Lab04-Wireshark DHCP Lab

Following the tips, I released and renew the IP address for my PC.

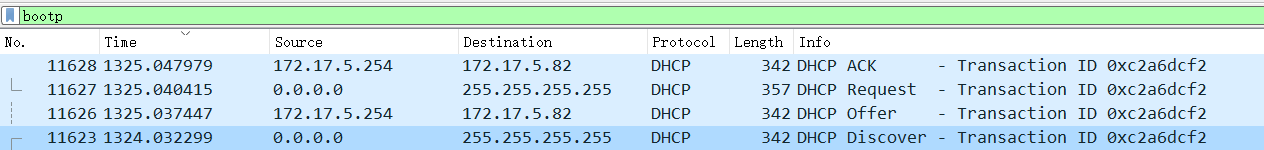


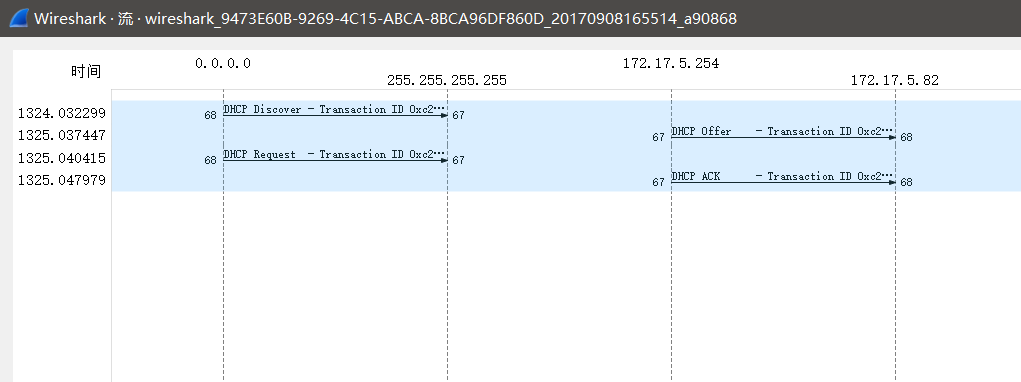
1. Q: *Are DHCP messages sent over UDP or TCP?*

A: **UDP**.

2. Q: *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?*

A: Look at the picture, these are that 4 packets.

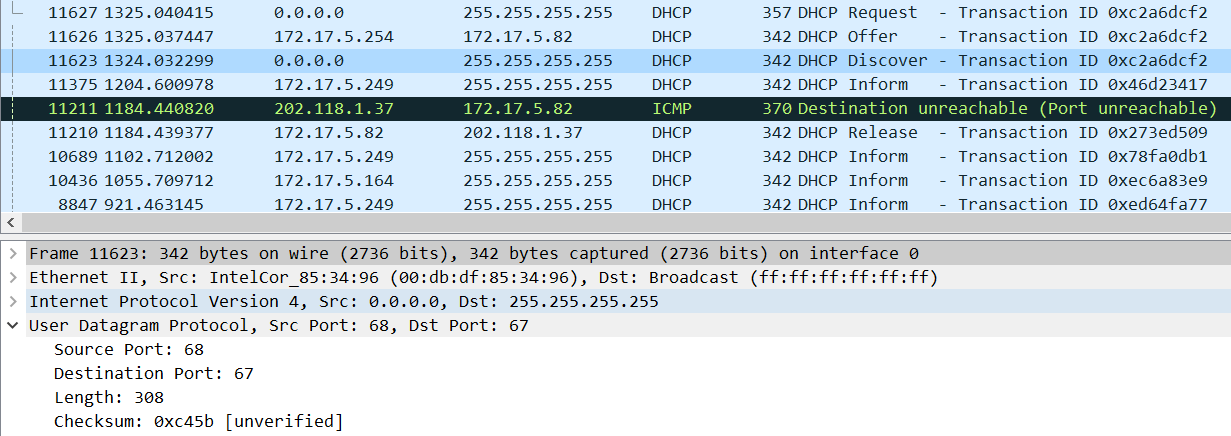




|  |  |  |  |
| --- | --- | --- | --- |
| Time Order | Packet | Src Port | Dst Port |
| 1 | Discover | 68 | 67 |
| 2 | Offer | 67 | 68 |
| 3 | Request | 68 | 67 |
| 4 | ACK | 67 | 68 |

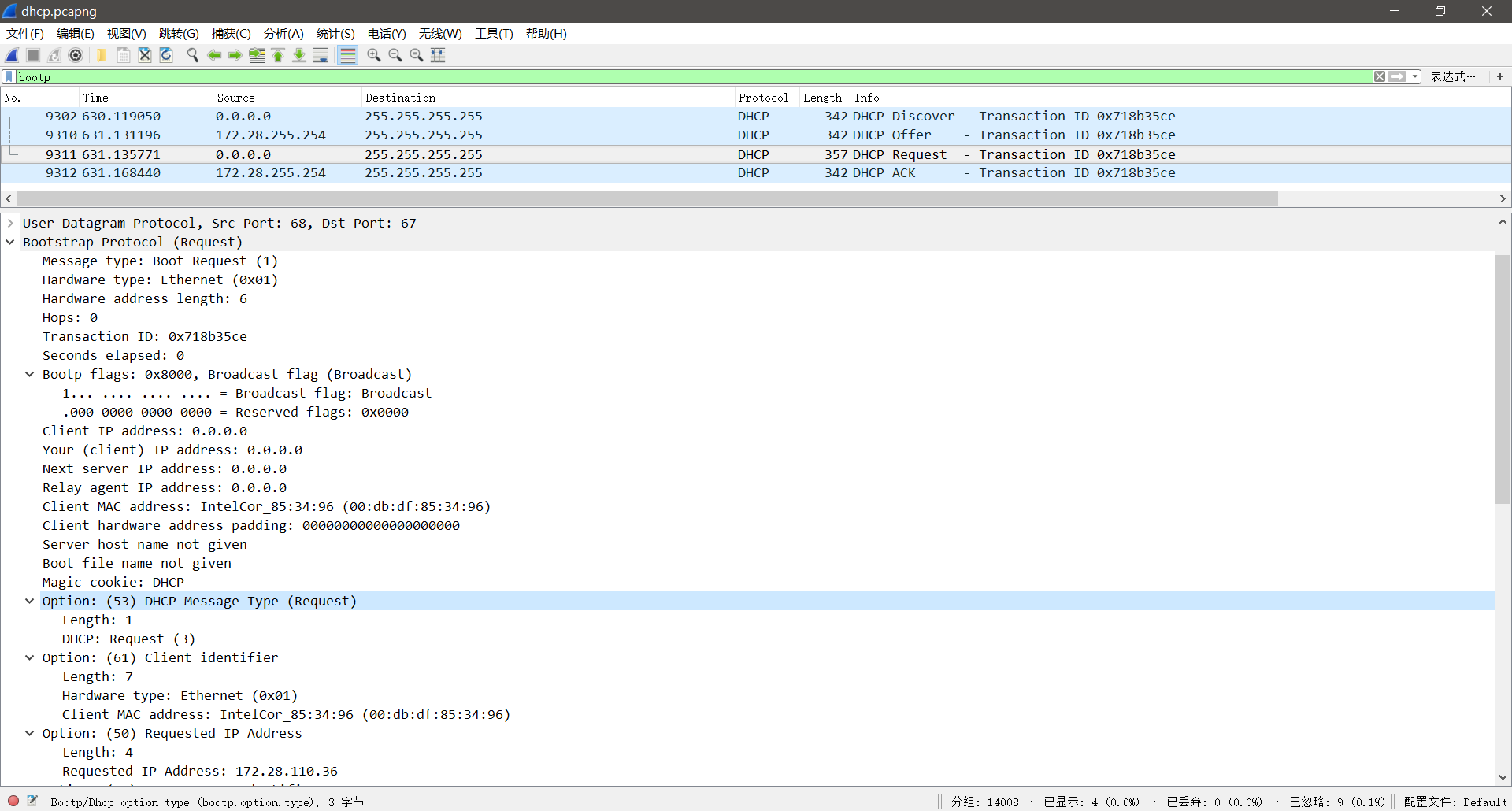
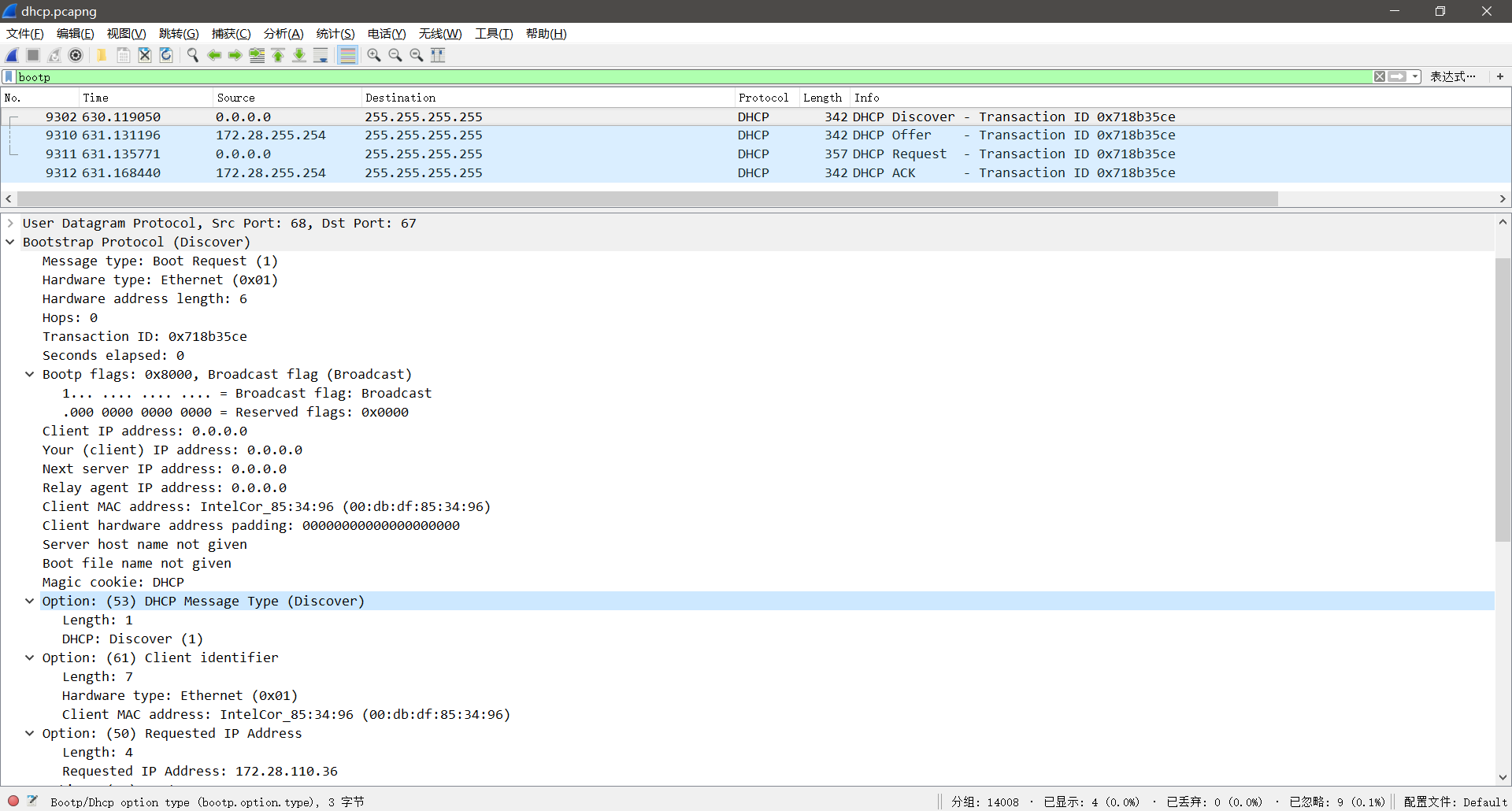
**Yes**, they are the same.

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



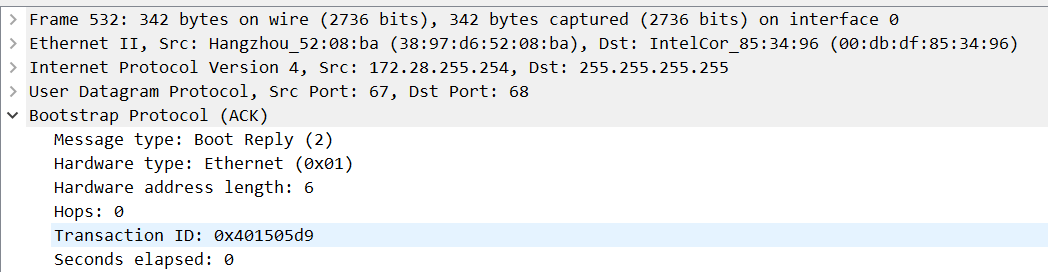
A: As the picture shows, I click the “Discover” packet. I can find my Ethernet address is **00:db:df:85:34:96**.

4. Q: *What values in the DHCP discover message differentiate this message from the DHCP request message?*

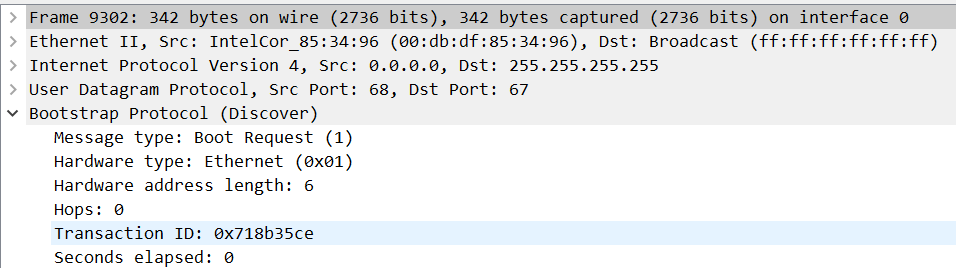


A: The value in the DHCP discover message differentiate this message from the DHCP request message is **Option 53**.

5. Q: *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?*



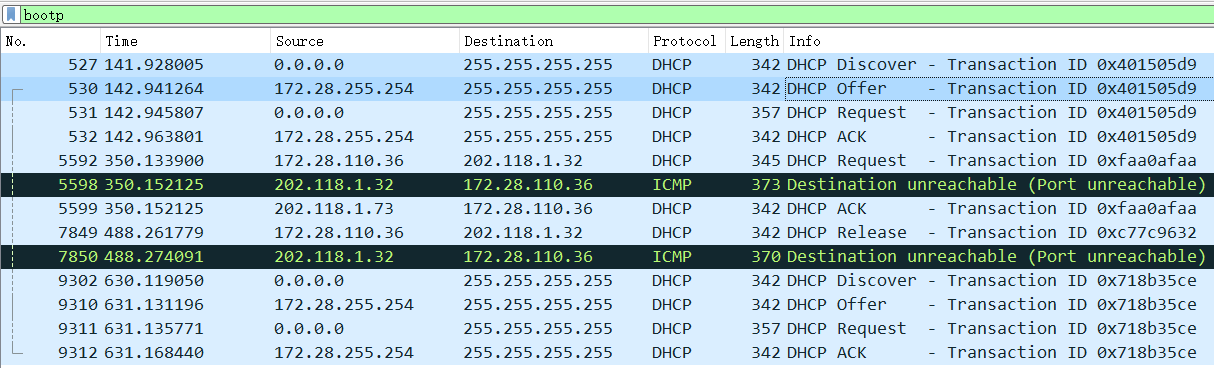
A: In the first four messages, all of Transaction-ID is **0x401505d9**. And in the second set, it’s **0x718b35ce**.



The client will compare these two Transaction-ID(Discover and Offer). If Offer’s ID is different from Discover’s ID, the client will ignore these DHCP OFFER. This rule can make the client get the right IP address.

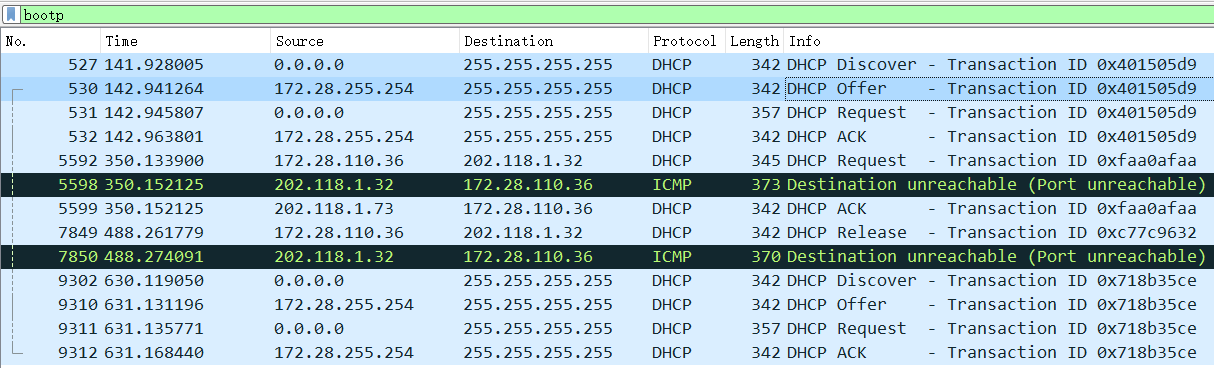
6. Q: *A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange?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

A:



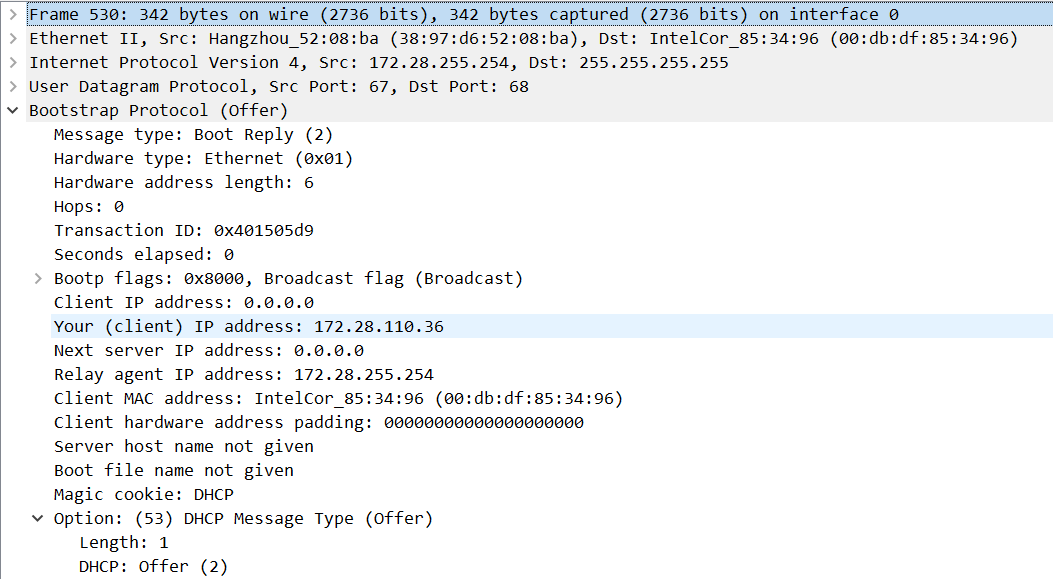
|  |  |  |
| --- | --- | --- |
| Message | Source IP | Destination IP |
| Discover | 0.0.0.0 | 255.255.255.255 |
| Offer | 172.28.255.254 | 255.255.255.255 |
| Request | 0.0.0.0 | 255.255.255.255 |
| ACK | 172.28.255.254 | 255.255.255.255 |

7. Q: *What is the IP address of your DHCP server?*



A: My DHCP server’s IP address is **172.28.255.254**.

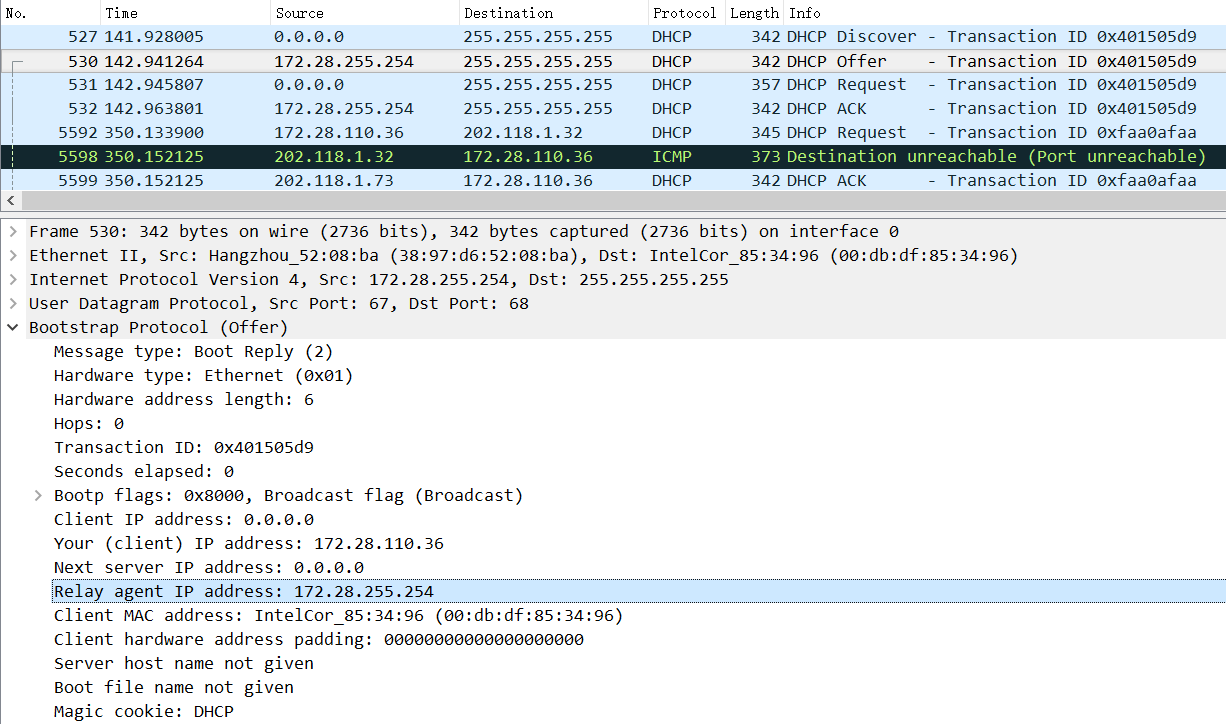
8. Q: *What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.*



DHCP server offer me a IP address, **172.28.110.36**.

**Option 53** contains the DHCP Message type with a length of 1 and the DHCP offer is (2).

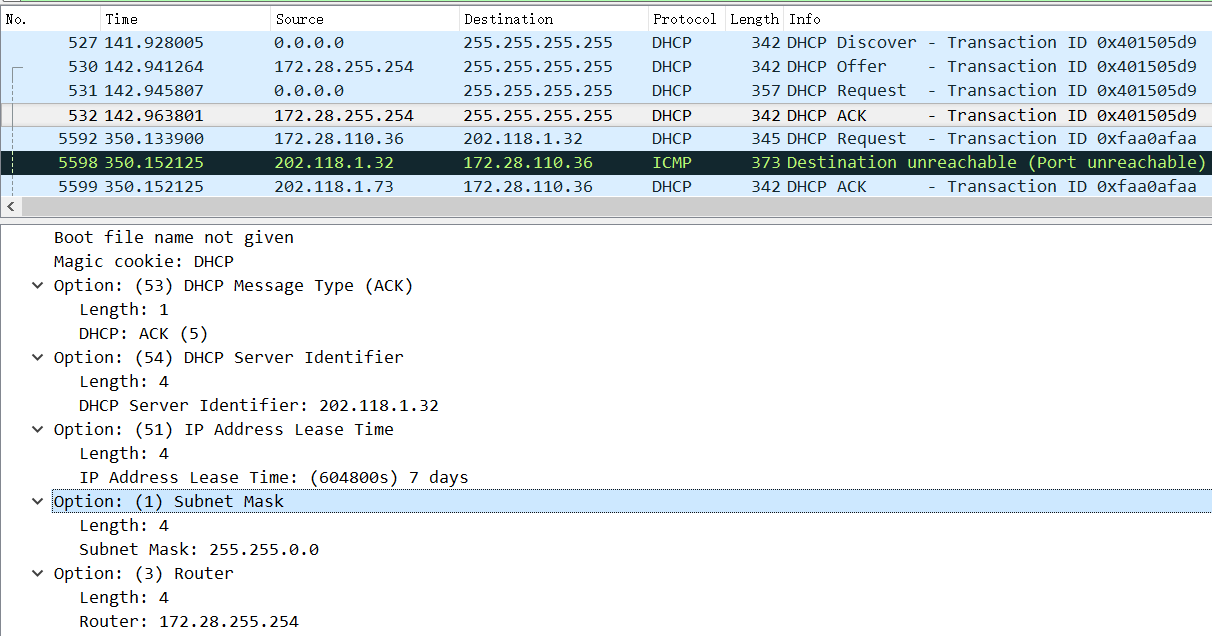
9. *In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?*



A: **In the Offer message and ACK message**, there are relay agent IP address items.

**Yes**, it’s IP address is **172.28.255.254**.

10. Q: *Explain the purpose of the router and subnet mask lines in the DHCP offer message.*

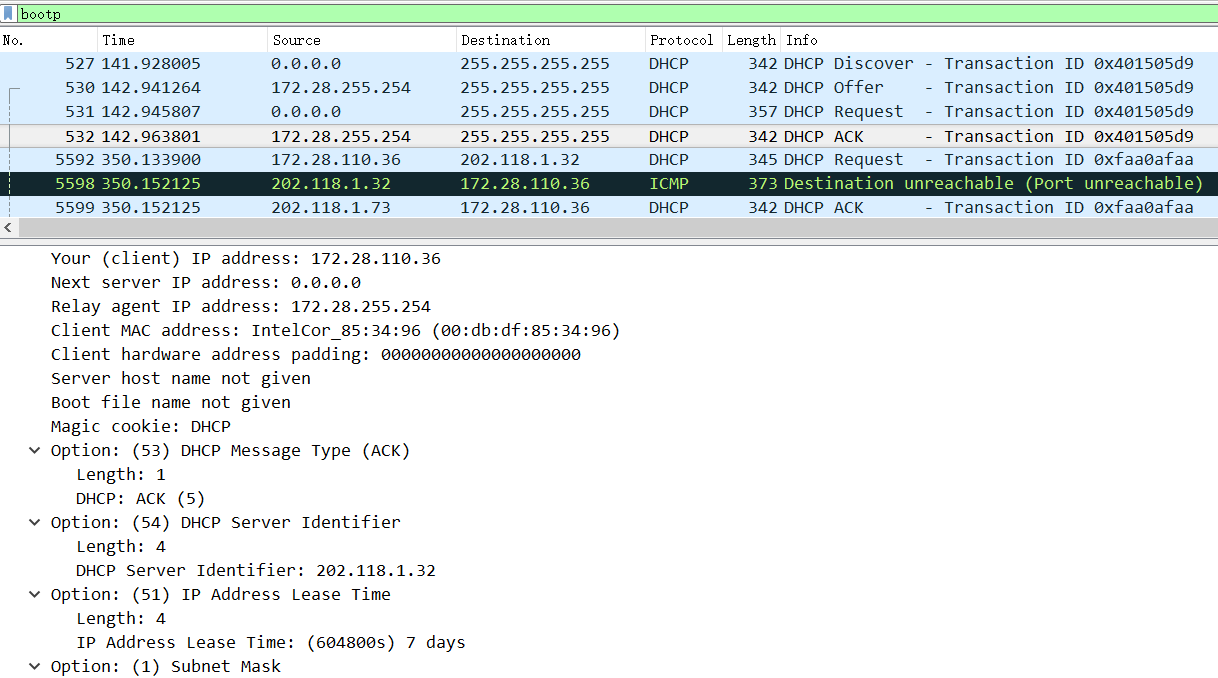


A: The Router line tells the client which one is it’s router. And the subnet mask line tells the client which subnet mask should be used.

11. Q: *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?*

A: **No**.

12. Q: *Explain the purpose of the lease time. How long is the lease time in your experiment?*



A: The Lease Time message is included in ACK packet.

It’s purpose is the amount of time the DHCP server assigns an IP address to a client. And in my experiment, the lease time is **7 days**.

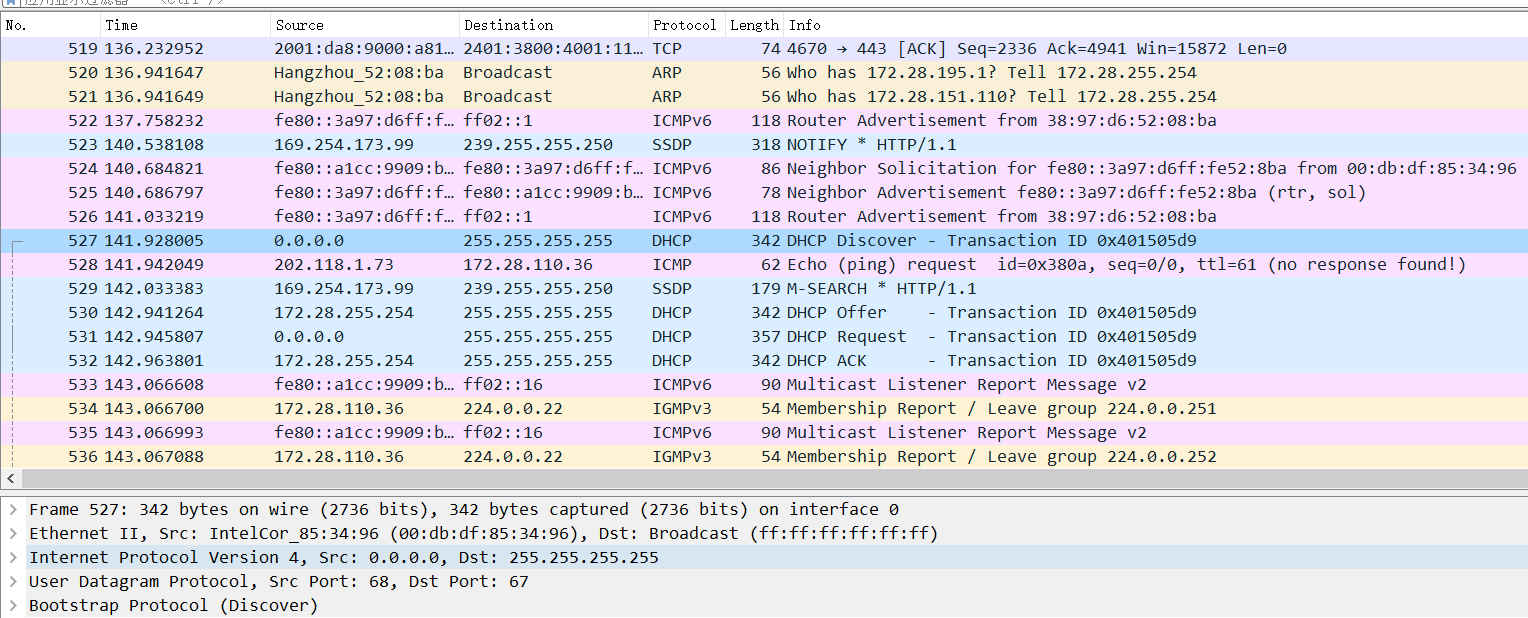
13. *What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?*

The purpose is that the client will sent a release message to the DHCP server to cancel the lease on its IP address allocated by the DHCP server.

Yes.

It would not change its IP address.

14. *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.*



The DHCP packet-exchange period is from No.527 to No.532. So, there is **not** any ARP packets in this period.