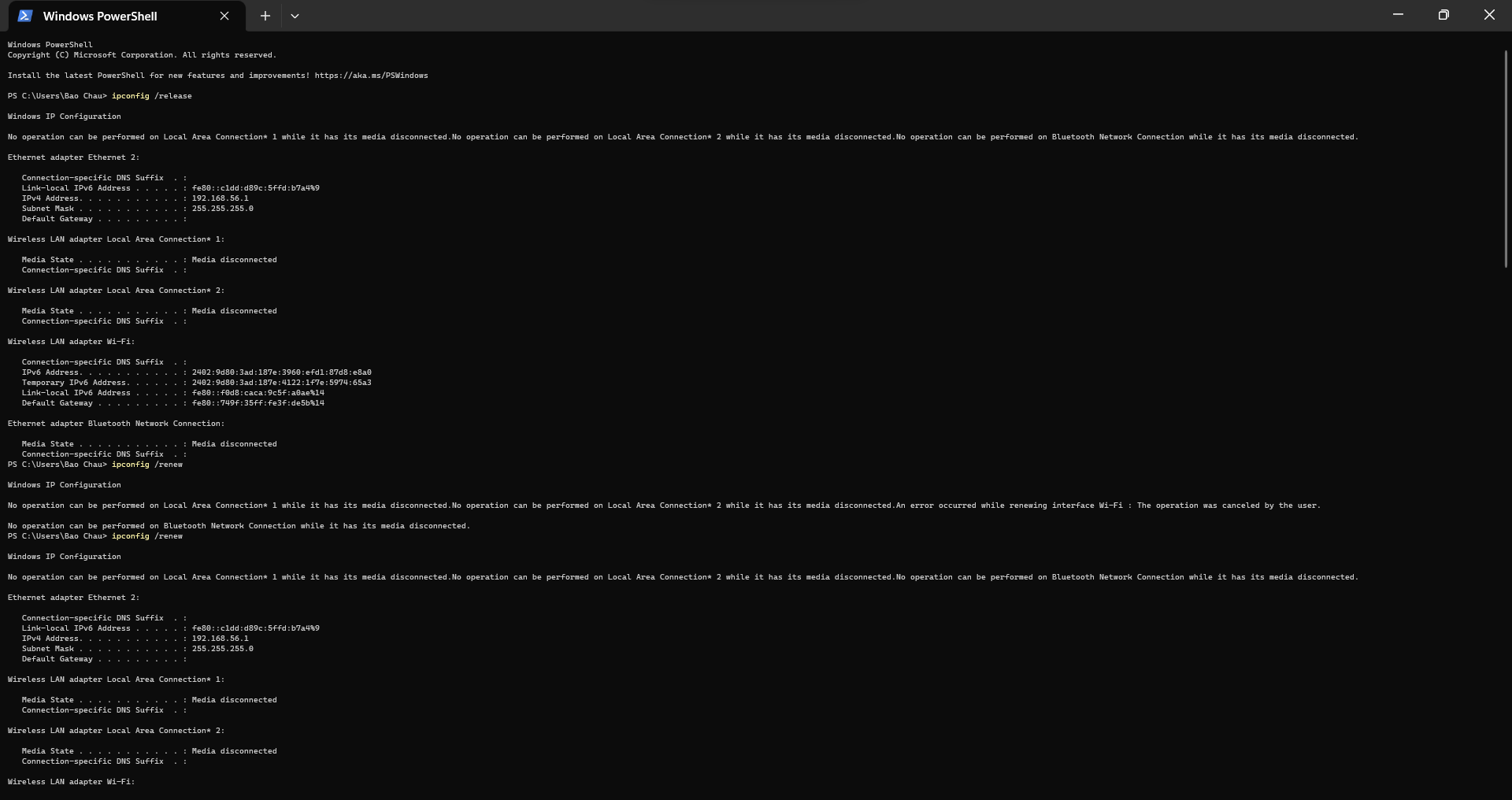
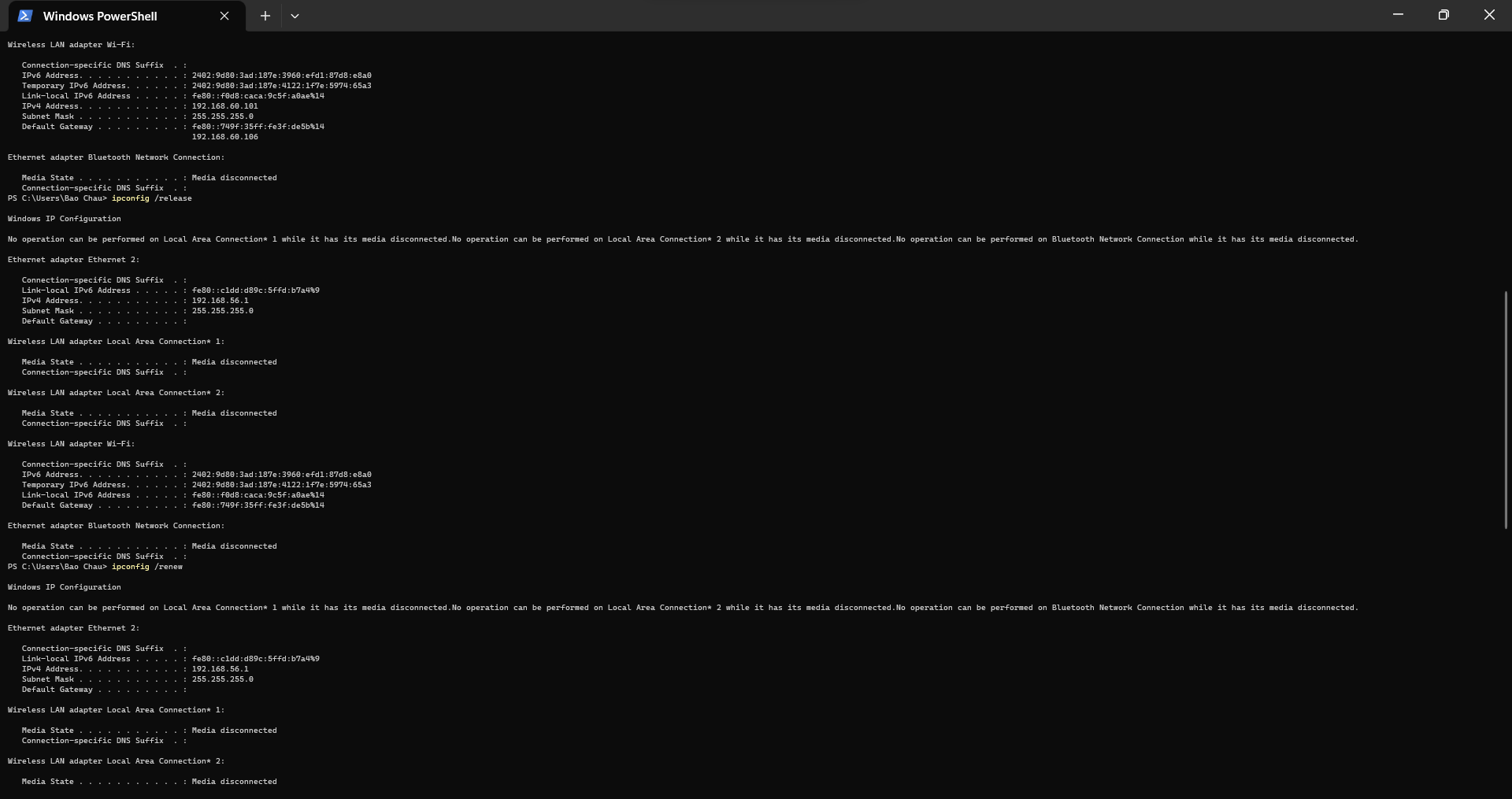
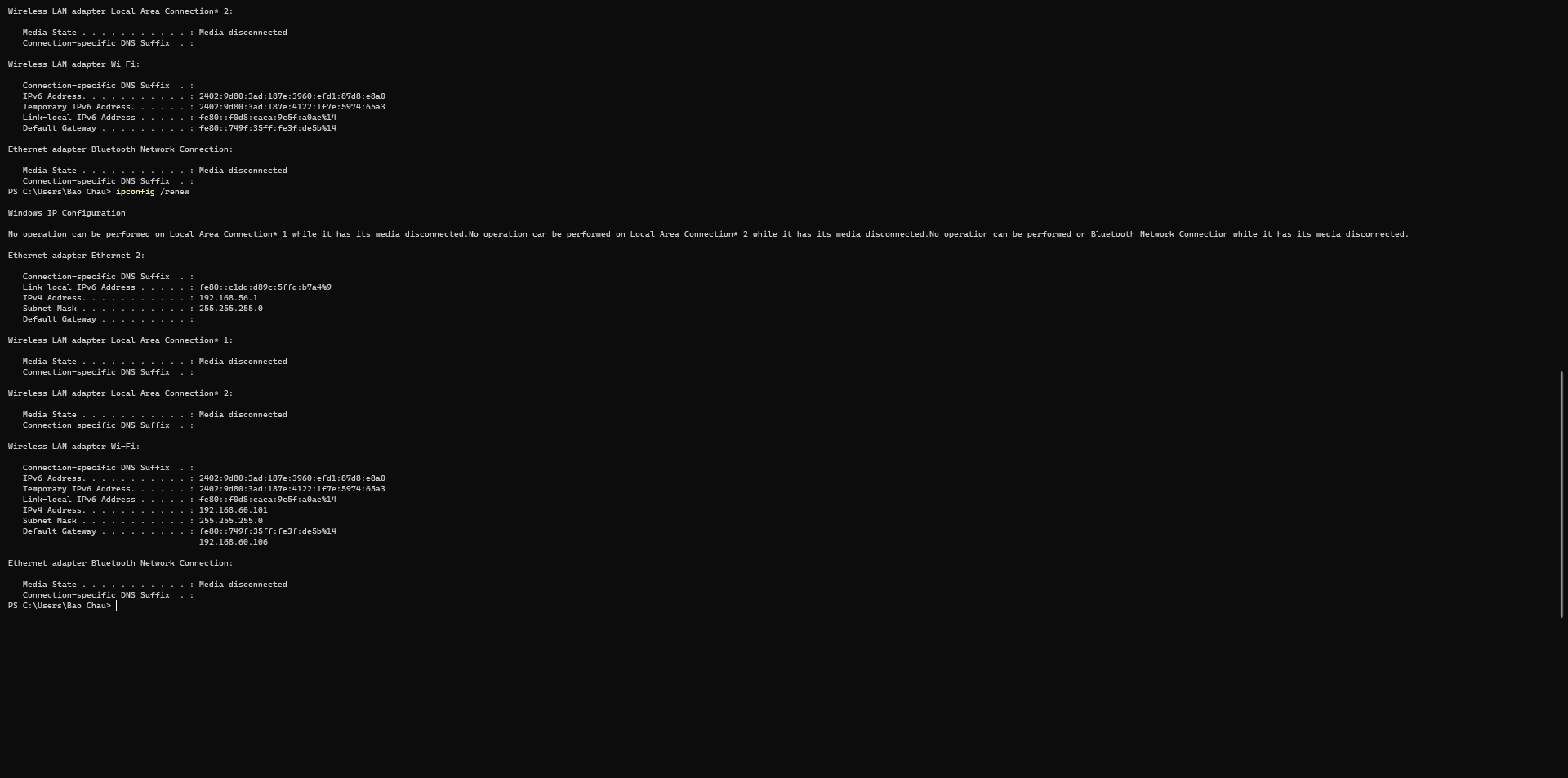
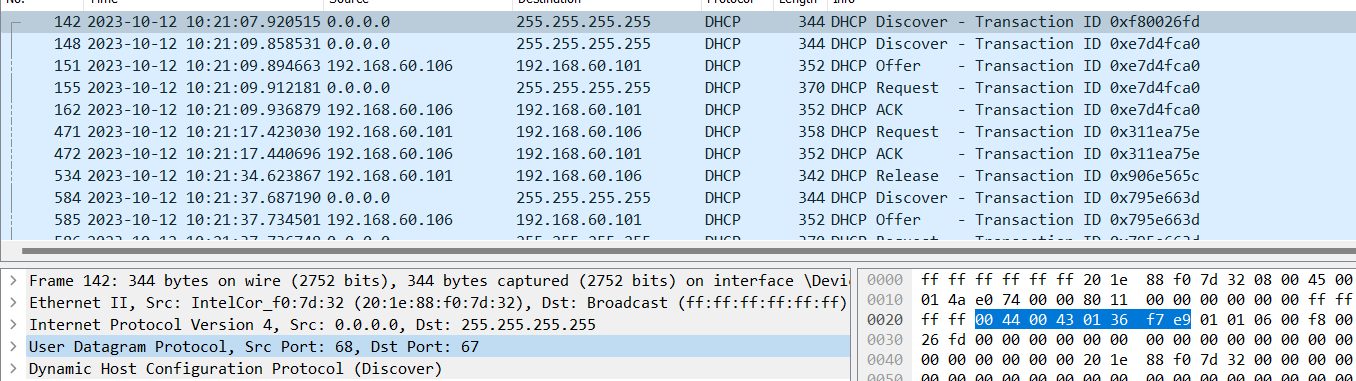
# LAB 4B Wireshark Lab: DHCP





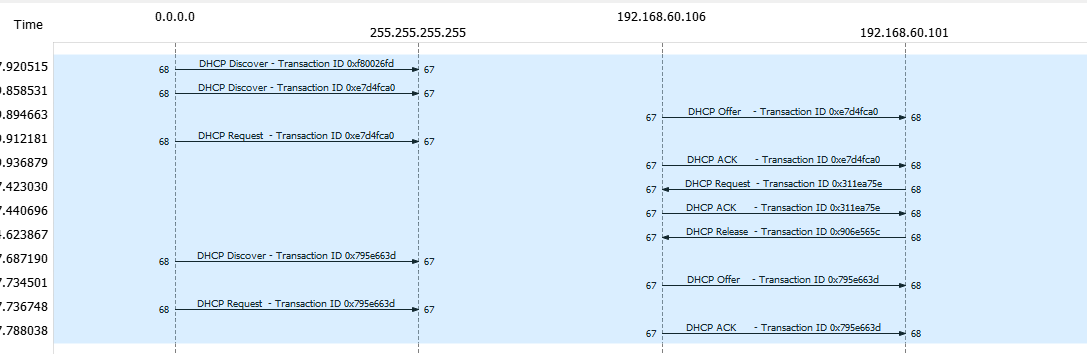


1. *Are DHCP messages sent over UDP or TCP?*



DHCP message are sent over UDP

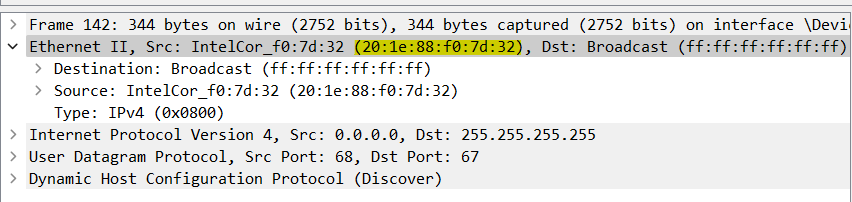
1. *Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?*



* The Discover packet has a source port of 68 and destination port of 67.
* The Offer packet has a source port of 67 and a destination port of 68.
* The Request packet has a source port of 68 and a destination of 67.
* The ACK packet has a source port of 67 and a destination of 68

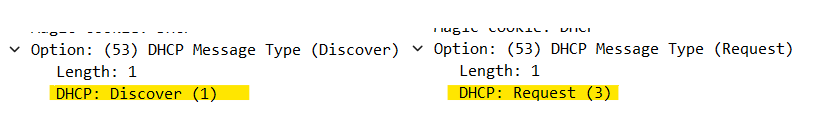
The port numbers are the same as in the example given in this lab assignment

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



The ethernet address of my host is 20:1e:88:f0:7d:32

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



The message type value for a discover message is 1, but the message type value for a request packet is 3.

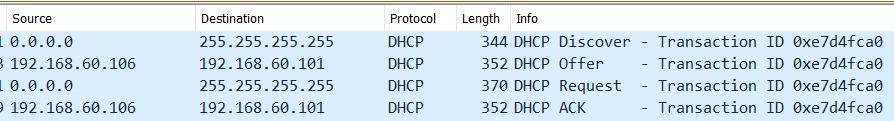
1. *What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?*



* The Transaction ID in the first four (Discover/Offer/Request/ACK) DHCP messages is 0xf80026fd, 0xe7d4fca0, 0xe7d4fca0, 0xe7d4fca0, 0xe7d4fca0.
* The transaction ID in the second set of messages is 0xe7d4fca0, 0x795e663d, 0x311ea75e, 0x311ea75e.

The purpose of the transaction ID is so that the DHCP server can differentiate between client request during the request process

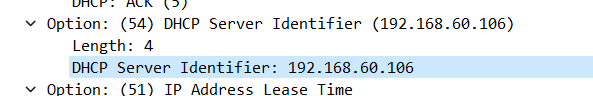
1. *A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For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



DHCP client and server both use 255.255.255.255 as destination address

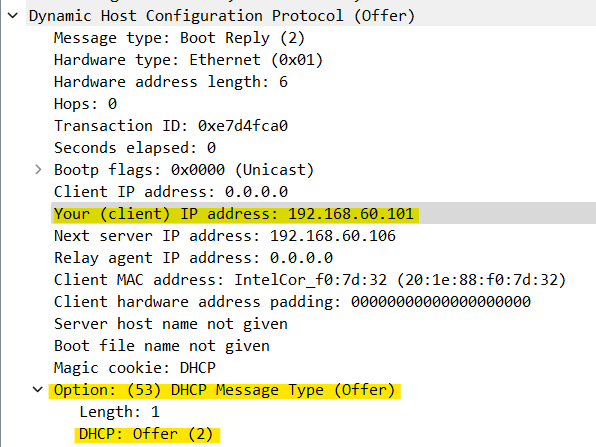
For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram in the picture above.

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



IP address of DHCP server is 192.168.60.106

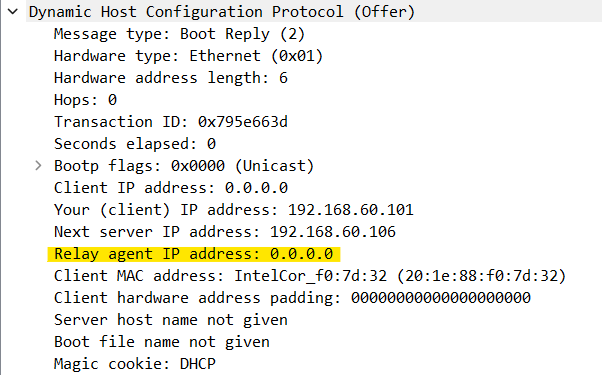
1. *What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.*



The DHCP server offered the IP address 192.168.60.101 to my client machine.

The DHCP address is offered in the DHCP offer message

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?*

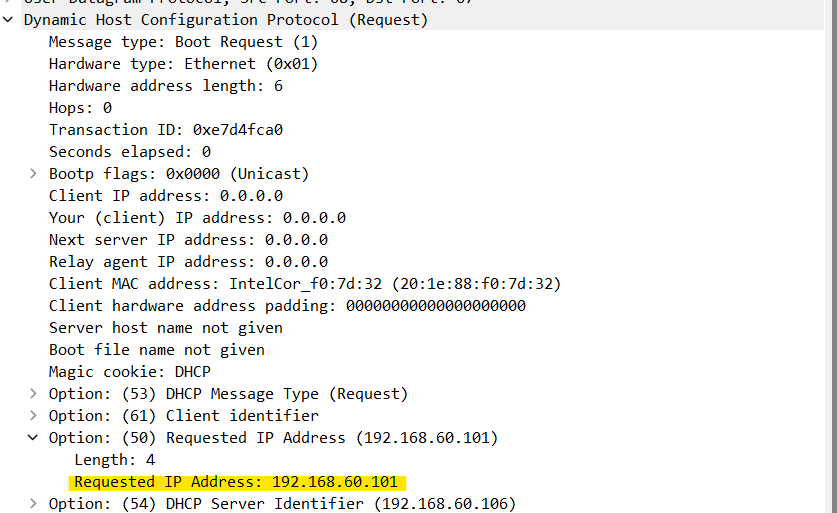


In the example given, the value that indicates there is no relay agent is 0.0.0.0. My relay agent IP address is 0.0.0.0 which indicates there is no relay agent.

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

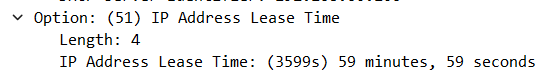
* The subnet mask line tells the client which subnet mask should use.
* The router line indicates where the client should send messages by default.

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?*



The client accepts the IP address offered by the DHCP server. The client’s response is in option 50 of the Request message

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



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. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. The lease time in my experiment is 3599 seconds or 59 minutes, 59 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?*

The client tells the DHCP server it no longer needs the IP address it was using by sending a DHCP Release message. The DHCP server doesn't respond to confirm this release. If the client's Release message gets lost, the DHCP server has to wait until the lease period expires before it can assign that IP address to another client.

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.*

Yes, the DHCP server sends out an ARP request. This happens before it gives an IP address to a client. The purpose is to check if the IP address is already being used by another workstation.