Practical – 4

Aim of the Practical :- To configure Dynamic Host Configuration Protocol (DHCP) in Cisco Packet Tracer for automatic IP address allocation and test using multiple client PCs.

Requirements :- Cisco Packet Tracer, PC's, Switches, Ethernet cable and Server.

Practical:-

DHCP Discover Message: From CLIENT to SERVER

DHCP Offer Message: From SERVER to CLIENT

DHCP Request Message: From CLIENT to SERVER

DHCP Acknowledgement: From Server to CLIENT

Part A: DHCP Server in the Same Network

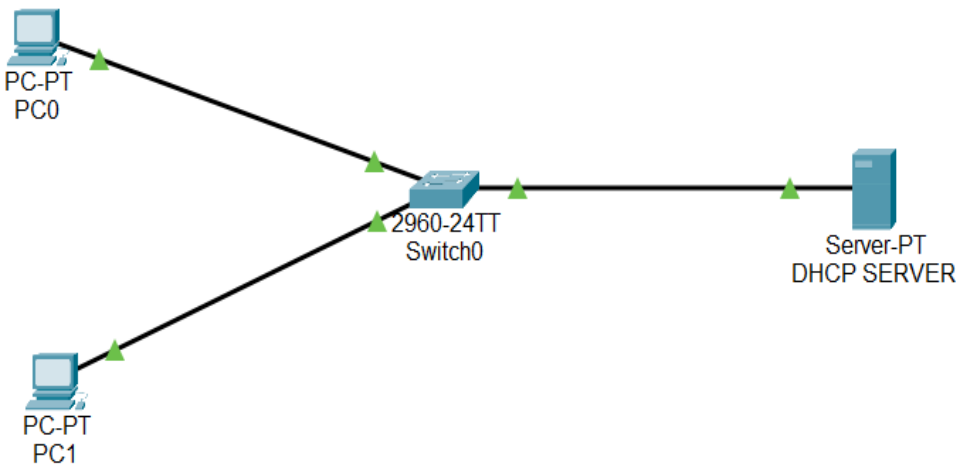

Figure 1: This image shows a simple LAN topology created in Cisco Packet Tracer. Two client PCs (PC0 and PC1) are connected to a switch (2960-24TT), which is also connected to a DHCP server. Since all devices are in the same network, DHCP messages can directly reach the server without the need for a relay agent.

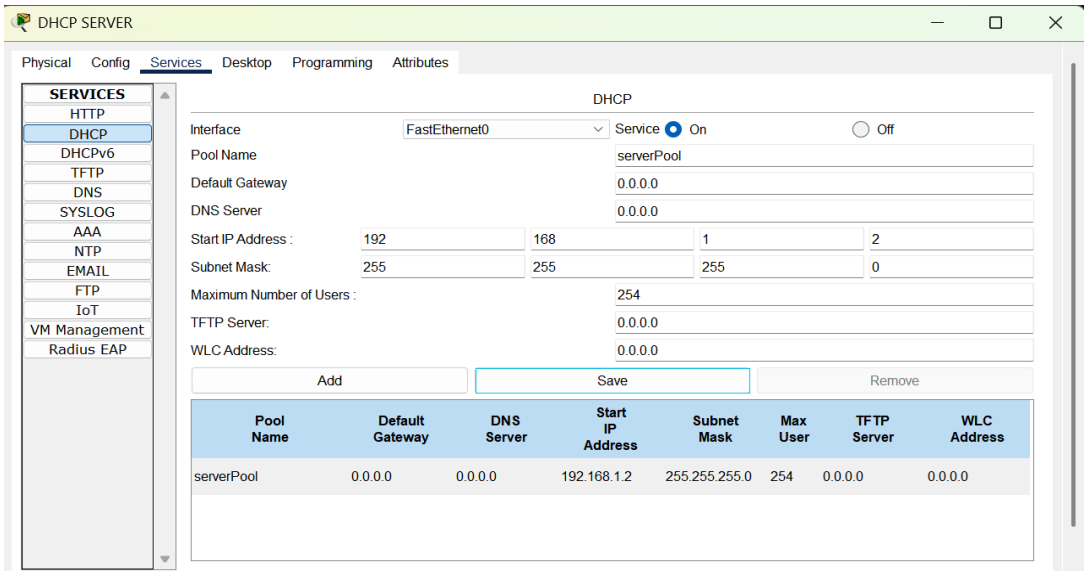

Figure 2: The DHCP service has been enabled on the server. A pool named *server Pool* is configured with the starting IP address 192.168.1.2 and subnet mask 255.255.255.0. The pool supports up to 254 users. No default gateway or DNS server has been defined, so those fields remain set to 0.0.0.0.

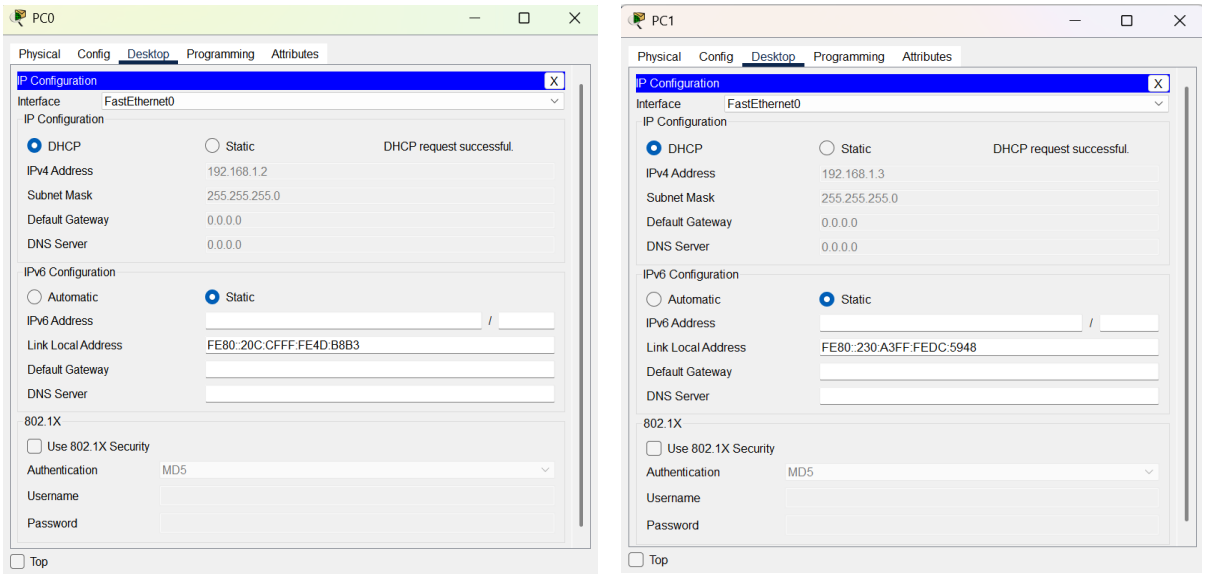

Figure 3: PC0 has been configured to obtain its IP address automatically using DHCP. The DHCP request was successful, and the client received the IP address 192.168.1.2 with a subnet mask of 255.255.255.0. Since the DHCP server did not provide a gateway or DNS, those fields remain blank (0.0.0.0).

Figure 4: PC1 has been configured to obtain its IP address automatically using DHCP. The DHCP request was successful, and the client received the IP address 192.168.1.3 with a subnet mask of 255.255.255.0. Since the DHCP server did not provide a gateway or DNS, those fields remain blank (0.0.0.0).

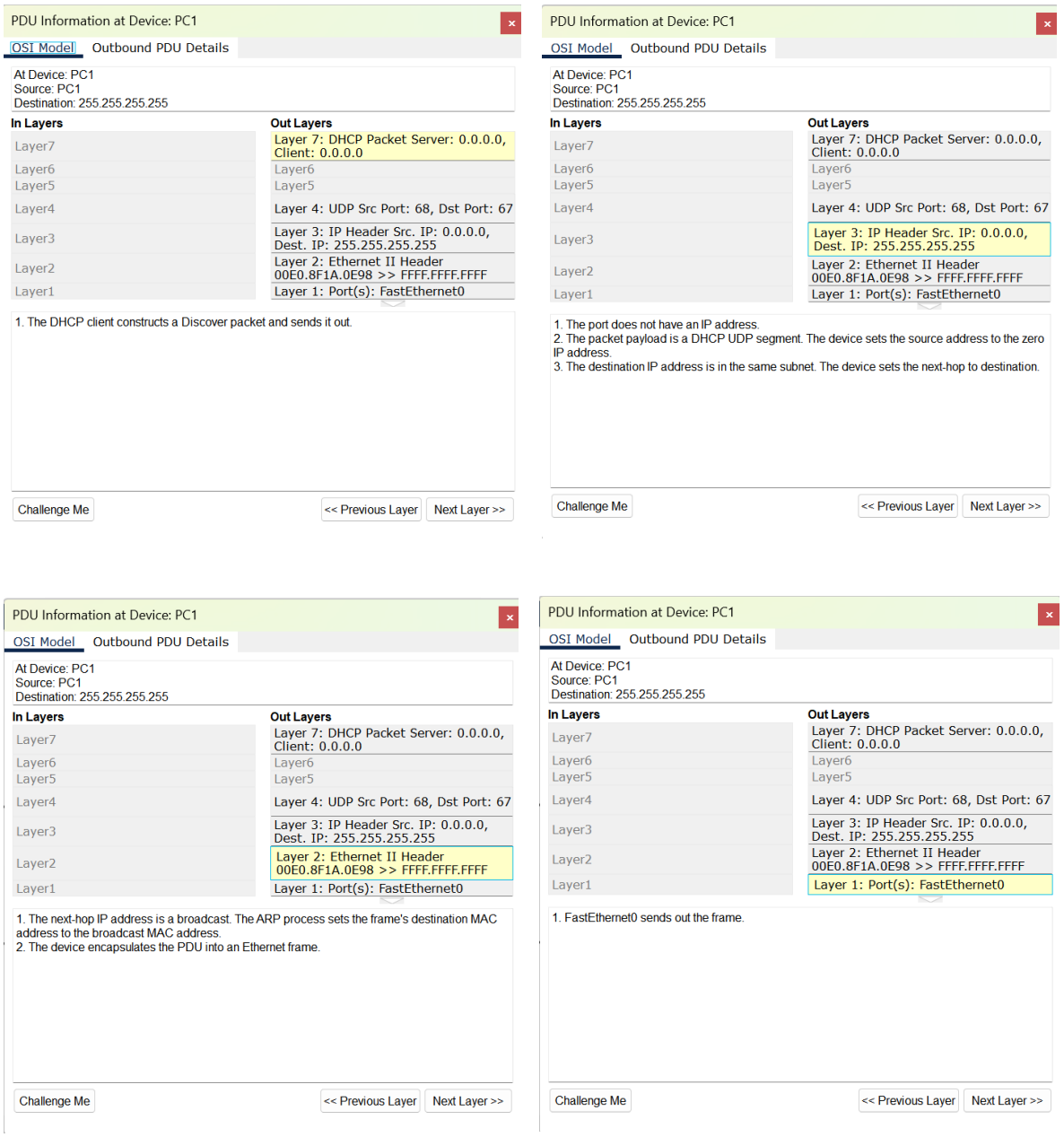

Figure 4 – 7: These images show details of the DHCP Discover packet sent by PC1. The sequence begins at Layer 7, where the PC, acting as a DHCP client, constructs the initial request to find a server. At the transport layer, the source port is 68, and the destination port is 67. At Layer 3, this data is wrapped in an IP header with a source address of 0.0.0.0 (as the client has no IP yet) and a broadcast destination of 255.255.255.255.

Next, at Layer 2, the packet is encapsulated into an Ethernet frame, using the client's physical MAC address as the source and the broadcast MAC address (FFFF.FFFF.FFFF) as the destination. Finally, at Layer 1, the fully formed frame is sent out onto the physical network wire through the FastEthernet0 port to be received by any device on the local network, including the DHCP server.

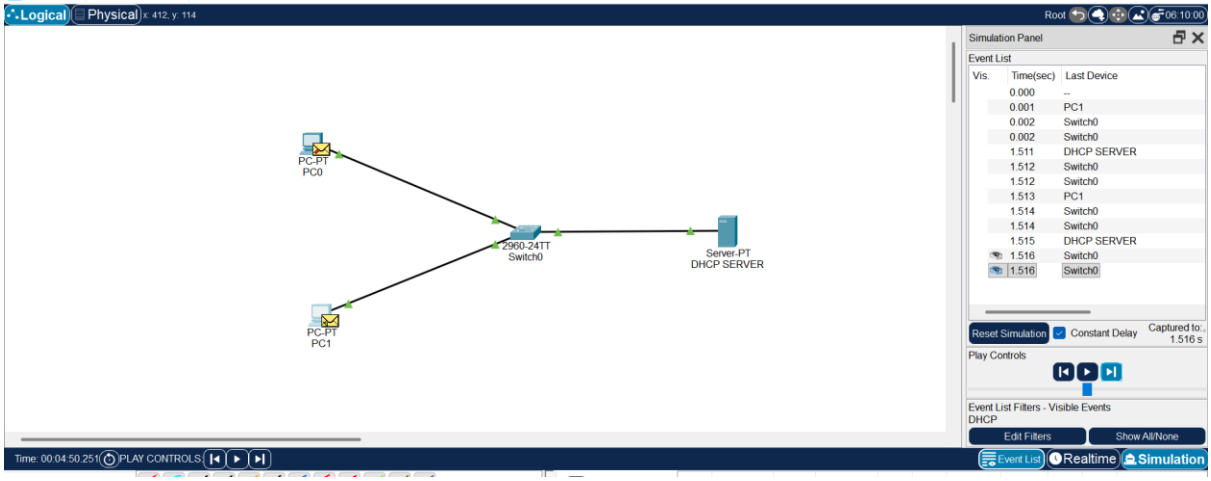

Figure 8: The simulation panel displays the sequence of DHCP communication between the client and server. PC1 sends a DHCP Discover packet, which is broadcast through the switch and received by the DHCP server. The server then replies with an Offer, continuing the DHCP handshake until the client obtains an IP address.

On the right, the "Event List" panel shows the captured sequence of network events. It meticulously logs the DHCP packet exchange, starting from the client's broadcast request to the server's final acknowledgment. This panel provides a timestamped, step-by-step visualization of the communication, confirming the successful automatic allocation of IP addresses to the client computers. The entire DHCP transaction for one PC is shown to have completed in about 1.5 seconds.

SETUP

The network was designed in Cisco Packet Tracer with the following components, as shown in the topology diagram:

- One Server (Server-PT) designated as the DHCP Server.
- One Switch (2960-24TT Switch0) to connect the devices.
- Two client PCs (PC0 and PC1).

All devices are connected via the switch, placing them in the same broadcast domain and local network.

Configuration Steps

1. DHCP Server Configuration

The server was configured to provide DHCP services. The key parameters were set under the Services > DHCP tab:

- Service: Turned On.
- Pool Name: server Pool.
- Start IP Address: 192.168.1.2.
- Subnet Mask: 255.255.255.0.
- Maximum Number of Users: 254.

This configuration creates a pool of IP addresses starting from 192.168.1.2 up to 192.168.1.255 for client allocation.

2. Client PC Configuration

Both PC0 and PC1 were configured to obtain their IP addresses automatically. In the Desktop > IP Configuration window for each PC, the DHCP option was selected.

Verification and Results

Upon enabling DHCP on the client PCs, the requests for IP addresses were successful.

- PC0 successfully obtained the IP address 192.168.1.2.
- PC1 successfully obtained the IP address 192.168.1.3.

Answers to Questions

1. **What is the source IP address when the client first sends a DHCP Discover message?**

   Ans: The source IP address is **0.0.0.0**. This is confirmed in the PDU details screenshot, which shows the Layer 3 IP Header Src. IP: 0.0.0.0.

2. **What is the destination IP address in the DHCP Discover message?**

   Ans: The destination IP address is the broadcast address **255.255.255.255**. The PDU details screenshot clearly shows Dest. IP: 255.255.255.255.

3. **Which UDP source port number is used by the client in the initial request?**

   Ans: The client uses UDP source port **68**, as seen in the Layer 4 information (UDP Src Port: 68).

4. **Which UDP destination port number does the request go to?**

Ans: The request is sent to UDP destination port **67**, which is the standard listening port for DHCP servers (Dst Port: 67).

5. **What happens if all addresses from the pool are consumed?**

   Ans: If all 254 available addresses from the pool (from 192.168.1.2 to 192.168.1.255) were leased out, a new client (e.g., a 255th PC) requesting an IP address would not receive a DHCP Offer from the server. The client's request would time out, and it would fail to get a valid IP address for the network.

Part B: DHCP Server in a Different Network (Relay Agent)

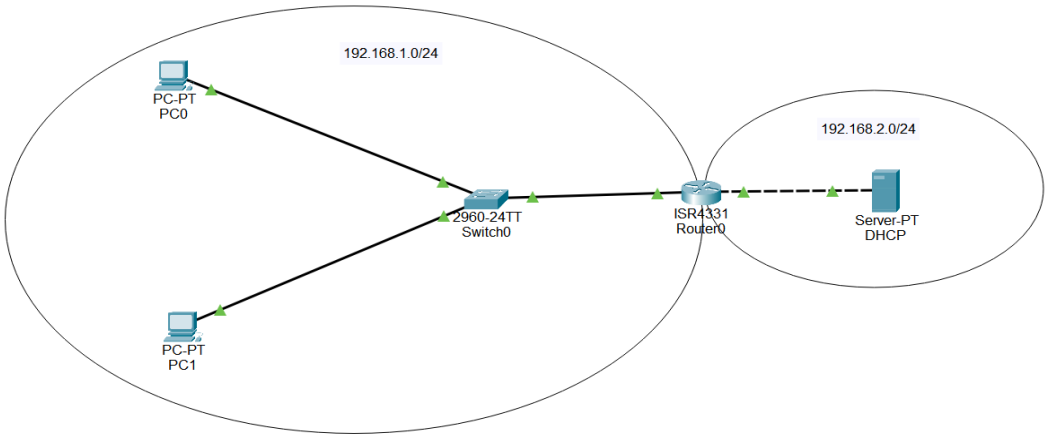

Figure 9: This diagram shows the complete Packet Tracer topology. The **192.168.1.0/24 network** contains two client PCs connected to a switch, which in turn connects to the router (ISR4331). The **192.168.2.0/24 network** contains a DHCP server connected to the router. The router interfaces act as gateways for both networks, and the left-side subnet requires DHCP relay to obtain IP addresses from the server located in the right-side subnet.

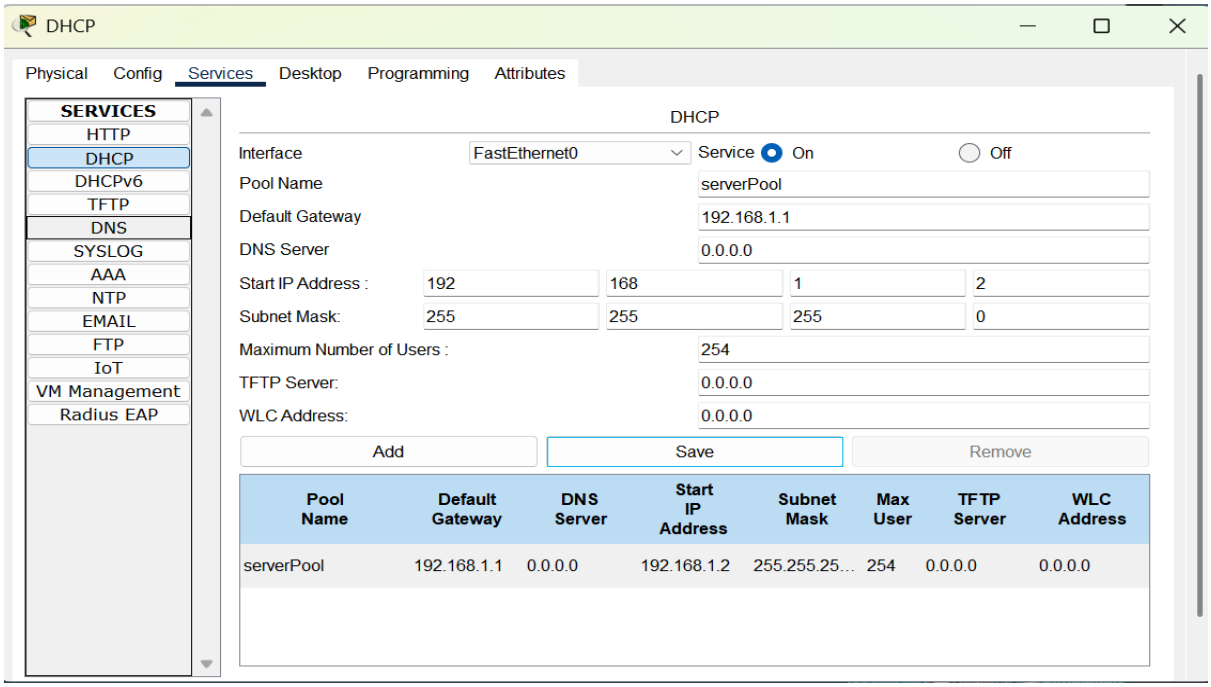

Figure 10: This screenshot displays the DHCP configuration on the server device in Packet Tracer. The server is configured with a pool named **serverPool**. The default gateway is set to 192.168.1.1, the IP range begins from 192.168.1.2, and the subnet mask is 255.255.255.0. The server assigns up to 254 clients dynamically. This ensures that PCs in the client network will obtain IP addresses automatically when requests are forwarded by the relay agent.

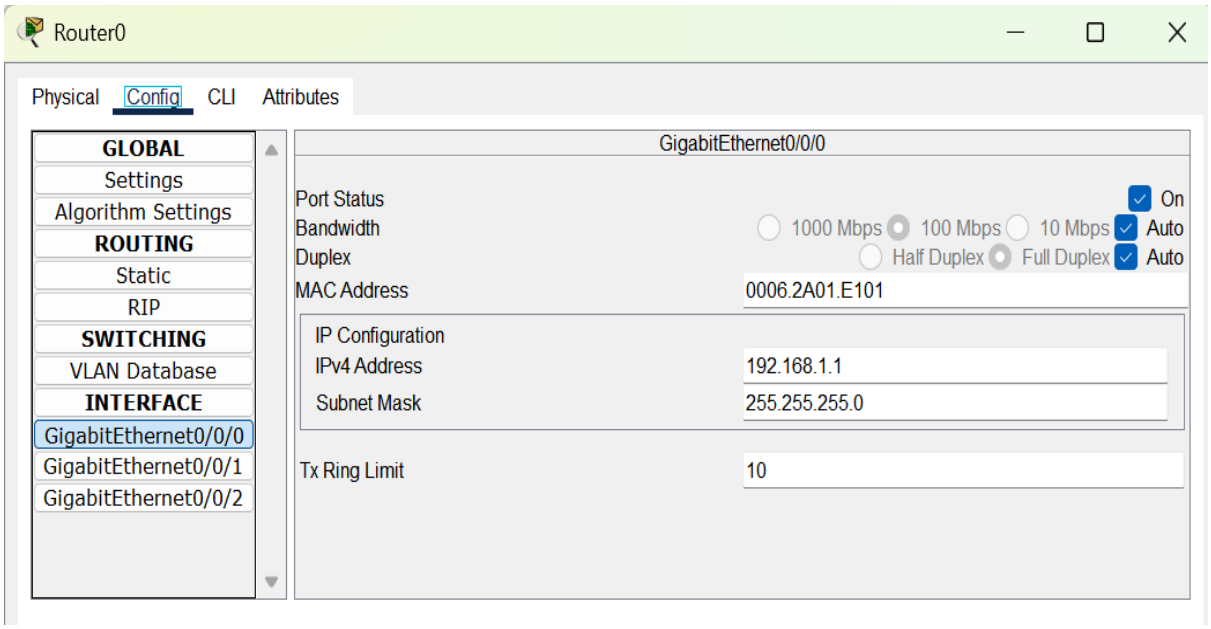

Figure 11: This image shows the configuration of **GigabitEthernet0/0/0** on the router. The interface is assigned the IP address **192.168.1.1/24**. This acts as the **default gateway** for the client PCs in the 192.168.1.0 network. The interface is turned on, allowing it to receive DHCP Discover broadcasts from the PCs and forward them using the helper-address.

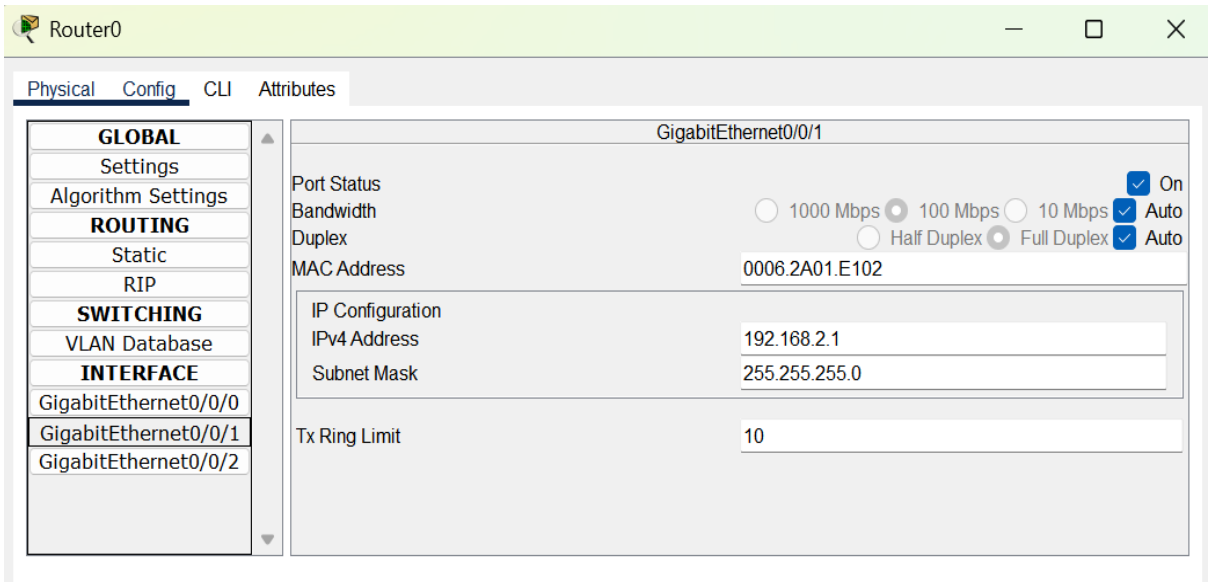

Figure 12: This screenshot shows the router's second interface, **GigabitEthernet0/0/1**, which is configured with IP address **192.168.2.1/24**. This interface connects the router to the DHCP server's network. It is responsible for forwarding client requests to the DHCP server and returning DHCP offers back to the client subnet.

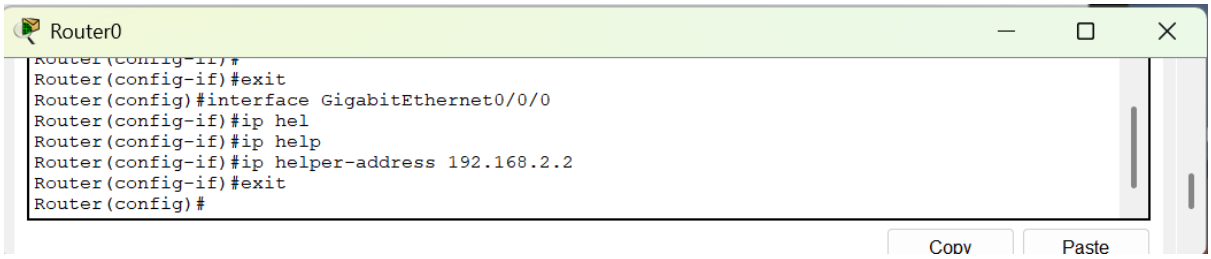

Figure 13: This image shows the CLI commands entered on the router. On interface G0/0/0, the command ip helper-address 192.168.2.2 has been configured. This command enables the router to act as a DHCP relay, forwarding broadcast DHCP Discover messages from the client PCs to the DHCP server at 192.168.2.2. Without this configuration, clients in a different subnet would not be able to receive IP addresses.

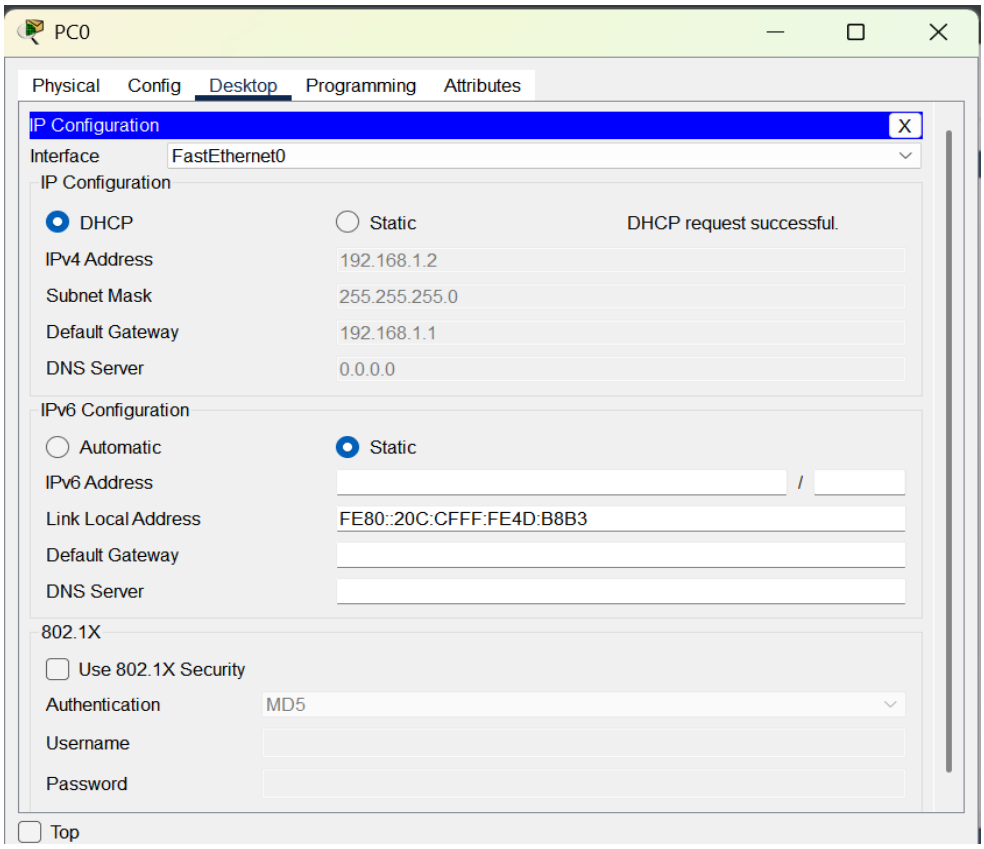

Figure 14: This screenshot shows the IP configuration of a client PC (PC0). The client is set to **DHCP mode**, and it has successfully received an IP address **192.168.1.2**, with subnet mask **255.255.255.0** and default gateway **192.168.1.1**. The status message confirms **"DHCP request successful"**, proving that the DHCP relay is functioning correctly and the server in another subnet has assigned the address dynamically.

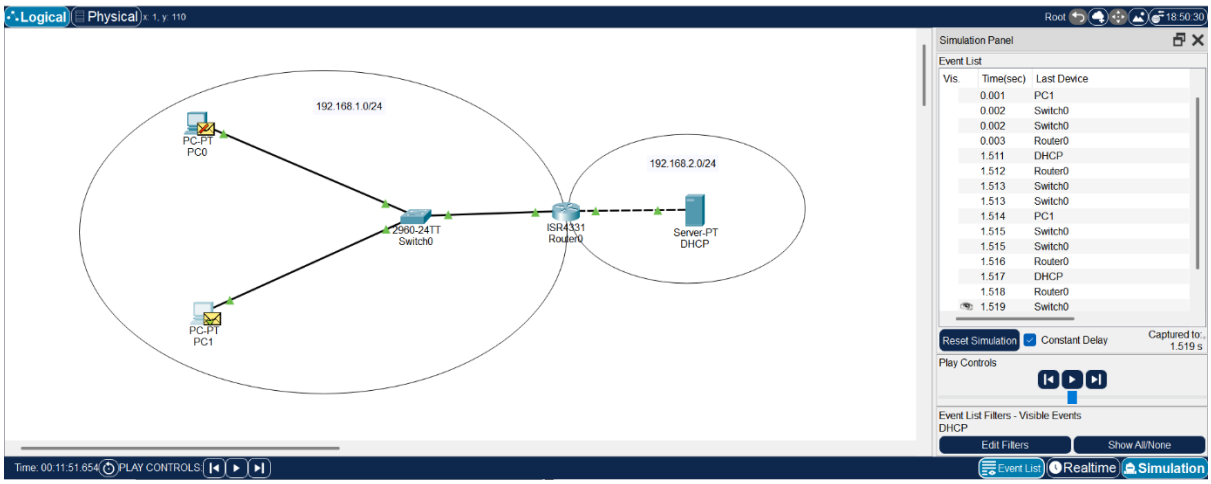

Figure 15: This screenshot shows the Cisco Packet Tracer simulation in action. The topology is displayed on the left, while the "Event List" on the right shows the flow of DHCP packets. The list details the journey of the request from the client PC, through the switch, being relayed by the router to the DHCP server, and the subsequent reply journey back to the client.

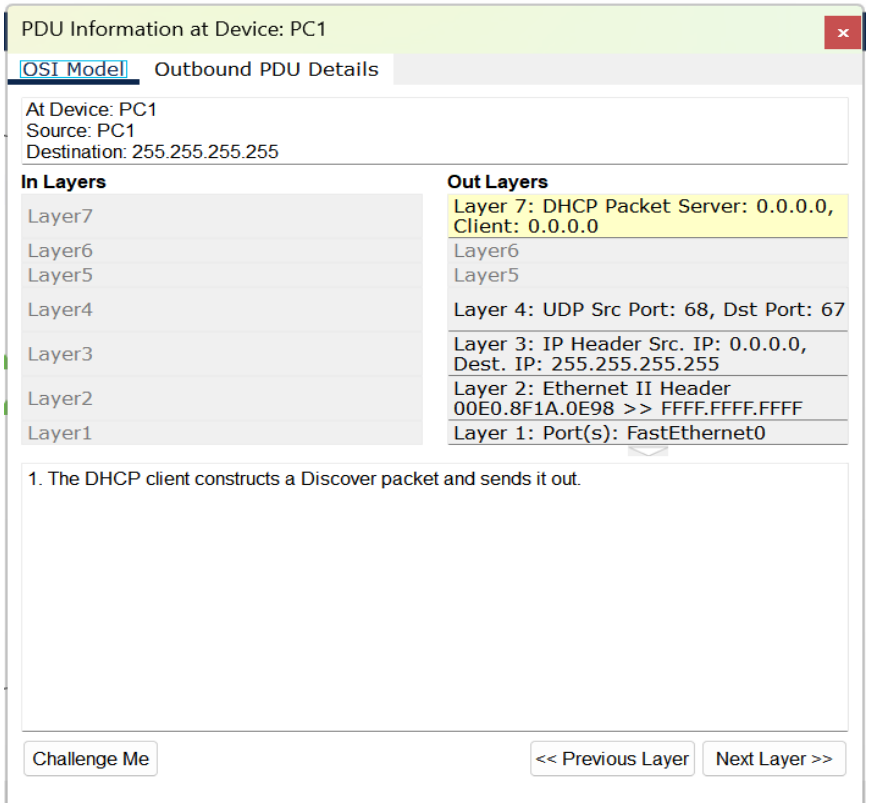

Figure 16: This image shows the PDU (Protocol Data Unit) details for the initial DHCP Discover packet sent from client PC1. It breaks down the packet by OSI model layers, showing the Layer 3 source IP as 0.0.0.0 and the destination as the broadcast address 255.255.255.255. The Layer 4 details confirm the use of UDP source port 68 and destination port 67. This view captures the packet from the client's perspective before it is processed by the DHCP relay agent.

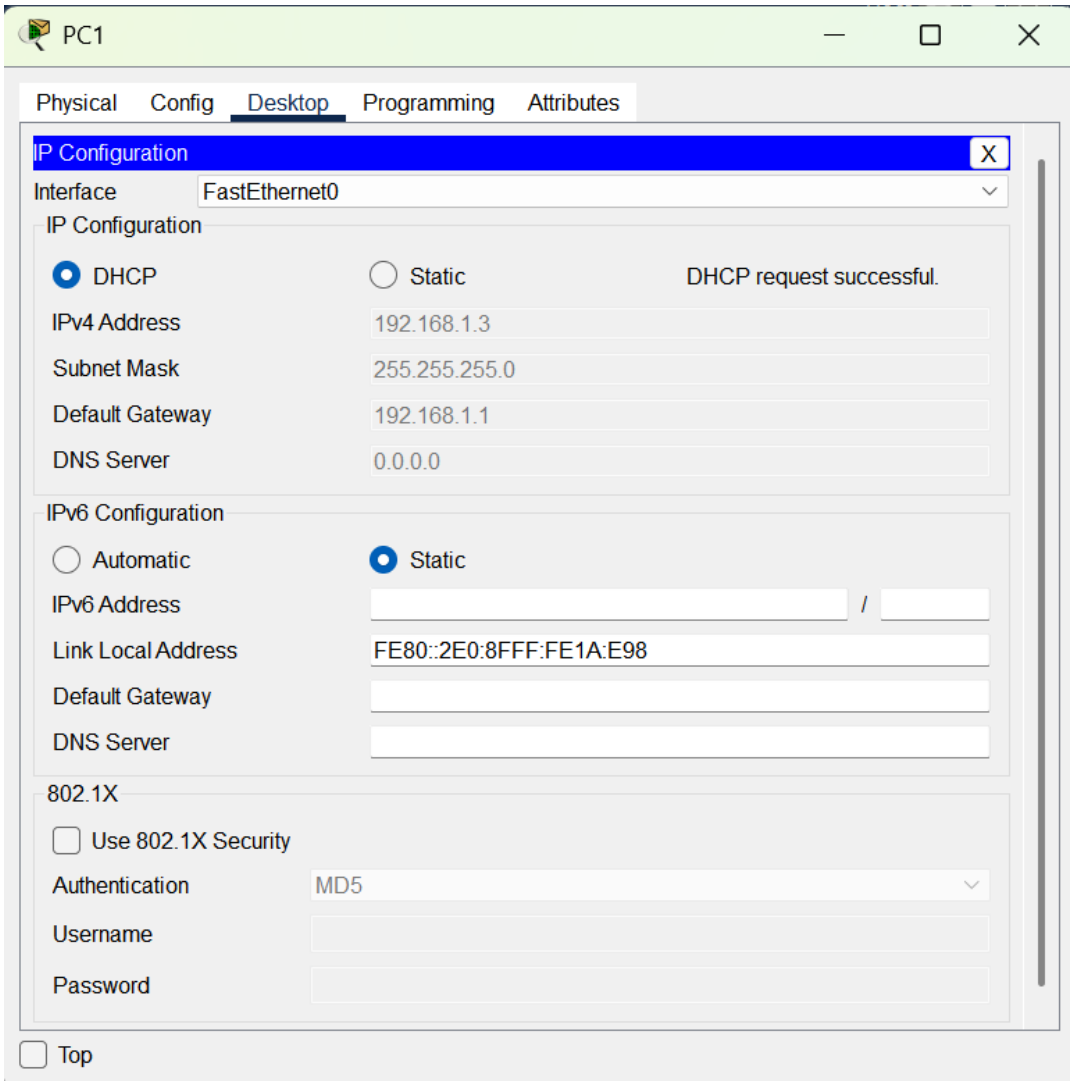

Figure 17: This screenshot shows the IP configuration window for client PC1. It confirms a successful DHCP request, as the PC has been assigned the IPv4 address 192.168.1.3 and the correct default gateway address 192.168.1.1. This demonstrates that the DHCP server can lease multiple addresses across the routed network.

SETUP

The network consists of two distinct broadcast domains connected by a router (Router0), as illustrated in the topology diagram:

- **Client Network (192.168.1.0/24):** Contains two client PCs (PC0, PC1) and a switch (Switch0).
- **Server Network (192.168.2.0/24):** Contains the DHCP server (Server-PT).

The router (ISR4331 Router0) serves as the gateway between these two networks.

Configuration Steps

1. Router Interface Configuration The router's interfaces were configured with static IP addresses to act as the default gateway for each network:

- **GigabitEthernet0/0/0 (Client Side):** IP address **192.168.1.1** with subnet mask 255.255.255.0.
- **GigabitEthernet0/0/1 (Server Side):** IP address **192.168.2.1** with subnet mask 255.255.255.0.

2. DHCP Relay Agent Configuration: The crucial step was to configure the router to forward DHCP broadcast messages from the client network to the DHCP server. This was done using the Command Line Interface (CLI) on the router's client-facing interface (GigabitEthernet0/0/0) with the following command:

- ip helper-address 192.168.2.2 This command tells the router to take any DHCP broadcast requests received on this interface and forward them as unicast packets to the DHCP server at 192.168.2.2.

3. DHCP Server Configuration: The DHCP server (with a static IP of 192.168.2.2) was configured to provide addresses for the client network (192.168.1.0/24):

- **Service:** Turned **On**.
- **Default Gateway:** Set to **192.168.1.1** (the router's client-side interface). This is essential for clients to be able to communicate beyond their local network.
- **Start IP Address:** 192.168.1.2.

Verification and Results

The configuration was successful. Analysis of the initial **DHCP Discover** packet sent by PC1 showed that the client sends a broadcast packet with a destination IP of 255.255.255.255, which is then intercepted and relayed by the router.

The client PCs on the 192.168.1.0/24 network were able to obtain IP addresses from the server on the 192.168.2.0/24 network.

- **PC0** received the IP address **192.168.1.2** and the default gateway **192.168.1.1**.
- **PC1** received the IP address **192.168.1.3** and the default gateway **192.168.1.1**.

The simulation event list confirms that the DHCP packets were successfully relayed by Router0 between the client and server networks.

Answers to Questions

1. **What is the destination IP address before relay (client's perspective)?**

   Ans: From the client's perspective, it does not know the location of the DHCP server, so it sends a broadcast message. The destination IP address is **255.255.255.255**. This is explicitly confirmed in the PDU details screenshot for the outbound packet from PC1.

2. **What does the router change as it forwards the packet to the DHCP server?**

   Ans: The router changes the packet from a broadcast to a unicast. It modifies the **source IP address** to its own (192.168.1.1) and the **destination IP address** to the DHCP server's IP (192.168.2.2), which was specified in the ip helper-address command.

3. **What is the client's UDP source port during the first request?**

   Ans: The client's UDP source port remains **68** (bootpc).

4. **Which UDP port does the DHCP server listen on?**

   Ans: The DHCP server still listens on UDP port **67** (bootps). The relay agent does not alter the port numbers.

Part C: No DHCP Server Available

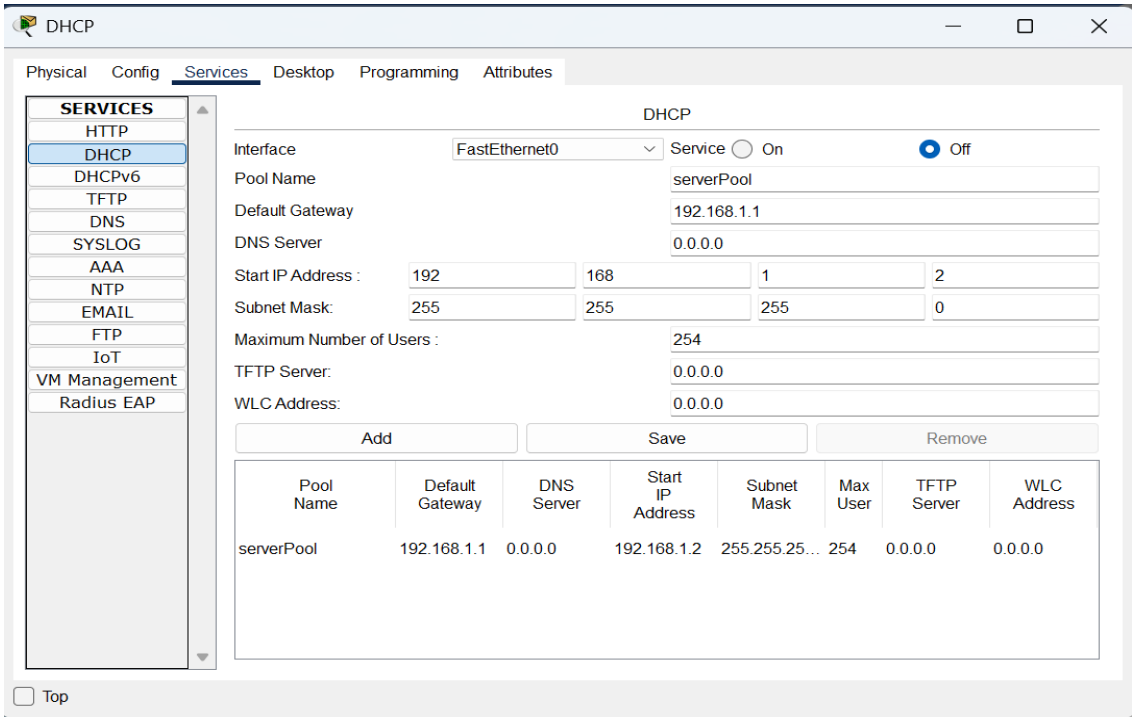

Figure 18: This screenshot shows the DHCP service configuration window on the server in Cisco Packet Tracer. The key detail in this image is that the DHCP service has been explicitly disabled, with the "**Off**" radio button selected. This action is the basis for the experiment in Part C, simulating an environment where no DHCP server is available to respond to client requests for IP addresses.

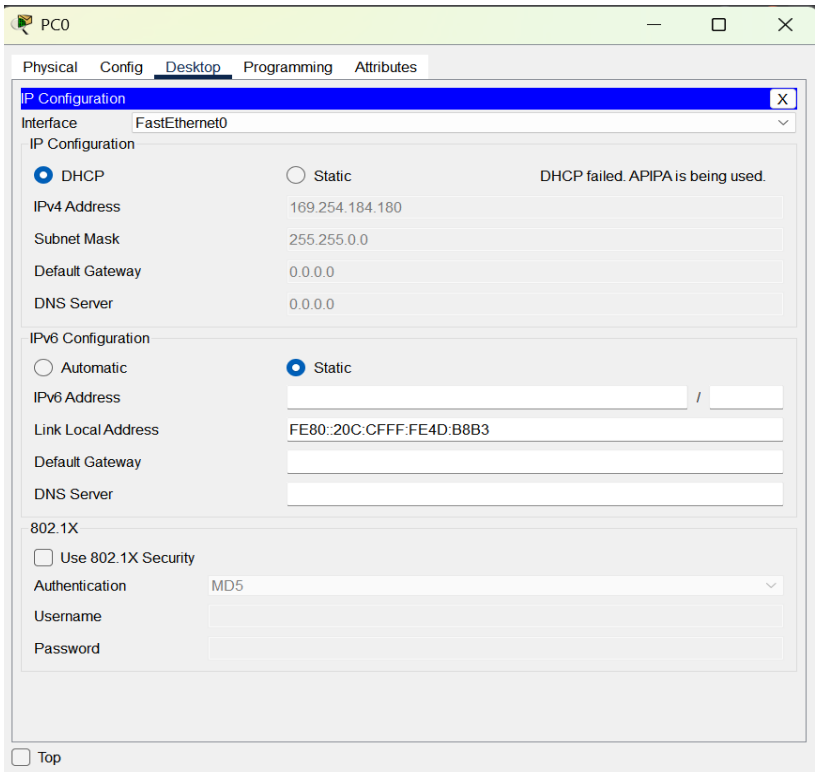

Figure 19: This image displays the IP Configuration window for client PC0. It clearly indicates that the DHCP request has failed. As a result, the PC has automatically assigned itself an APIPA address of 169.254.184.180 with a subnet mask of 255.255.0.0. This demonstrates the default fallback behaviour of a device unable to lease an address from a DHCP server.

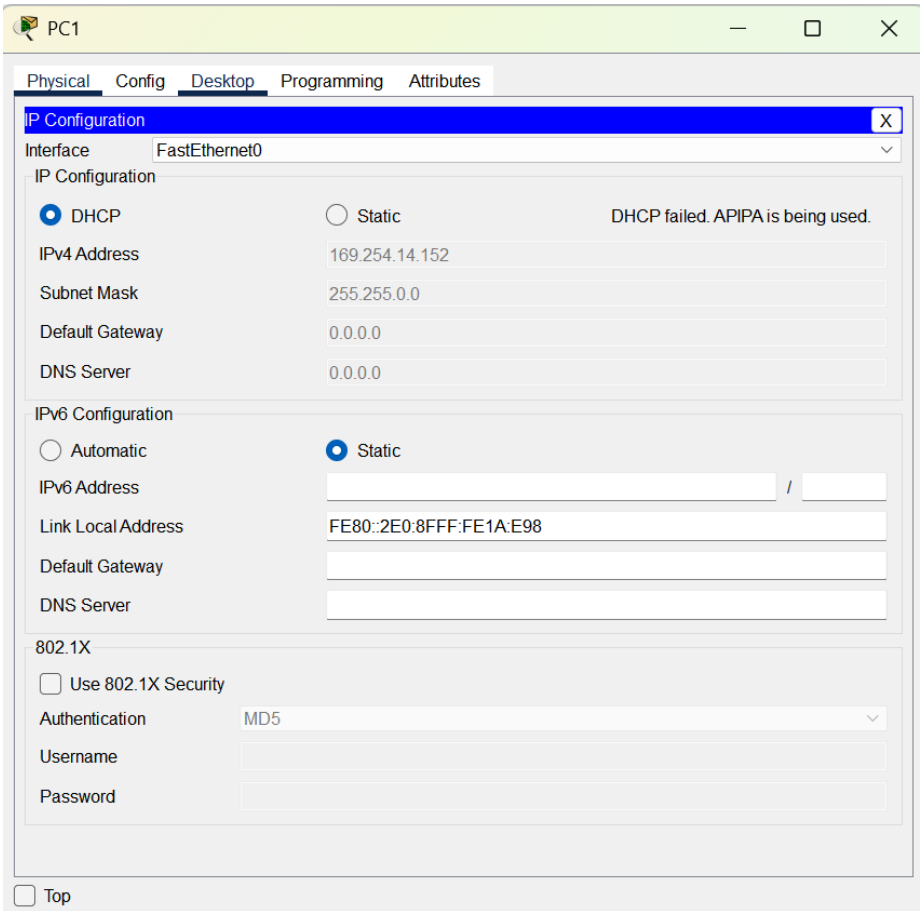

Figure 20: This screenshot shows the IP configuration details for client PC1. Similar to PC0, it displays the message "DHCP failed. APIPA is being used." The PC has self-assigned the IP address 169.254.14.152, which is within the designated APIPA range. This result further confirms the expected outcome when a DHCP server is unreachable on the network.

SETUP

For this part of the experiment, the network topology remained the same, but a critical change was made on the server. The **DHCP service was manually turned off**, as shown in the configuration screenshot. This simulates a scenario where a DHCP server is offline or does not exist on the network.

The client PCs (PC0 and PC1) were then set to obtain their IP addresses via DHCP. As expected, the requests failed because no server responded. The results were as follows:

- Both PC0 and PC1 displayed the message: "**DHCP failed. APIPA is being used.**"
- The operating system on each PC then automatically assigned itself an **APIPA (Automatic Private IP Addressing)** address:
    - **PC0** received the IP address: **169.254.184.180**

  - **PC1** received the IP address: **169.254.14.152**

- Both PCs received a subnet mask of **255.255.0.0**, which is standard for APIPA. No Default Gateway or DNS Server addresses were assigned.

This confirms the expected fallback mechanism in the absence of a DHCP server.

Answers to Questions

1. **What IP address does the PC get when there is no DHCP server available? (In CISCO Packet Tracer)**

   Ans: When a PC cannot find a DHCP server, it assigns itself an **APIPA (Automatic Private IP Addressing)** address. These addresses are in the reserved range of **169.254.0.1** to **169.254.255.254**. In this experiment, PC0 got 169.254.184.180 and PC1 got 169.254.14.152, which are both valid APIPA addresses.

Conclusion

This practical successfully demonstrated the configuration, operation, and importance of the Dynamic Host Configuration Protocol (DHCP) in various network scenarios. Through a series of three distinct parts, the fundamental principles of automatic IP address allocation were explored and verified using Cisco Packet Tracer.

In **Part A**, a DHCP server was successfully configured to serve clients within the same local area network. This established the foundational DORA (Discover, Offer, Request, Acknowledge) process, proving how DHCP simplifies network administration by automating IP assignment and eliminating manual configuration errors.

In **Part B**, the experiment was scaled to a multi-network environment. By configuring a router as a DHCP Relay Agent using the ip helper-address command, it was proven that DHCP services can be centralized. This showed how a single server can manage IP allocation for multiple, separate subnets, a critical concept for efficient and scalable network design in larger organizations.

Finally, **Part C** investigated the network's behaviour in the absence of a DHCP server. It was observed that client devices, upon failing to contact a server, automatically assigned themselves an APIPA (Automatic Private IP Addressing) address from the 169.254.0.0/16 range. This demonstrated the built-in resiliency that allows for limited, local-link communication even when the primary IP allocation service fails.