect through this computer's Internet connection check box.
Step:9: If you are sharing a dial-up Internet connection, select the Establish a dial-up connection whenever a computer on my network attempts to access the Internet check box if you want to permit your computer to automatically connect to the Internet.
Step:10: Click OK, you receive the following
When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0.1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?
Step:11: Click Yes.
The connection to the Internet is shared to other computers on the local area network (LAN).
The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0.1 and a subnet mask of 255.255.255.0

On the client computer:

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP Configuration, and then configure the client computer. To confirm the LAN adapter IP configuration,
follow these steps:

Step:1: Log on to the client computer as Administrator or as Owner.
Step:2: Click Start, and then click Control Panel.
Step:3: Click Network and Internet Connections.
Step:4: Click Network Connections.
Step:5: Right-click Local Area Connection and then click Properties.
Step:6: Click the General tab, click Internet Protocol (TCP/IP) in the connection uses the following items list, and then click Properties.
Step:7: In the Internet Protocol (TCP/IP) Properties dialog box, click Obtain an IP address automatically (if itis not already selected), and then click OK.
Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 192.168.0.254. For example, you can assign the following static IP address, subnet mask, and default gateway:
Step:8: IP Address 192.168.31.202
Step:9: Subnet mask 255.255.255.0
Step:10: Default gateway 192.168.31.1
Step:11: In the Local Area Connection Properties dialog box, click OK.
Step:12: Quit Control Panel.

Results:
Successfully established a Local Area Network where client computers can access the Internet through the host computer.

Conclusion:
This practical demonstrates the procedure for setting up a Local Area Network and sharing an Internet connection among multiple computers. The configuration involves enabling Internet Connection Sharing on the host computer and setting up the network adapter properties on the client computers. Proper understanding of IP addressing and network settings ensures seamless connectivity and optimal performance.

Lab no: 5 **Date: 2025/10 /08**

Study of basic network command and network configuration commands.

Objectives:
Study of basic network command and network configuration commands.

Apparatus (Software):
Command Prompt / Packet Tracer.

Procedure:
To perform this experiment, follow these steps:

In this EXPERIMENT- students have to understand basic networking commands e.g ping, tracert. All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This command includes.

- **Configuring the Router commands:**
  Commands used to set up and configure router interfaces (e.g., assigning IP addresses, enabling Ip address).

- **General Commands to configure network:**
  General commands for managing network settings (e.g., setting default gateways, configuring VLANs.

- **Privileged Mode commands of a router:**
  Learn commands used in privileged mode for accessing advanced features and settings**.**

- **Router Processes & Statistics:**
  Commands to monitor and analyze router performance, such as show running-config and show Processes.

- **IP Commands:**
  Commands related to IP configuration and troubleshooting, including ping, tracert, and ipconfig.

- **Other IP Commands (e.g. show ip route etc):**
  Use advanced commands like show ip route to view routing tables.

Command Descriptions:

ping:

The ping command is used to test network connectivity by sending an ICMP ECHO_REQUEST packet to a specified host. If the host is reachable, it responds with an ICMP ECHO_REPLY, confirming connectivity.

Usage example: Ping 8.8.8

This checks connectivity to Google's public DNS server.

```
C:\>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=1ms TTL=64
Reply from 192.168.101.1: bytes=32 time=1ms TTL=64
Reply from 192.168.101.1: bytes=32 time=1ms TTL=64
Reply from 192.168.101.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.101.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

tracert:

The tracert command (short for trace route) displays the path that packets take to reach a specific destination. It lists all intermediary routers (hops) the packet passes through. It also measures the time taken for each hop.

Usage example: tracert www.example.com

This traces the route taken to reach the domain **www.example.com**.

```
C:\>tracert 192.168.101.1

Tracing route to 192.168.101.1 [192.168.101.1]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.101.1 [192.168.101.1]

Trace complete.
```

Conclusion:

This experiment offered hands-on experience with both basic and advanced network configuration commands. By practicing commands like ping, tracert, and various router configuration commands, students developed a deeper understanding of:

- Verifying network connectivity.
- Tracing the paths of network packets.
- Configuring and managing routers efficiently.

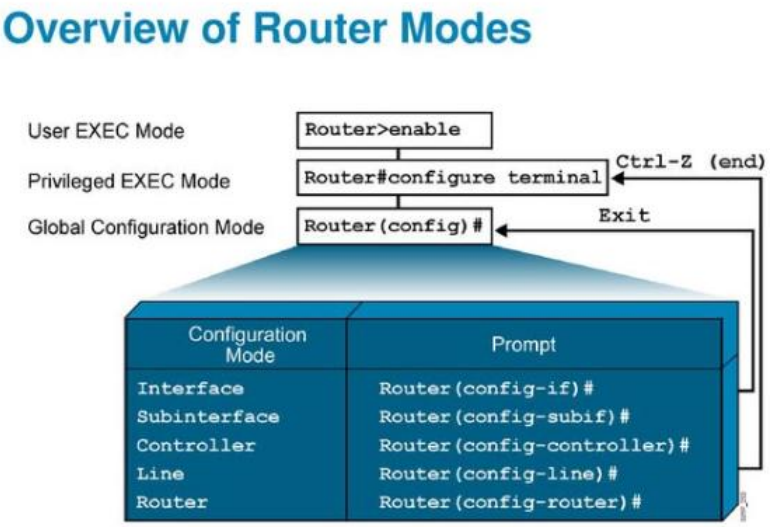
These skills are fundamental for troubleshooting, optimizing network performance, and performing system administration tasks, forming a strong foundation for advanced networking concepts

Lab no: 6 **Date: 2025/10 /11**

Introduction to Packet Tracer: Basic Router Configuration

Objective(s):
To understand basic commands for router configuration.

Packet Tracer:
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.



Features of Cisco Packet Tracer:

- **High-Fidelity Emulation:** Simulates Cisco network devices and protocols with high accuracy.
- **Dynamic Topology Design:** Create and modify complex network topologies with real-time updates.
- **CLI Emulation:** Provides a command-line interface similar to actual Cisco devices for real-world command practice.
- **Detailed Device Management:** Configure settings such as IP addresses, VLANs, and routing protocols.

Interface of Cisco Packet Tracer:
The interface of Cisco Packet Tracer is designed to be user-friendly, with various panels and tools that simplify network design and simulation.

Workspace Details:
The Workspace in Cisco Packet Tracer serves as the central area where users can design, configure, and manage network topologies. It offers an interactive, visual environment for creating and adjusting network setups. Users can easily drag and drop devices like routers, switches, and end devices onto the workspace and connect them using a variety of cables.

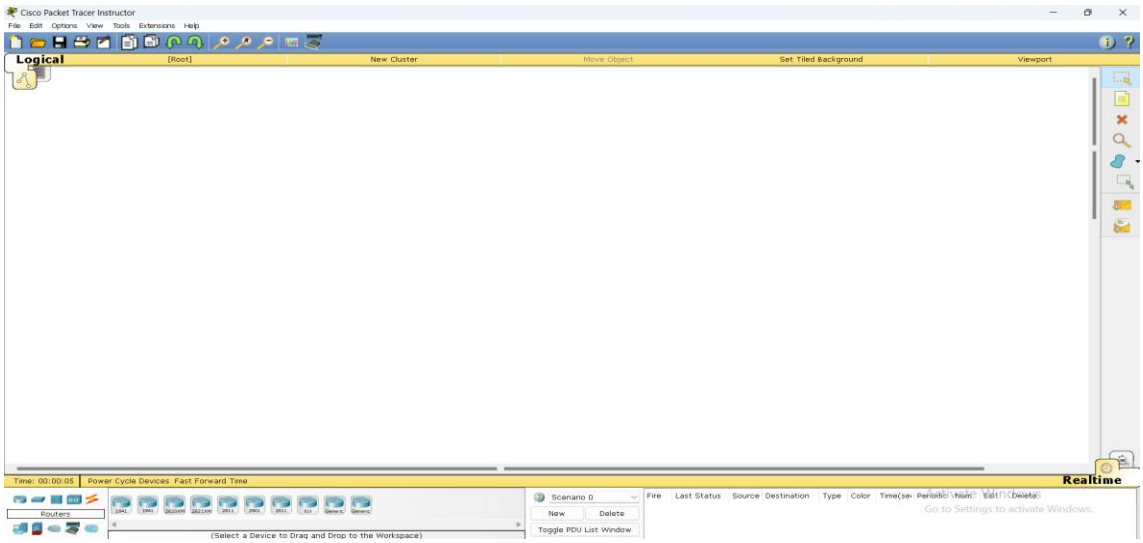


Fig: Cisco packet tracer workspace

Toolbar:
The Toolbar in Cisco Packet Tracer offers quick access to essential functions, such as saving and opening files, zooming in and out, and controlling the simulation process. It also allows users to switch between different views, like physical and logical views, of the network. The toolbar enhances workflow efficiency by providing direct access to frequently used tools and settings.

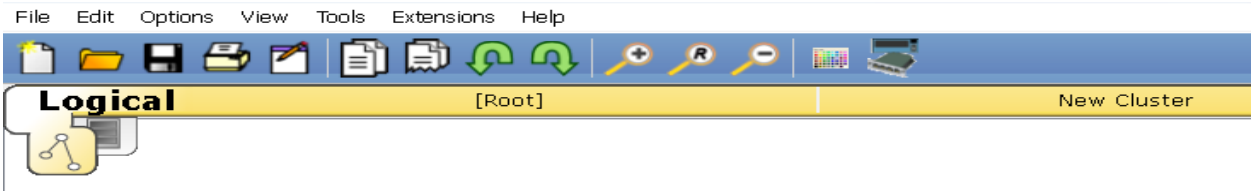


Fig: Toolbar in cisco packet tracer

Device-Type Selection Panel
The Device-Type Selection Panel, located on the left side of the interface, organizes network devices into categories such as Routers, Switches, End Devices, Wireless Devices, and more. This structure makes it easy to select and place devices into the network topology. Using drag-and-drop functionality, users can quickly add devices to the workspace. The panel typically includes search and filter options, allowing for fast access to specific devices

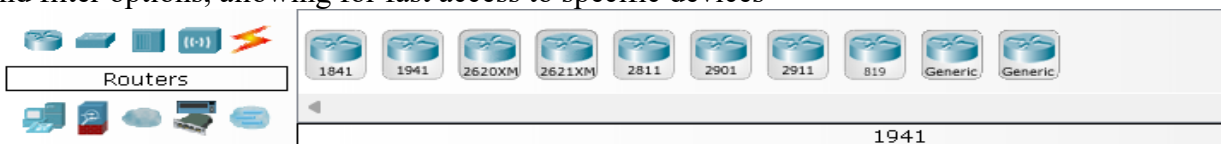


Fig: Device selection panel

Device Configurations

After adding a device to the workspace, its settings can be customized through a configuration window. This includes tasks such as assigning IP addresses, setting up routing protocols, and enabling features like DHCP or NAT. Users have the flexibility to choose between a graphical interface or a command-line interface (CLI) for configuration.

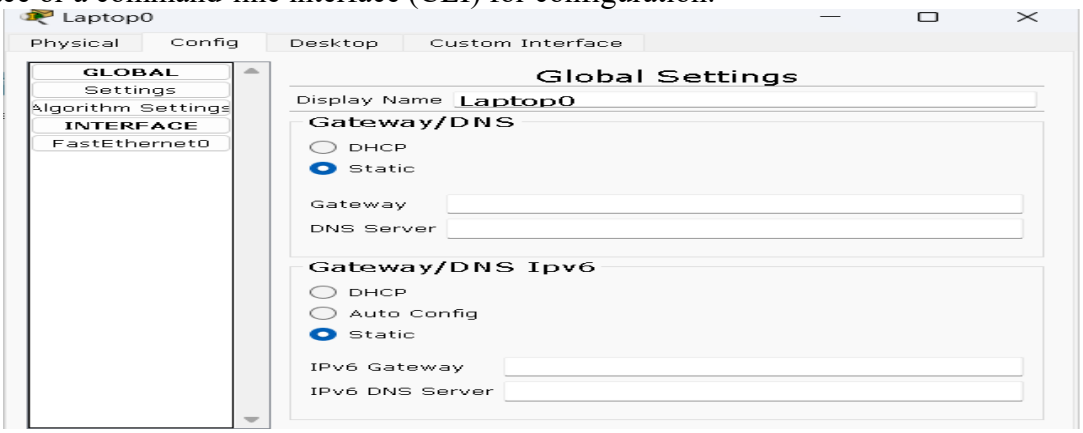


Fig: Device configuration setting

Real-Time and Simulation Mode:

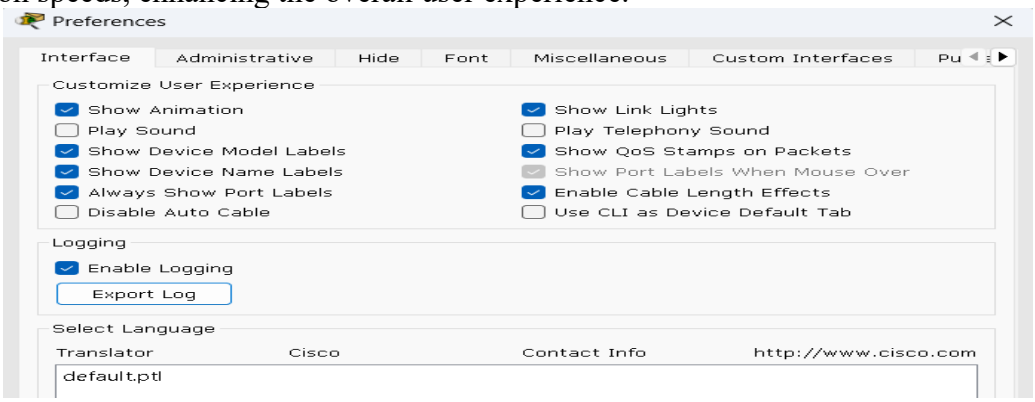
In Cisco Packet Tracer, Real-Time Mode and Simulation Mode provide distinct functionalities for network design and analysis.

- **Real-Time Mode** simulates live, real-world network operations, allowing users to interact with and configure the network in real-time, with immediate feedback on changes.
- **Simulation Mode** offers a more detailed analysis by allowing users to pause and step through network operations, enabling them to observe packet flow and network behavior.

Fig: Different modes in cisco packet tracer

Options and Preferences

The Options and Preferences menu in Cisco Packet Tracer allows users to customize the software environment according to their preferences. Through this menu, users can adjust visual settings like background color and font size, set default values for device configurations, and control simulation speeds, enhancing the overall user experience.



Activity Wizard:

The Activity Wizard is a tool in Cisco Packet Tracer designed to create interactive learning modules. It enables educators to develop structured tasks, provide step-by-step instructions, and set up assessments for students. This feature is particularly valuable in educational settings, as it allows instructors to design engaging exercises that guide students through practical networking scenarios, helping them apply theoretical knowledge in a hands-on, controlled environment.

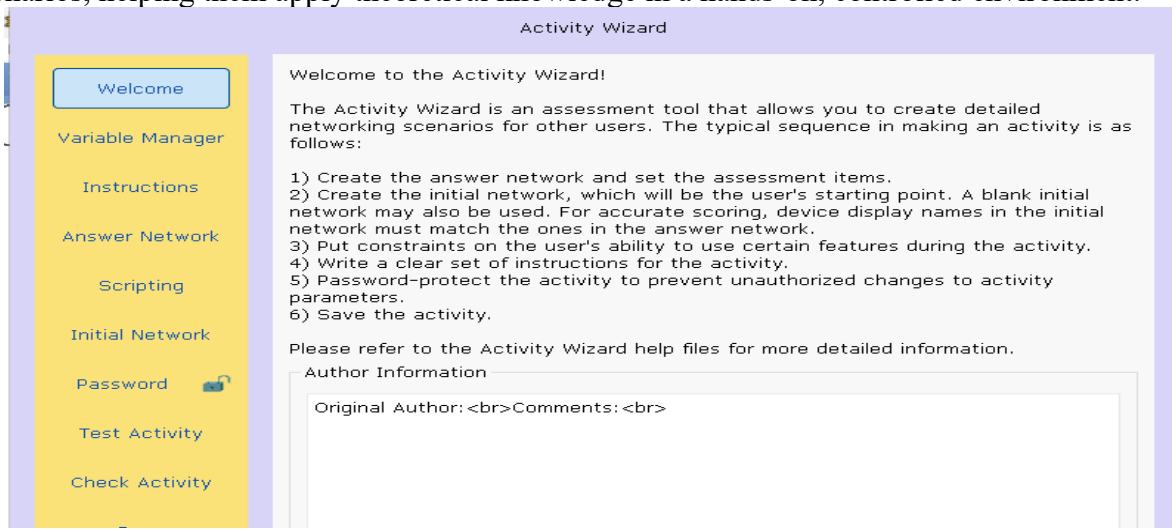


Fig: Activity wizard features

Configuration Steps:

1. Change Hostname (Cisco)
2. Configure passwords (password: cisco & secret: class)
3. Secure Console Port and Terminal lines (password: cisco)
4. Encrypt Passwords (service password-encryption)
5. Configure Clock (clock)
6. Configure Banners (banner motd)
7. Configure Interface (IP Address) on Router (interface fa0/0 or fa0/1)
8. Configure VLAN on Switch (interface vlan 1)
9. Save configurations (running-config to startup-config)
10. Use show commands:

```
show running-config
show startup-config
show ip interface brief
show interface vlan 1
```

11. Configure PCs
12. Verify Connectivity (ping)

Conclusion:

Cisco Packet Tracer offers a comprehensive environment for network design and analysis. It enables detailed configuration of network devices, supports both real-time interactions and advanced simulations for in-depth analysis, and provides intuitive icons and labels to effectively organize and visualize network components.

Lab no: 7 **Date: 2025/11/14**

Creating a LAN and testing the connectivity using Packet Tracer

Theory:
A Local Area Network (LAN) connects computers and devices within a confined geographical area, such as a home, office, or building. LANs enable resource sharing, including files, printers, and internet connections, among multiple devices. Due to their limited coverage, LANs typically offer higher data transfer speeds and lower latency compared to larger networks like Wide Area Networks (WANs).

Objective(s):
To design a LAN in Packet Tracer and test device connectivity.

Apparatus (Software):
Packet Tracer Software

Star Topology
A star topology is a network structure where all devices are connected to a central hub, switch, or computer. This central device is often called the hub or switch, and it acts as a server for the network. In a star topology, devices don't connect to each other directly, but instead send messages to the hub, which then forwards them to the intended recipient.

Component Used
Hardware: Switches (1), Ethernet cables, End devices(5).
Software: Cisco Packet Tracer

Network Diagram

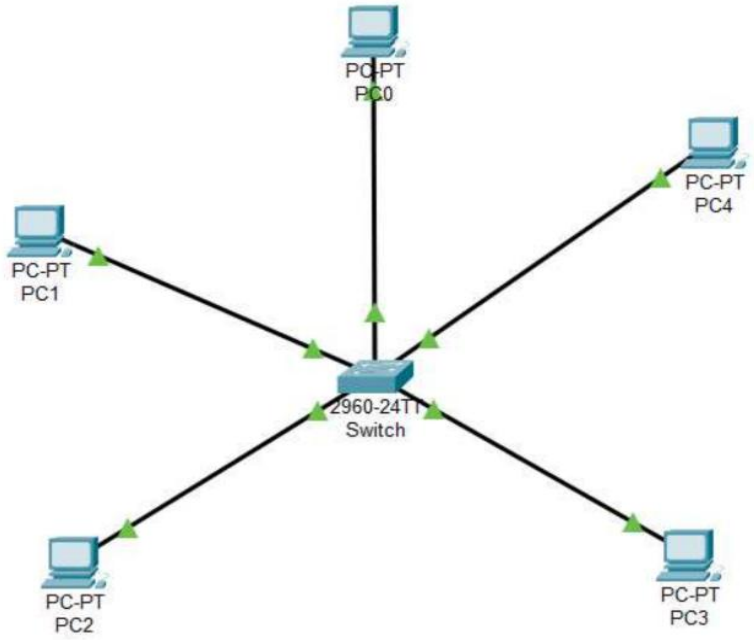


Fig: Network map for star topology

Procedure:
Here is the procedure for creating the Star Topology shown in the image using Cisco Packet Tracer:

Step 1: Launch Cisco Packet Tracer

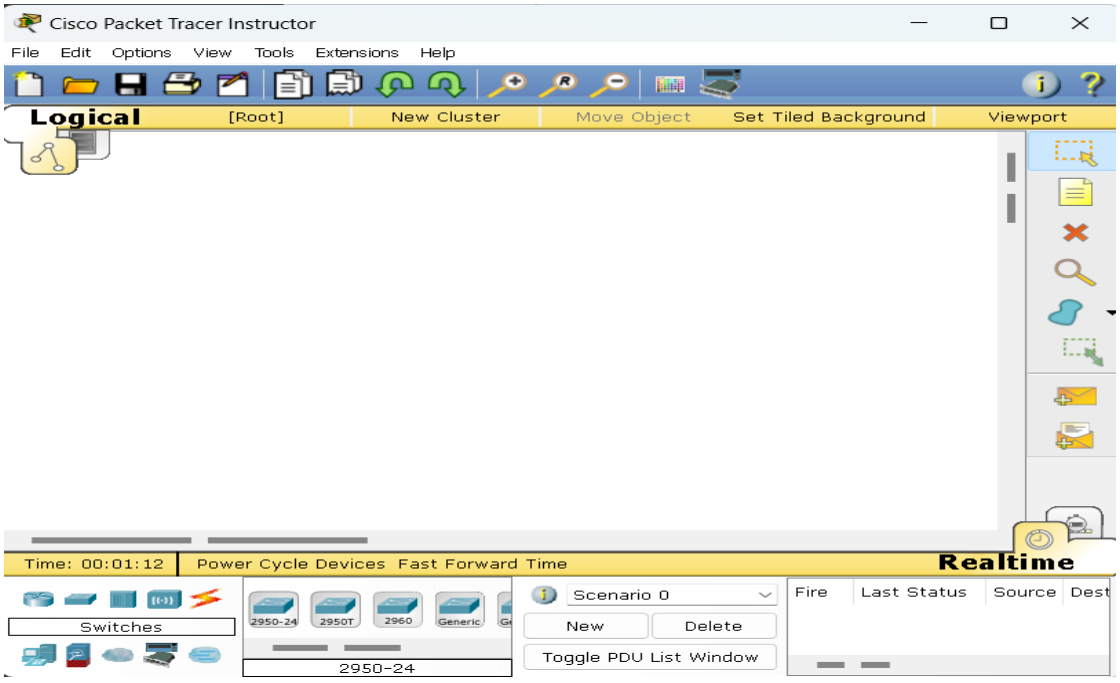


Fig: Workspace for cisco packet tracer

Step 2: Add the network devices to the workspace.

2.1 From the Device-Type Selection box, choose the following devices and add them to the workspace:
2.2 One 2960-24TT Switch
2.3 Five PCs (labeled PC0, PC1, PC2, PC3and PC4)

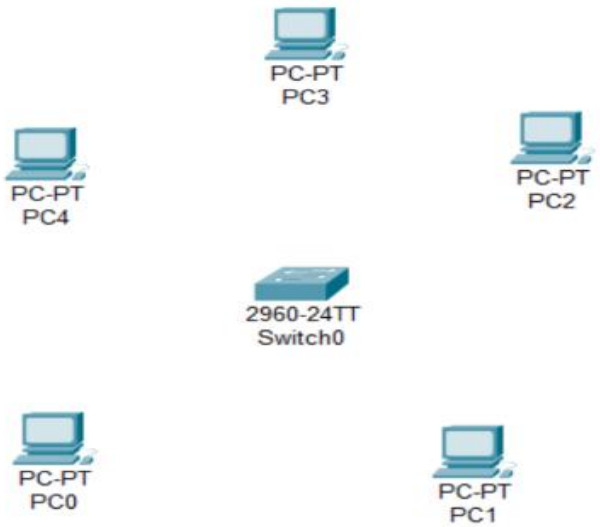


Fig: switches and PC's for star topology

Step 3: Connect the devices

3.1 Use the copper straight-through cable to connect each PC to one of the available ports on the switchs.

3.2 Ensure that each connection is made properly.

3.3 Also renamed the PC's as PC0(10.0.0.1), PC1(10.0.0.2), PC2(10.0.0.3), PC3(10.0.0.4) and PC4(10.0.0.5).

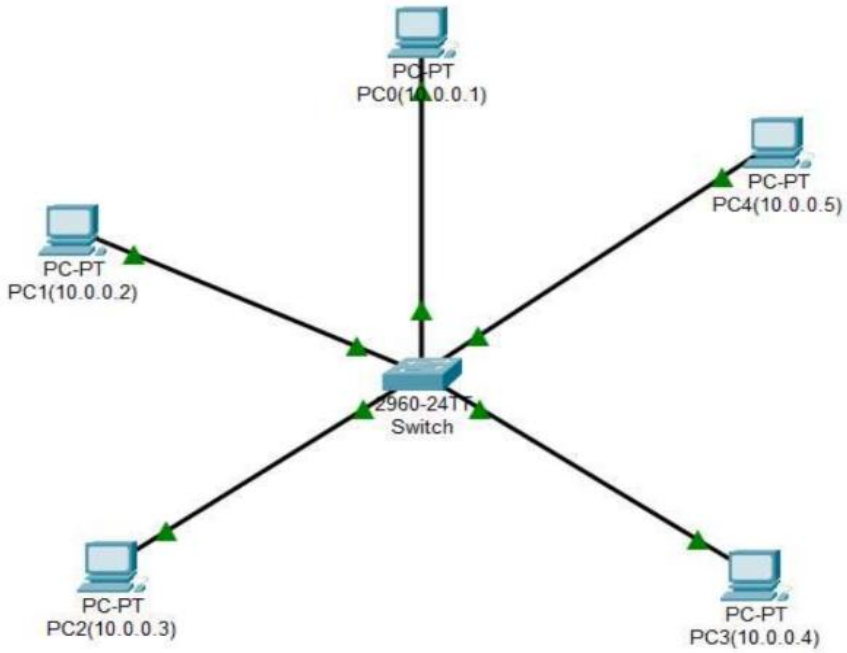


Fig: Connection between switch and PC's

Step 4: Configure IP addresses

4.1 Right-click on each PC and select "IP Configuration."

4.2 In the IP Configuration window, enter the IP address as (10.0.0.1 to 10.0.0.5), subnet mask, and default gateway for each PC .

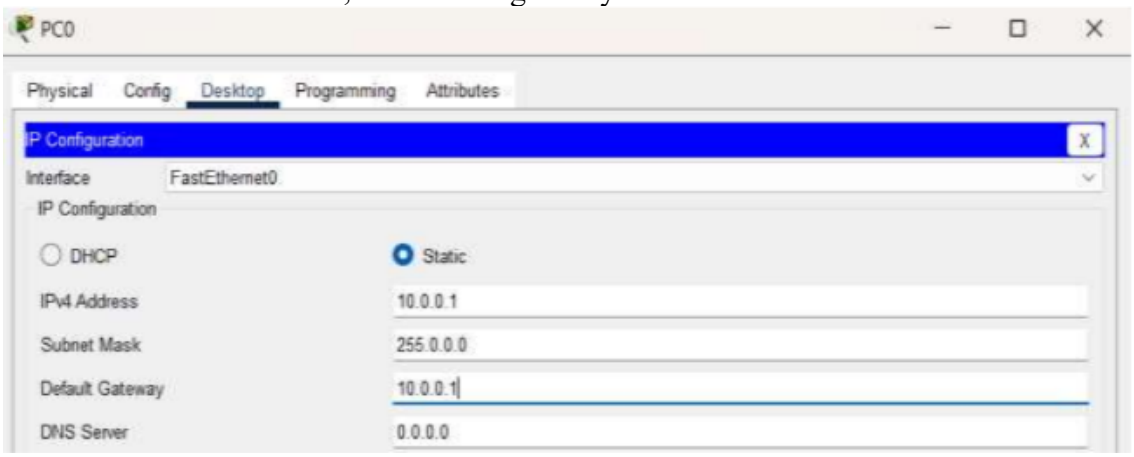


Fig: IP configuration

Step 5: Verify connectivity:

5.1 To test whether the network is working, you can ping other devices on the network from each PC.

5.2 Now ping PC0(10.0.0.1) from PC2(10.0.0.3) and vice-versa.

5.3 If the ping is successful, you should see replies from the other device.

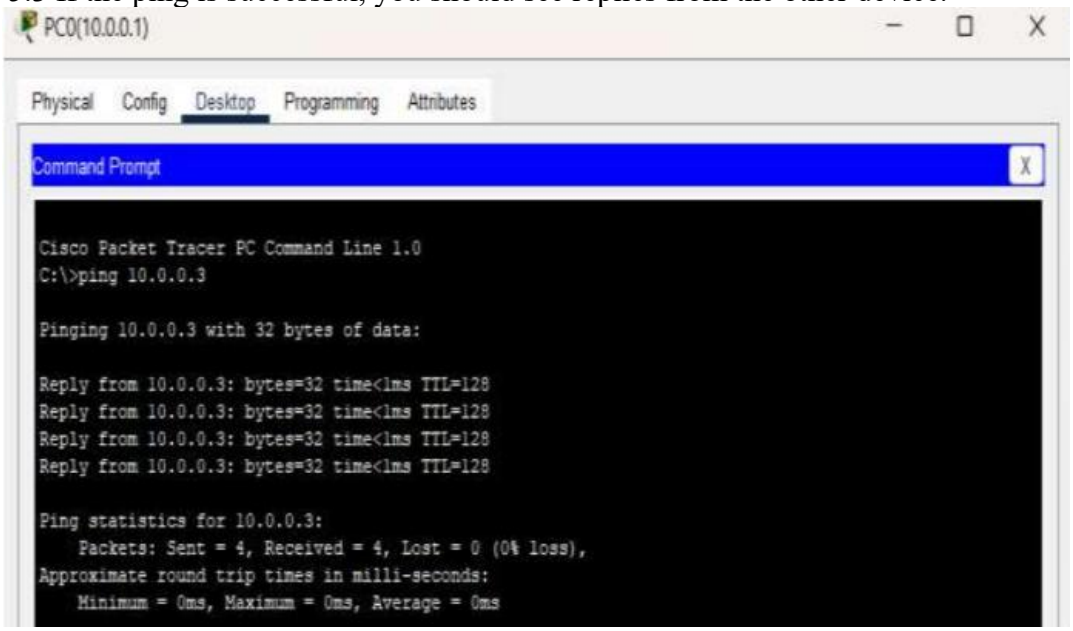


Fig:Connectivity test from PC0(10.0.0.1) to PC2(10.0.0.3)

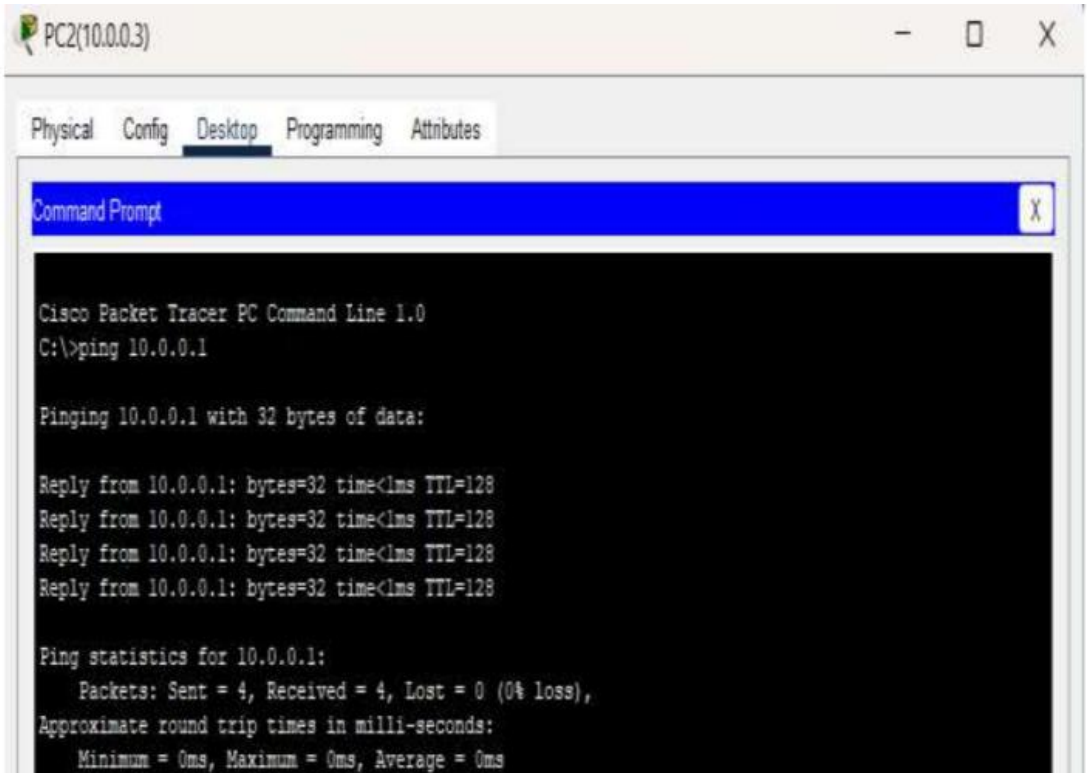


Fig: Connectivity test from PC2(10.0.0.3) to PC0(10.0.0.1)

Conclusion

In conclusion, creating network topologies using Cisco Packet Tracer offers a powerful and flexible approach to network design and simulation. By using its comprehensive set of tools and device-type selection panel, and various configuration options, users can accurately model and analyze all network topologies. This hands-on experience enhances understanding and prepares users for practical applications in real-world networking tasks. Overall, Packet Tracer is an invaluable resource for both learning and professional development in the field of networking.

Lab no: 8 **Date: 2025/10/13**

Configuring a Network Using Distance Vector Routing Protocol (RIP)

Objectives:
Configuring a network using the Distance Vector Routing Protocol (RIP).

Apparatus (Software):
Packet Tracer Software

Procedure:

1. Introduction to RIP:

RIP (Routing Information Protocol) is a Distance Vector Routing Protocol that helps determine best route for data packets within a network. It uses hop count as a metric to find the shortest path, with a maximum hop count of 15, which limits the size of the network it can handle.

2. Topology Design:

Create the Network Topology:

- Use Cisco Packet Tracer to design a network topology.
- Add multiple routers, switches, and end devices (PCs) as needed.
- Connect devices using the appropriate cables:
    - Crossover cables for router-to-router connections.
    - Straight-through cables for router-to-switch or switch-to-PC connections.

3. Configuring RIP via GUI:

Assign IP Addresses:

- Assign unique IP addresses to all router interfaces and end devices within their respective subnets.

Enable RIP on Routers:

1. Open the configuration window for each router.
2. Go to the Routing tab and select RIP.
3. Add the network addresses connected to each router into the RIP routing table.
4. Save the configuration.

Verify Connectivity:

- Use the Simulation Tool in Packet Tracer to send packets from one network segment to another.
- Ping devices across different subnets to ensure routing is working correctly.

4. Testing the Configuration:

Verify Router Communication:

- Check that routers are exchanging routing information by verifying RIP routes.
- Use the show ip route command (optional, via CLI) to inspect RIP routing tables on each router.

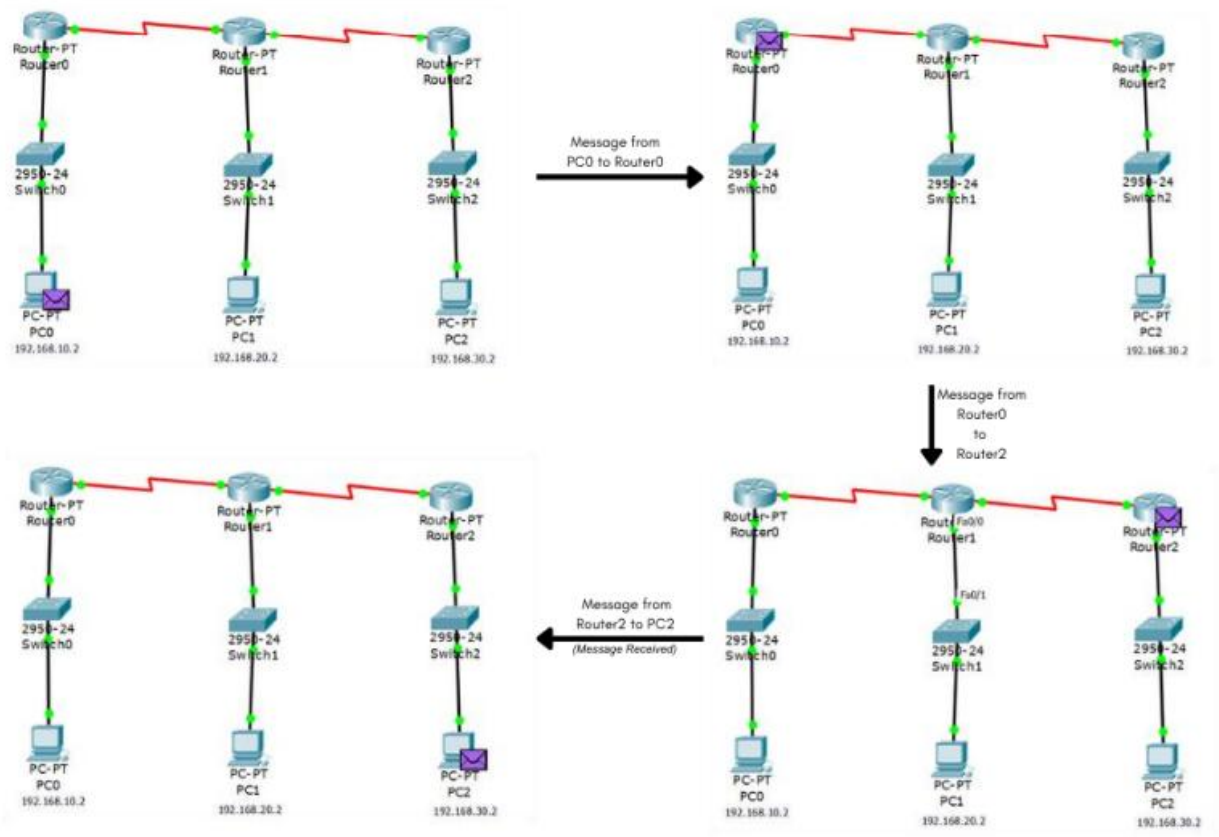
Confirm Device Connectivity:

- Ensure that all connected devices can communicate with each other seamlessly, confirming the proper functionality of the RIP configuration.

Observations:

- All routers successfully exchanged RIP routing tables.
- Devices within different subnets were able to communicate with each other.
- Packets followed the expected shortest path based on the hop count.

Simulation Diagram (Stepwise):



Conclusion:

The network was successfully configured using RIP as the Distance Vector Routing Protocol. The routing tables were properly populated, enabling effective inter-subnet communication. This practical exercise highlighted the key concepts of Distance Vector Routing and demonstrated its practical application in network design and management.

Sarfraj Alam

MBM
Madan Bhandari Memorial College

Lab no: 9 **Date: 2025/10 /16**

Configuring a Network Using Link-State Vector Routing Protocol (OSPF)

Objectives:
• To understand and configure a network using the link-state routing protocol.
• To implement Open Shortest Path First (OSPF) routing in a simulated environment.

Apparatus/ Software:
Cisco Packet Tracer

OSPF:
Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system.

OSPF operates by:
1. Establishing Neighbor Relationships
2. Building Link-State Advertisements (LSAs)
3. Calculating Shortest Paths
4. Updating Dynamically

Procedure:

Step 1: Setting Up the Network Topology
- Open Cisco Packet Tracer and create a new project.
- Place the routers, switches, and end devices (such as PCs) in a structured and logical topology layout.
- Connect devices using the correct cables:
  - **Straight-through cables** for router-to-switch or switch-to-PC connections.
  - **Crossover cables** for router-to-router connections.

Step 2: Configuring Basic Router Settings
- Assign IP addresses to each router interface and the connected end devices.
- Plan and allocate the subnets, ensuring logical IP address distribution across the network.
- Configure each router with essential settings, including:
  - Assigning a hostname to uniquely identify each router.
  - Activating r
  - outer interfaces to enable network communication (e.g., using the no shutdown command).

Step 3: Enabling OSPF Routing Protocol
- Access the configuration terminal of each router.
- Enable the OSPF routing protocol by entering the configuration mode.
- Assign a unique process ID to the OSPF instance on each router.

- Define OSPF areas and associate router interfaces with specific areas to establish proper OSPF routing.

Step 4: Verifying OSPF Configuration

- Use commands like show ip ospf neighbor to verify OSPF neighbor relationships.
- Check the routing tables with show ip route to confirm the OSPF routes are properly included.

Step 5: Testing Connectivity

- Utilize ping and traceroute to ensure end-to-end connectivity across the network.
- Verify that packets are routed using the optimal OSPF path, minimizing latency and maximizing efficiency.

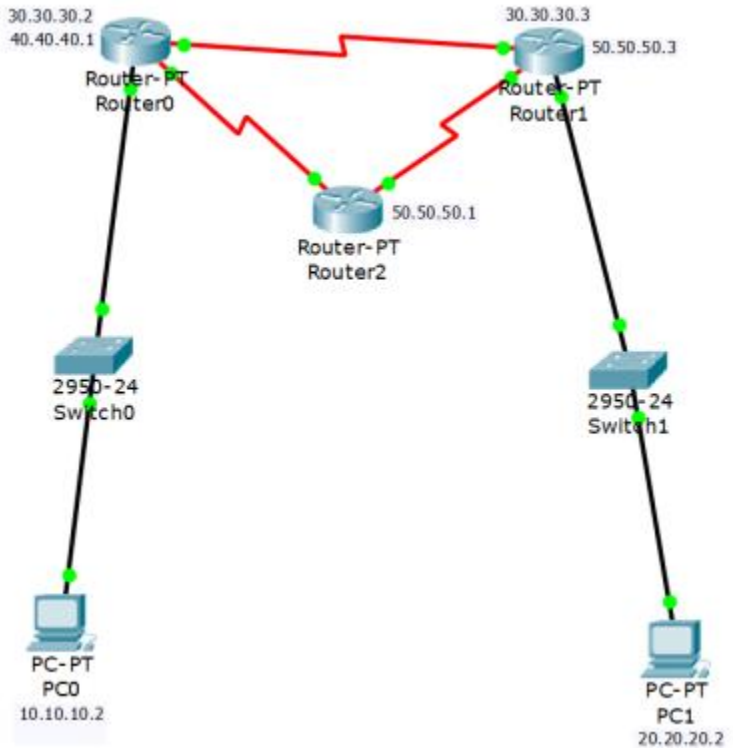
Step 6: Monitoring Packet Transfers

- Switch to simulation mode in Cisco Packet Tracer.
- Monitor OSPF-specific packets such as Hello, DBD (Database Description), Link State Request, and Link State Update to ensure proper packet exchange.

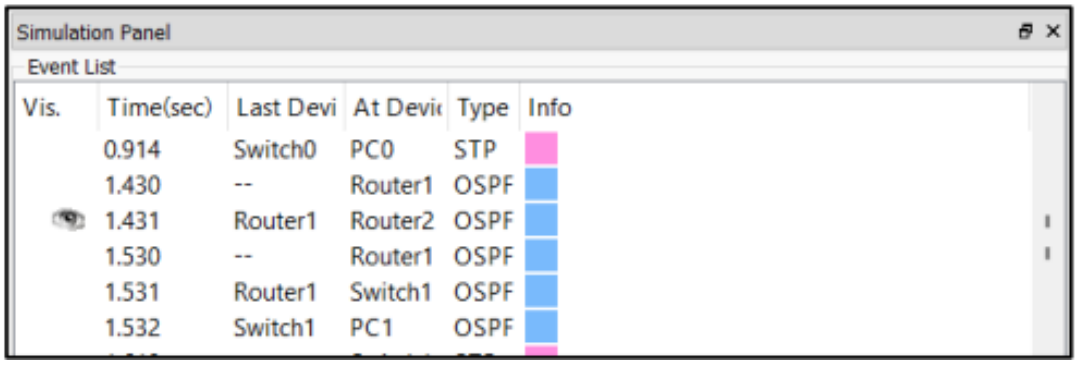
Observations:

- OSPF adjacencies and neighbor relationships were successfully established.
- The shortest path was selected, ensuring minimal latency and optimal network performance.
- Route convergence time and packet delivery ratios met acceptable standards, indicating efficient network operation.

Simulation diagram:



Simulation output:



Conclusion:

This lab demonstrated the successful implementation of the OSPF routing protocol in a simulated environment. OSPF's link-state approach enabled optimized routing, highlighting its effectiveness in managing complex and dynamic networks.

Sarfraj Alam

MBM
Madan Bhandari Memorial College

Lab no: 10 **Date: 2025/10/1**

OS Installation in a Virtual Machine using VMware Workstation

Objectives:

- Install a Linux OS (Fedora) on a virtual machine using VMware Workstation.
- Learn the steps to set up a virtual machine and configure the OS.
- Understand virtualization and its role in running multiple OS on one physical machine.

Introduction

In this lab, we will install Fedora, a Linux operating system, on a virtual machine using VMware Workstation. Fedora is a great choice because:

1. **Latest Features:** It includes the newest tools and technologies, perfect for developers and tech enthusiasts.
2. **Community Support:** A strong community offers plenty of resources for learning and troubleshooting.
3. **Stable and Fast:** Fedora is known for its reliability, performance, and hardware support with the latest Linux kernel.
4. **Great for Developers:** It supports various programming languages and tools, making it ideal for coding and application development.
5. **User-Friendly Interface:** The GNOME desktop provides a simple and intuitive experience.
6. **Frequent Updates:** Regular updates ensure you have the latest features and security patches.
7. **Educational Value:** Fedora is great for learning Linux, including package management, system setup, and shell scripting.

Installing Fedora in a virtual machine allows safe experimentation without affecting the host system. This report outlines the steps to create a virtual machine, install Fedora, and configure it for use.

Apparatus:

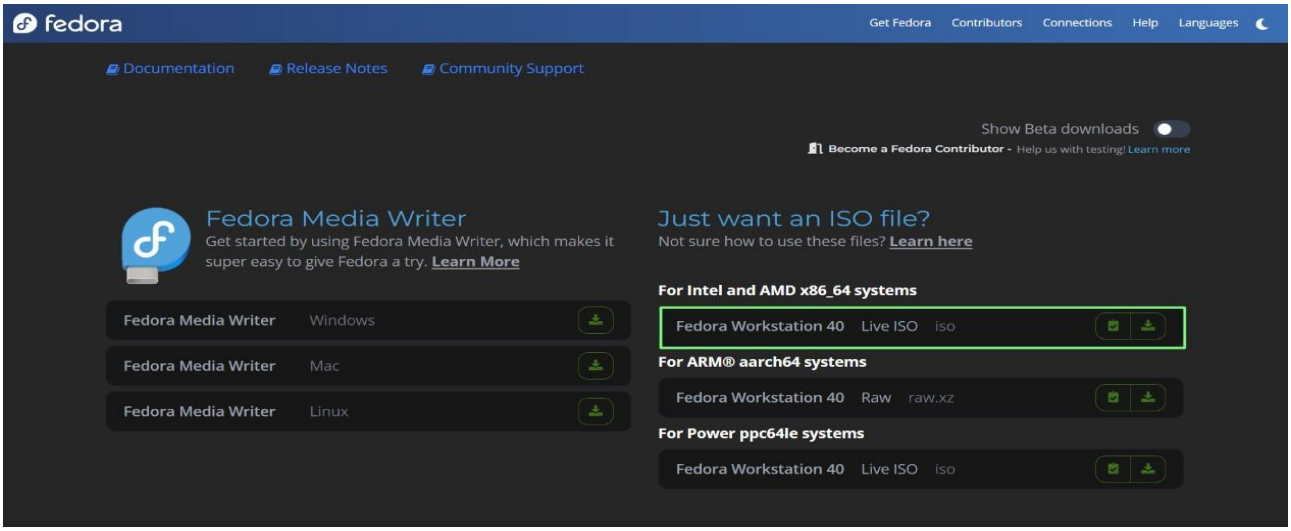
1. **VMware Workstation:** Installed on the host system.
2. **Fedora ISO File:** Downloaded from the official Fedora website.
3. **Host System:** A PC or laptop running Windows, Ubuntu, or CentOS.
4. **Minimum System Requirements for VMware Workstation:**
    - 64-bit processor
    - 2 GB RAM (4 GB or more recommended)
    - 2 GB disk space for VMware Workstation
    - ~20 GB or more free disk space for Fedora installation

Procedure:

Step:1: Download Fedora ISO:

- Visit the Fedora official website: https://fedoraproject.org/workstation/download.
- Select the latest version of Fedora (Workstation or Server Edition).

- Choose the appropriate architecture (64-bit for most PCs).
- Download and save the ISO file to an accessible location.

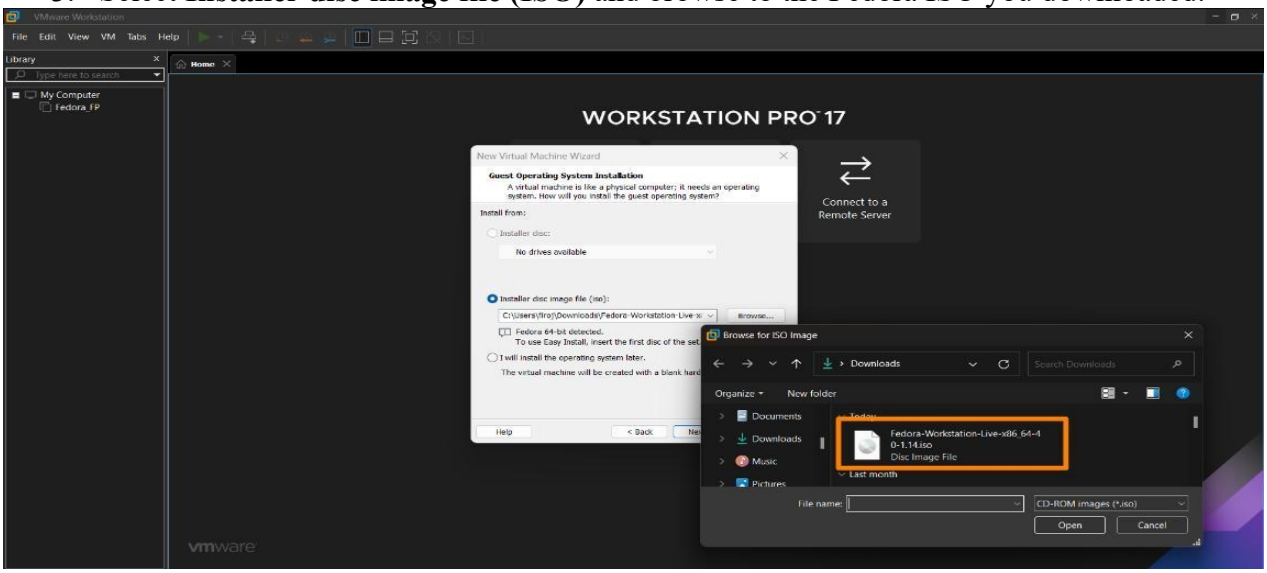


Step:2: Install VMware Workstation:

- Download VMware Workstation from the official VMware website if not already installed.
- Follow the installation steps and launch the application.

Step:3: Create a New Virtual Machine in VMware:

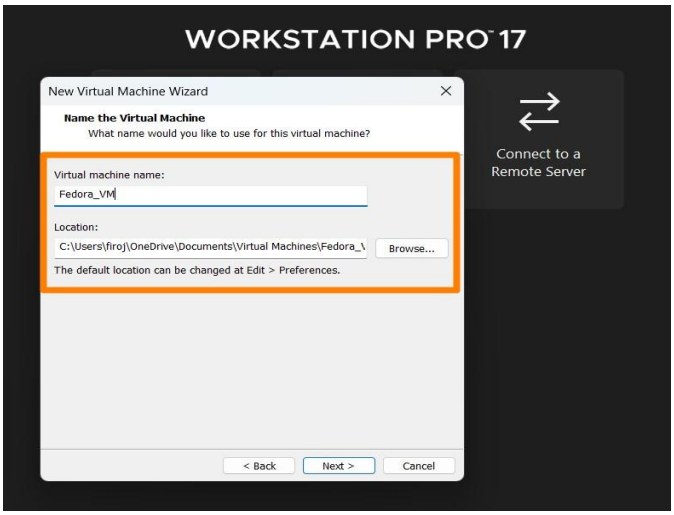
1. Open VMware Workstation and select **Create a New Virtual Machine**.
2. Choose **Custom (advanced)** for detailed configuration or **Typical** for a standard setup.
3. Select **Installer disc image file (ISO)** and browse to the Fedora ISO you downloaded.



Step:4: Configure the Virtual Machine:

1. Name the virtual machine (e.g., **Fedora_VM**) and choose a location to save the virtual machine files.

2. Set the disk capacity. Create a new virtual hard disk with at least 20 GB (30 GB or more recommended).
3. Click **Customize Hardware** to adjust the memory (default is 2 GB), network adapter, and other devices as needed.
4. Click **Finish** to create the virtual machine.



Step:5: Booting and Installing Fedora:

1. Start the virtual machine from the VMware dashboard. Select the virtual machine and click **Power on this Virtual Machine**.
2. The virtual machine will boot from the Fedora ISO image, and the Fedora installer will load.
3. From the boot menu, select **Start Fedora** to begin the installation.

Step:6: Fedora Installation Process:

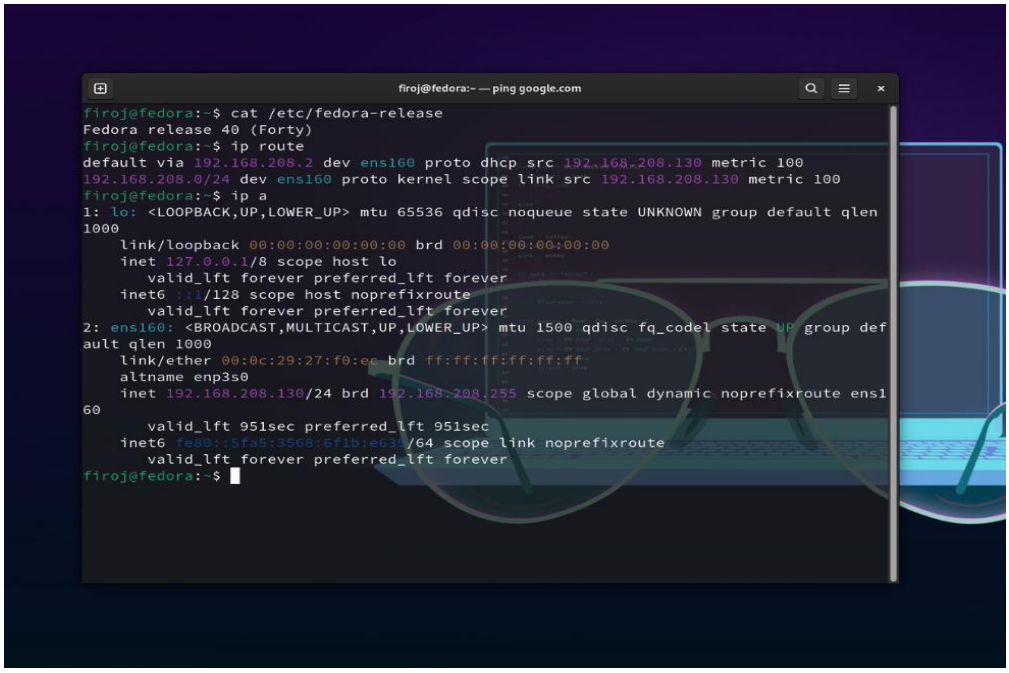
1. Choose your preferred **language** and click **Continue**.
2. Select the **installation destination** (the virtual disk created earlier). Use **Automatic Partitioning** unless you need custom partitioning.
3. Set your **time zone** and **keyboard layout** (Fedora will detect the default settings automatically).
4. Set the **root password** and create a **user account** with administrative privileges.
5. Click **Begin Installation** and allow the process to complete. This may take several minutes, depending on your system.

7. Testing the Installation:

- After installation, verify that Fedora is working by performing basic tasks:
  - Open a terminal and run system commands.
  - Check network connectivity.
  - Run the update command:

```
sudo dnf update
```

  - Install essential software (e.g., web browser, text editor).



Result:
Fedora was successfully installed on the virtual machine using VMware Workstation. The system is fully operational, and all necessary configurations have been completed.

Conclusion:
This lab offered valuable hands-on experience in setting up a virtual machine, installing Fedora, and configuring it for use. It also demonstrated how VMware Workstation enables the creation of isolated environments for OS installations, making it an effective tool for system testing, development, and learning without affecting the host system.

Lab no: 11 **Date: 2025/ 11 /22**

Router Configuration using Command Line Interface

Objective

The objective of this lab is to configure a Cisco router using Command Line Interface (CLI) commands. The configuration process involves:

- Setting the router's hostname.
- Securing the device with passwords.
- Configuring network interfaces.
- Enabling login access.

This lab is conducted in an educational environment as part of networking exercises, with "MBM" serving as the host identifier for the router.

Equipment Used

- Cisco Router (Physical or virtual via Cisco Packet Tracer)
- Console Cable (for physical setups)
- PC or Terminal Emulator Software (e.g., PuTTY)
- Access to Cisco IOS version 12.4(15)T1
-

Steps Performed

1. **Initial Router Setup**
   When the router was powered on, the startup configuration appeared, displaying the device specifications and the Cisco IOS version. The router then prompted whether to continue with the configuration dialog or proceed directly to the CLI.

```
Router>
```

- **Command Used:** None (during the startup phase).
- **Observation:** The router booted into EXEC mode, ready for configuration.

2. **Exploring Available Commands**
   While in EXEC mode (indicated by the Router> prompt), the ? help function was used to explore available commands. This provided a list of commands with brief descriptions, include
   - **connect**: Establish a connection.
   - **disable**: Exit privileged EXEC mode.
   - **enable**: Enter privileged EXEC mode.
   - **show**: Display device information.

```
Router>?
```

- **Observation:** The ? function effectively lists all available commands along with concise descriptions.

3. **Setting the Hostname**
   The router was switched to global configuration mode to assign the hostname "MBM."

- **Commands Used:**

```
Router>enable
Router#configure terminal
Router(config)#hostname MBM
MBM(config)#
```

- **Observation:** The router prompt updated to reflect the new hostname: MBM>.

4. **Securing the Router**
   To secure access, a password was configured for the console line, and login functionality was enabled.

- **Commands Used:**

```
MBM(config)#line console 0
MBM(config-line)#password cisco
MBM(config-line)#login
MBM(config-line)#exit
```

- **Observation:** The console now requires a password for authentication, enhancing security.

5. **Configuring Interfaces**
   To configure interfaces such as FastEthernet0/0, IP addresses and subnet masks were assigned according to the network requirements. The interface was then activated by using the no shutdown command, enabling network communication through that interface.

- **Commands Used:**

```
MBM(config)#interface FastEthernet0/0
MBM(config-if)#ip address 192.168.1.1 255.255.255.0
MBM(config-if)#no shutdown
MBM(config-if)#exit
```

6. **Saving the Configuration**
   After completing the configuration of the router's interfaces and settings, the configuration was saved to the router's startup configuration file. This ensures that all changes persist after a reboot.

- **Commands Used:**

```
MBM#write memory
```

- **Observation:**
  Upon saving the configuration, the router displayed a confirmation message indicating that the configurations had been successfully saved to the startup configuration. This prevents the loss of configurations during a restart or power cycle.

Security Features Implemented

1. **Password Protection:**
   - Console access secured with password (password cisco and login enabled).
   - Enable password set for privileged EXEC mode.
2. **Access Verification:**
   - Users prompted for authentication before access.
3. **Interface Management:**
   - Interfaces configured with IP addresses and activated using no shutdown.

Errors and Troubleshooting

1. **Invalid Input:**
   - Errors due to typos or incorrect syntax, resolved using the? help function.
2. **Interface Status:**
   - Interfaces initially "administratively down," resolved with no shutdown.

Final Configuration Summary

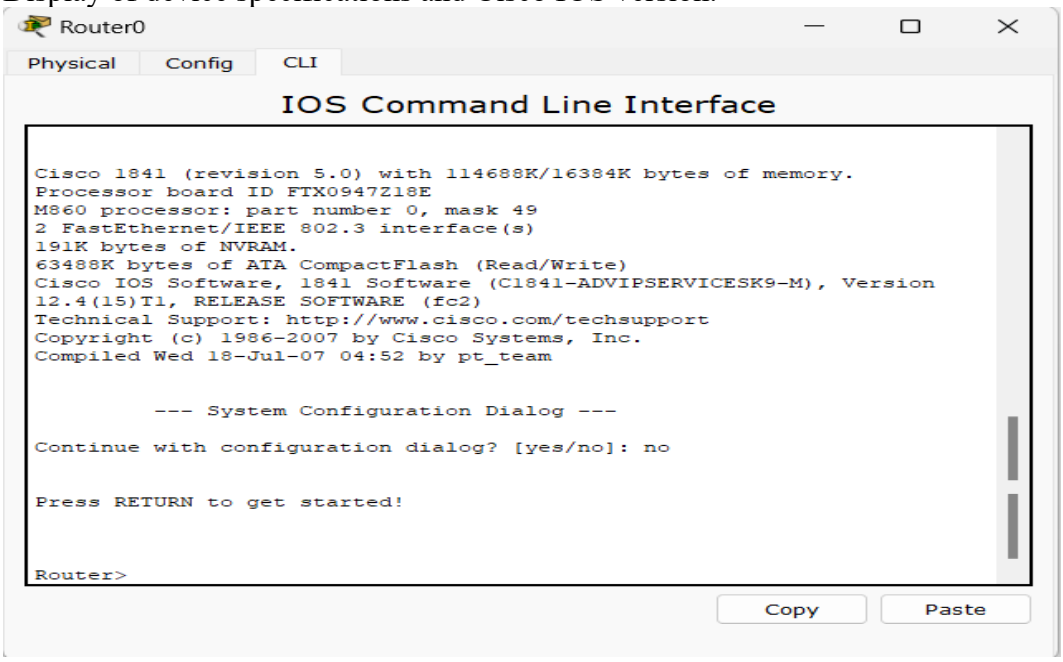
Below is a summary of the final router configuration:

```
hostname MBM
line console 0
 password cisco
 login
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
```

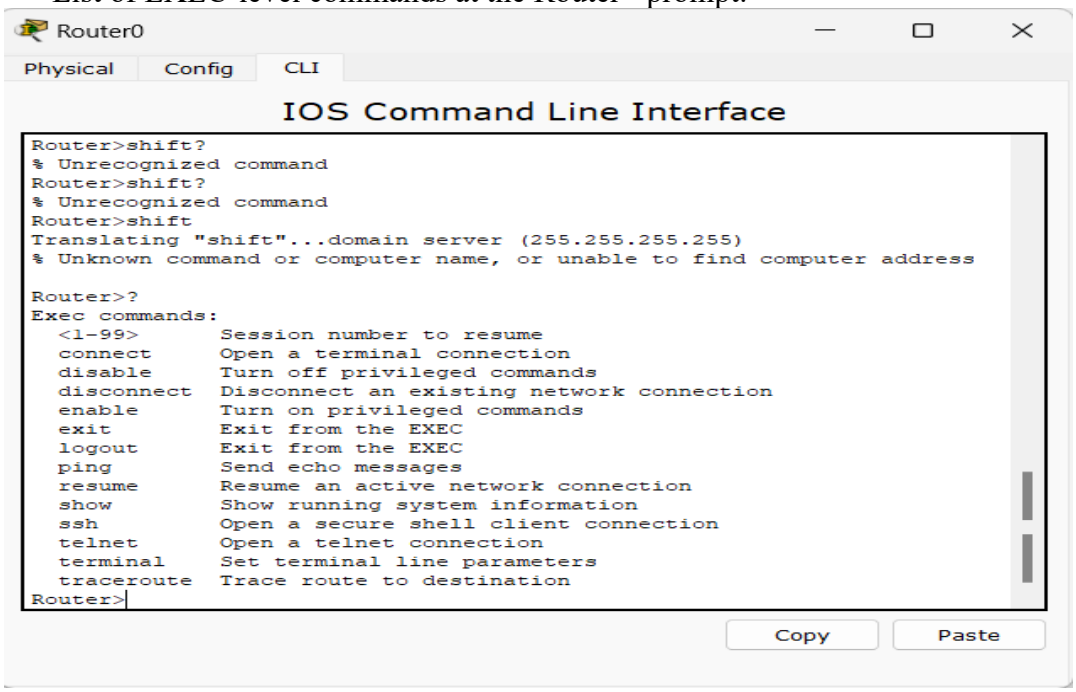
Screenshot Attachments

This section includes screenshots documenting the configuration process and its outcomes. Each screenshot is labeled with the corresponding step number and description for clarity.

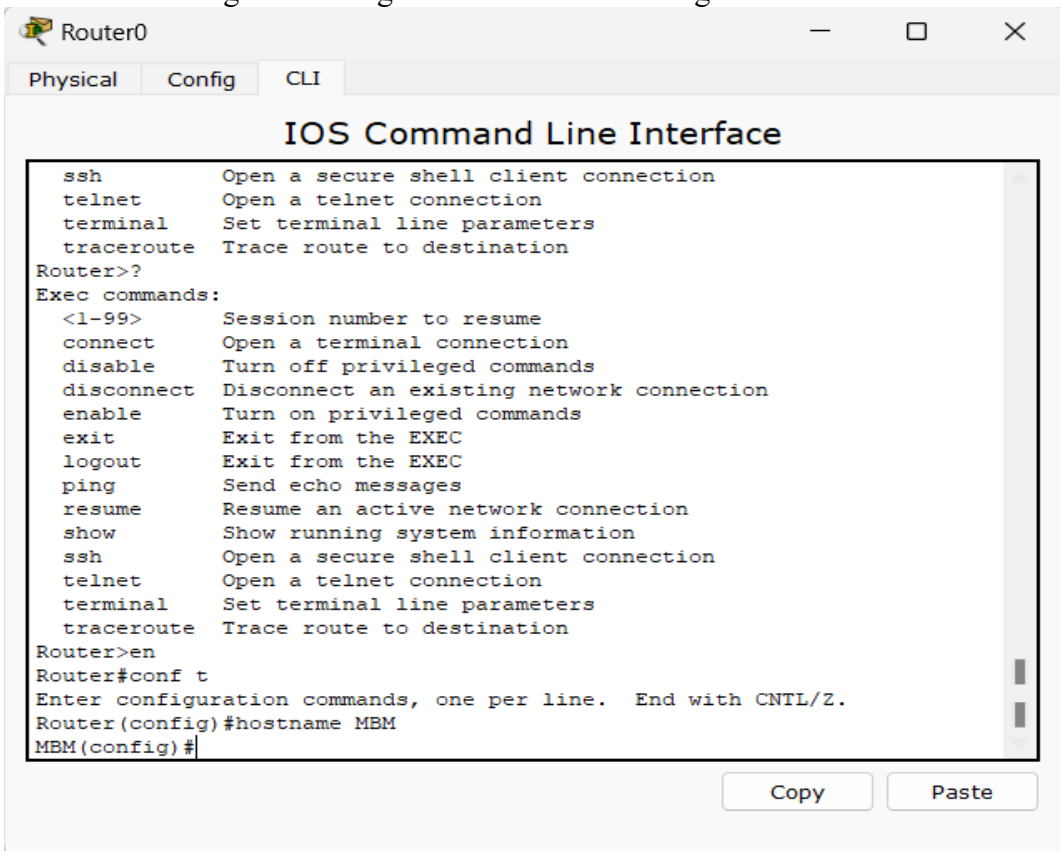
1. **Startup Configuration:**
   - Display of device specifications and Cisco IOS version.



2. **Available Commands:**
   - List of EXEC-level commands at the Router> prompt.



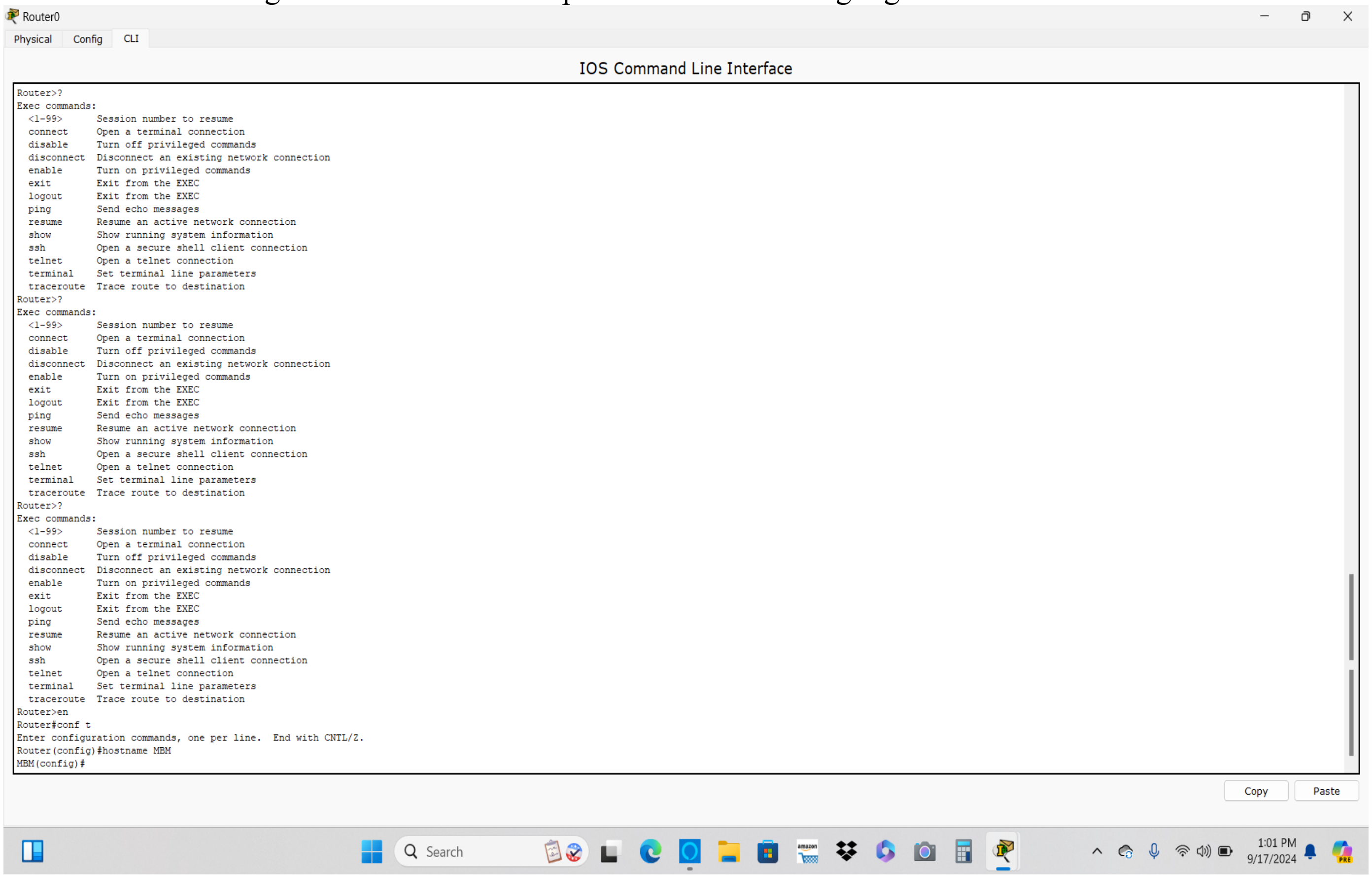
3. **Hostname Configuration:**
   - Transition to global configuration mode and setting the hostname to "MBM."

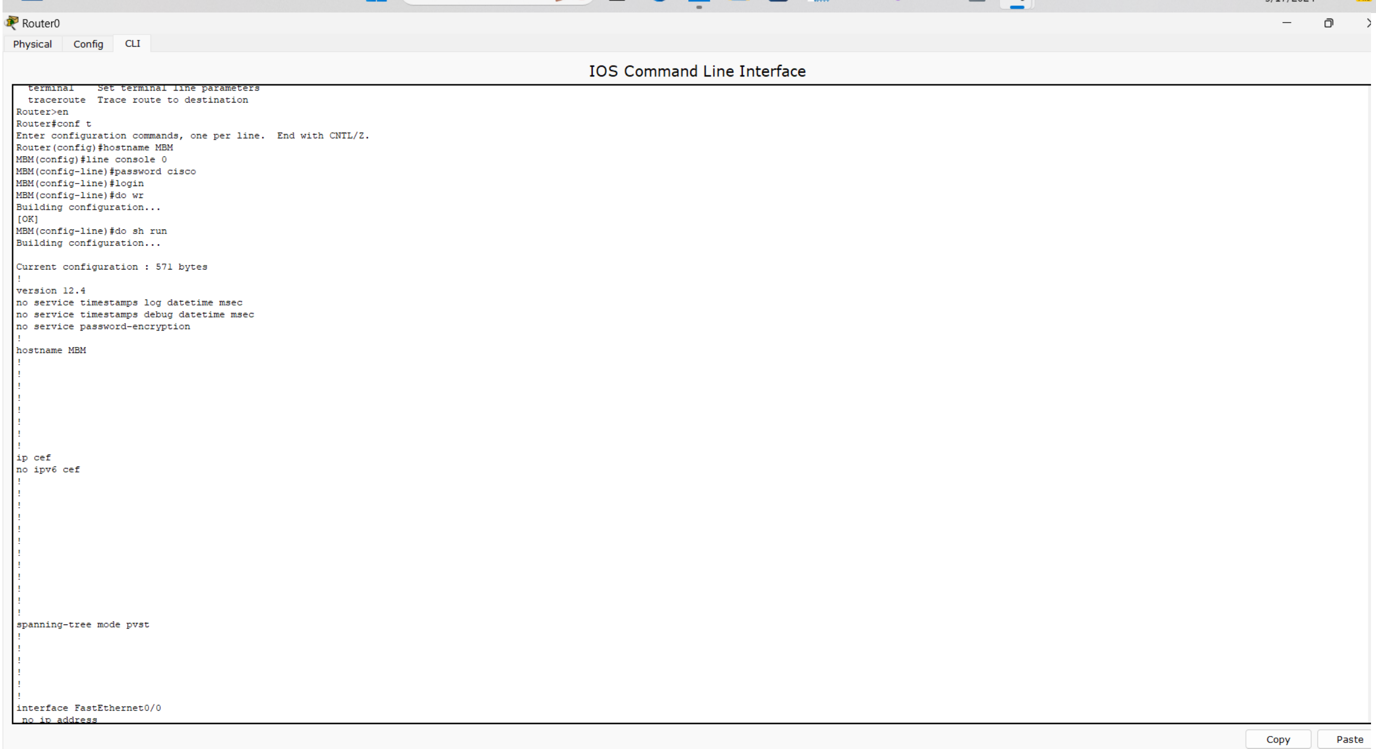


Sarfraj Alam

4. Password Protection:

- Configuration of the console password and enabling login.





Physical Config CLI

IOS Command Line Interface

```
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


MBM(config-line)#
```

Copy Paste

Physical Config CLI

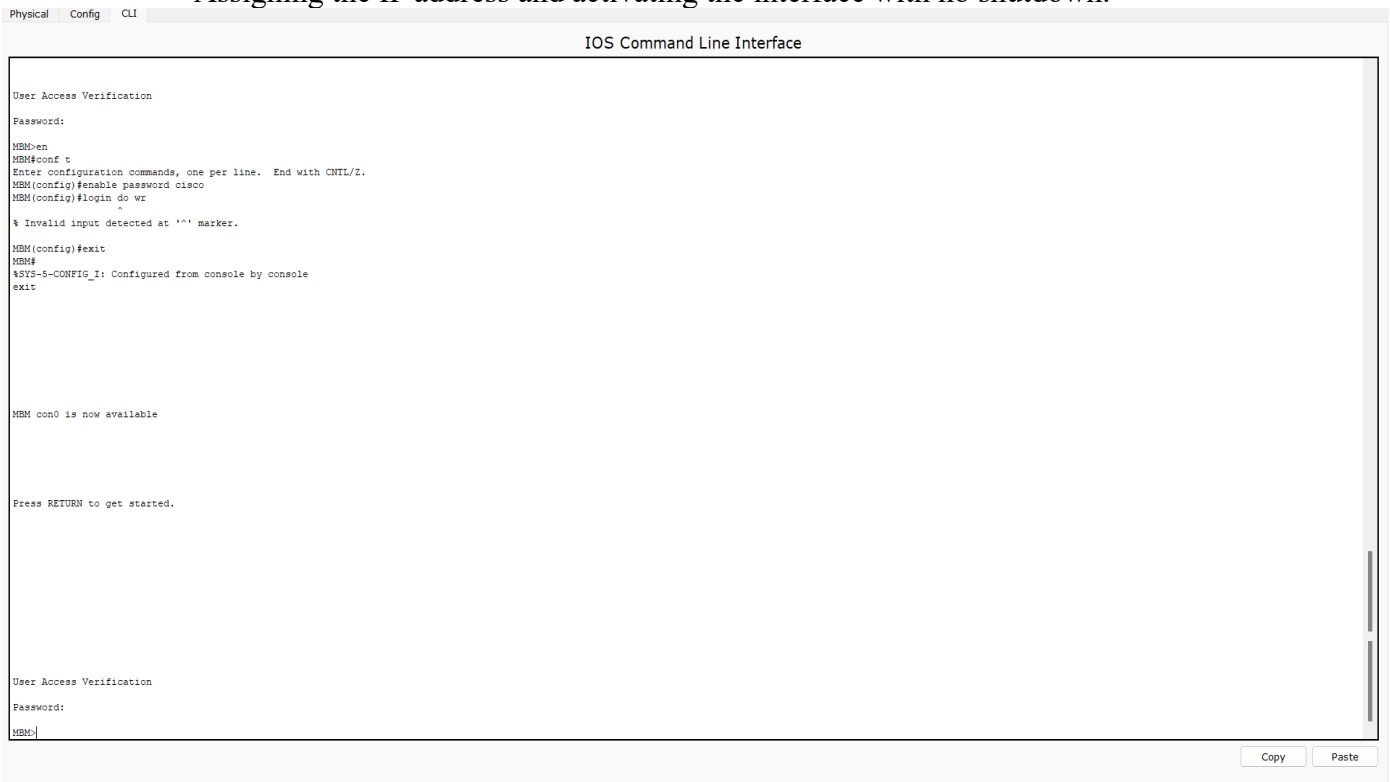
IOS Command Line Interface

```
!
!
end


MBM(config-line)#exit
MBM(config)#exit
MBM#
%SYS-5-CONFIG_I: Configured from console by console
exit









MBM con0 is now available




Press RETURN to get started.


















User Access Verification

Password:

MBM>en
MBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MBM(config)#enable password cisco
MBM(config)#login do wr
                    ^
% Invalid input detected at '^' marker.

MBM(config)#
```

Copy Paste

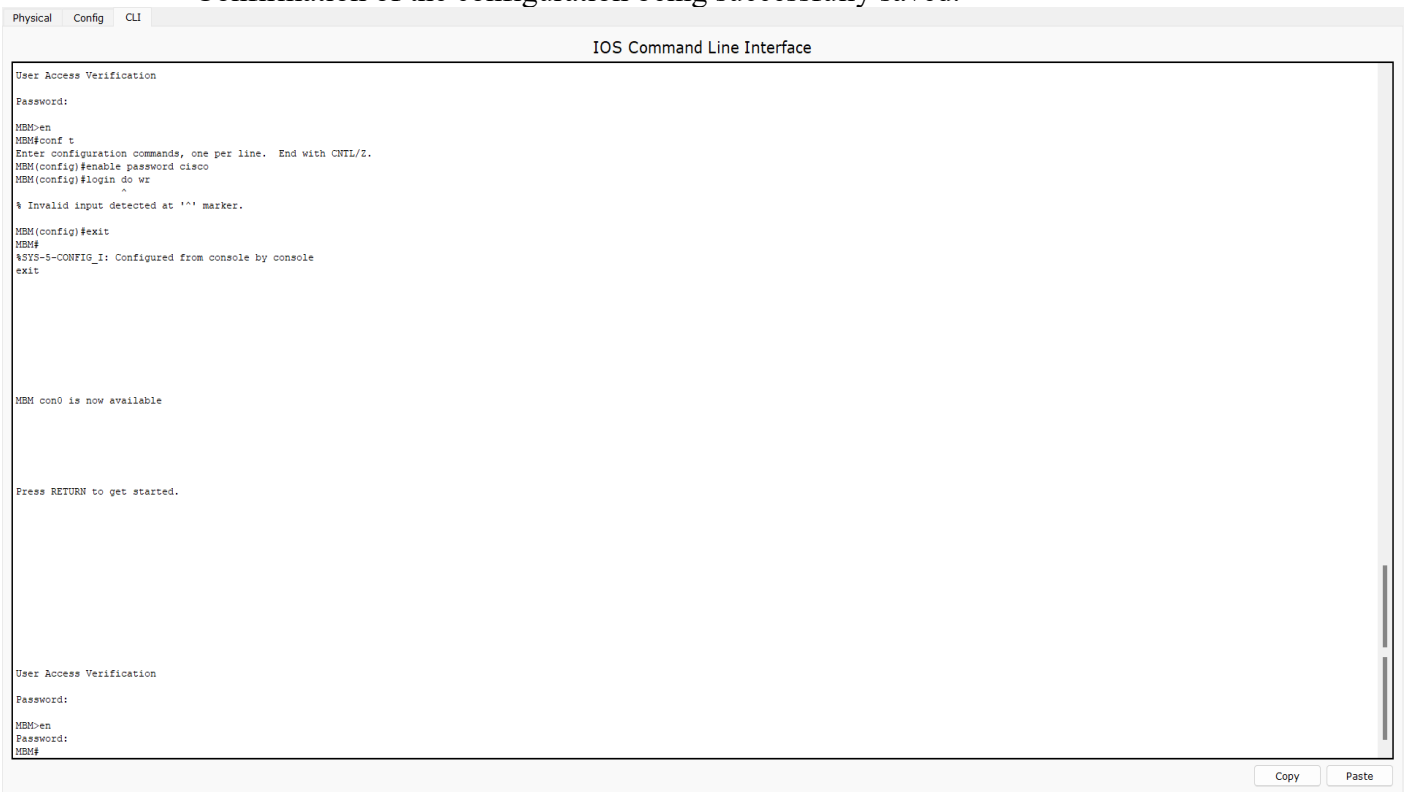
5. Interface Configuration:

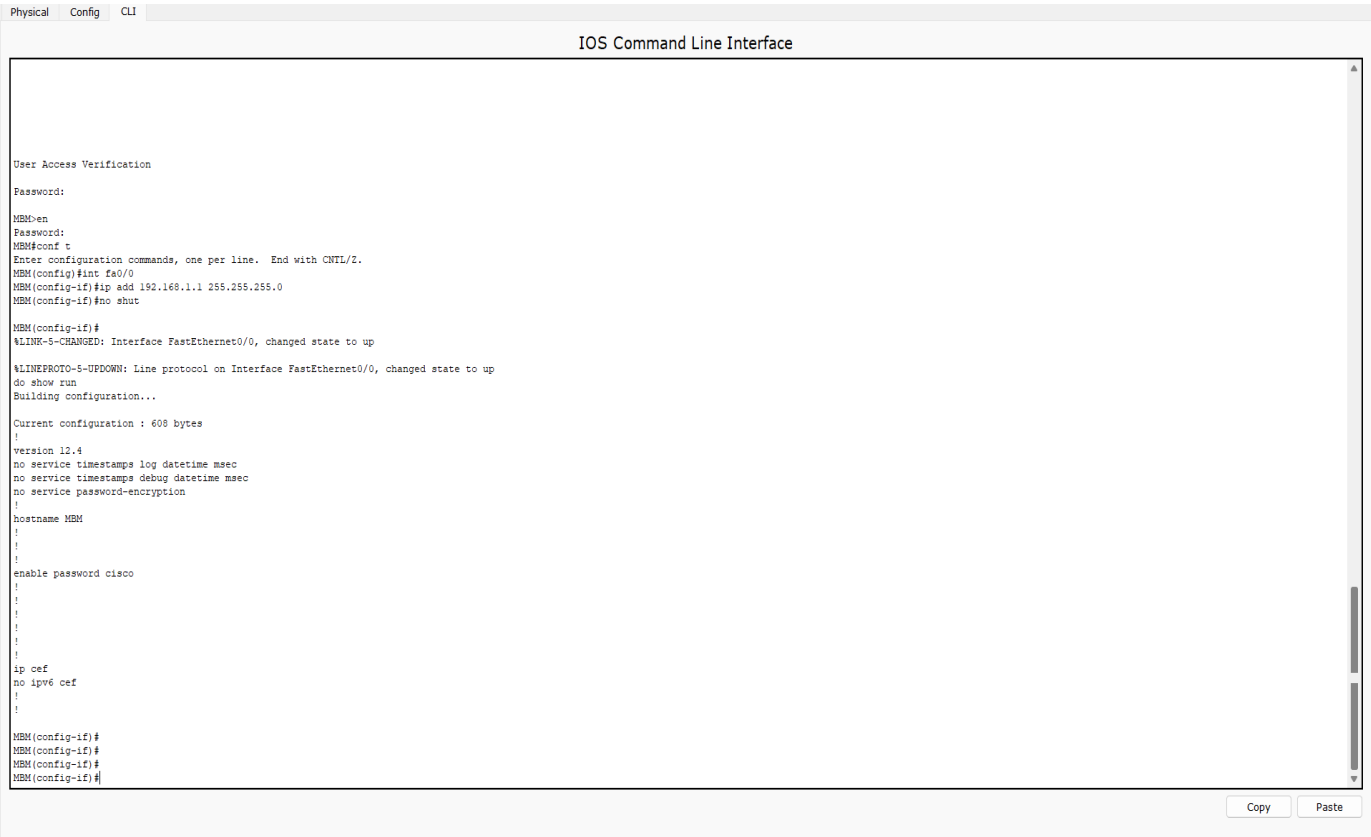
- Assigning the IP address and activating the interface with no shutdown.



6. Saving Configuration:

- Confirmation of the configuration being successfully saved.





Conclusion

This lab successfully showcased the process of configuring a Cisco router using the command-line interface (CLI). The key tasks involved included setting the router's hostname, implementing security measures through password protection, configuring network interfaces, and ensuring that configurations were saved for persistence. By configuring access controls and managing interfaces properly, the setup ensures a secure and operational network environment. These hands-on configurations provide essential knowledge of router management, which is critical for securing, troubleshooting, and maintaining a reliable network infrastructure.

Lab no: 12 . **Date: 2025/10/15**

Configuring DNS Server and HTTP Server for Domain Name Mapping.

Objectives:

- Configure and test the DNS server to resolve domain names to IP addresses.
- Set up and configure an HTTP server to serve web content.
- Verify network connectivity between devices using DHCP for automatic IP allocation.

Equipment and Software:

- **Cisco Packet Tracer**
- **Network Components:**
  - PC-PT (PC0)
  - Laptop-PT (Laptop0)
  - Server-PT (Server0)
  - 2960-24TT Switch

Part 1: DNS Server Configuration

Configuration Steps:

1. **Configure DNS Server on Server0:**
   - Enabled the DNS service on Server0.
   - Added a resource record:
     - **Name:** facebook.com
     - **Type:** A Record
     - **IP Address:** 192.168.1.1
   - Saved the record to ensure proper domain-to-IP mapping.
2. **Set up Web Page (index.html):**
   - Created a basic HTML page on Server0 under the HTTP service.
   - Page content includes:
     - **Title:** "Facebook"
     - Links to additional pages like helloworld.html, copyrights.html, and images.
   - Saved the file as index.html in the file manager.
3. **Verify Domain Name Resolution:**
   - Accessed the web page hosted on the HTTP server by entering http://facebook.com in the web browser on Laptop0.
   - The page loaded successfully, confirming that domain name resolution and DNS mapping were functioning correctly.

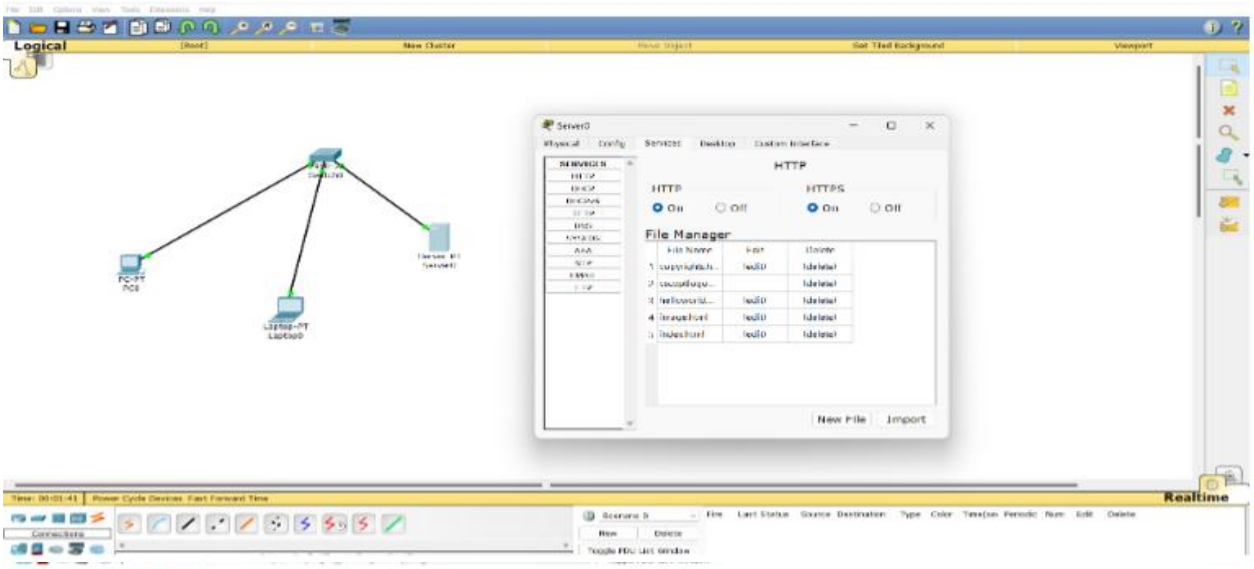
Part 2: HTTP Server Configuration

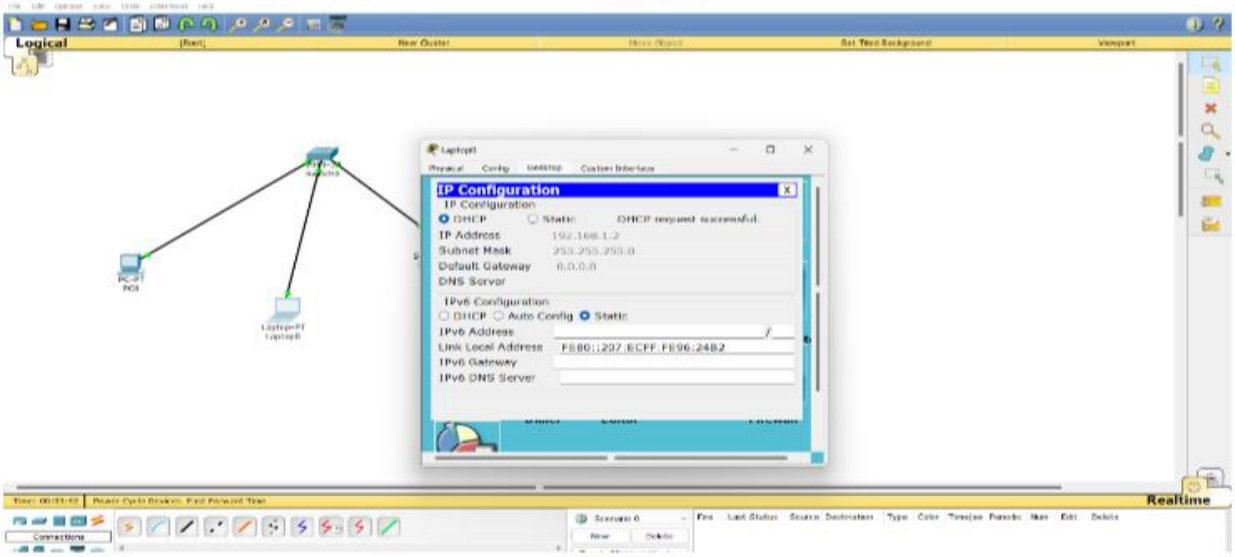
Configuration Details:

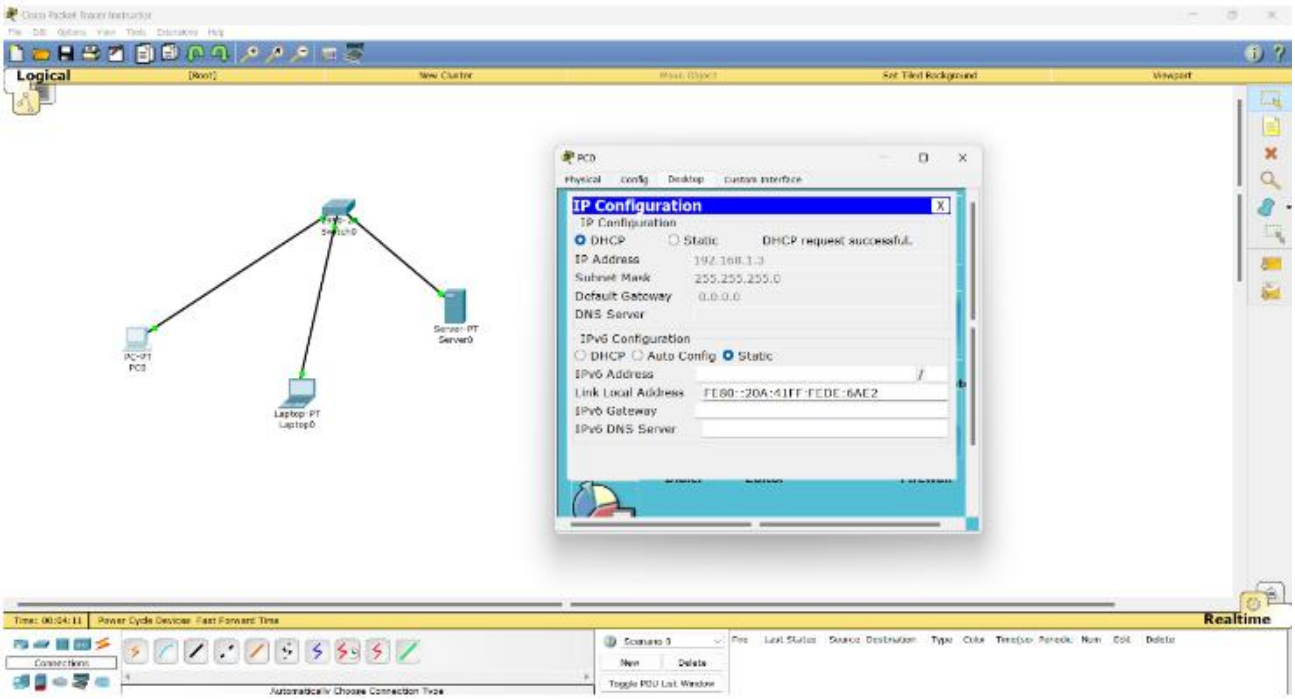
1. Enabled the HTTP service on Server0.
2. Uploaded several HTML files to the file manager:
   - **index.html:** The home page for the server.
   - **helloworld.html:** A basic HTML page with additional content.
   - **image.html:** A page displaying images hosted on the server.
   - **copyrights.html:** An informational page.
   - **ciscoptlogo.jpg:** An image file hosted for use on the web pages.
3. Verified the functionality of the HTTP server by accessing http://facebook.com from Laptop0, confirming successful page loading.

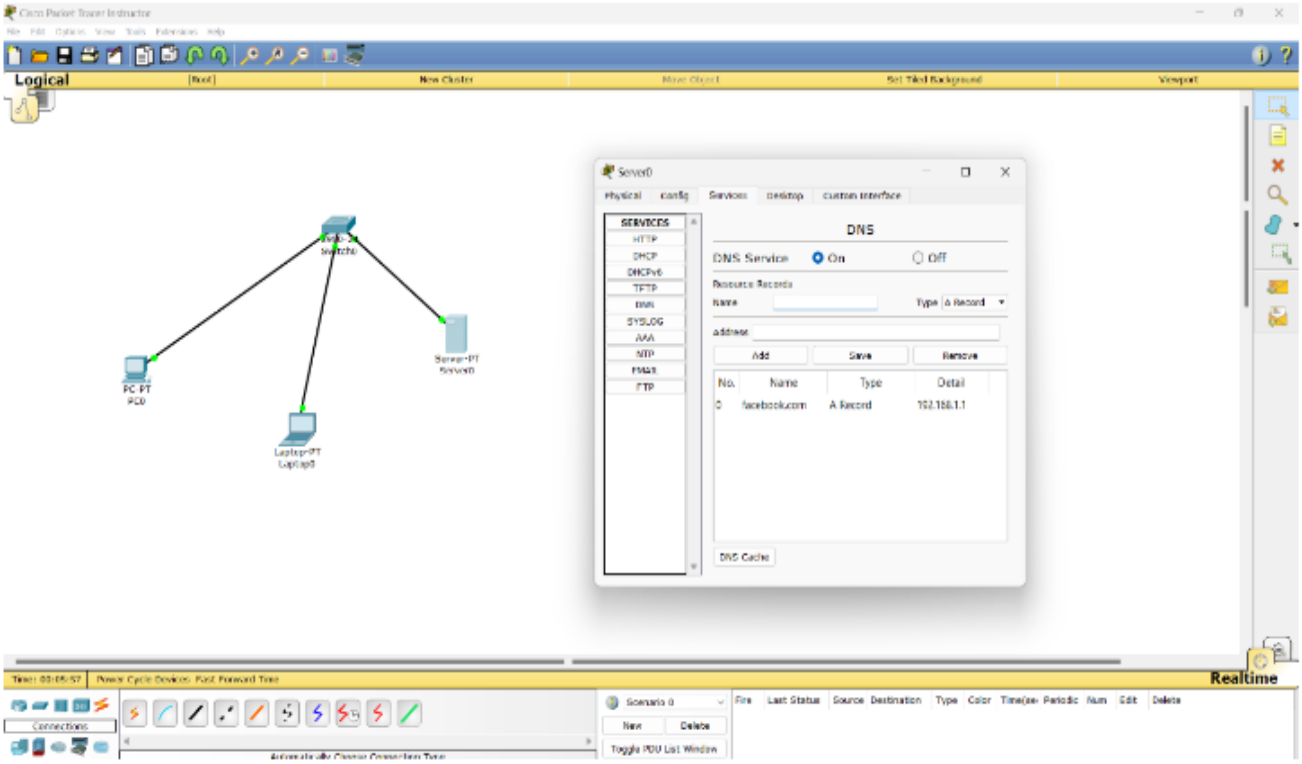
Part 3: DHCP Configuration for Dynamic IP Allocation
Observations:

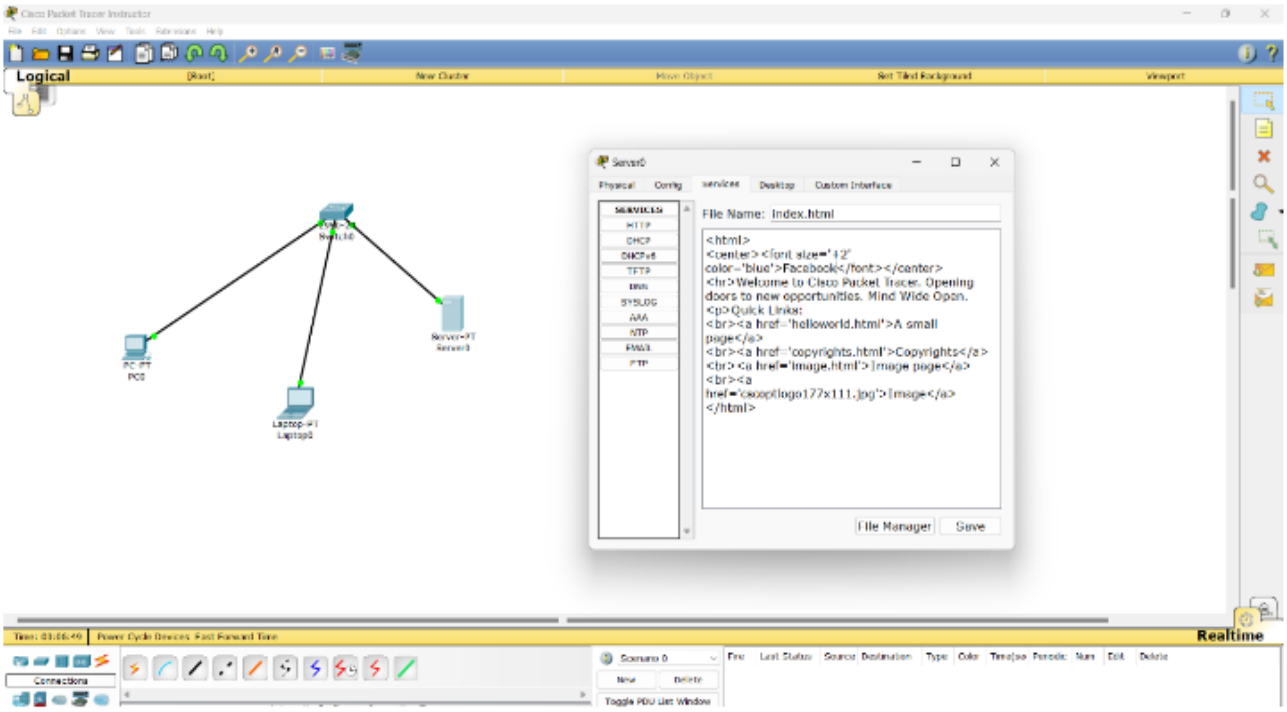
1. **Laptop0 DHCP Configuration:**
    - Successfully obtained an IP address via DHCP:
        - **IP Address:** 192.168.1.2
        - **Subnet Mask:** 255.255.255.0
        - **Default Gateway:** Not configured (0.0.0.0).
    - **IPv6 Auto Configuration:**
        - **Link-Local Address:** FE80::207:ECFF:FE96:24B2
2. **PC0 DHCP Configuration:**
    - Successfully obtained an IP address via DHCP:
        - **IP Address:** 192.168.1.3
        - **Subnet Mask:** 255.255.255.0
        - **Default Gateway:** Not configured (0.0.0.0).
    - **IPv6 Auto Configuration:**






Logical
PC0
IP Configuration
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FEDE:6AE2
IPv6 Gateway
IPv6 DNS Server
Realtime


Logical
Server0
DNS
DNS Service
On
Off
Name
Type
Address
Add
Save
Remove
No.
Name
Type
Detail
0
facebook.com
A Record
192.168.1.1
DNS Cache
Realtime


Logical
Server0
Physical
Config
Services
Desktop
Custom Interface
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
File Name: index.html
<html>
<font size="12"
color="blue">Facebook

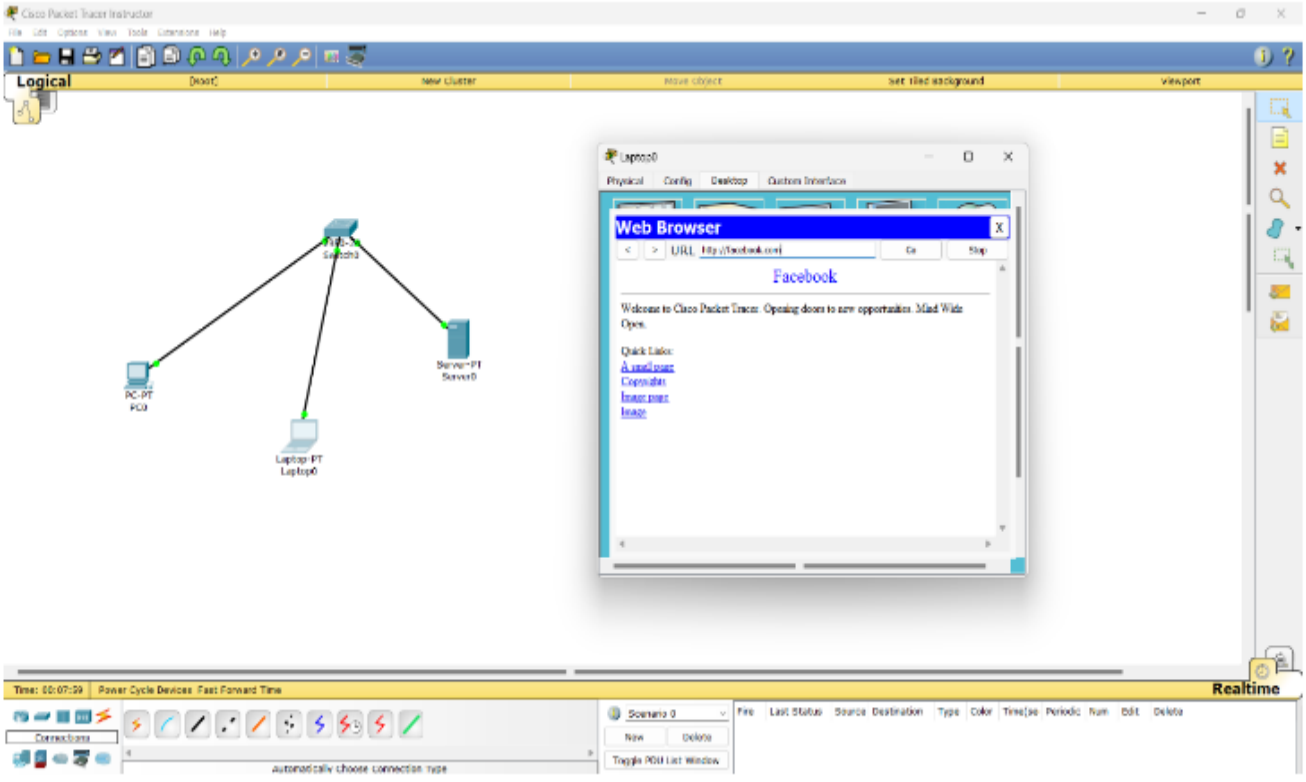
Welcome to Cisco Packet Tracer. Opening
doors to new opportunities. Mind Wide Open.
<p>Quick Links:

A small
page

Copyrights

Image page

<a
href="ciscopiclogo177x111.jpg">Image
</html>
File Manager
Save
PC-PT
PC0
Server-PT
Server0
Laptop-PT
Laptop0
Realtime


Logical
Laptop0
Physical
Config
Desktop
Custom Interface
Web Browser
URL http://facebook.com
Go
Stop
Facebook
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
PC-PT
PC0
Server-PT
Server0
Laptop-PT
Laptop0
Realtime

Network Design:

- **Topology Overview:**
  - Server0, PC0, and Laptop0 are connected to a switch via Ethernet.
  - DNS and HTTP services are enabled on Server0, and DHCP is used for dynamic IP allocation.
- **Services Deployed:**
  - DNS service for domain name resolution.
  - HTTP service to host web content.
  - DHCP for automatic IP assignment to PC0 and Laptop0.

Testing and Verification:

1. **Laptop0:**
   - Accessed http://facebook.com, confirming the DNS and HTTP services were working.
2. **PC0:**
   - Successfully pinged Server0 (192.168.1.1) and accessed the web page at http://facebook.com, confirming proper connectivity and DNS resolution.

Conclusion:

The lab demonstrated:

1. Successful DNS and HTTP server configuration.
2. DHCP working for dynamic IP allocation.
3. Proper device connectivity and domain resolution.

Lab no: 13 **Date: 2025/11 /26**

Firewall Implementation, Router Access Control List (ACL)

Objective:

- Understand and implement Router Firewall: Access Control Lists (ACLs).

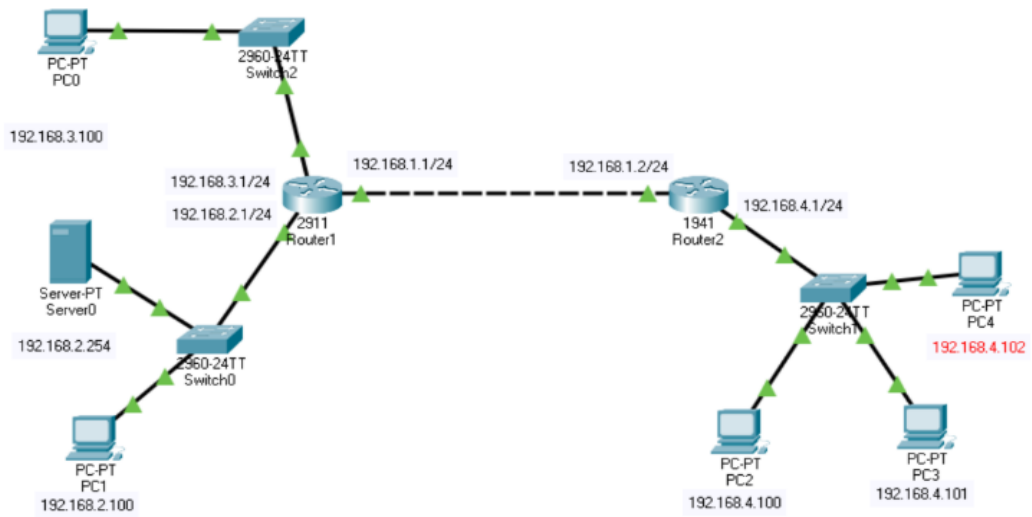
Theory:

Packet filtering at the network level is implemented using Access Control Lists (ACLs) on a router, functioning as a router firewall. ACLs manage inbound and outbound traffic based on criteria such as source and destination IP addresses, protocols (IP, TCP, UDP), and port numbers. They enhance network security by regulating traffic flow.

Types of ACLs:

1. **Standard ACL**
   - Filters traffic based only on the source IP address.
   - Range: **1–99**.
   - Typically applied near the destination.
   - Examples:
     - Denying traffic from a specific host.
     - Permitting all other traffic.
2. **Extended ACL**
   - Filters traffic based on source/destination IP addresses, protocols, and port numbers.
   - Range: **100–199**.
   - Typically applied near the source.
   - Examples:
     - Blocking ICMP (ping) traffic.
     - Allowing HTTP (port 80) traffic.

Configurations:



Router 1 Configuration :

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)# interface gigabitEthernet 0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)# interface gigabitEthernet 0/2
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Router(config-if)# exit
Router(config)# ip route 192.168.4.0 255.255.255.0 192.168.1.2
Router(config)# exit
Router#
```

Router 2 Configuration:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)# interface gigabitEthernet 0/1
Router(config-if)# ip address 192.168.4.1 255.255.255.0
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

```
Router(config-if)# exit
Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1
Router(config)# ip route 192.168.3.0 255.255.255.0 192.168.1.1
Router(config)# exit
Router#
```

1. Standard ACL Implementation

Objective: Block a host (192.168.4.101) in the network 192.168.2.0.

1. **Create the Access List (Standard: Range 1-99):**
   - Place specific deny statements at the top.
   - Place general permit statements at the bottom.
   - Remember: Every access list has an implicit deny any at the end.
2. **Apply the access list to an interface (0utbound).**

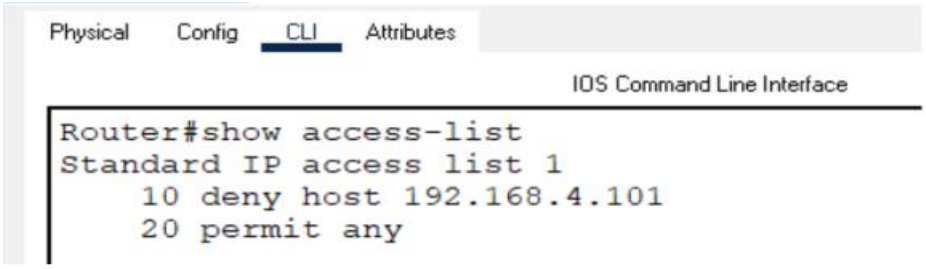
Router 1 Configuration

Objective:

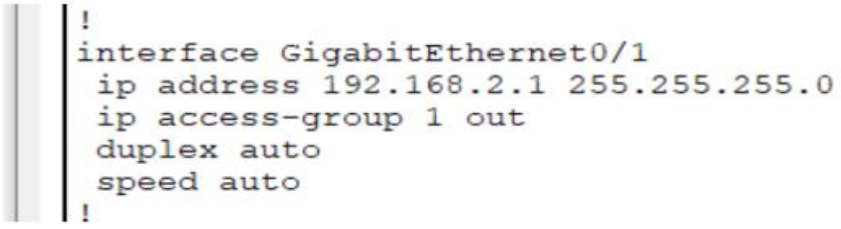
- Deny traffic from a specific source IP address (192.168.4.100).
- Permit traffic from any other IP address.
- Note: An implicit "deny any" exists at the end by default.

Configuration:

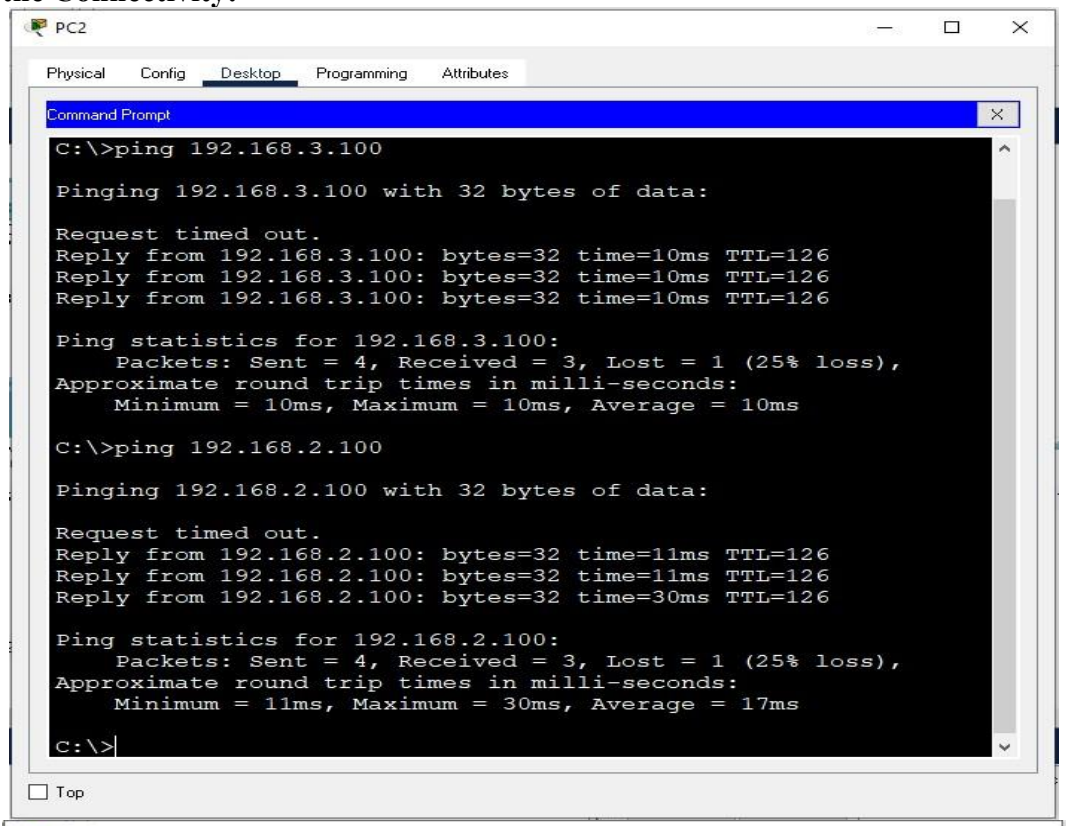
```
Router(config)# access-list 1 deny 192.168.4.100 0.0.0.0
Router(config)# access-list 1 permit any
Router(config)# exit
Router# show access-list
```

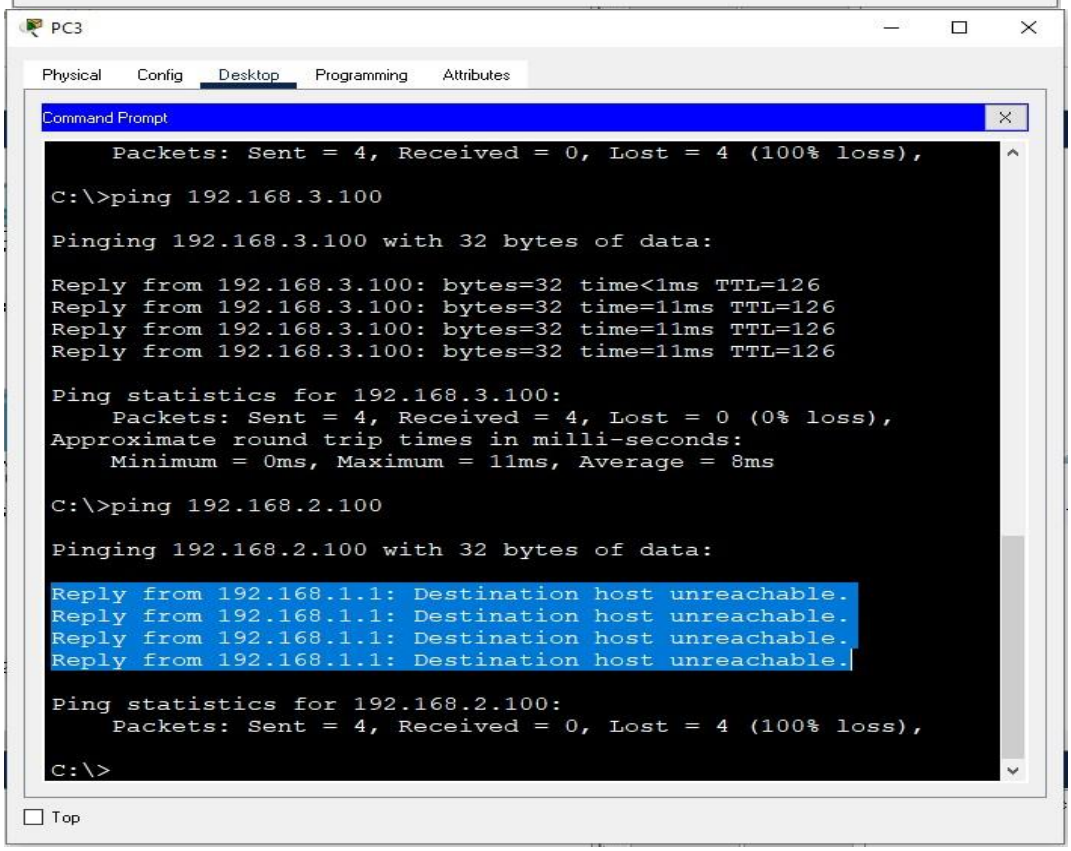



```
Router(config)#interface gigabitethernet 0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show run
```



Verify the Connectivity:



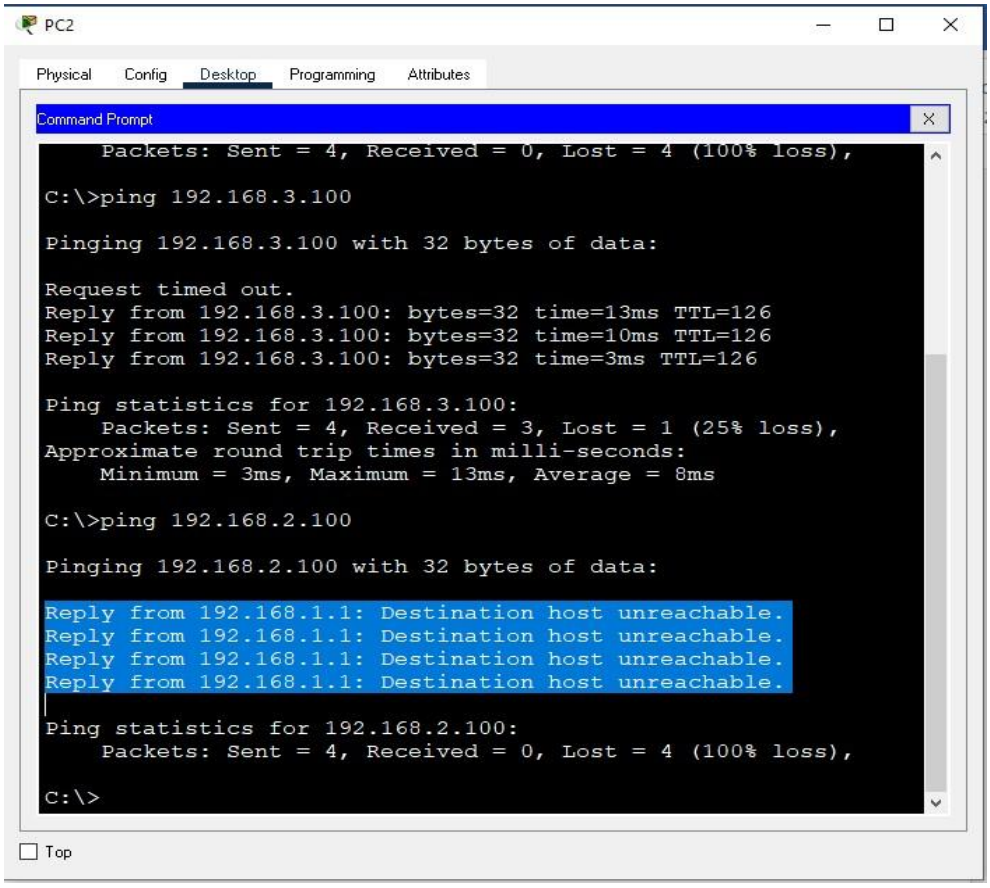


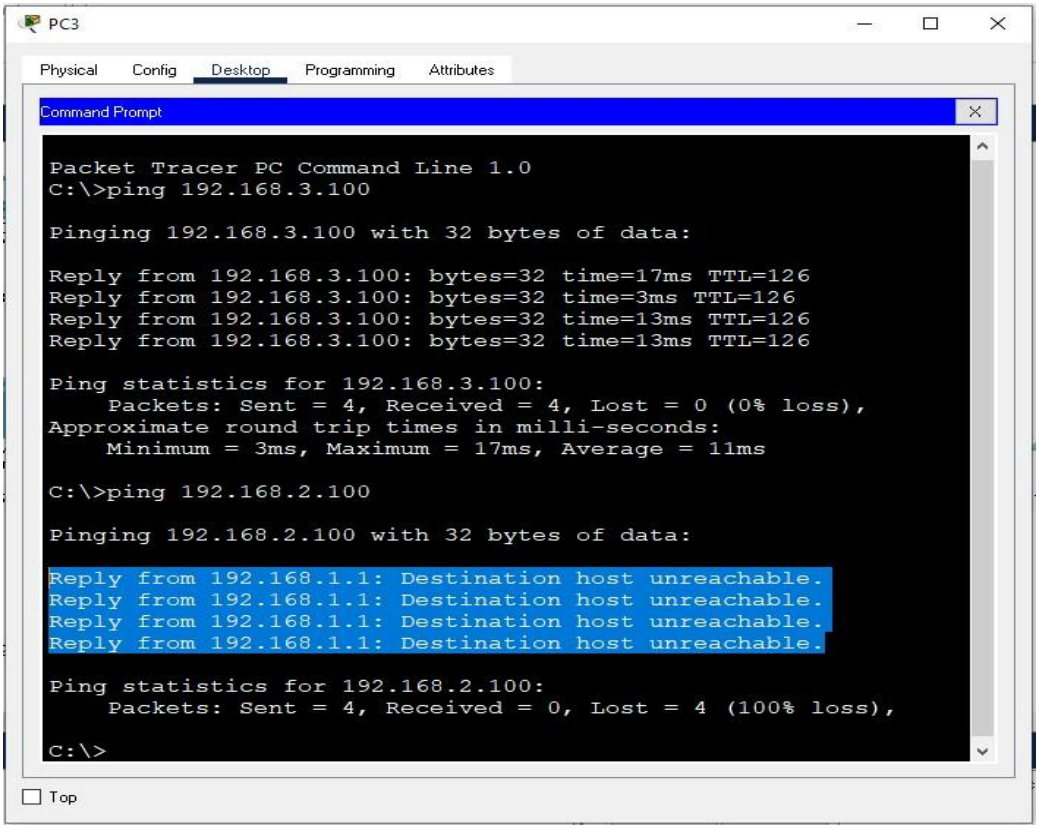
b. Blocking a Network (E.g 192.168.4.0)

We should use wild mask (0.0.0.255) for the Class C network when we need to block the whole network e.g 192.168.4.0.

```
Router(config)#no access-list 1
Router(config)#access-list 1 deny 192.168.4.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#exit
Router#show access-lists
```

```
Router#show access-lists
Standard IP access list 1
    10 deny 192.168.4.0 0.0.0.255
    20 permit any
```




PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.100
Pinging 192.168.3.100 with 32 bytes of data:
Reply from 192.168.3.100: bytes=32 time=17ms TTL=126
Reply from 192.168.3.100: bytes=32 time=3ms TTL=126
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126
Reply from 192.168.3.100: bytes=32 time=13ms TTL=126
Ping statistics for 192.168.3.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 17ms, Average = 11ms
C:\>ping 192.168.2.100
Pinging 192.168.2.100 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 192.168.2.100:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top