EXPERIMENT: 15

CONFIGURATION OF DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) IN PACKET TRACER

Aim: To configure DHCP (dynamic host configuration protocol) in packet tracer.

Software/Apparatus required: Packet Tracer/End devices, Hubs, connectors.

Algorithm:

1.   Start:

•   Set up the network topology in Packet Tracer with a DHCP server and DHCP clients connected to a switch.

2.   Configure the DHCP server:

•   Assign an IP address to the server interface.

•   Enable the DHCP service on the server.

•   Define the IP address pool range that the server can assign to clients.

•   Specify additional DHCP options like default gateway, DNS server, and subnet mask.

3.   Configure the switch.

•   Enable the switch interfaces that connect to the DHCP clients.

4.   Configure the DHCP clients.

•   Configure the clients to obtain their IP addresses automatically using DHCP.

•   Verify that the clients are set to use DHCP as the preferred method for IP assignment.

5.   Client request and server response:

•   When a DHCP client boots up or its lease expires, it sends a DHCP discover message as a broadcast on the local network.

•   The DHCP server receives the discover message and responds with a DHCP offer message containing an available IP address from the configured IP address pool.

•   The server includes other network configuration parameters in the offer message.

6.   Client selection and request:

•   The client receives multiple offer messages from different DHCP servers if available.

•   The client selects one offer and sends a DHCP request message to the chosen server, requesting the offered IP address and confirming other network parameters.

7.   Server acknowledgement:

•   The DHCP server receives the request message and sends a DHCP acknowledge (ACK) message to the client, confirming the IP address assignment and providing additional network

configuration details.

8.	Client configuration:

•	The client receives the ACK message and configures its network interface with the assigned IP address, subnet mask, default gateway, DNS server, and any other parameters provided by the DHCP server.

9.	Lease renewal and expiration:

•	The client periodically contacts the DHCP server to renew its lease before it expires.

•	If the client doesn't renew the lease or is unable to contact the DHCP server, the IP address lease eventually expires, and the IP address returns to the pool for future assignment.

10.	End:

Procedure:

1.	Launch Cisco Packet Tracer and create a new network topology or open an existing one.

2.	Add the necessary network devices to your topology, including a DHCP server, switch, and DHCP clients. Connect them using appropriate cables.

3.	Configure the DHCP server:

•	Select the DHCP server device and open its configuration panel.

•	Assign an IP address to the server interface connected to the switch.

•	Enable the DHCP service on the server by checking the "DHCP" option.

•	Define the IP address pool range that the server can assign to clients. Specify the starting and ending IP addresses.

•	Optionally, set other DHCP options like default gateway, DNS server, and subnet mask.

•	Save the configuration.

4.	Configure the switch:

•	Select the switch device and open its configuration panel.

•	Enable the interfaces that connect to the DHCP clients. This allows the clients to communicate with the DHCP server.

•	Save the configuration.

5.	Configure the DHCP clients:

•	Select each DHCP client device and open its configuration panel.

•	Set the IP address assignment method to "DHCP" or "Obtain an IP address automatically."

•	Save the configuration for each client.

6.	Start the simulation:

•	Click the "Start/Stop Simulation" button to start the simulation.

7.	Verify DHCP operation:

- Wait for the DHCP clients to boot up or refresh their IP configurations.

- Check if the DHCP clients receive IP addresses from the DHCP server.

- Verify that the clients have the correct IP address, subnet mask, default gateway, and DNS server settings.
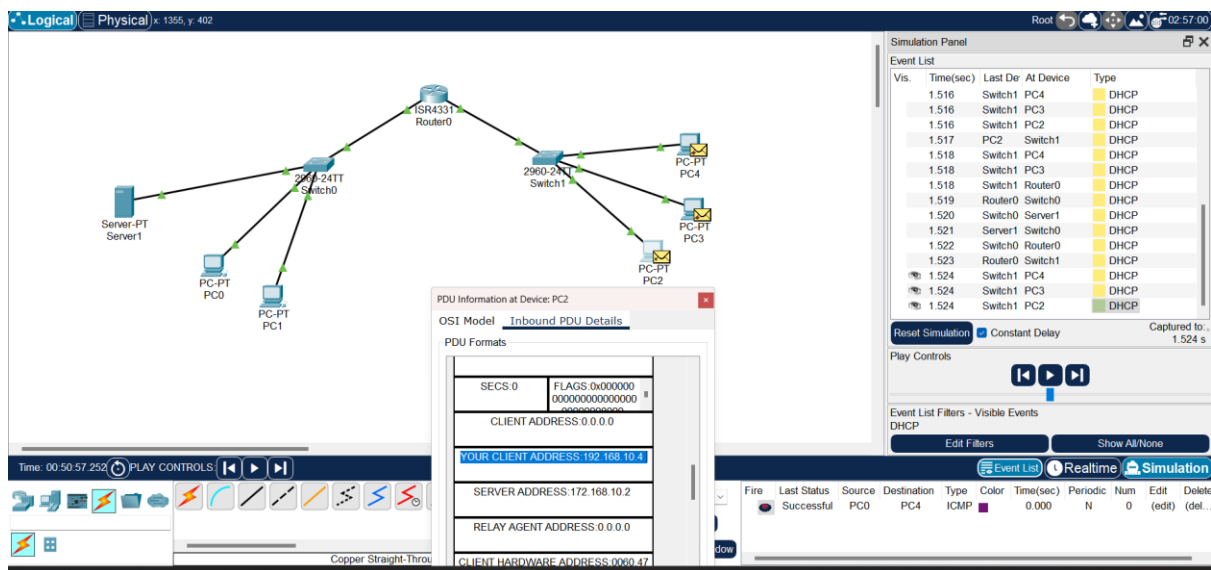
Result: Therefore the configuration for DHCP has been successfully executed using packet tracer.