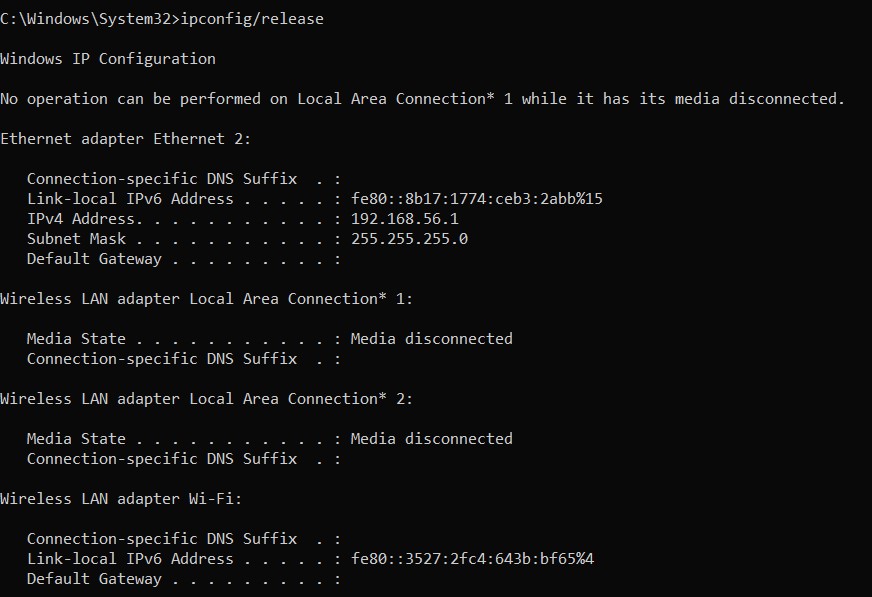
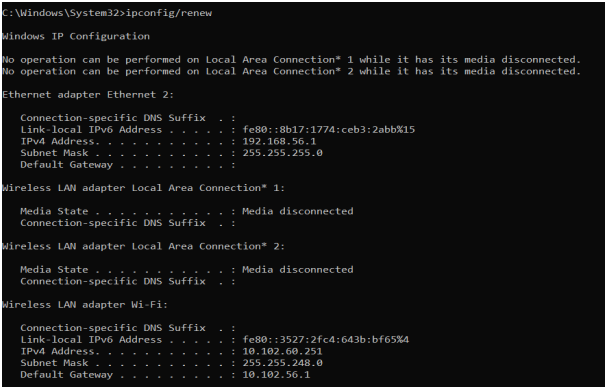
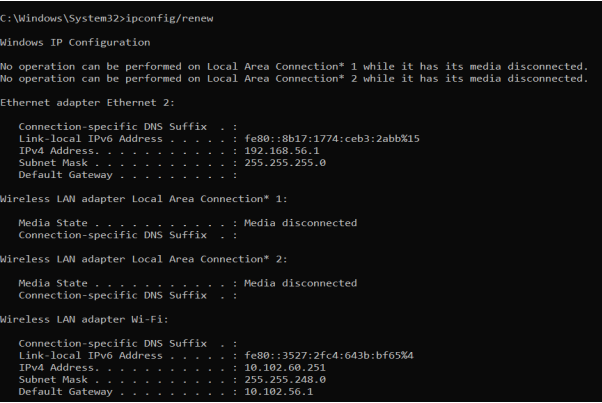
Wireshark Lab: DHCP

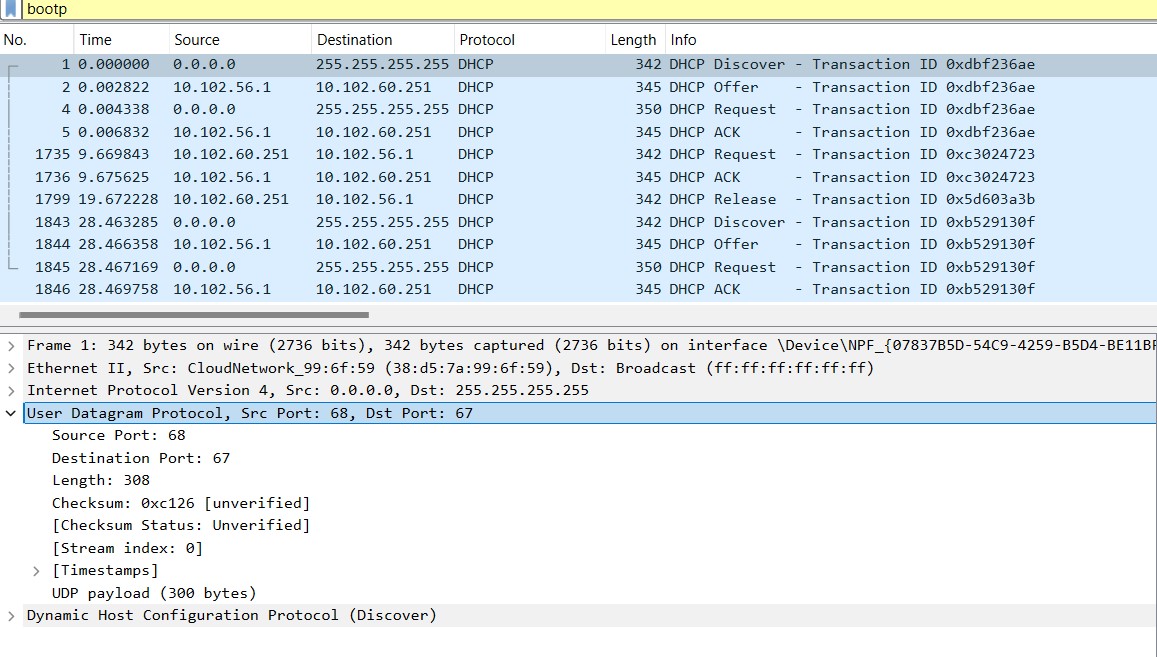
Anushttha Srivastava

Roll no: 22/11/EC/024





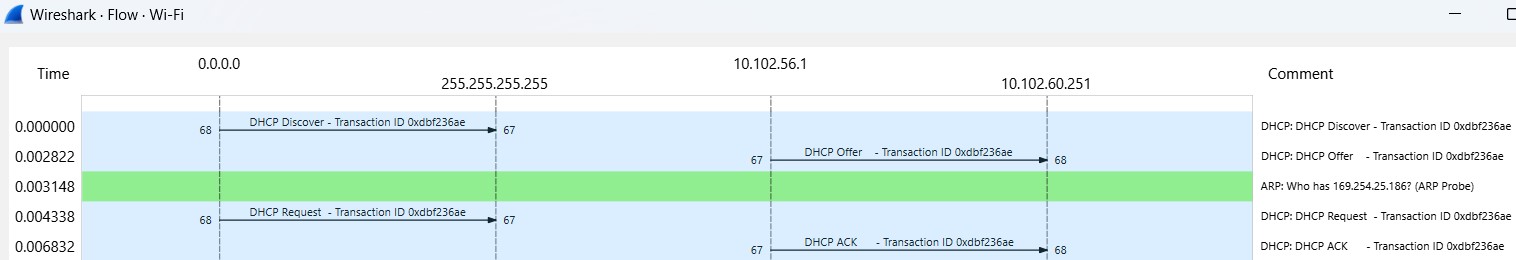




1. Are DHCP messages sent over UDP or TCP? DHCP messages are sent over the User Datagram Protocol(UDP).

**Ans: They are sent over UDP.**

1. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicate the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?



**Ans: DHCP Discover: Source Port = 68 Destination Port = 67**

**DHCP Offer: Source Port = 67 Destination Port = 68**

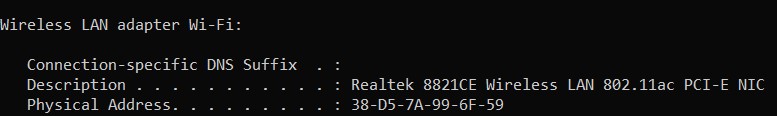
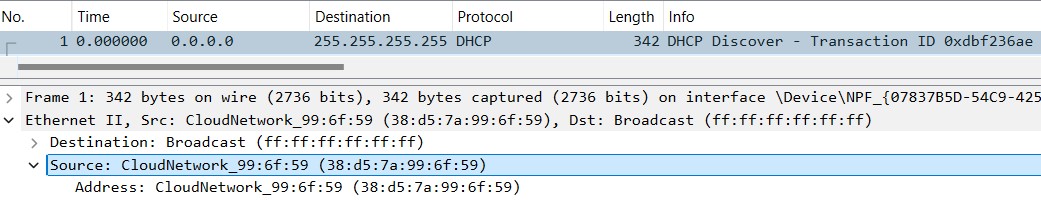
**DHCP Request:Source Port = 68 Destination Port = 67**

**DHCP ACK:Source Port = 67 Destination Port = 68**

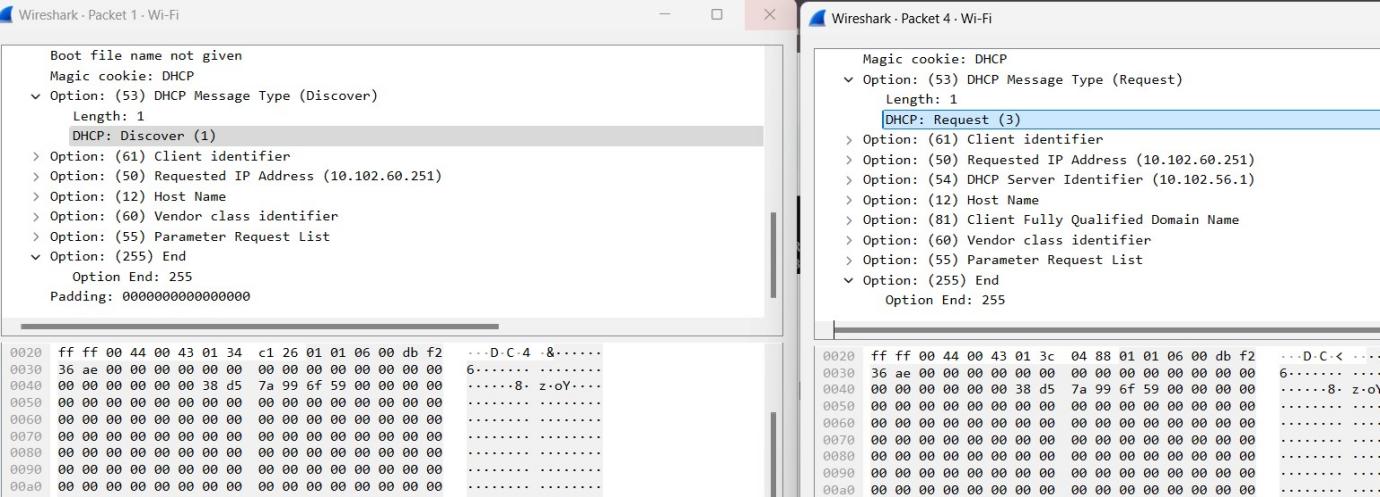
**Yes, the port numbers are the same as in the example given in this lab assignment.**

1. What is the link-layer (e.g., Ethernet) address of your host?

Ans: The link-layer address of the host is - 38:d5:7a:99:6f:59



1. What values in the DHCP discover message differentiate this message from the DHCP request message?

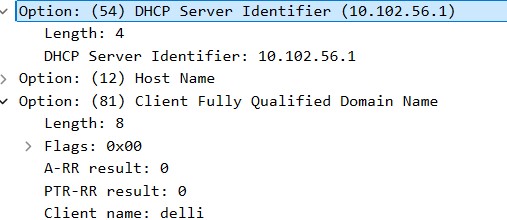


**Ans: In the DHCP Discover packet, in the field Option: (53), the message type is set to Discover (1).**

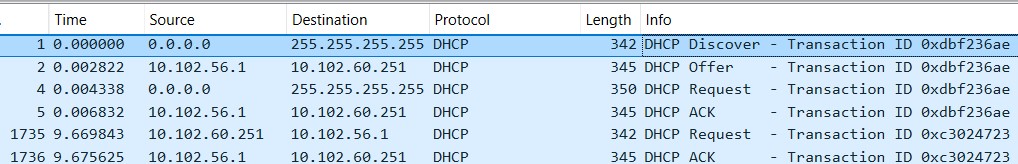
**However, in the DHCP Request packet, in the field Option: (53), the message type is set to Request (3).**

**Also, the DHCP Request packet has two extra option fields namely: Option: (54) DHCP Server Identifier**

**Option: (81) Client Fully Qualified Domain name These two fields are not present in the DHCP Discover packet.**



1. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?



**Ans: In each of the first four DHCP messages, the value of the**

**Transaction-ID is 0xdbf236ae**

**In the second set of DHCP messages, the value of the**

**Transaction-ID is 0xc3024723**

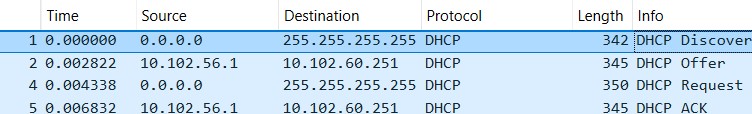
**The Transaction-ID field serves as a unique identifier in matching the requests and responses during the process of DHCP communication. When the client broadcasts a DHCP discover message, a random Transaction-ID is generated and when the DHCP server responds with a DHCP Offer or ACK or NAK, the same Transaction-ID is mentioned so that the client can identify that the response is intended for it.**

**This helps in avoiding confusion in a multi-client environment and also helps in maintaining the communication state.**

6. A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages

(Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

**Ans:**



**DHCP Discover:**

**Source IP: 0.0.0.0**

**Destination IP: 255.255.255.255 DHCP Offer:**

**Source IP: 10.102.56.1**

**Destination IP: 10.102.60.251 DHCP Request:**

**Source IP: 0.0.0.0**

**Destination IP: 255.255.255.255**

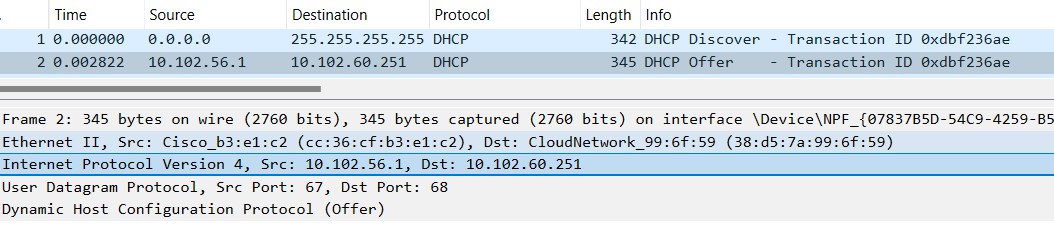
**DHCP ACK:**

**Source IP: 10.102.56.1**

**Destination IP: 10.102.60.251**

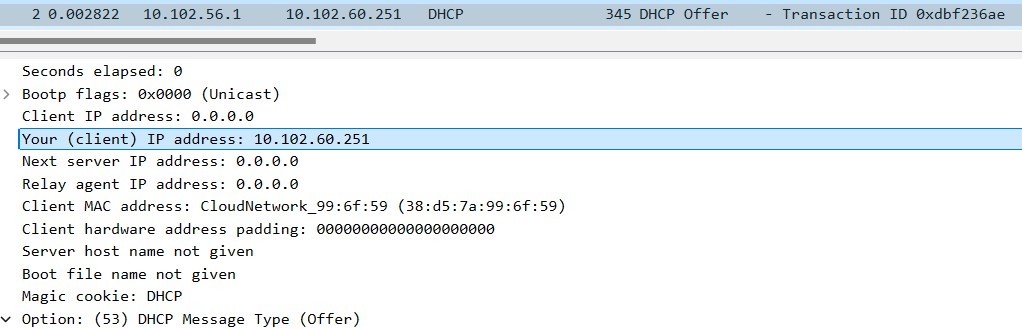
**So, until the end of the four-message exchange, the client always uses 0.0.0.0 as its source IP and broadcasts the message by using 255.255.255.255 as the** **destination IP. But the DHCP server uses its IP address as the source IP and uses that IP as the destination IP, which it is going to assign to the client.**

1. What is the IP address of your DHCP server?



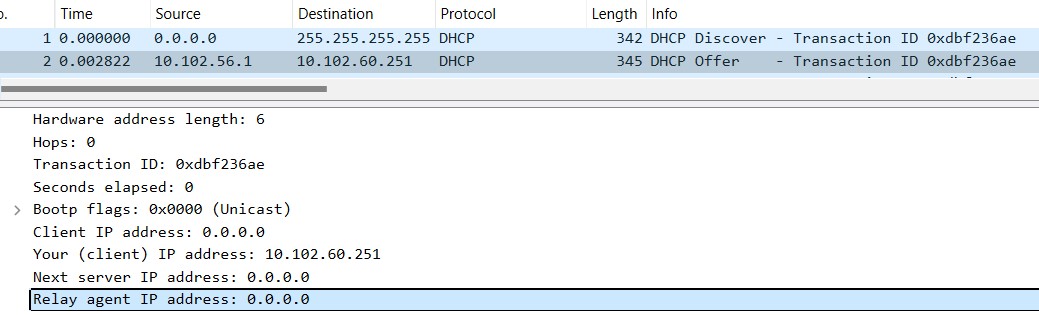
**Ans: The IP address of the DHCP server is 10.102.56.1**

1. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.



**Ans: The DHCP server offered the IP address 10.102.60.251 to the host.**

1. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so, what is the IP address of the agent?



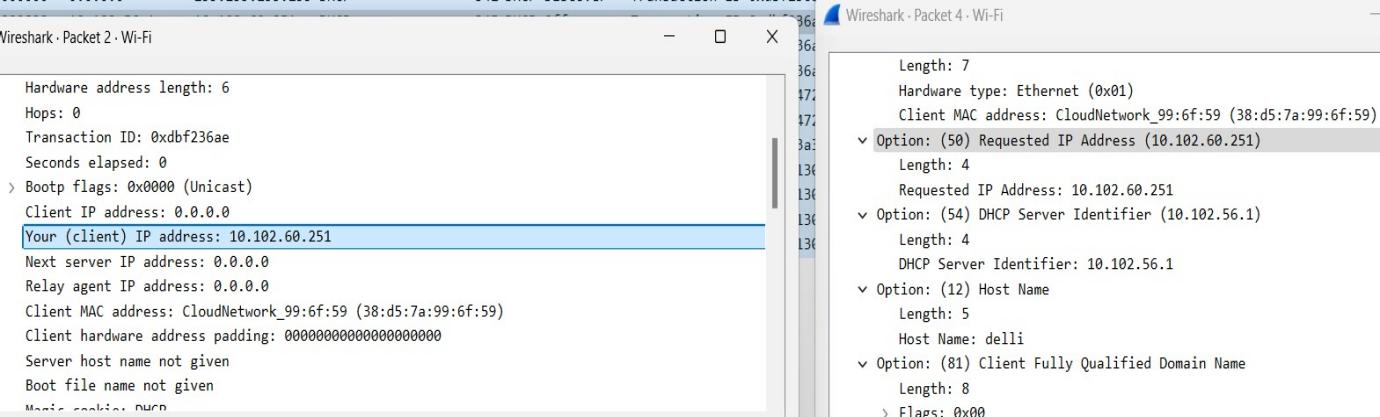
**Ans: If the relay agent IP address is 0.0.0.0, then this indicates that there is no relay agent involved in between the client and the DHCP server and both the client and the DHCP server are on the same network. When the client and the server are on different networks, then a relay agent is needed. There is no relay agent in my experiment as well.**

1. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

**Ans: The route defines the default internet gateway**

**The subnet mask defines the subnet that is available**

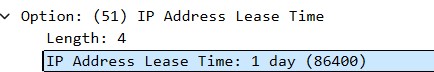
1. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client’s response to the first server OFFER message, does the client accept this IP address? Where in the client’s RESPONSE is the client’s requested address?



**Ans: The client accept the IP address given in the offer massage within the request message. After being offered the IP address 10.102.68.251 in the offer massage, my client sent back a message further requesting that specific IP address**

1. Explain the purpose of the lease time. How long is the lease time in your experiment?

**Ans: The purpose of lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one**



**The IP Address Lease time in my experiment is 1 day or 86400 seconds.**

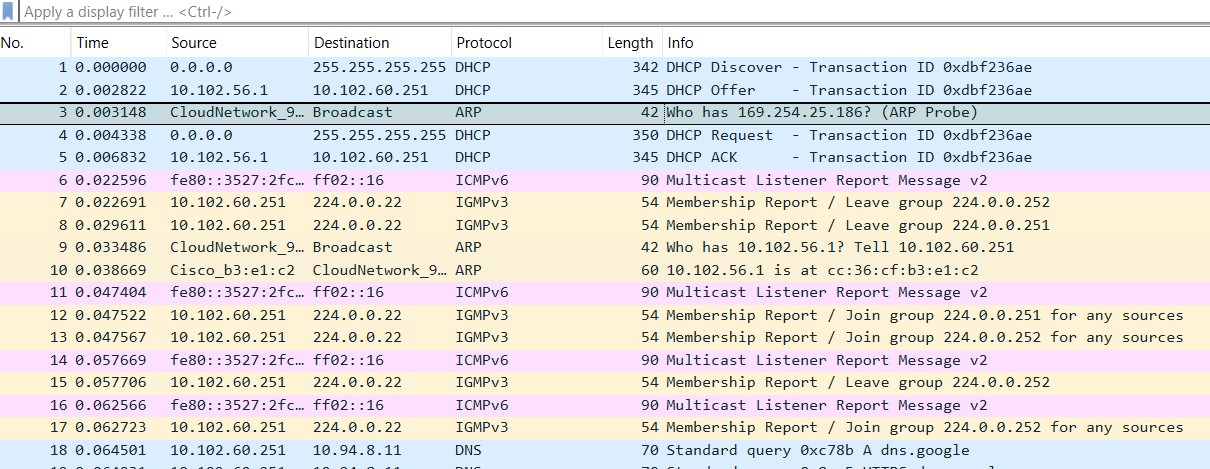
1. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

**Ans: The purpose of the release message is to release the IP address back to the serverThere is no verification that the release message has been received by the server**

**If the message is lost, the client releases the IP address, but the server will not**

**reassign that address until the client lease on the address expires**

1. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.



**Ans: Yes, ARP (Address Resolution Protocol) packets are typically observed during the DHCP packet exchange period**.