Ex.No: 06 **WLAN and DHCP Configuration Using Cisco Packet Tracer**

Date:

Objectives:

- Configure a Wireless LAN (WLAN) in Cisco Packet Tracer.
- Implement a DHCP Server to assign IP addresses dynamically.
- Establish connectivity between wireless and wired devices.
- Verify network connectivity using simulation tools.
- Save the configuration and close Packet Tracer.

Introduction:

A Wireless Local Area Network (WLAN) allows devices to connect to a network without physical cables. The Dynamic Host Configuration Protocol (DHCP) automates IP address allocation, reducing manual configuration errors. This experiment involves setting up WLAN and DHCP to enable seamless connectivity.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
    - 1 Switch (2960-24TT)
    - 1 Server (DHCP Server)
    - 2 Wireless Access Points
    - 1 PC
    - 1 Laptop
    - 1 Tablet
- Connection Cables:
    - Copper Straight-Through Cables (for wired connections)
    - Wireless signals (for wireless devices)

Steps to Configure WLAN and DHCP

Step 1: Adding Network Devices

- Drag and drop the switch, server, access points, PC, laptop, and tablet into the workspace.

Step 2: Connecting the Devices

- Use copper straight-through cables to connect the DHCP server and access points to the switch.

- Ensure the laptop and tablet connect wirelessly to the access points.

Step 3: Configuring the DHCP Server

1. Click on the **Server** and navigate to the **Services** tab.
2. Select **DHCP**, turn it **ON**, and configure:
    - **Pool Name**: WLAN-Pool
    - **Default Gateway**: 192.168.1.1
    - **Subnet Mask**: 255.255.255.0
    - **DNS Server**: 192.168.1.254
    - **Starting IP Address**: 192.168.1.10
3. Click **Save** and **Exit**.

Step 4: Configuring Access Points

1. Click on each **Access Point** and set:
    - **SSID**: WLAN-Network
    - **DHCP Mode**: Enabled
    - **Security Mode**: WPA2
    - **Password**: wlanpassword

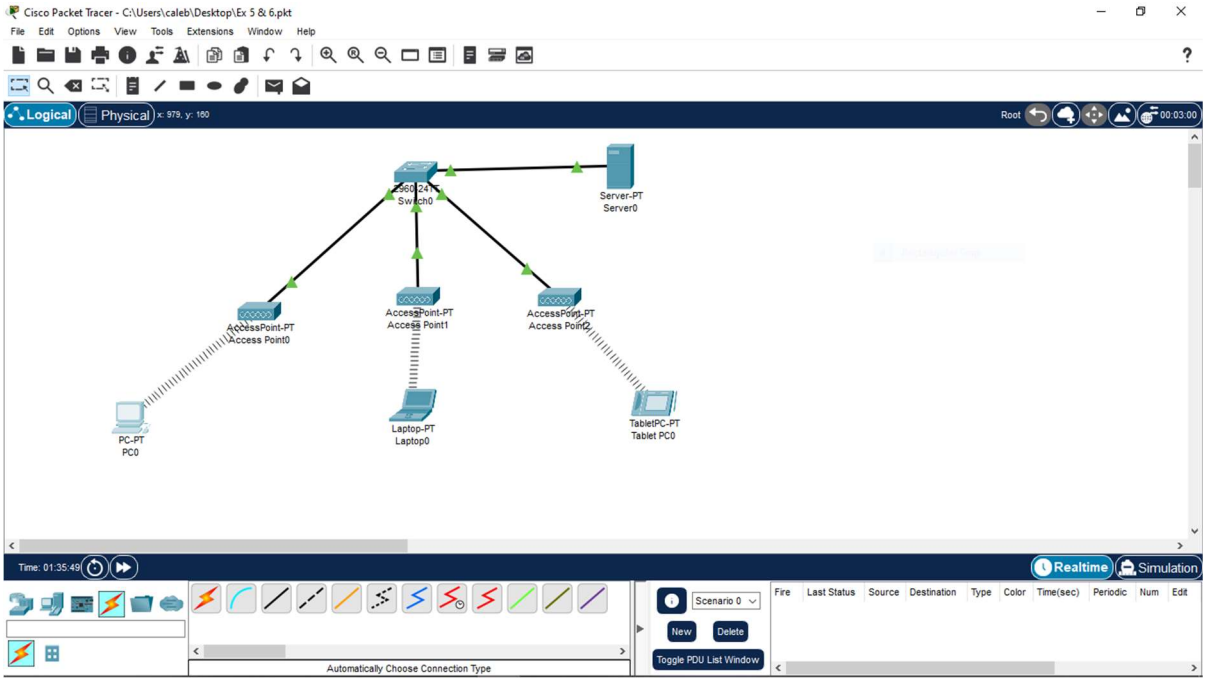
Step 5: Configuring Client Devices

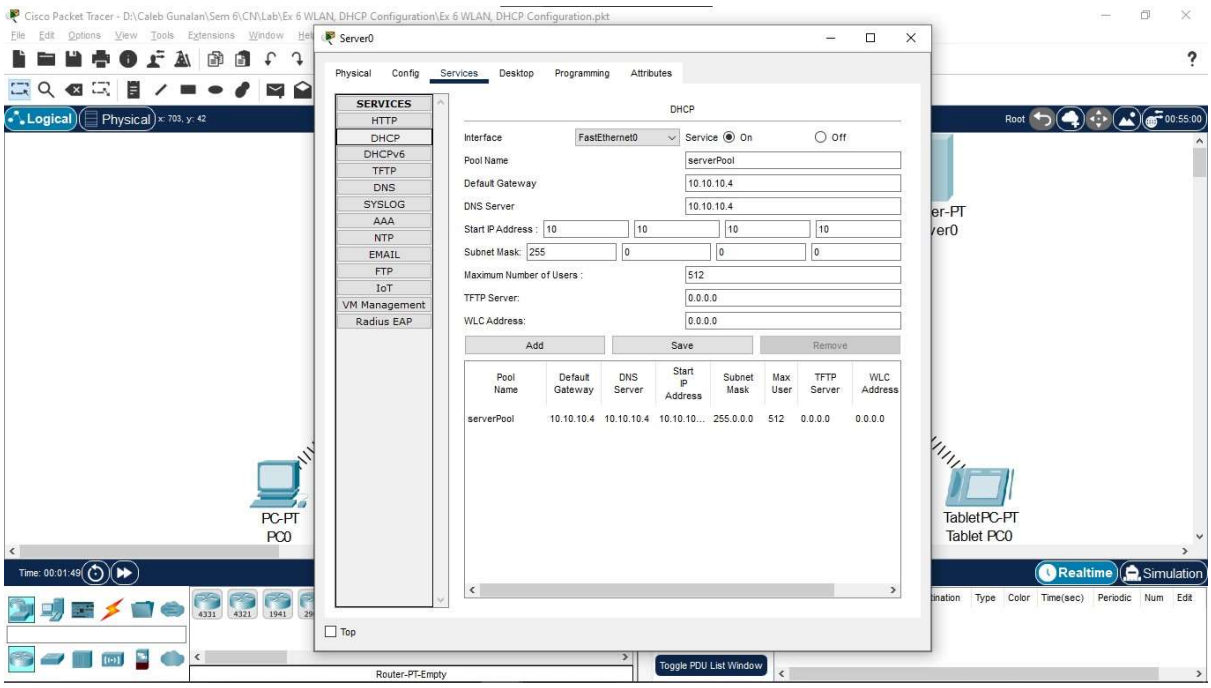
1. Click on the **Laptop** and **Tablet**, navigate to the **Wireless0** interface.
2. Select the **SSID: WLAN-Network** and enter the password **wlanpassword**.
3. Set the IP configuration to **DHCP**.

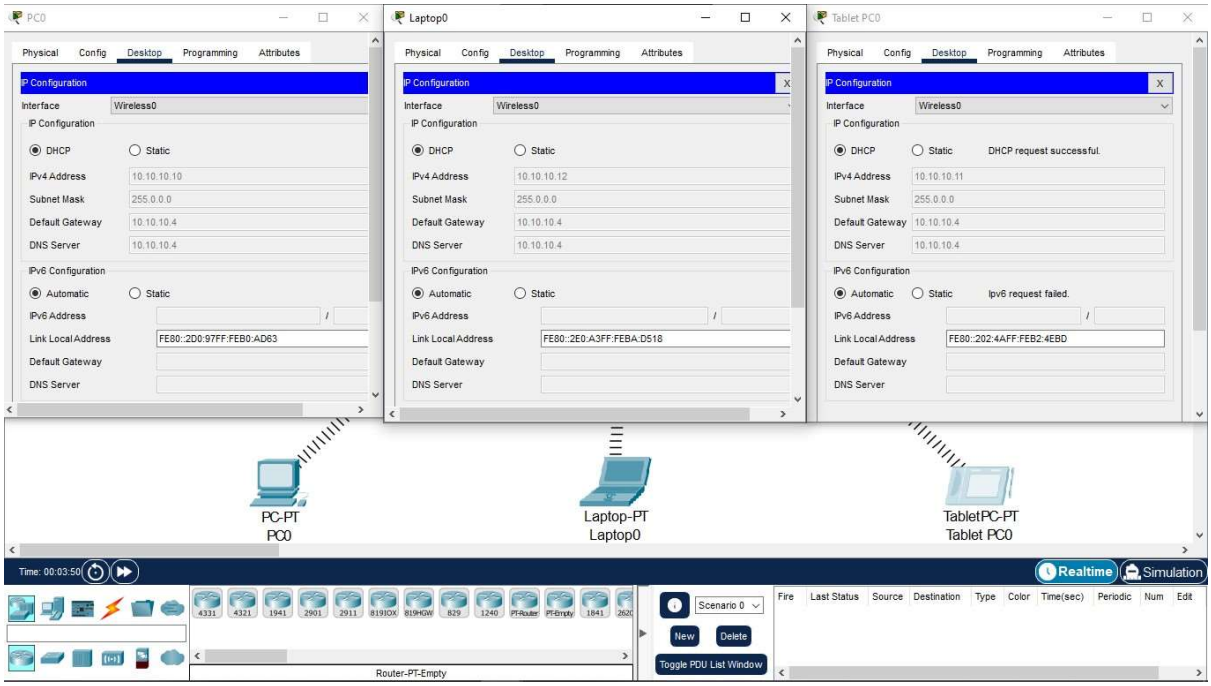
Step 6: Verifying Network Connectivity

- Click on the **PC**, **Laptop**, and **Tablet**.
- Open the **Command Prompt** and type:
- ipconfig
- ping 192.168.1.1
- Ensure successful replies to confirm network connectivity.

Output Screenshots:







Result:

A WLAN was successfully configured with DHCP, enabling dynamic IP assignment and wireless connectivity between devices.

Ex.No: 07 Spanning Tree Protocol (STP) Configuration Using Cisco Packet Tracer

Date:

Objectives:

- Understand the purpose of Spanning Tree Protocol (STP) in preventing network loops.
- Configure STP on multiple switches in Cisco Packet Tracer.
- Identify the Root Bridge and verify the STP process.
- Observe the blocking and forwarding states of switch ports.
- Ensure network stability and redundancy.

Introduction:

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. STP achieves this by selectively blocking redundant paths while allowing alternate paths to be available in case of failure. This experiment involves configuring STP on multiple switches and verifying network stability.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
    - 3 Switches (2960-24TT)
    - 2 PCs
    - 1 Server
- Connection Cables:
    - Copper Straight-Through Cables (for end devices to switches)
    - Copper Cross-Over Cables (for switch-to-switch connections)

Steps to Configure STP

Step 1: Adding Network Devices

- Drag and drop the switches, PCs, and server into the workspace.
- Connect the devices using appropriate cables as per the network topology.

Step 2: Enabling STP on Switches

1. Click on each **Switch** and access the **CLI**.
2. Enter **privileged EXEC mode** by typing:
3. enable

4. Enter **global configuration mode**:
5. configure terminal
6. Configure STP with the following commands:
7. spanning-tree mode pvst
8. spanning-tree vlan 1 priority 24576

(This sets the switch priority to influence root bridge selection.)

Step 3: Identifying the Root Bridge

1. On each switch, run the command:
2. show spanning-tree
3. Verify which switch has the lowest Bridge ID (Root Bridge).

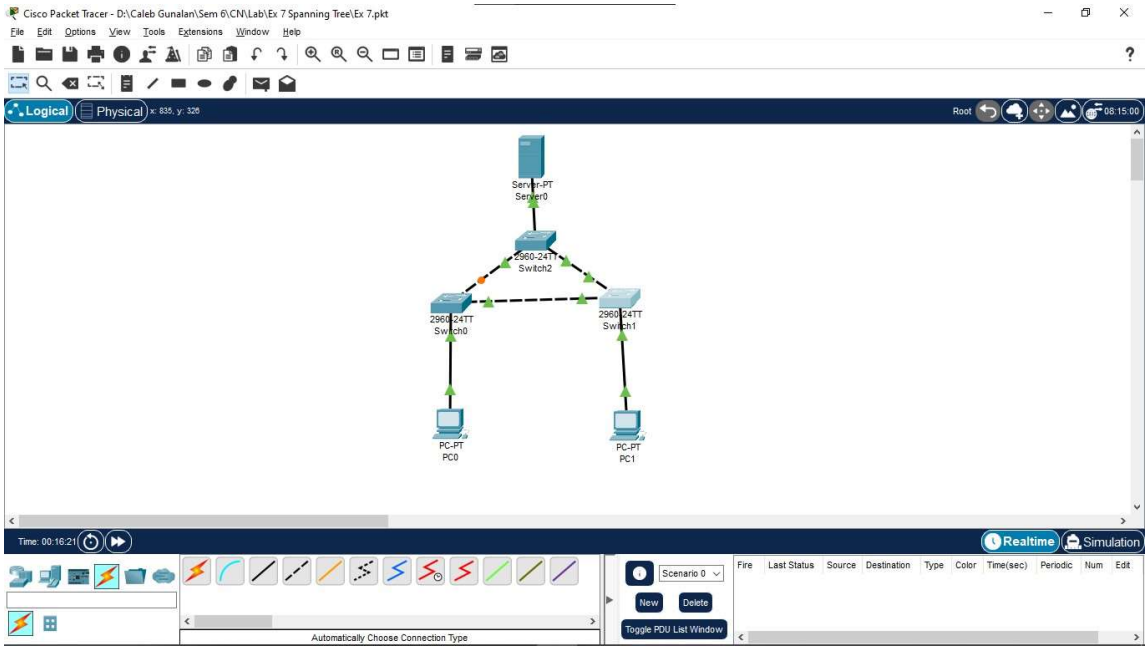
Step 4: Observing Port Roles

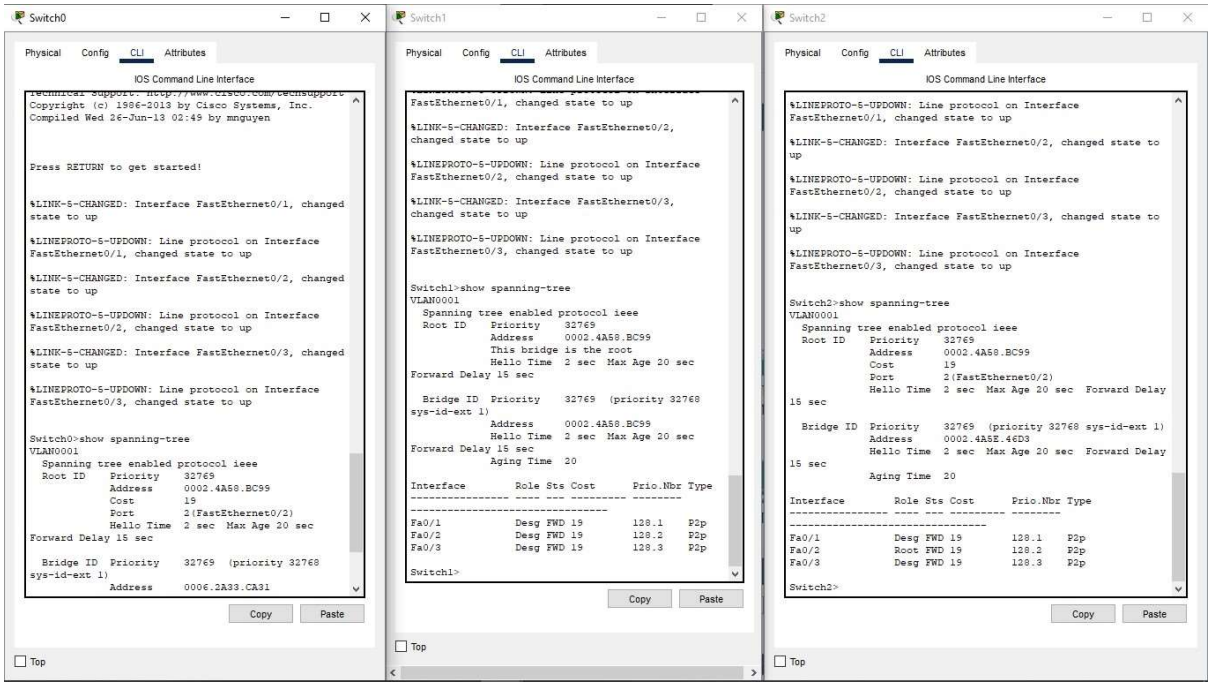
- Run the command:
- show spanning-tree
- Identify **Root Ports**, **Designated Ports**, and **Blocked Ports**.

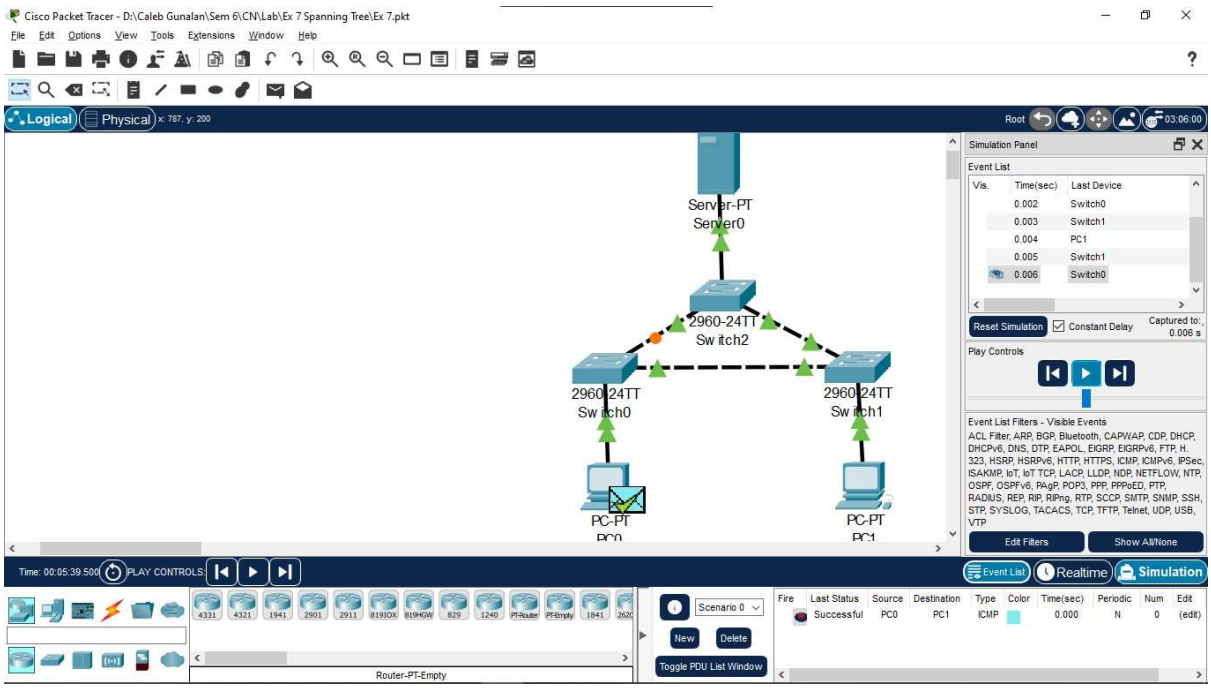
Step 5: Testing Network Stability

1. Open **Command Prompt** on each PC.
2. Test connectivity using the command:
3. ping 192.168.1.2
4. Disconnect a link and observe if STP recalculates paths and re-establishes connectivity.

Output Screenshots:







Result:

Spanning Tree Protocol (STP) was successfully configured to prevent network loops and ensure redundancy while maintaining a stable network topology.

Ex.No: 8 **MAC Learning Using ARP Table**
Date:

Objectives:

- Understand how MAC addresses are learned and stored in the ARP table.
- Observe ARP request and reply mechanisms in a network.
- Verify MAC address entries in the ARP table of a switch and end devices.
- Capture ARP packets using Cisco Packet Tracer simulation.

Introduction:

Address Resolution Protocol (ARP) is a fundamental network protocol used to map IP addresses to MAC addresses in a local network. When a device wants to communicate with another device on the same network, it first checks its ARP table for the corresponding MAC address. If the address is not found, the device sends an ARP request to obtain it. This experiment demonstrates MAC learning through ARP table inspection in Cisco Packet Tracer.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
  - 1 Server
  - 1 Switch (2960-24TT)
  - 3 PCs (Client Devices)
- Connection Cables:
  - Copper Straight-Through Cables (for wired connections)

Steps to Perform MAC Learning Using ARP Table

Step 1: Setting Up the Network Topology

- Drag and drop the **Server**, **Switch**, and **PCs (PC0, PC1, PC2)** into the Packet Tracer workspace.
- Connect all devices using **Copper Straight-Through** cables as follows:
  - **Server0** → **Switch0**
  - **PC0** → **Switch0**
  - **PC1** → **Switch0**
  - **PC2** → **Switch0**

Step 2: Assigning IP Addresses

- Configure the following IP addresses:
    - **Server0**: 192.168.1.1 /24
    - **PC0**: 192.168.1.2 /24
    - **PC1**: 192.168.1.3 /24
    - **PC2**: 192.168.1.4 /24

Step 3: Verifying the Initial ARP Table

1. Click on **PC0** → Open **Command Prompt**.
2. Type the following command to check the ARP table:
3. arp -a
4. The table should be empty initially since no communication has taken place.

Step 4: Sending ARP Requests

1. From **PC0**, ping **PC1** using the command:
2. ping 192.168.1.3
3. Since PC0 does not have the MAC address of PC1, it will send an **ARP Request**.
4. PC1 responds with an **ARP Reply**, providing its MAC address.
5. The MAC address is then stored in **PC0's ARP table**.
6. Repeat this step for PC2 and Server0.

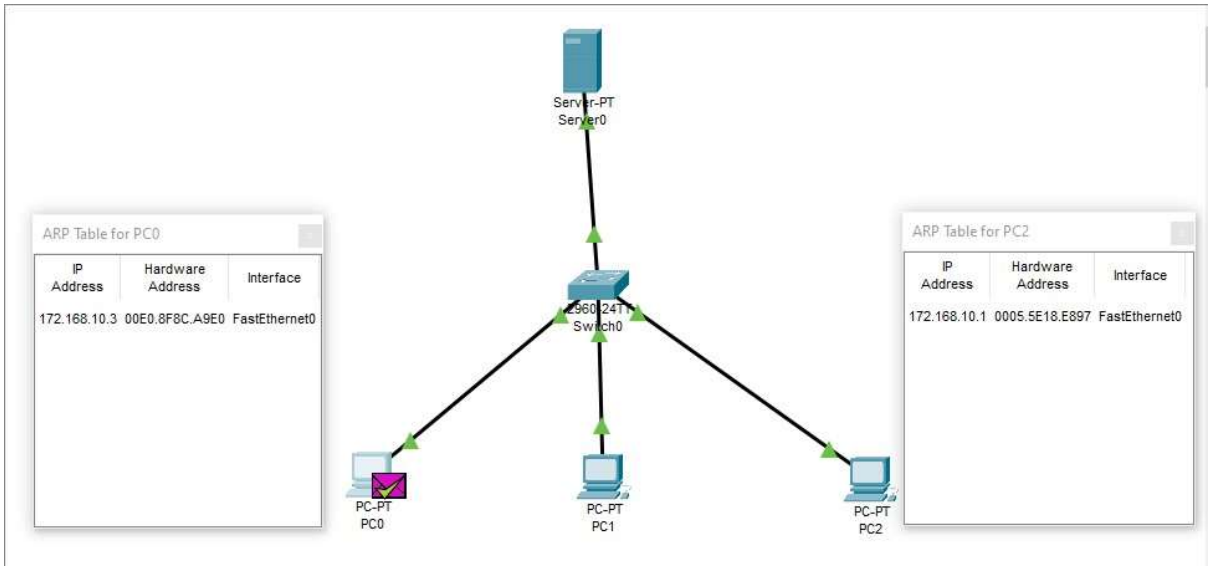
Step 5: Viewing the Updated ARP Table

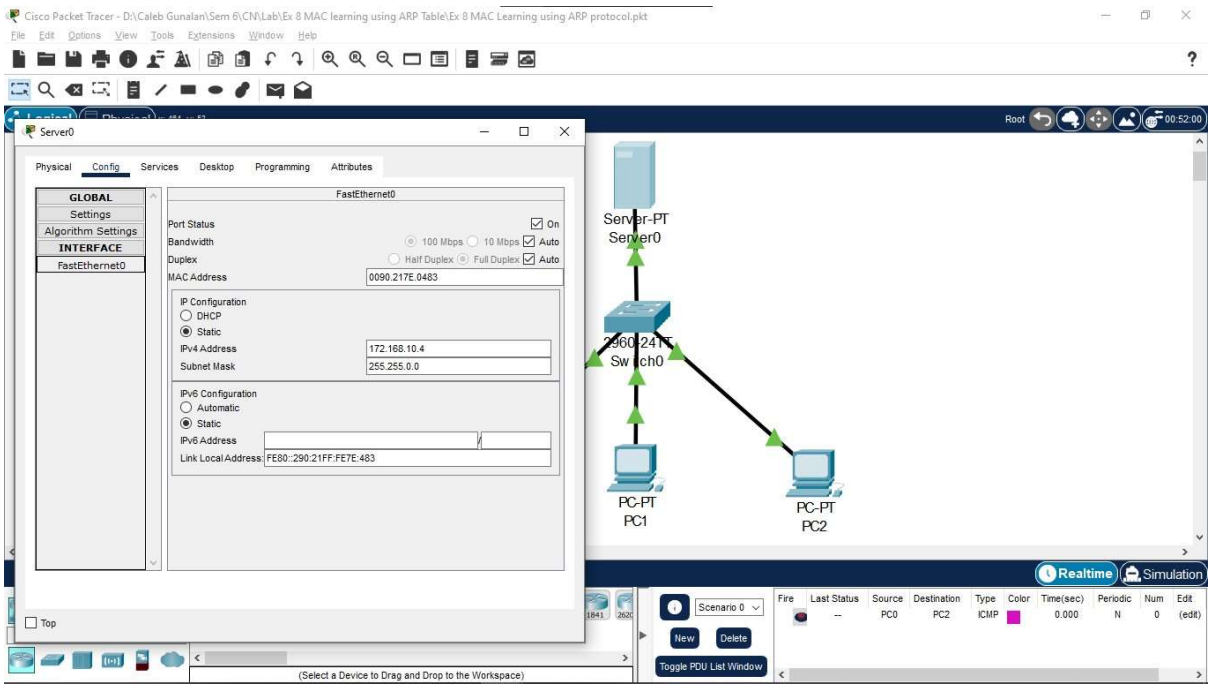
1. After successful pings, check the ARP table again using:
2. arp -a
3. The table should now display the **MAC addresses** of the communicated devices.

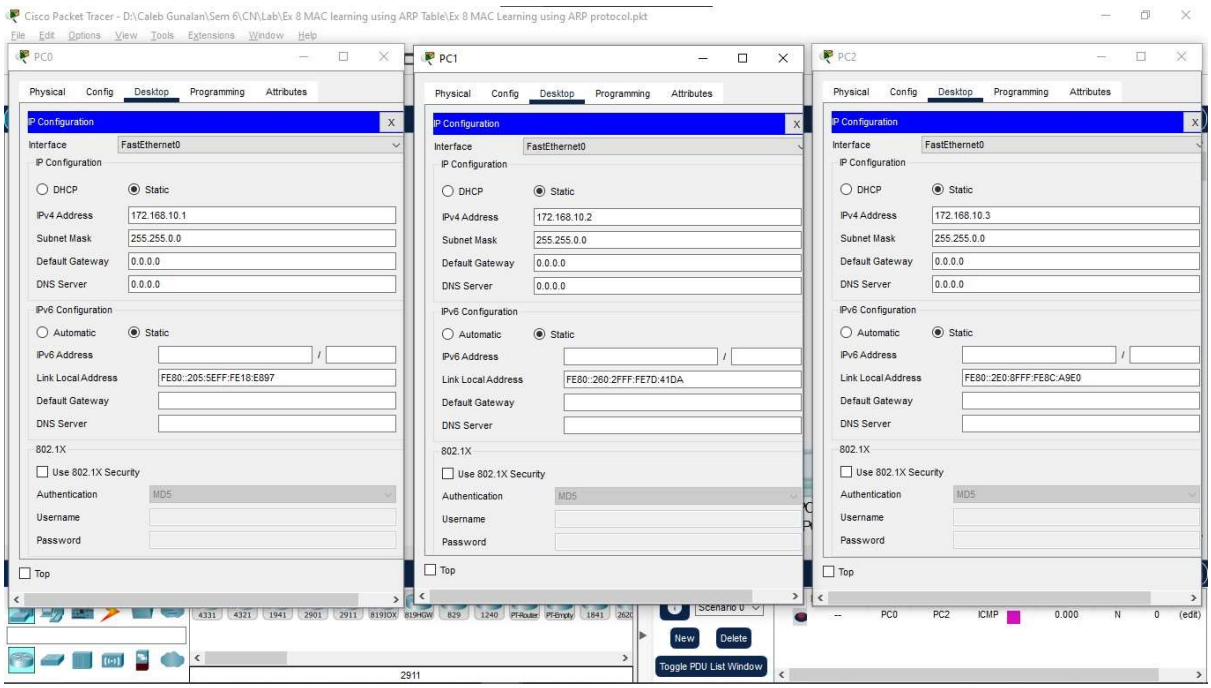
Step 6: Capturing ARP Packets (Optional)

1. Click on **Simulation Mode** in Packet Tracer.
2. Filter packets to display only **ARP packets**.
3. Initiate a new ping from **PC0 to PC1**.
4. Observe the **ARP request and reply** exchanges.

Output Screenshots:







Result:

The experiment demonstrated MAC address learning through ARP table entries. The ARP process was successfully observed and verified using Packet Tracer.

Ex.No: 09 **Subnetting in Cisco Packet Tracer**
Date:

Objectives:

- Understand and implement subnetting in a network.
- Assign appropriate IP addresses based on subnet calculations.
- Configure network devices using subnetted IP addresses.
- Verify connectivity using network testing tools.
- Save the configuration and close Packet Tracer.

Introduction:

Subnetting is the process of dividing a larger network into smaller, manageable subnetworks to optimize performance, improve security, and utilize IP addresses efficiently. In this experiment, we will create subnetworks, assign appropriate IP addresses, and verify connectivity using Cisco Packet Tracer.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
  - 1 Router
  - 2 Switches
  - 4 PCs (Client Devices)
- Connection Cables:
  - Copper Straight-Through Cables (for wired connections)

Steps to Configure Subnetting

Step 1: Defining the Network Address

- Given network address: **192.168.1.0/24**
- Subnet mask: **255.255.255.192** (Using /26 for 4 subnets)
- Number of hosts per subnet: **62 (2 reserved for network and broadcast addresses)**

Step 2: Assigning Subnet Addresses

- **Subnet 1:** 192.168.1.0/26 (First usable IP: 192.168.1.1, Last usable IP: 192.168.1.62)
- **Subnet 2:** 192.168.1.64/26 (First usable IP: 192.168.1.65, Last usable IP: 192.168.1.126)

Step 3: Configuring IP Addresses

- Assign IP addresses to the devices:
  - **Router (Interface 1 - Subnet 1):** 192.168.1.1

- **Router (Interface 2 - Subnet 2):** 192.168.1.65
- **Switch 1:** Connected to Subnet 1
- **Switch 2:** Connected to Subnet 2
- **PC1:** 192.168.1.2 (Subnet 1)
- **PC2:** 192.168.1.3 (Subnet 1)
- **PC3:** 192.168.1.66 (Subnet 2)
- **PC4:** 192.168.1.67 (Subnet 2)

Step 4: Configuring Router Interfaces

1. Click on the **Router** and navigate to the **CLI**.
2. Enter the following commands:
3. enable
4. configure terminal
5. interface GigabitEthernet0/0
6. ip address 192.168.1.1 255.255.255.192
7. no shutdown
8. exit
9. interface GigabitEthernet0/1
10. ip address 192.168.1.65 255.255.255.192
11. no shutdown
12. exit
13. end
14. write memory

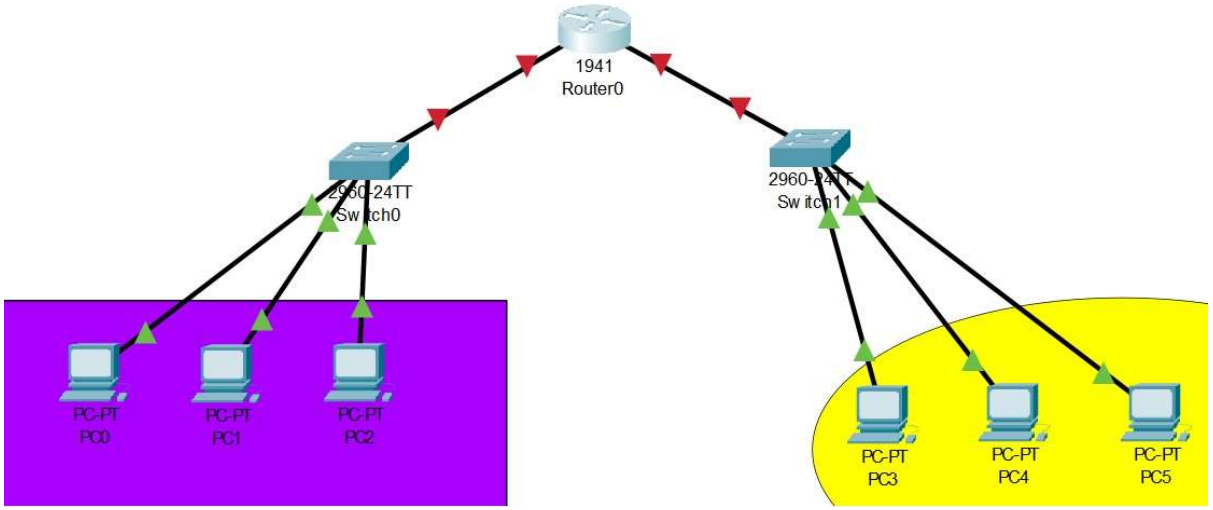
Step 5: Configuring PCs

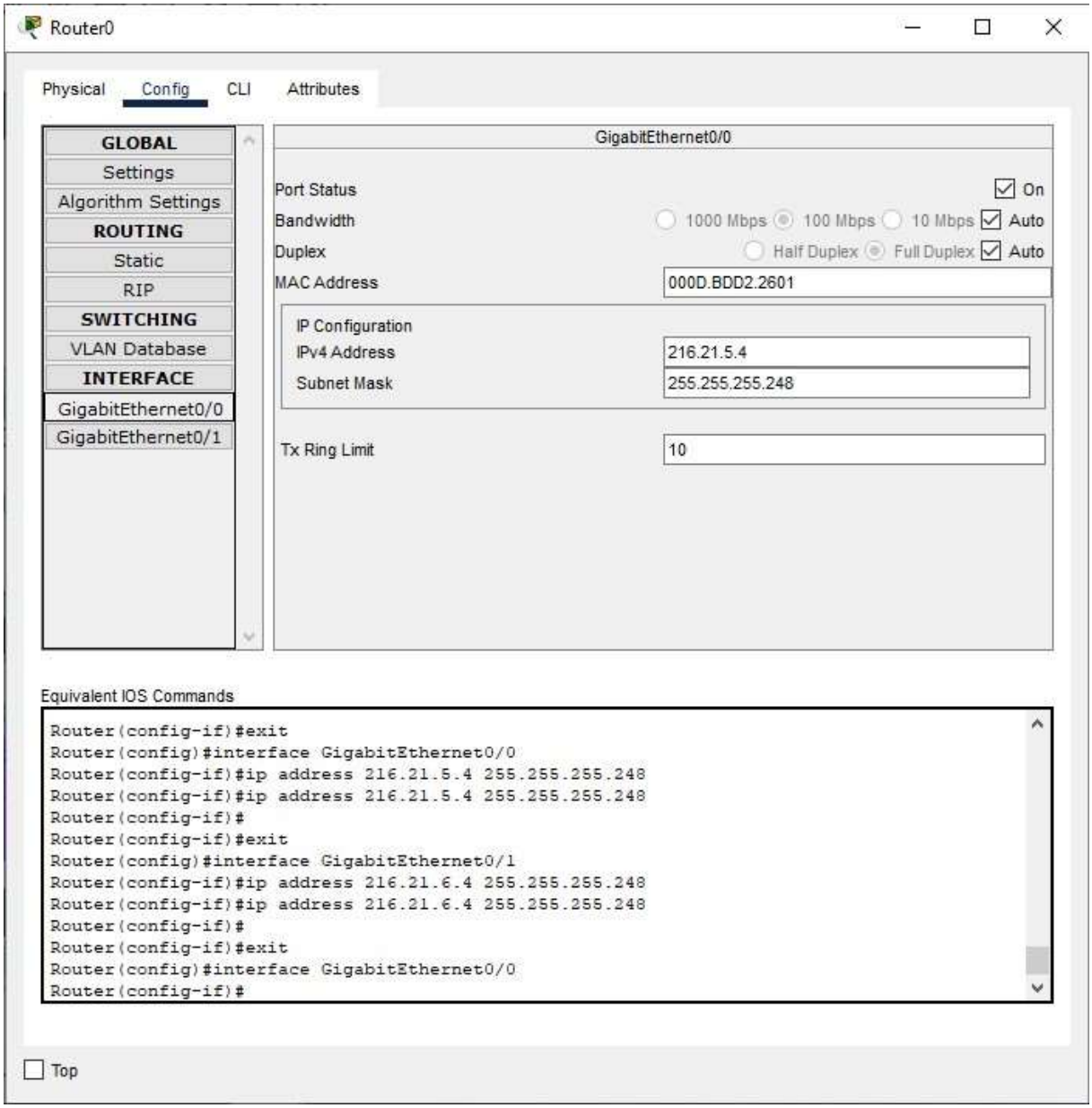
1. Click on each **PC**, navigate to the **IP Configuration** tab.
2. Assign the respective IP addresses and set the default gateway (Router interface IP).

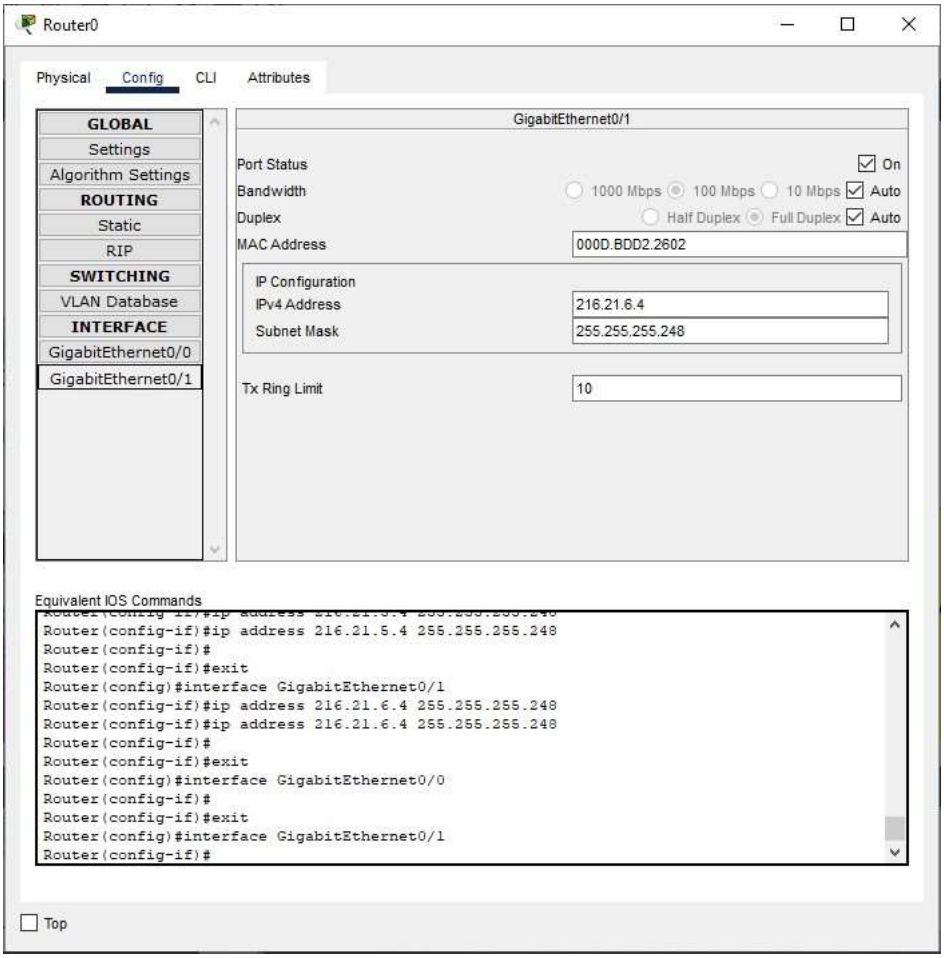
Step 6: Verifying Network Connectivity

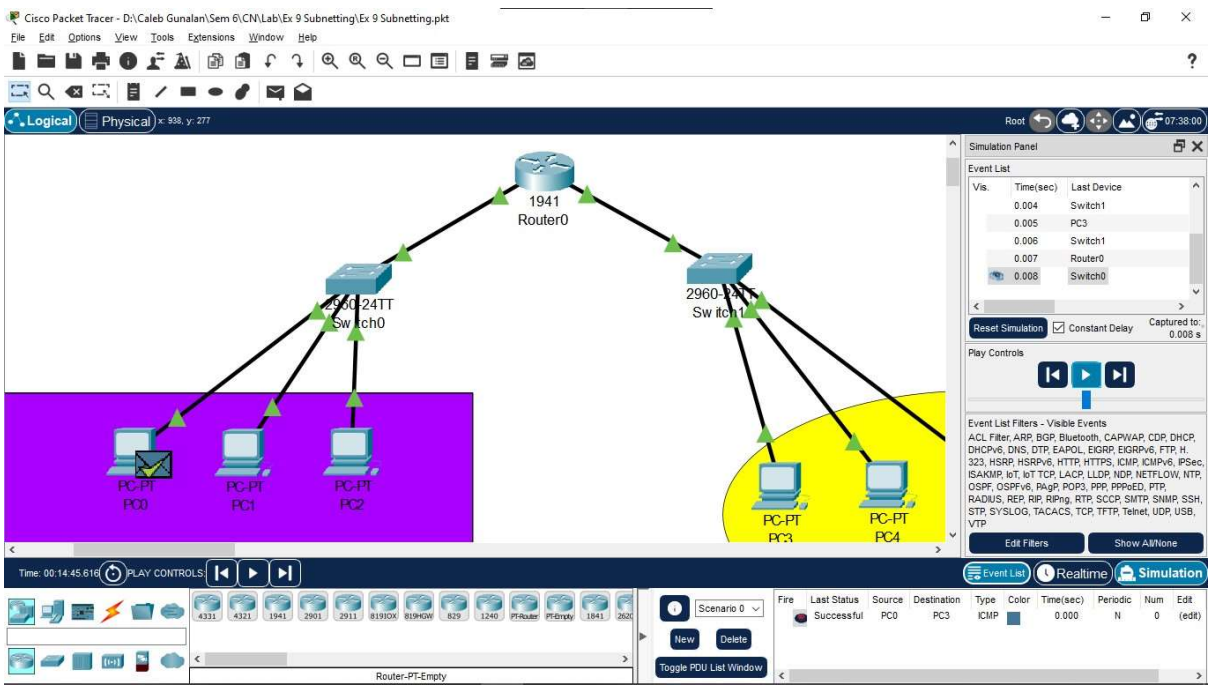
- Open the **Command Prompt** on a PC and use the following commands:
- ipconfig
- ping 192.168.1.1
- ping 192.168.1.65
- Ensure successful replies from the router and other devices.

Output Screenshots:









Result:

Subnetting was successfully implemented in Cisco Packet Tracer, allowing optimized IP address allocation and connectivity between subnetted networks.

Ex.No: 10 **Manual Routing Using Cisco Packet Tracer**
Date:

Objectives:

- Configure manual (static) routing in Cisco Packet Tracer.
- Establish connectivity between different networks using a router.
- Verify connectivity between client devices.
- Save the configuration and close Packet Tracer.

Introduction:

Manual or static routing is a method where routes are manually configured in the router's routing table. Unlike dynamic routing, it does not automatically update routes when network topology changes. This experiment focuses on manually adding static routes to enable communication between different networks.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
    - 2 Routers
    - 2 Switches
    - 4 PCs (Client Devices)
- Connection Cables:
    - Copper Straight-Through Cables (for connecting PCs to switches)
    - Copper Cross-Over Cables (for connecting routers)

Steps to Configure Manual Routing

Step 1: Adding Network Devices

- Drag and drop the routers, switches, and PCs into the workspace.
- Connect the devices using appropriate cables.

Step 2: Assigning IP Addresses

- Assign IP addresses to the devices as follows:

Router 1:

- **Interface G0/0**: 192.168.1.1/24 (connected to Switch 1)
- **Interface G0/1**: 10.0.0.1/30 (connected to Router 2)

Router 2:

- **Interface G0/0**: 192.168.2.1/24 (connected to Switch 2)

- **Interface G0/1**: 10.0.0.2/30 (connected to Router 1)

PC1 (Connected to Switch 1): 192.168.1.2/24
PC2 (Connected to Switch 1): 192.168.1.3/24
PC3 (Connected to Switch 2): 192.168.2.2/24
PC4 (Connected to Switch 2): 192.168.2.3/24

Step 3: Configuring Static Routes

1. **On Router 1:**
    - Enter configuration mode:
    - Router1> enable
    - Router1# configure terminal
    - Add a static route to the 192.168.2.0 network via Router 2:
    - Router1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
    - Exit configuration mode:
    - Router1(config)# exit
2. **On Router 2:**
    - Enter configuration mode:
    - Router2> enable
    - Router2# configure terminal
    - Add a static route to the 192.168.1.0 network via Router 1:
    - Router2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
    - Exit configuration mode:
    - Router2(config)# exit

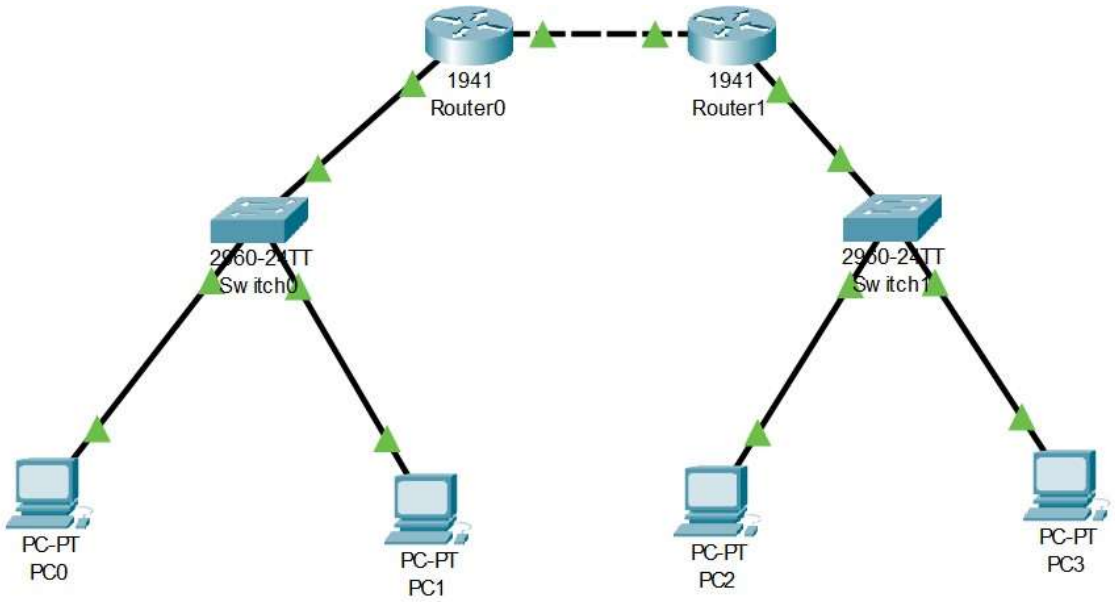
Step 4: Configuring Default Gateways on PCs

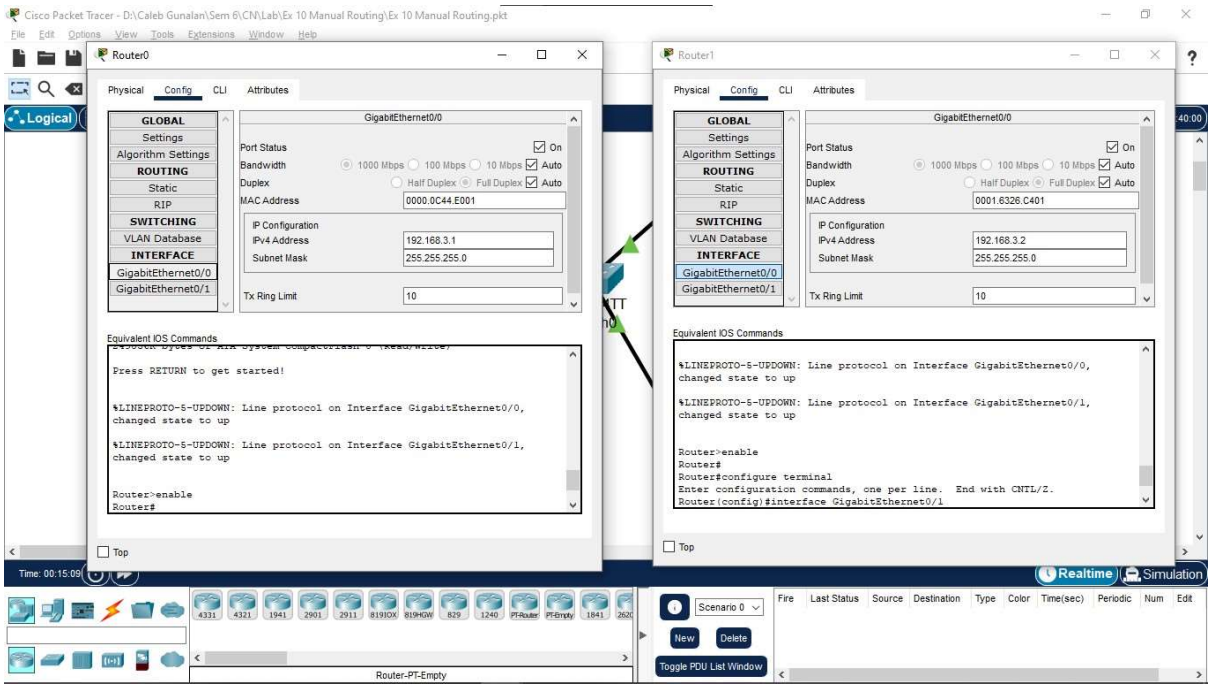
- On each PC, set the default gateway to the respective router's interface:
    - **PC1 & PC2:** 192.168.1.1
    - **PC3 & PC4:** 192.168.2.1

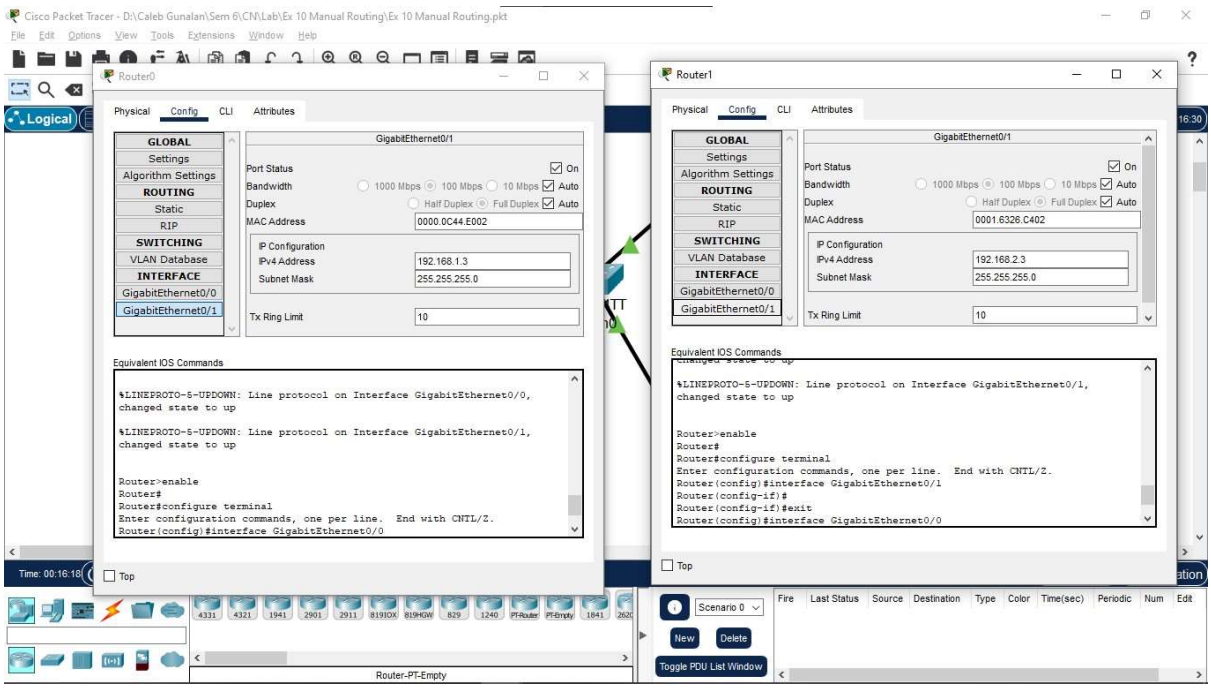
Step 5: Verifying Connectivity

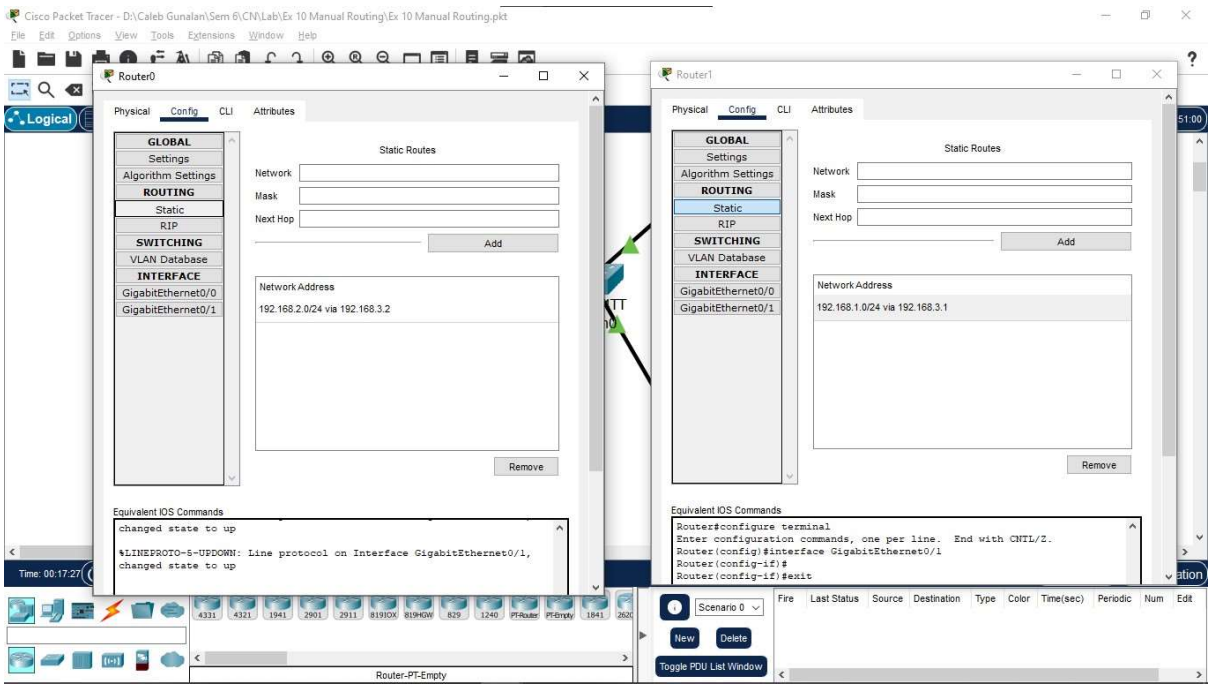
- Use the **ping** command from PC1 to PC3 to check connectivity:
- ping 192.168.2.2
- If successful, the manual routing configuration is correct.

Output Screenshots:









Result:

Manual routing was successfully configured in Cisco Packet Tracer, enabling communication between different networks using static routes.

Ex.No: 10 Network Protocol Analysis: Capture and Analyze ICMP Packets in Wireshark
Date:

Objectives:

- Capture ICMP packets using Wireshark.
- Analyze ICMP request and reply messages.
- Understand the purpose and functionality of ICMP in network communication.
- Save the captured packets for further analysis.

Introduction:

The Internet Control Message Protocol (ICMP) is a fundamental protocol used in network troubleshooting and diagnostics. It is primarily used for sending error messages and operational information, such as when a requested service is unavailable or a router cannot forward packets. The most common use of ICMP is the **ping** command, which tests network connectivity between devices. This experiment involves capturing ICMP packets using Wireshark and analyzing their structure and behavior.

Requirements:

- Wireshark Packet Analyzer Software
- Cisco Packet Tracer Software (Optional for Simulation)
- Network Devices:
  - 2 PCs (Client Devices)
  - 1 Switch (Optional)
  - 1 Router (Optional for multi-network communication)
- Connection Cables:
  - Copper Straight-Through Cables (for wired connections)

Steps to Capture and Analyze ICMP Packets in Wireshark

Step 1: Setting Up the Network

1. Connect two PCs directly using a switch or configure them on the same subnet.
2. Assign static IP addresses:
   - **PC1**: 192.168.1.10/24
   - **PC2**: 192.168.1.11/24
3. Ensure both devices can communicate using the ping command.

Step 2: Starting Wireshark Capture

1. Open **Wireshark** on PC1.

2. Select the appropriate network interface (Ethernet/Wireless) and click **Start Capture**.
3. In the terminal/command prompt of PC1, type:
4. ping 192.168.1.11

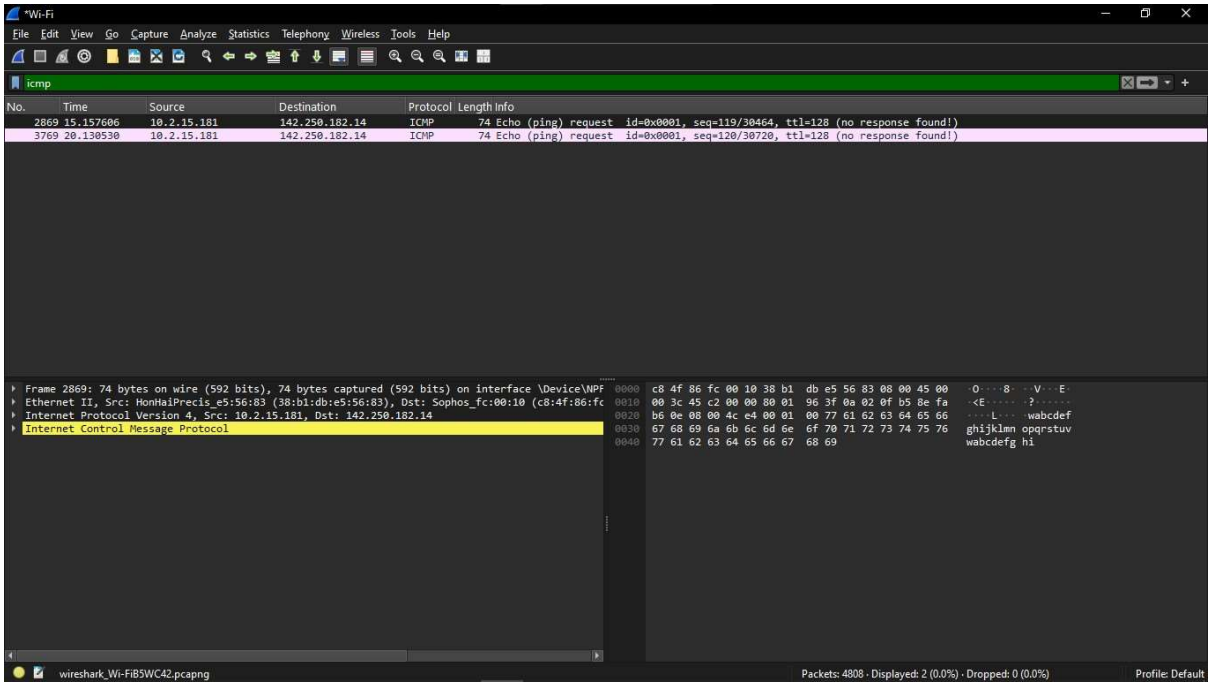
This sends ICMP Echo Requests to PC2 and receives Echo Replies.

5. Stop the packet capture in Wireshark after a few seconds.

Step 3: Analyzing ICMP Packets

1. In **Wireshark**, filter the captured packets using the **ICMP filter**.
    - Type icmp in the display filter bar and press **Enter**.
2. Identify **Echo Request** and **Echo Reply** packets.
3. Analyze key fields such as:
    - **Source and Destination IPs**
    - **Type and Code Values** (Type 8 = Echo Request, Type 0 = Echo Reply)
    - **Sequence Number and Identifier**
4. Save the captured packets for documentation.

Output Screenshots:



Result:

ICMP packets were successfully captured and analyzed using Wireshark, demonstrating the role of ICMP in network communication and troubleshooting.

Ex.No: 12 Network Protocol Analysis: Capture and Analyze IP Packets, TCP Segments, and UDP Datagrams in Wireshark

Date:

Objectives:

- Capture and analyze IP packets using Wireshark.
- Understand the structure and functionality of TCP segments.
- Observe the characteristics of UDP datagrams.
- Interpret network traffic for different protocol layers.
- Save the captured results for further analysis.

Introduction:

Wireshark is a powerful packet analyzer used for network troubleshooting, analysis, and protocol development. It allows users to capture live traffic and inspect the details of different network protocols. In this experiment, we will capture and analyze IP packets, TCP segments, and UDP datagrams to understand their structures and behaviors.

Requirements:

- Wireshark installed on a PC
- A network connection (wired or wireless)
- Any two devices in the network (PCs, servers, or virtual machines)
- Basic knowledge of network protocols

Steps to Capture and Analyze Packets in Wireshark

(a) Capture and Analyze IP Packets

1. **Open Wireshark** and select the active network interface.
2. Click **Start Capture** to begin recording network traffic.
3. Open a web browser and visit a website (e.g., https://www.example.com).
4. Stop the capture after some traffic is recorded.
5. In the **Filter** bar, type ip and press Enter to display only IP packets.
6. Click on an IP packet to analyze its fields:
    - **Source and Destination IP addresses**
    - **Protocol used (TCP/UDP/ICMP, etc.)**
    - **Total length and fragmentation details**
7. Take a screenshot of the captured IP packets.

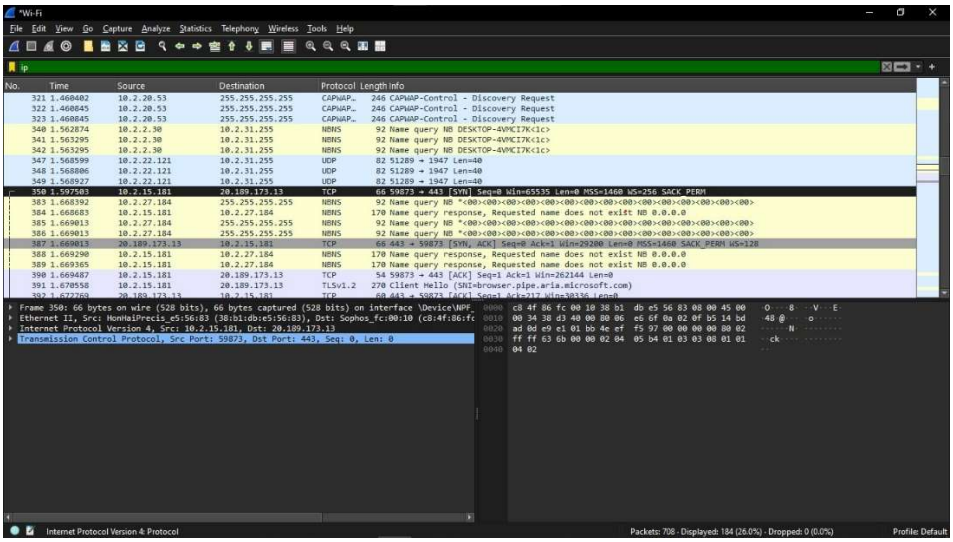
(b) Capture and Analyze TCP Segments

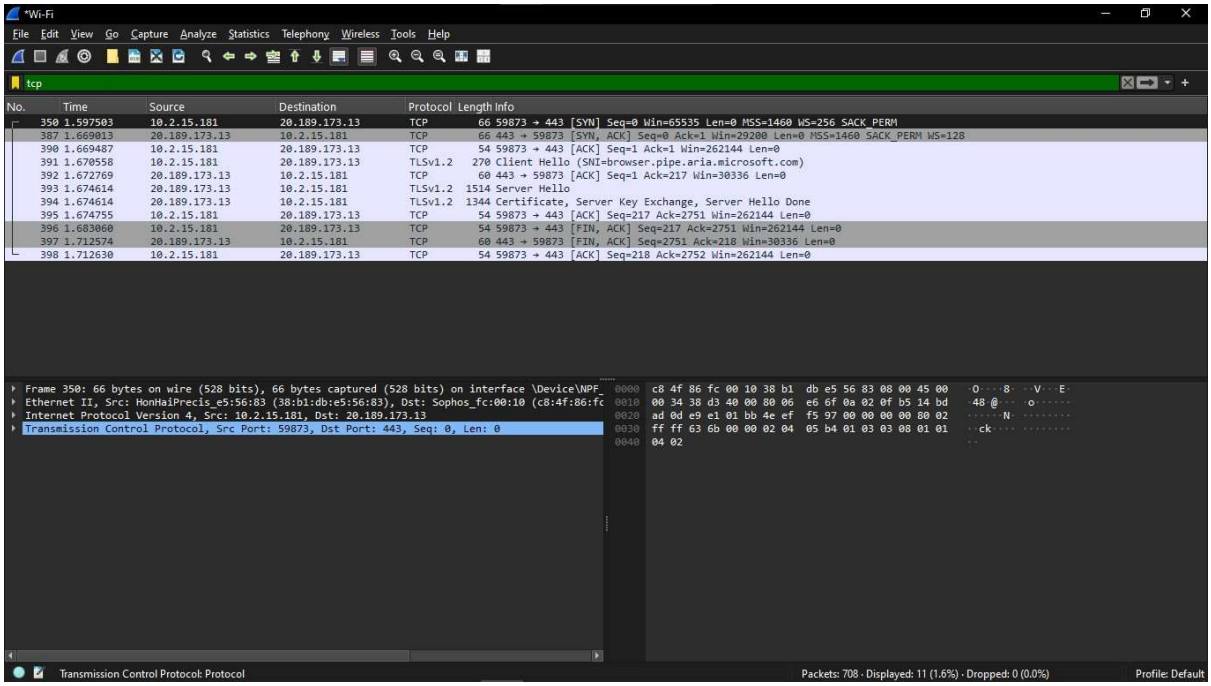
1. Start a new capture in Wireshark.
2. Open a Command Prompt or Terminal and run:
3. ping www.example.com -n 5 (Windows)
4. ping -c 5 www.example.com (Linux/Mac)
5. Stop the capture after the ping completes.
6. Apply the **Filter**: tcp and analyze:
    - **Source and Destination ports**
    - **Sequence and Acknowledgment numbers**
    - **TCP flags (SYN, ACK, FIN, etc.)**
    - **Window size and retransmissions**
7. Take a screenshot of the captured TCP segments.

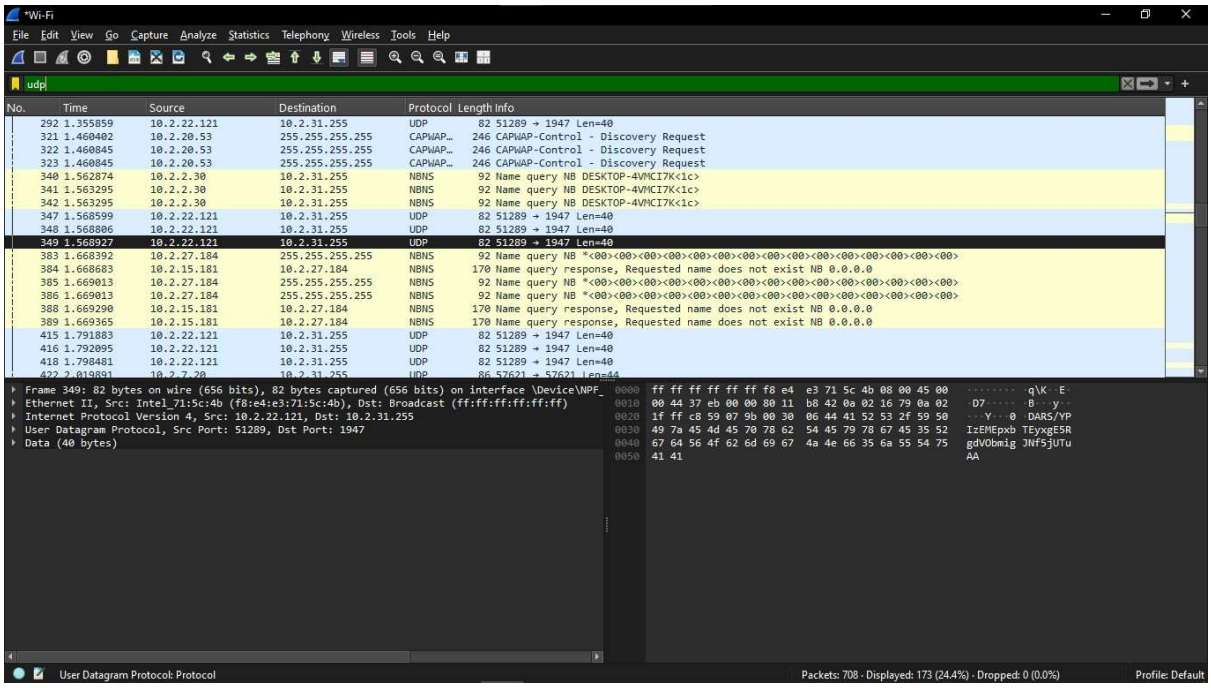
(c) Capture and Analyze UDP Datagrams

1. Start a new capture in Wireshark.
2. Open a Command Prompt or Terminal and run:
3. nslookup example.com
4. Stop the capture after the DNS query completes.
5. Apply the **Filter**: udp and analyze:
    - **Source and Destination ports**
    - **Length and checksum values**
    - **DNS query or response details**
6. Take a screenshot of the captured UDP datagrams.

Output Screenshots:







Result:

IP packets, TCP segments, and UDP datagrams were successfully captured and analyzed using Wireshark, demonstrating key aspects of network protocol functionality.

Ex.No: 13 Network Protocol Analysis: Capture and Analyze DNS and HTTP Packets in Wireshark

Date:

Objectives:

- Capture and analyze **DNS (Domain Name System) packets** in Wireshark.
- Capture and analyze **HTTP (Hypertext Transfer Protocol) packets** in Wireshark.
- Understand the communication between client and server using DNS and HTTP protocols.
- Interpret the structure and significance of captured packets.

Introduction:

Network protocols such as **DNS** and **HTTP** play a crucial role in web communications. DNS is responsible for translating domain names into IP addresses, while HTTP facilitates data transfer between web clients and servers. In this experiment, we use **Wireshark**, a powerful network protocol analyzer, to inspect DNS and HTTP packet structures.

Requirements:

- **Wireshark** installed on a computer.
- **Internet connection** or a local network with a DNS and Web Server.
- A **Web Browser** to generate traffic for packet capture.

Part A: Capture and Analyze DNS Packets

Step 1: Start Packet Capture in Wireshark

1. Open **Wireshark**.
2. Select the active network interface (e.g., Ethernet, Wi-Fi).
3. Click **Start** to begin packet capture.

Step 2: Generate DNS Traffic

1. Open a web browser and enter any domain name (e.g., www.example.com).
2. Press **Enter** to load the webpage.
3. DNS queries will be generated as the browser resolves the domain name.

Step 3: Filter DNS Packets

1. In Wireshark's **filter bar**, type:
2. dns
3. Press **Enter** to display only DNS-related packets.

Step 4: Analyze DNS Packet Structure

1. Click on a **DNS request packet**.

2. Expand the **DNS section** in the packet details.
3. Observe the **Query Type (A, AAAA, MX, etc.)**, domain name, and transaction ID.
4. Click on a **DNS response packet** and check the resolved IP address.

Part B: Capture and Analyze HTTP Packets

Step 1: Start Packet Capture in Wireshark

1. Ensure Wireshark is still running and capturing packets.
2. If not, restart packet capture on the active network interface.

Step 2: Generate HTTP Traffic

1. Open a web browser and visit an **HTTP website** (e.g., http://example.com).
2. Avoid HTTPS (https://) sites, as they use encryption (TLS/SSL), making HTTP packets unreadable.

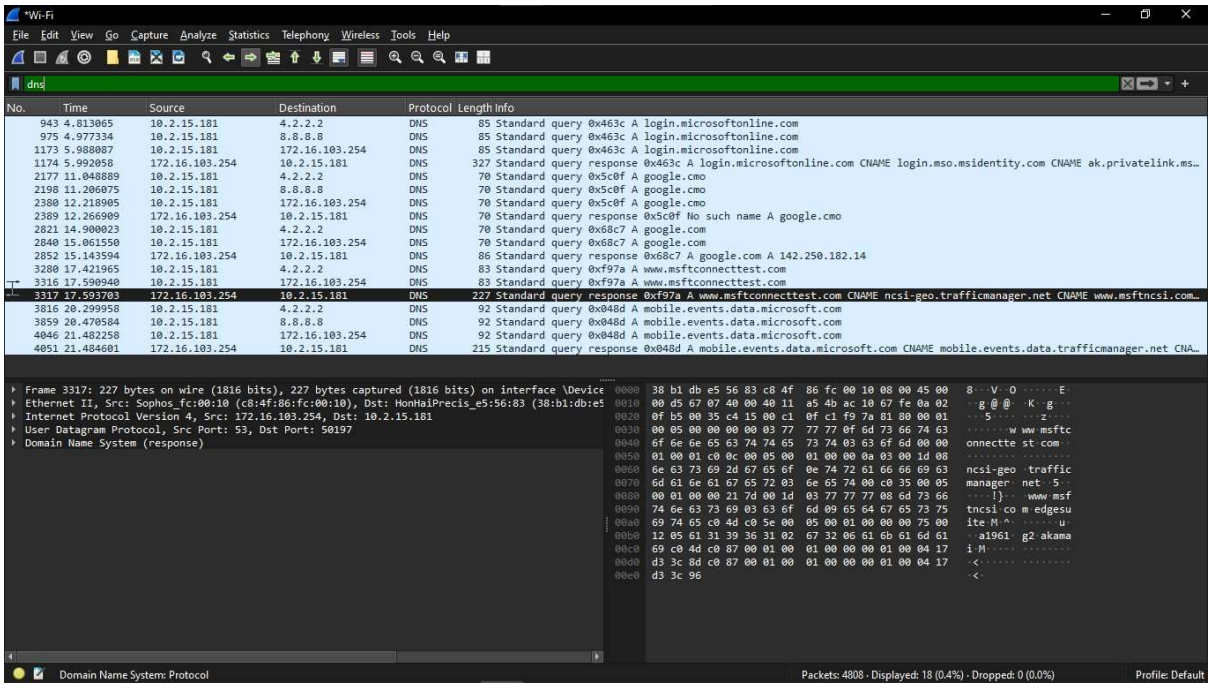
Step 3: Filter HTTP Packets

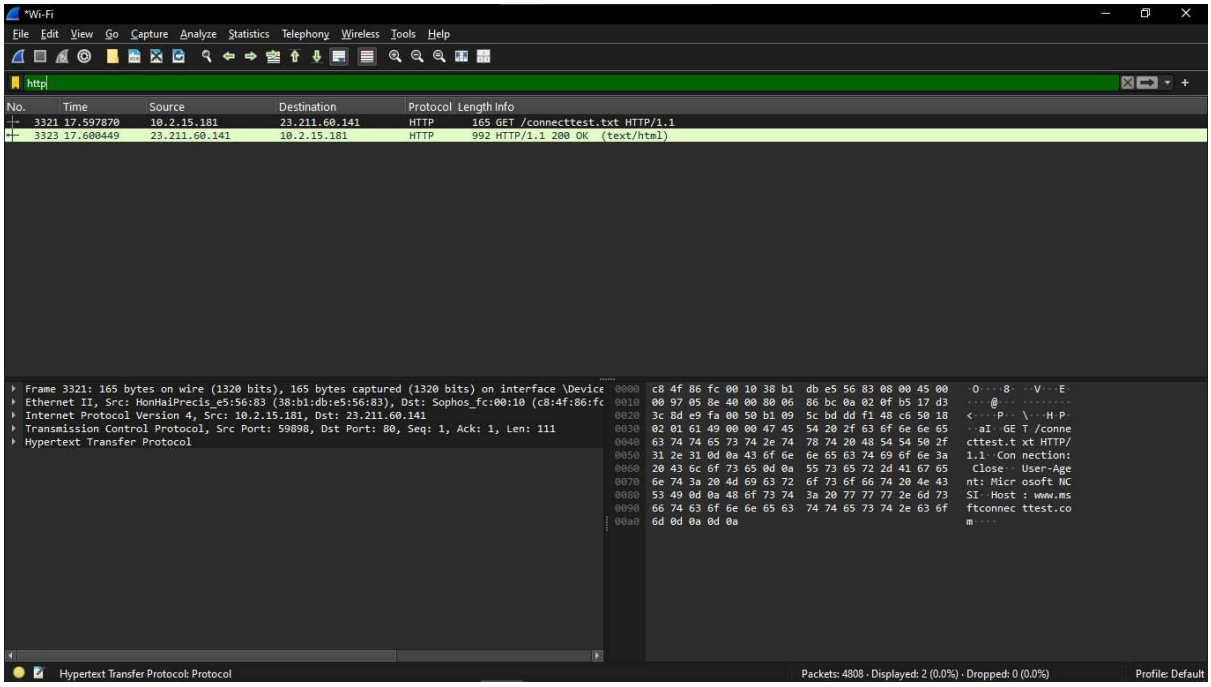
1. In Wireshark's **filter bar**, type:
2. http
3. Press **Enter** to display only HTTP packets.

Step 4: Analyze HTTP Packet Structure

1. Click on an **HTTP request packet**.
2. Expand the **Hypertext Transfer Protocol section**.
3. Observe:
    - **Request Method** (GET, POST, etc.).
    - **Requested URL**.
    - **User-Agent** (identifies the browser/client).
4. Click on an **HTTP response packet**.
5. Observe:
    - **HTTP Status Code** (e.g., 200 OK, 404 Not Found).
    - **Content-Type** (HTML, JSON, etc.).
    - **Server Information**.

Output Screenshots:





Result:

DNS and HTTP packets were successfully captured and analyzed using Wireshark. The experiment provided insights into how domain resolution and web communication occur at the network level.

Ex.No: 14 **Configuration of DNS and Web Server Using Cisco Packet Tracer**
Date:

Objectives:

- Configure a DNS and Web Server in Cisco Packet Tracer.
- Enable domain name resolution for client devices.
- Host a simple webpage on the Web Server.
- Verify connectivity using client devices.
- Save the configuration and close Packet Tracer.

Introduction:

The Domain Name System (DNS) is a crucial service that translates domain names into IP addresses, making it easier for users to access websites. A Web Server hosts webpages that can be accessed through a browser. This experiment involves setting up both a DNS and a Web Server to enable browsing within the network.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
    - 1 Router (Gateway)
    - 1 Switch (LAN Connection)
    - 1 Server (DNS & Web Server)
    - 2 PCs (Client Devices)
- Connection Cables:
    - Copper Straight-Through Cables (for wired connections)

Steps to Configure DNS and Web Server

Step 1: Adding Network Devices

- Drag and drop the router, switch, server, and PCs into the workspace.
- Connect the devices using appropriate cables.

Step 2: Configuring IP Addressing

- Assign the following IP addresses:
    - **Server (DNS & Web Server)**: 192.168.1.10/24
    - **PC1 (Client)**: 192.168.1.11/24
    - **PC2 (Client)**: 192.168.1.12/24
    - **Router (Default Gateway)**: 192.168.1.1/24

Step 3: Configuring the DNS Server

1. **Open the Server**:
    - Click on the **Server**, navigate to the **Services** tab.
    - Select **DNS** and turn the service **ON**.
2. **Create a DNS Entry**:
    - Set the domain name (e.g., www.example.com).
    - Assign it to the web server's IP address (192.168.1.10).
    - Click **Add** and **Save**.

Step 4: Configuring the Web Server

1. **Enable HTTP Service**:
    - In the **Services** tab, select **HTTP**.
    - Ensure the HTTP service is turned **ON**.
2. **Edit the Web Page**:
    - Click **Edit** and modify the default webpage content.
    - Save the changes.

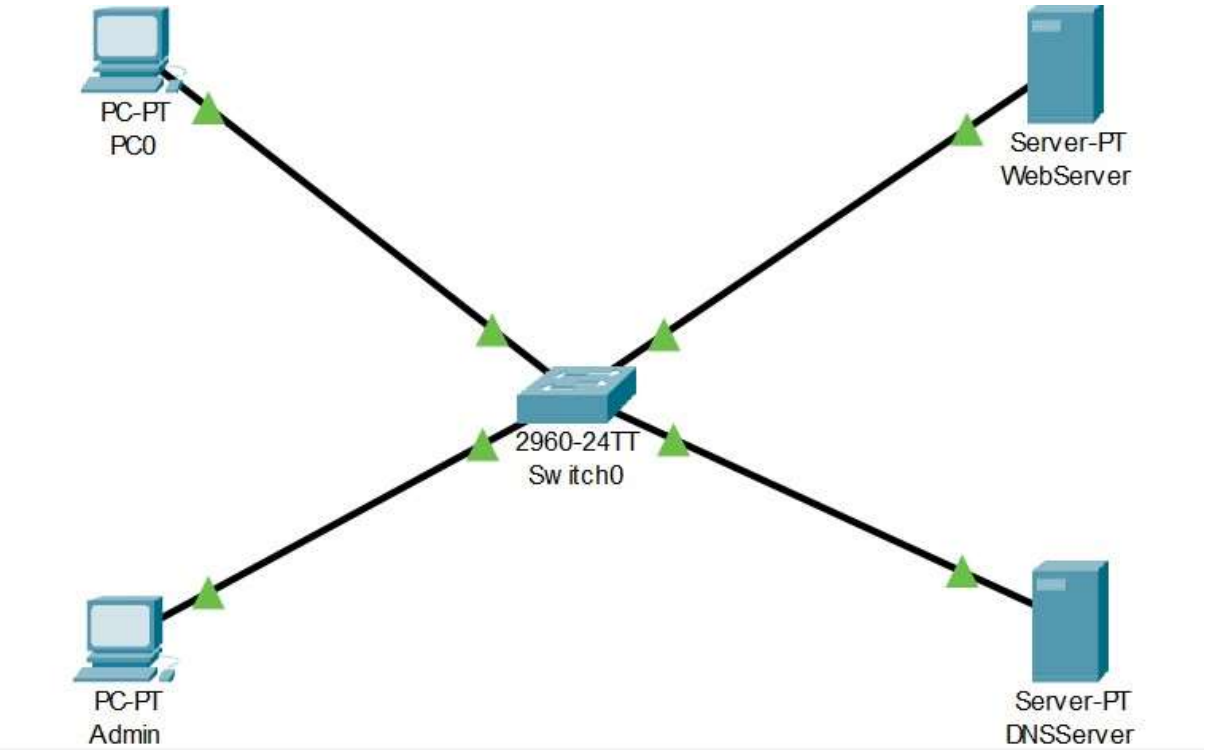
Step 5: Configuring Client Devices

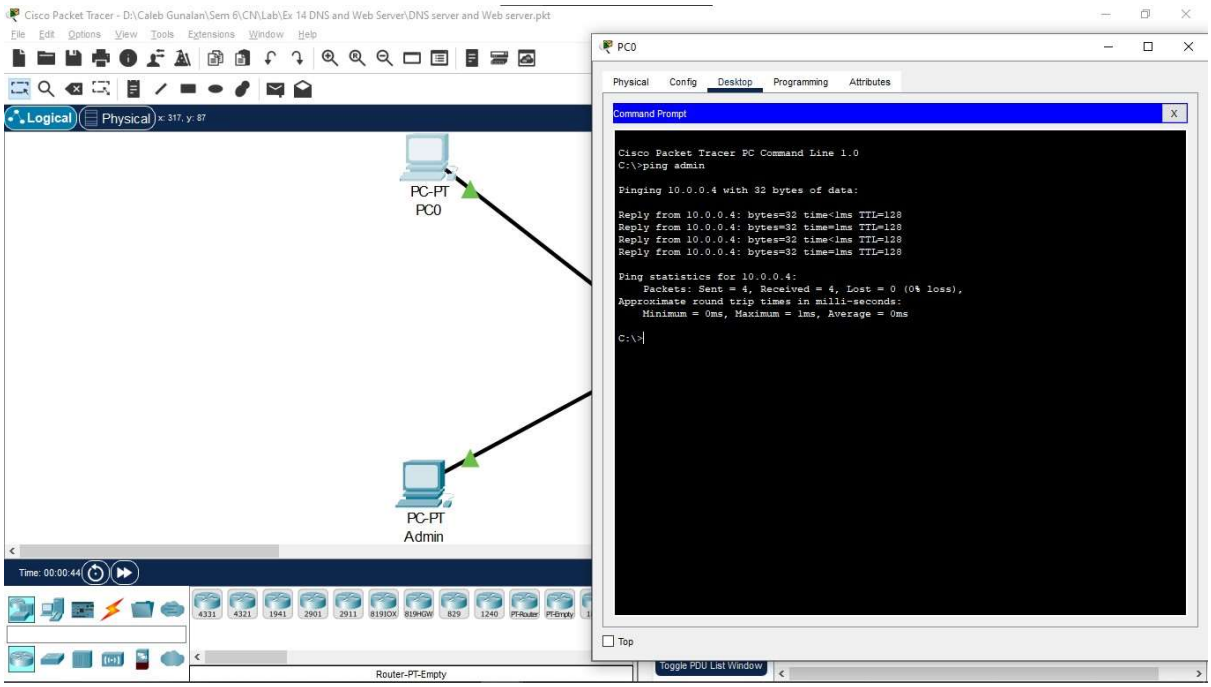
1. **Set IP Configuration**:
    - Click on **PC1** and **PC2**, navigate to the **IP Configuration** tab.
    - Assign the correct IP addresses and default gateway.
2. **Verify DNS Resolution**:
    - Open the **Command Prompt** on a client PC and type:
    - nslookup www.example.com
    - Ensure the domain resolves to 192.168.1.10.
3. **Access the Webpage**:
    - Open a **Web Browser** on a client PC.
    - Type www.example.com in the address bar.
    - Ensure the webpage loads successfully.

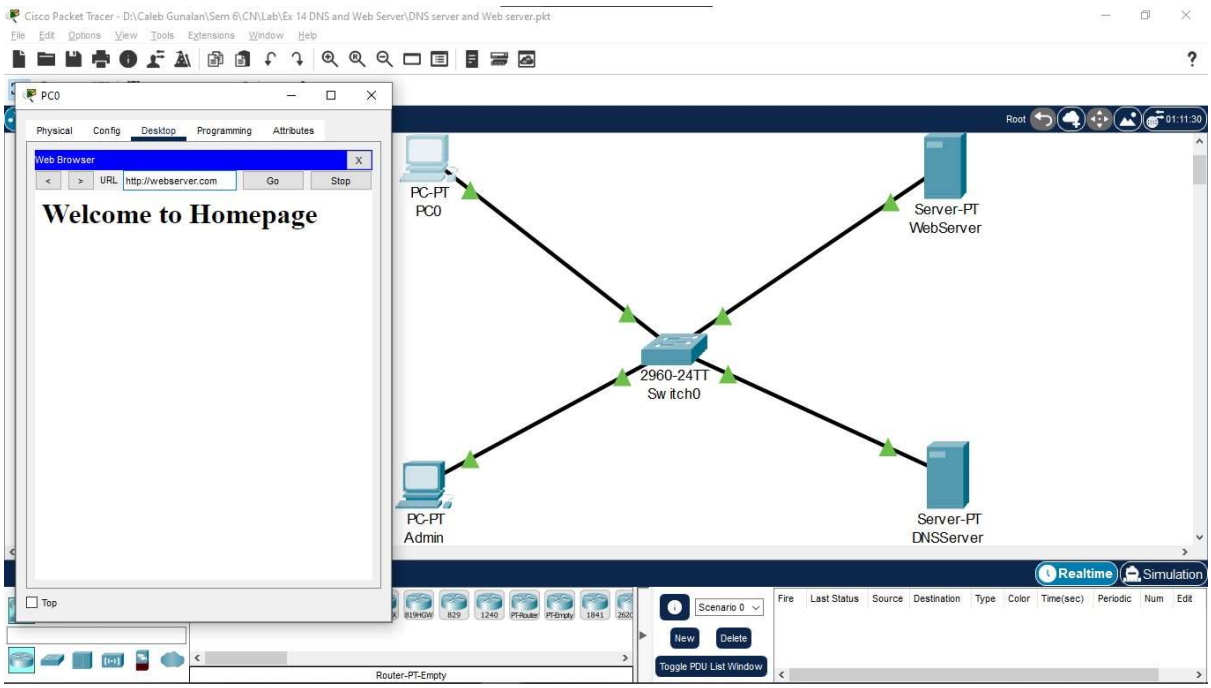
Step 6: Verifying Network Connectivity

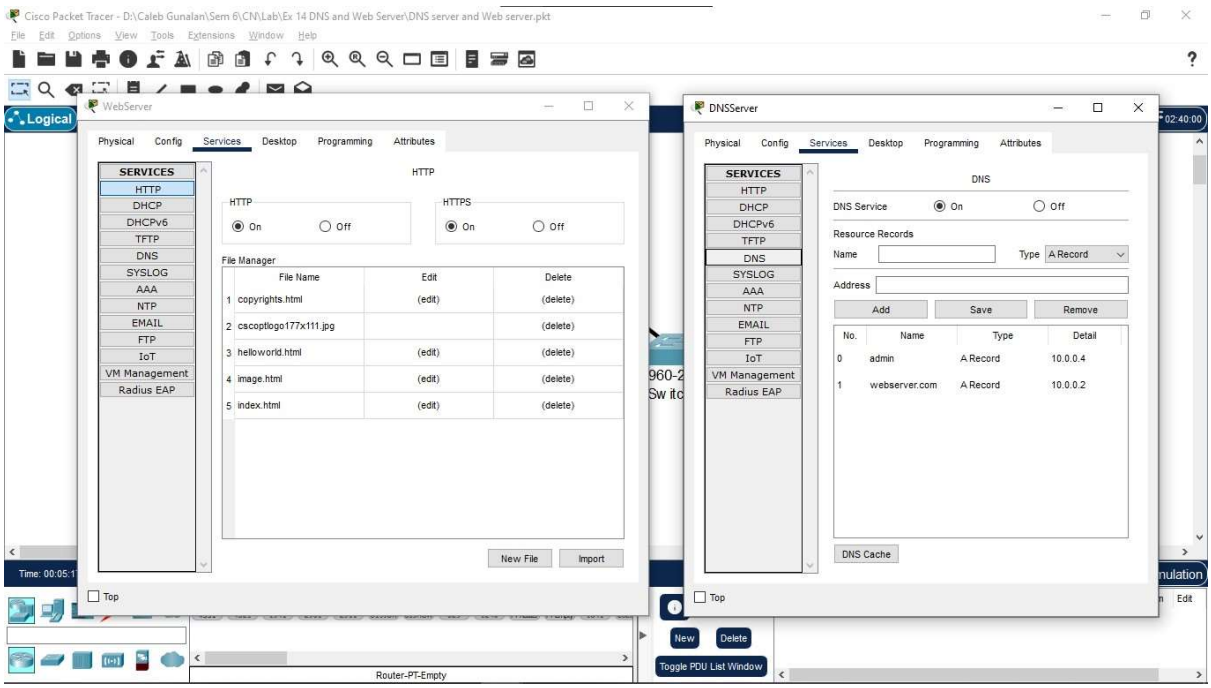
- Test connectivity by pinging the web server from the clients.
- Troubleshoot any DNS or web access issues.

Output Screenshots:









Result:

A DNS and Web Server were successfully configured using Packet Tracer, enabling domain name resolution and webpage hosting within the network.

Ex.No: 15 **Configuration of Email Server Using Cisco Packet Tracer**
Date:

Objectives:

- Configure an Email server in Cisco Packet Tracer.
- Enable email communication between client devices.
- Implement user authentication for secure email access.
- Verify email functionality using client devices.
- Save the configuration and close Packet Tracer.

Introduction:

Email communication is an essential service in computer networks, allowing users to send and receive messages securely. In this experiment, we will configure an Email server to provide email functionality within a local network.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
    - 1 Router (Gateway)
    - 1 Switch (LAN Connection)
    - 1 Server (Email Server)
    - 2 PCs (Client Devices)
- Connection Cables:
    - Copper Straight-Through Cables (for wired connections)

Steps to Configure Email Server

Step 1: Adding Network Devices

- Drag and drop the router, switch, server, and PCs into the workspace.
- Connect the devices using appropriate cables.

Step 2: Configuring IP Addressing

- Assign the following IP addresses:
    - **Email Server**: 192.168.1.10/24
    - **PC1 (Client)**: 192.168.1.11/24
    - **PC2 (Client)**: 192.168.1.12/24
    - **Router (Default Gateway)**: 192.168.1.1/24

Step 3: Configuring the Email Server

1. **Open the Email Server**:
    - Click on the **Server**, navigate to the **Services** tab.
    - Select **Email** and turn on both **SMTP** and **POP3** services.
2. **Create User Accounts**:
    - Add a username (e.g., user1) and set a password (password123).
    - Create another user (e.g., user2) for testing email exchanges.
3. **Save the Configuration**.

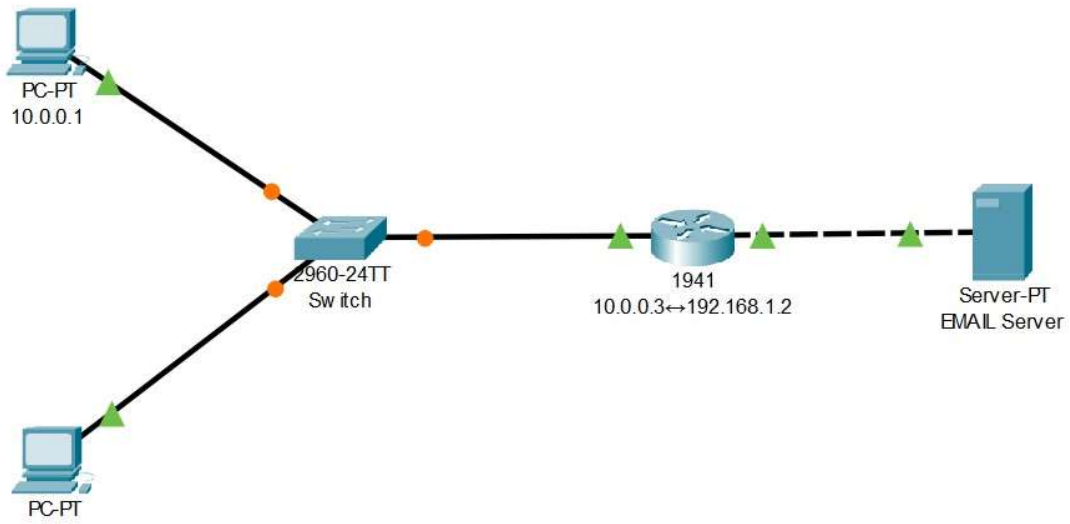
Step 4: Configuring Client Devices

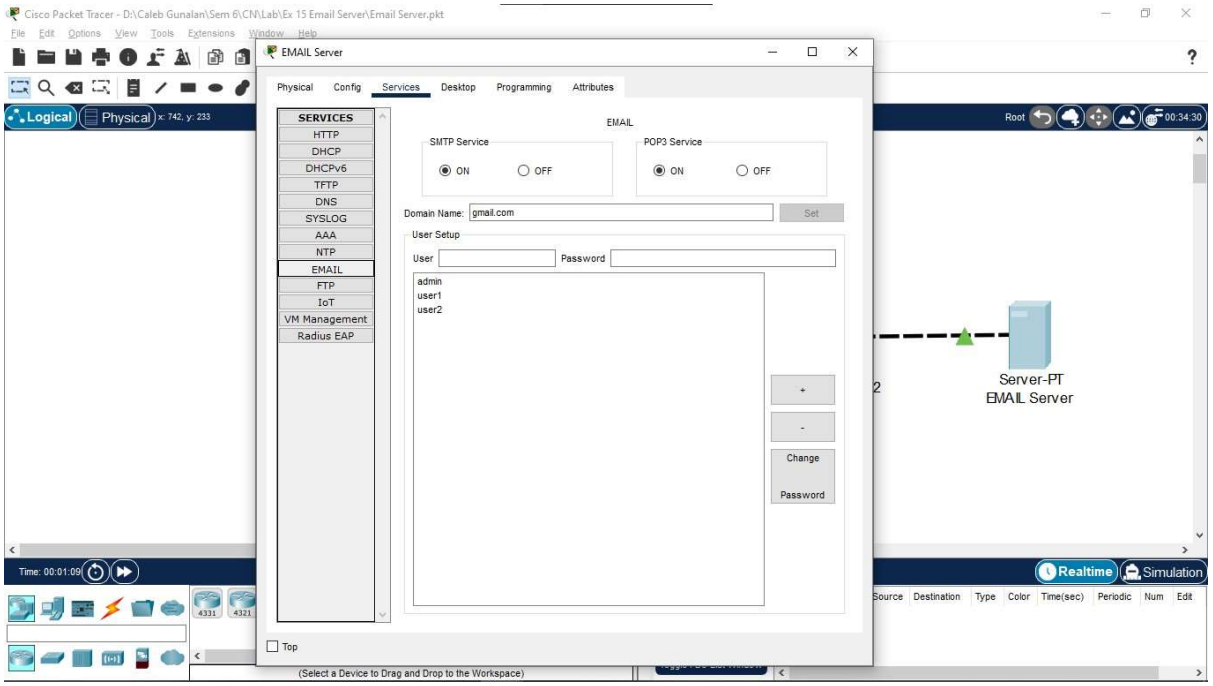
1. **Set IP Configuration**:
    - Click on **PC1** and **PC2**, navigate to the **IP Configuration** tab.
    - Assign the correct IP addresses and default gateway.
2. **Set Up Email Accounts**:
    - Open the **Email Client** application on PC1 and PC2.
    - Configure the following settings:
        - **Incoming Mail Server (POP3)**: 192.168.1.10
        - **Outgoing Mail Server (SMTP)**: 192.168.1.10
        - **Username and Password**: As configured on the server.
3. **Send and Receive Emails**:
    - Compose an email on PC1 and send it to user2.
    - Check the inbox on PC2 to verify the email reception.

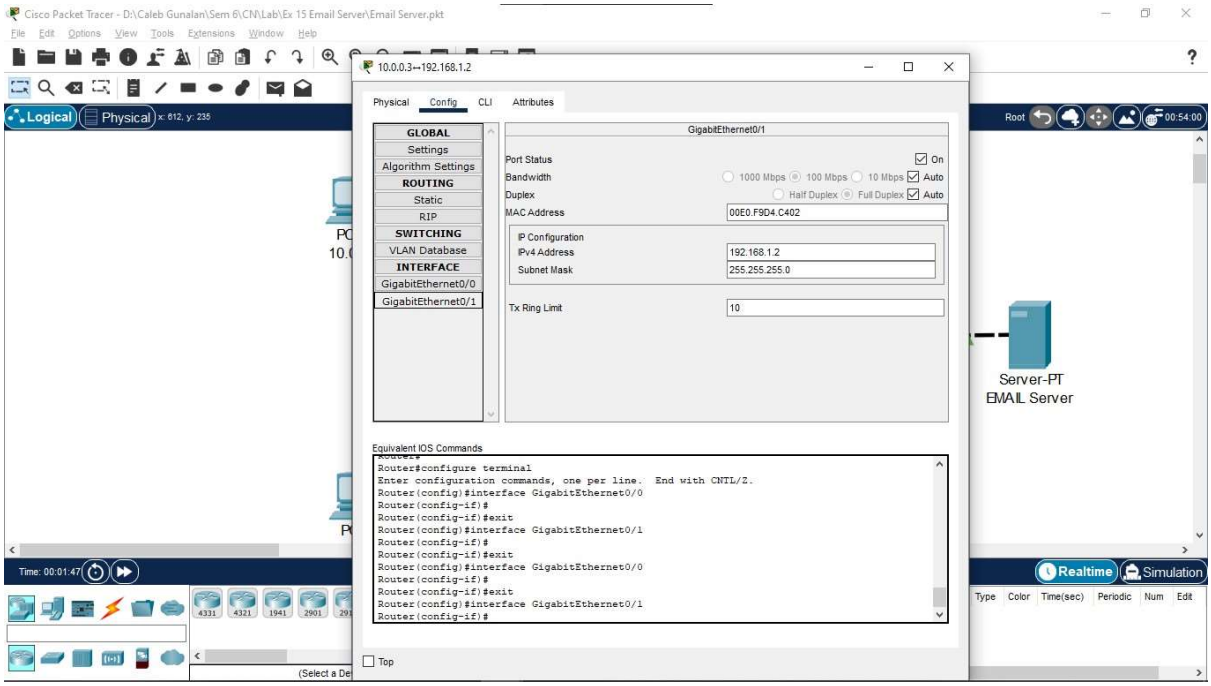
Step 5: Verifying Email Communication

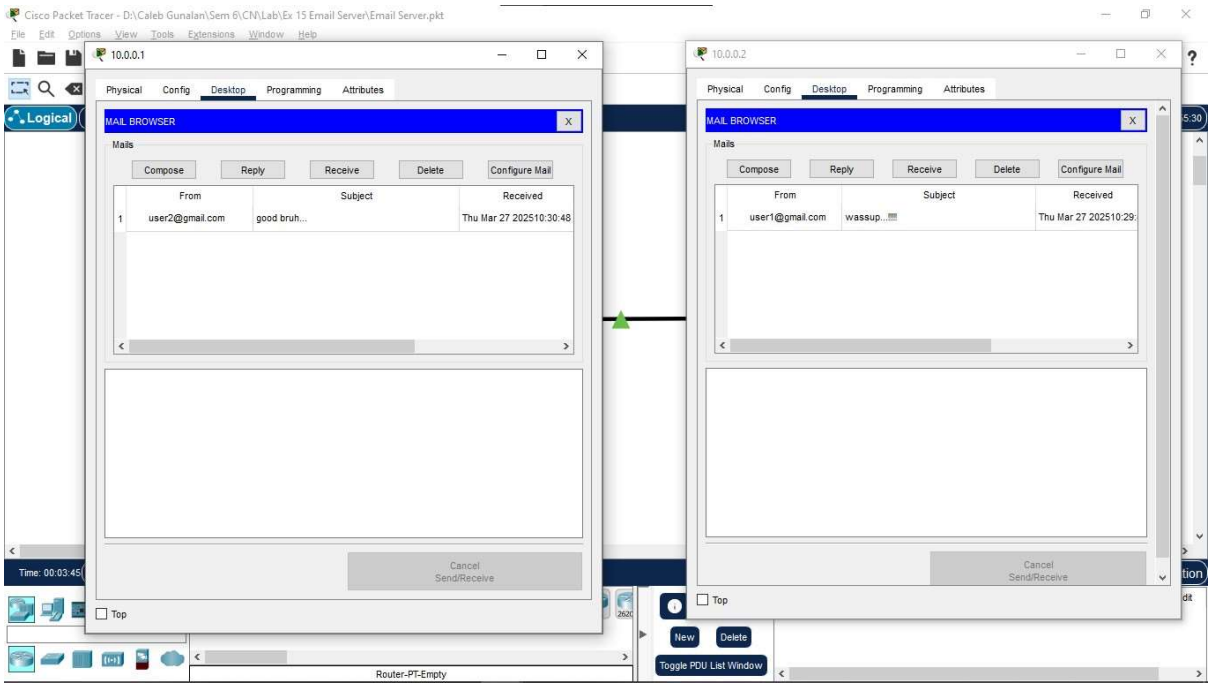
- Ensure emails are successfully sent and received.
- Troubleshoot any connectivity or authentication issues.

Output Screenshots:









Result:

An Email server was successfully configured using Packet Tracer, allowing secure email communication between client devices.

Ex.No: 08 **Configuration of FTP Server Using Cisco Packet Tracer**
Date:

Objectives:

- Configure an FTP server in Cisco Packet Tracer.
- Enable file transfer between devices within the network.
- Implement user authentication for secure file access.
- Verify FTP functionality using client devices.
- Save the configuration and close Packet Tracer.

Introduction:

File Transfer Protocol (FTP) is a standard network protocol used to transfer files between a client and a server over a network. In this experiment, we will configure an FTP server to allow file sharing and authentication within a local network.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
  - 1 Router (Gateway)
  - 1 Switch (LAN Connection)
  - 1 Server (FTP Server)
  - 2 PCs (Client Devices)
- Connection Cables:
  - Copper Straight-Through Cables (for wired connections)

Steps to Configure FTP Server

Step 1: Adding Network Devices

- Drag and drop the router, switch, server, and PCs into the workspace.
- Connect the devices using appropriate cables.

Step 2: Configuring IP Addressing

- Assign the following IP addresses:
  - **FTP Server**: 192.168.1.10/24
  - **PC1 (Client)**: 192.168.1.11/24
  - **PC2 (Client)**: 192.168.1.12/24
  - **Router (Default Gateway)**: 192.168.1.1/24

Step 3: Configuring the FTP Server

1. **Open the FTP Server**:
    - Click on the **Server**, navigate to the **Services** tab.
    - Select **FTP** and turn it **ON**.
2. **Create FTP User Accounts**:
    - Add a username (e.g., user1) and set a password (password123).
    - Assign read/write permissions to allow file transfers.
3. **Save the Configuration**.

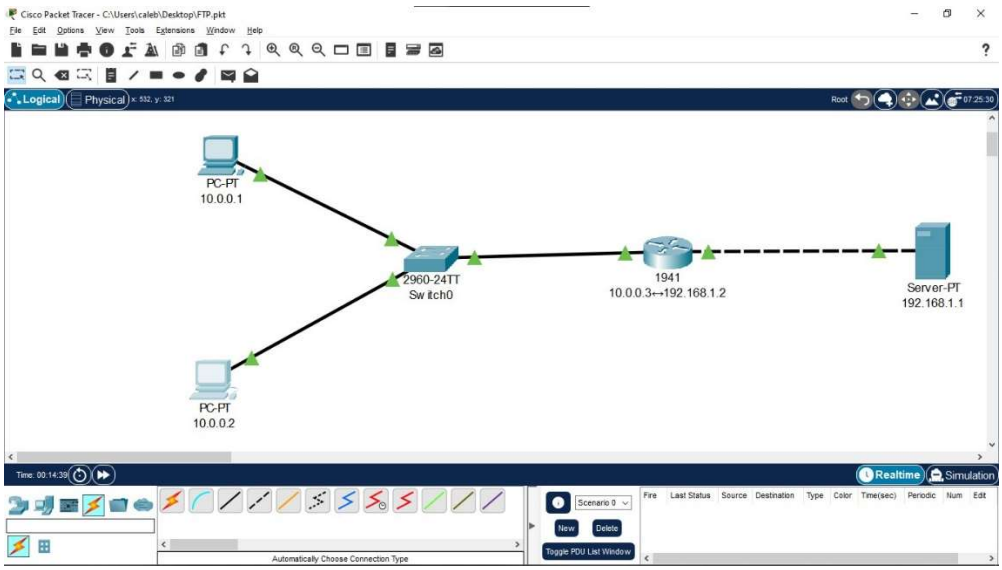
Step 4: Configuring Client Devices

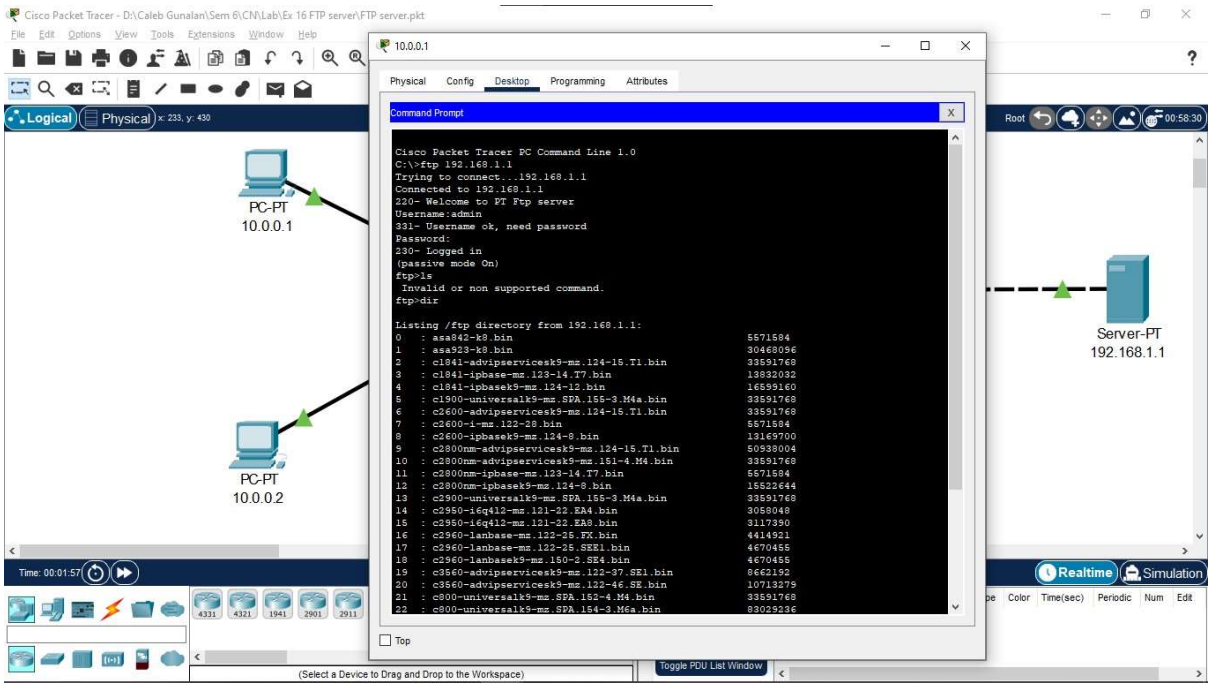
1. **Set IP Configuration**:
    - Click on **PC1** and **PC2**, navigate to the **IP Configuration** tab.
    - Assign the correct IP addresses and default gateway.
2. **Access the FTP Server**:
    - Open the **Command Prompt** on PC1 and PC2.
    - Type the command to access the FTP server:
    - ftp 192.168.1.10
    - Enter the username and password when prompted.
    - Use commands like ls, get filename, and put filename to download or upload files.

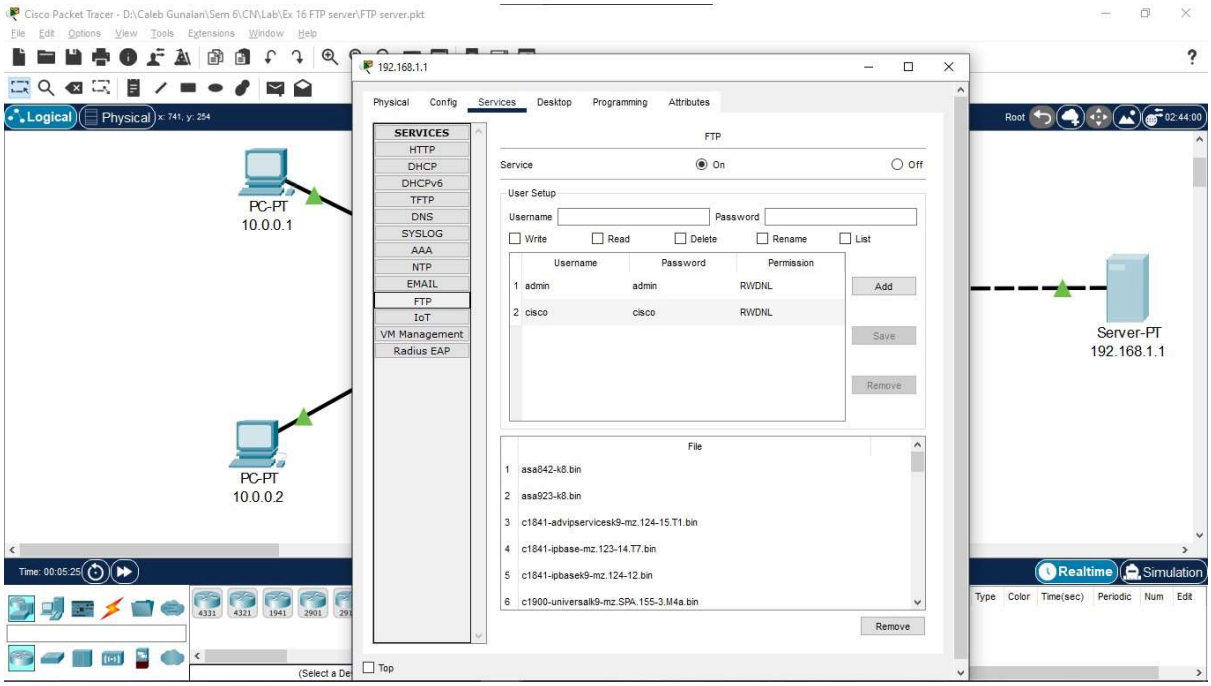
Step 5: Verifying FTP Connection

- Test file transfers by uploading and downloading files using FTP commands.
- Ensure authentication works as expected.

Output Screenshots:







Result:

An FTP server was successfully configured using Packet Tracer, allowing secure file transfers between client devices and the server.

Ex.No: 07 **Configuration of Firewall Using Cisco Packet Tracer**
Date:

Objectives:

- Configure a firewall to filter network traffic in Cisco Packet Tracer.
- Implement Access Control Lists (ACLs) to restrict or allow specific traffic.
- Establish connectivity between different network zones (Internal, DMZ, and External).
- Verify firewall rules using simulation tools.
- Save the configuration and close Packet Tracer.

Introduction:

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. By configuring a firewall in Cisco Packet Tracer, we can enforce network policies and protect internal systems from unauthorized access.

Requirements:

- Cisco Packet Tracer Software
- Network Devices:
  - 1 Router (Firewall)
  - 2 Switches (Core Switch & DMZ Switch)
  - 1 Server (Web Server in DMZ)
  - 2 PCs (Internal Network & External Network)
- Connection Cables:
  - Copper Straight-Through Cables (for wired connections)

Steps to Configure Firewall

Step 1: Adding Network Devices

- Drag and drop the router, switches, PCs, and server into the workspace.
- Connect the devices using appropriate cables.

Step 2: Configuring IP Addressing

- Assign the following IP addresses:
  - **Internal Network (LAN)**: 192.168.1.0/24
  - **DMZ Network**: 192.168.2.0/24
  - **External Network (WAN)**: 203.0.113.0/24
- Configure default gateways on PCs and servers to route traffic through the firewall.

Step 3: Enabling and Configuring ACLs on the Firewall

1. **Access the Firewall Router** and enter privileged EXEC mode:
2. enable
3. configure terminal
4. **Create an ACL to Allow Internal Network Access:**
5. access-list 100 permit ip 192.168.1.0 0.0.0.255 any
6. **Block External Network from Accessing Internal Network:**
7. access-list 100 deny ip 203.0.113.0 0.0.0.255 192.168.1.0 0.0.0.255
8. **Allow HTTP Traffic to the Web Server in DMZ:**
9. access-list 100 permit tcp any 192.168.2.10 eq 80
10. **Apply the ACL to the Firewall's Interfaces:**
11. interface GigabitEthernet0/0
12. ip access-group 100 in
13. exit

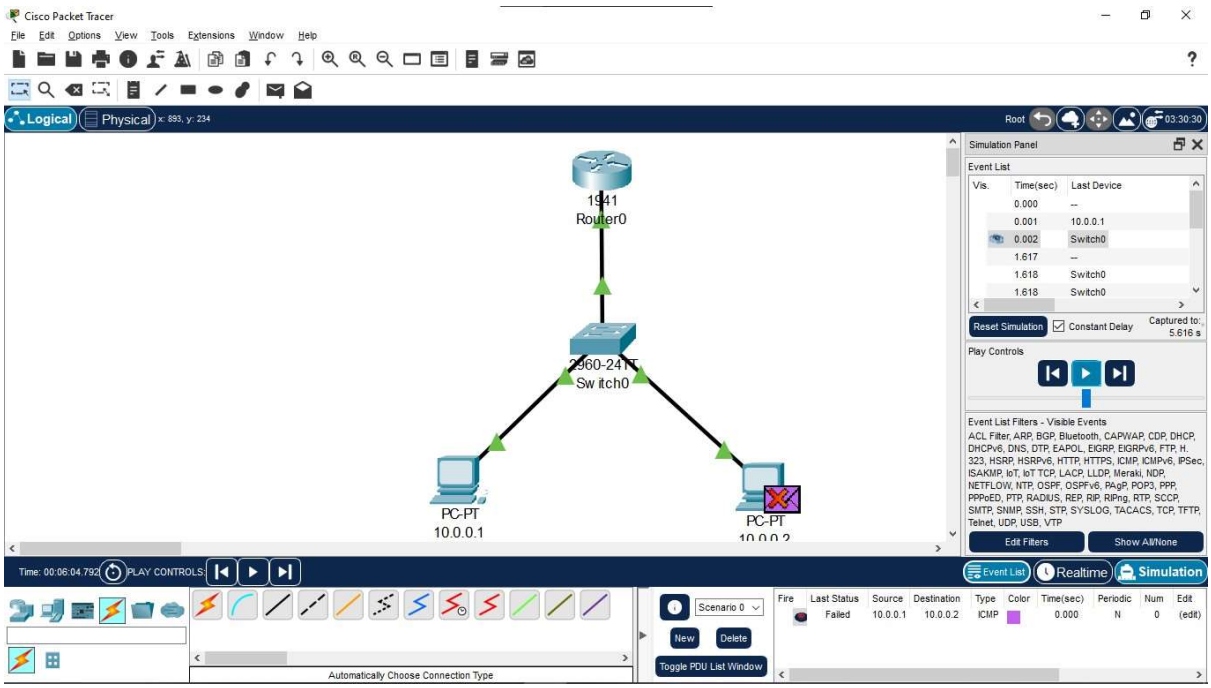
Step 4: Configuring NAT for Internet Access

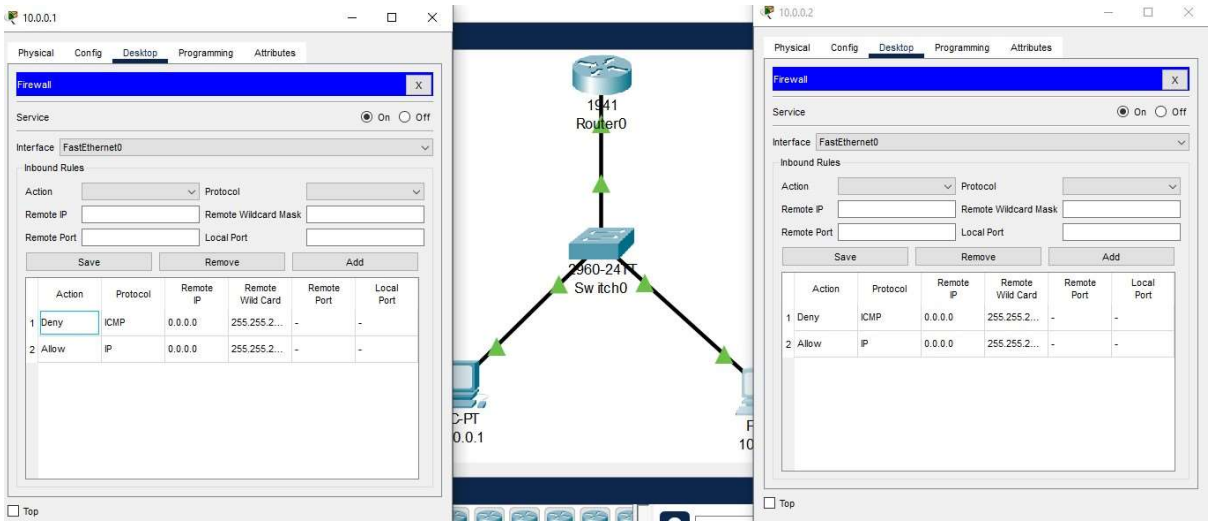
1. Enable NAT on the firewall to allow internal users to access external networks:
2. ip nat inside source list 100 interface GigabitEthernet0/1 overload
3. Define inside and outside NAT interfaces:
4. interface GigabitEthernet0/0
5. ip nat inside
6. exit
7. interface GigabitEthernet0/1
8. ip nat outside
9. exit

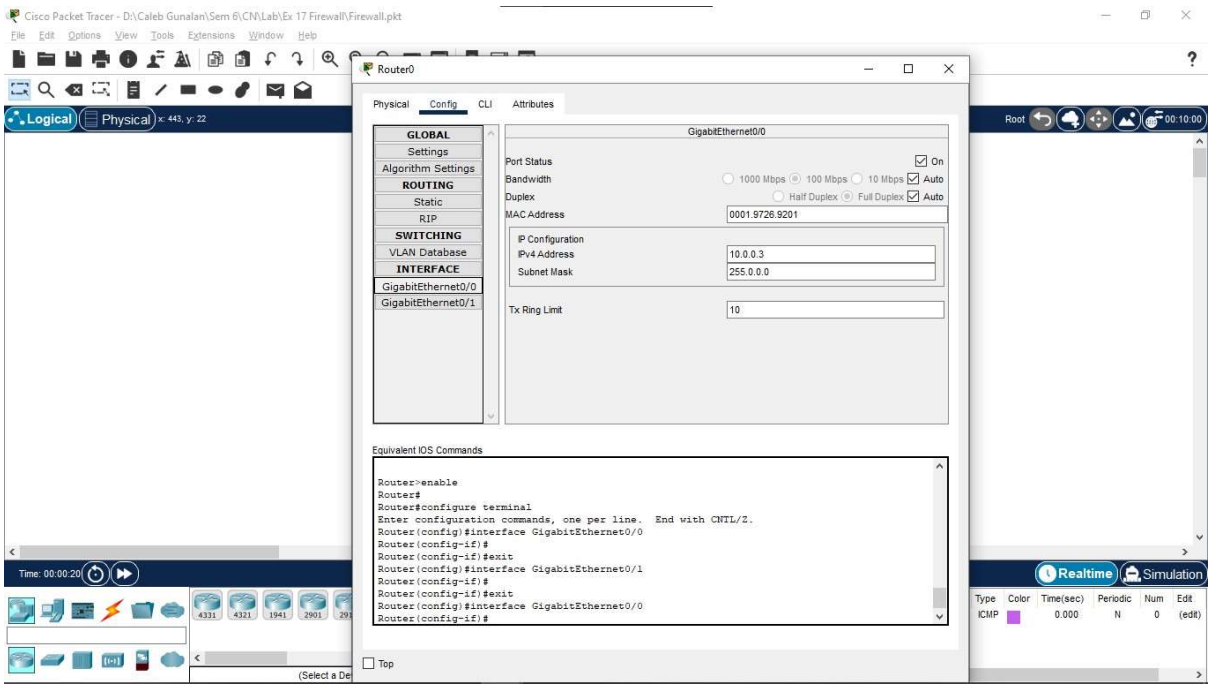
Step 5: Verifying Firewall Rules

- Open the **Command Prompt** on PCs and run:
- ping 192.168.2.10 (Check DMZ connectivity)
- ping 203.0.113.1 (Check External network access)
- Ensure successful or blocked responses based on the configured ACLs.

Output Screenshots:







Result:

A firewall was successfully configured using Packet Tracer, enforcing security rules through ACLs and enabling controlled network access.