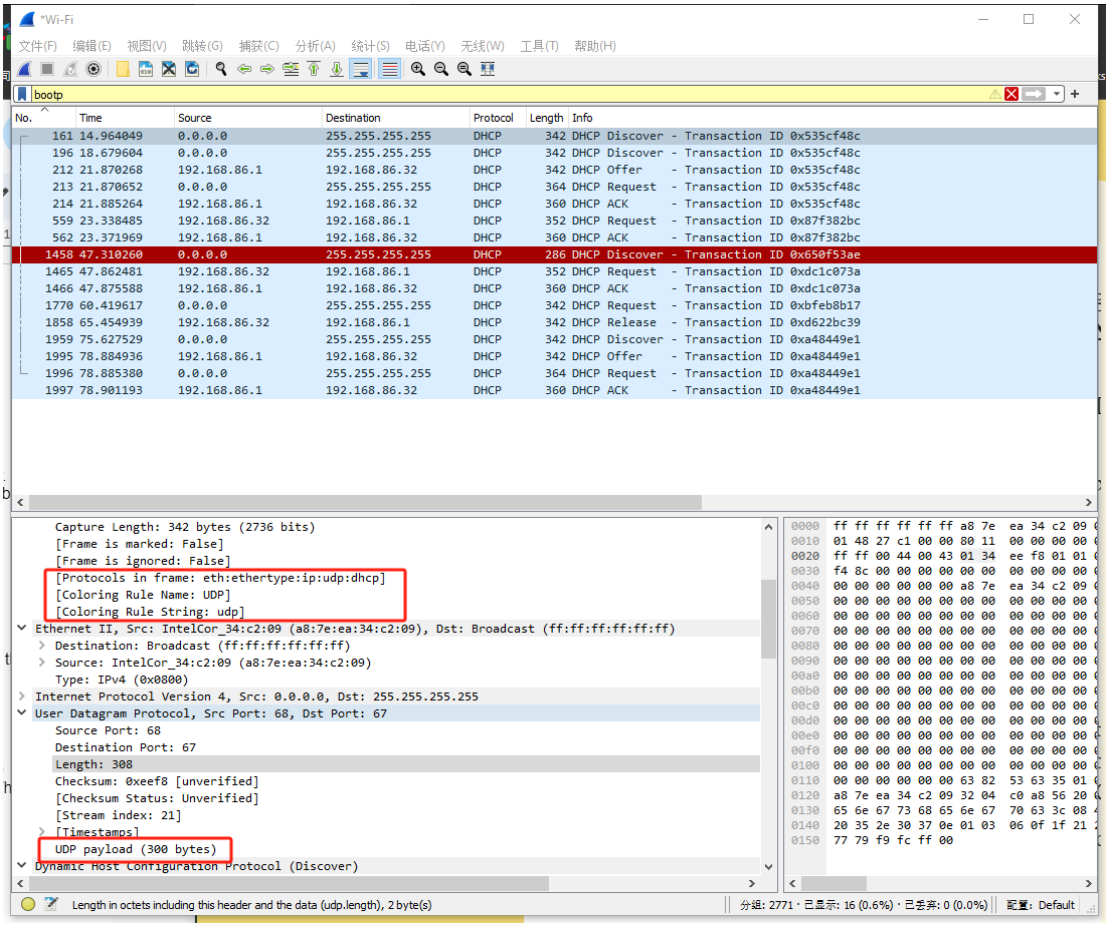
Sheng Wang

Wireshark-DHCP Lab 1

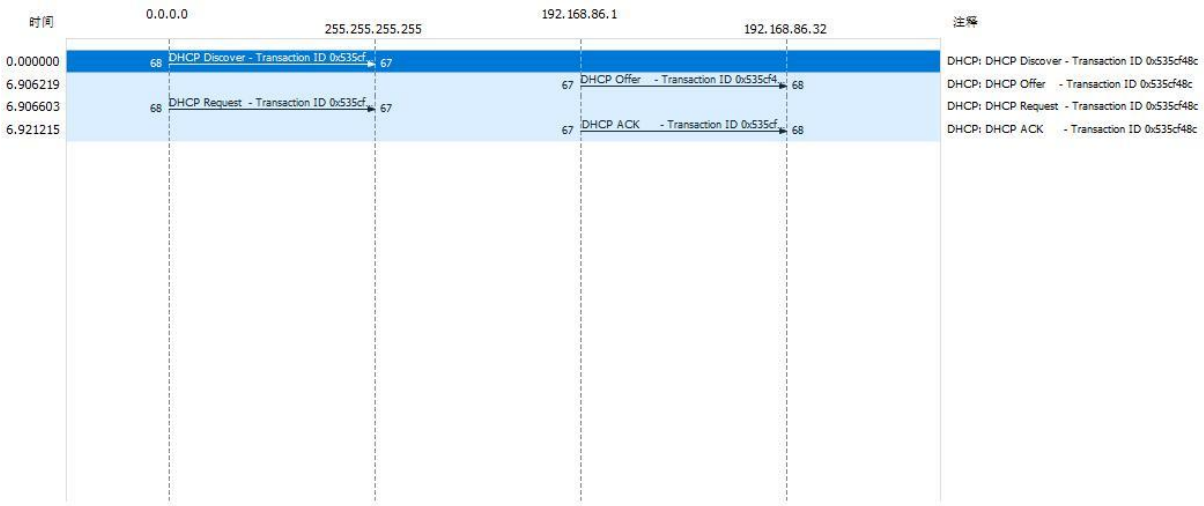
EE450

1. Are DHCP messages sent over UDP or TCP?



DHCP messages sent over UDP

2. 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?



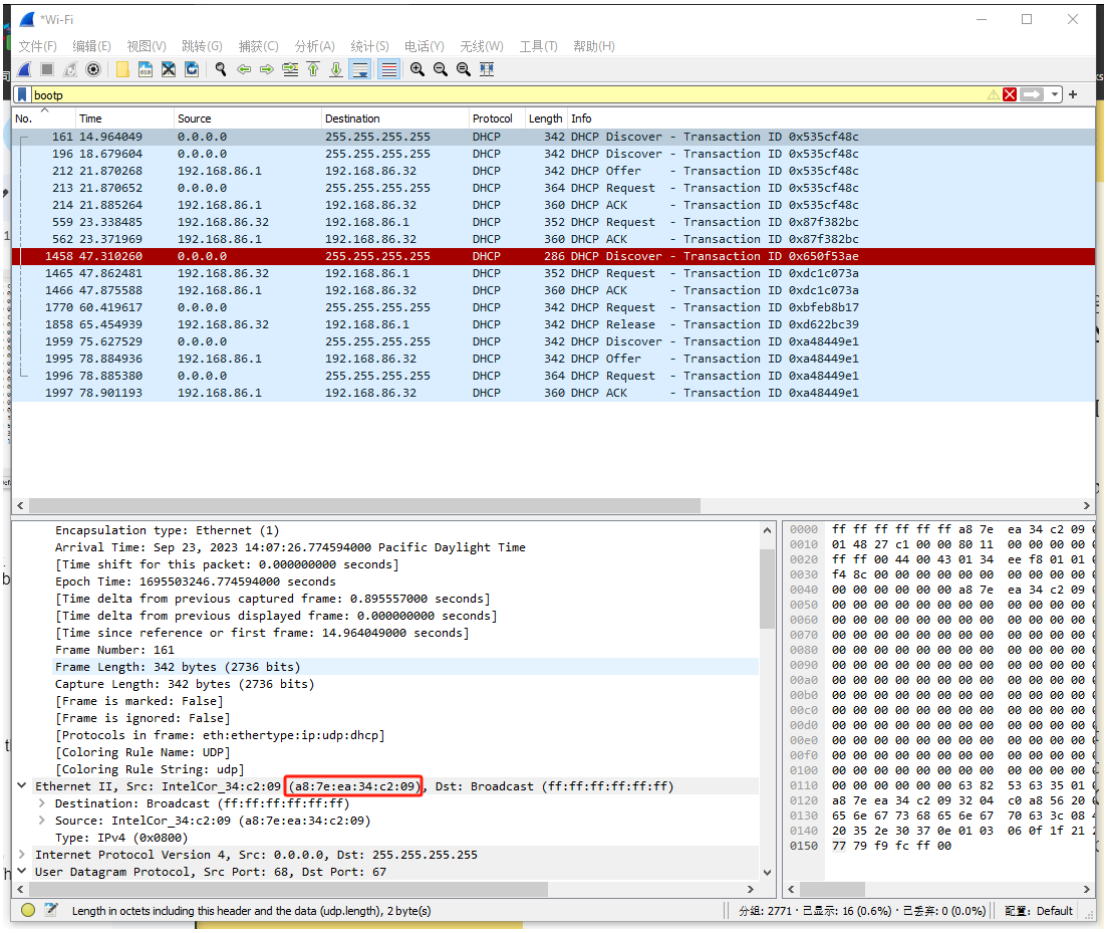
1. Discover:
   Source port: 68
   Dest port: 67

Source ip: 0.0.0.0
Dest ip: Broadcast (255.255.255.255)
Source MAc: a8:7e:ea:34:c2:09
Dst MAC: Broadcast (ff:ff:ff:ff:ff:ff)

2. Offer:
   Source port: 67
   Dest port: 68
   Source ip:192.168.86.1
   Dest ip: 192.168.86.32
   Source MAC: b0:6a:41:c7:5f:d8
   Dst MAC: a8:7e:ea:34:c2:09
3. Request:
   Source port: 68
   Dest port: 67
   Source ip: 0.0.0.0
   Dest ip: Broadcast (255.255.255.255)
   Source MAc: a8:7e:ea:34:c2:09
   Dst MAC: Broadcast (ff:ff:ff:ff:ff:ff)
4. ACK:
   Source port: 67
   Dest port: 68
   Source ip:192.168.86.1
   Dest ip: 192.168.86.32
   Source MAC: b0:6a:41:c7:5f:d8
   Dst MAC: a8:7e:ea:34:c2:09

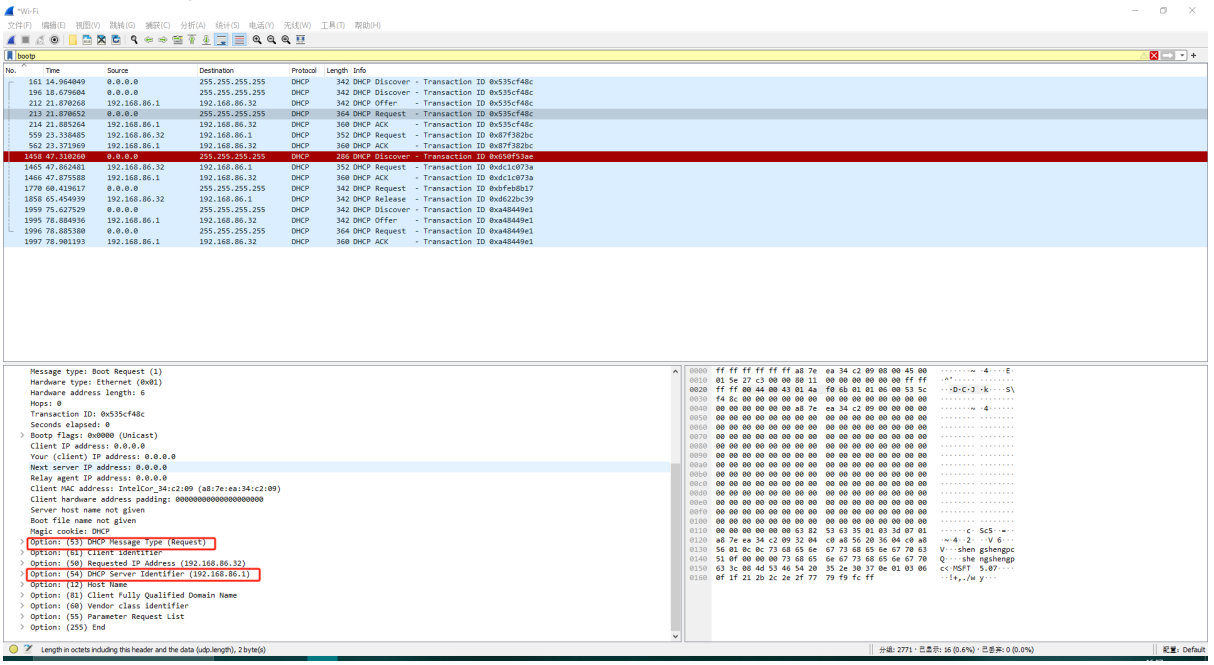
Yes, They have the same port numbers.

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



a8:7e:ea:34:c2:09

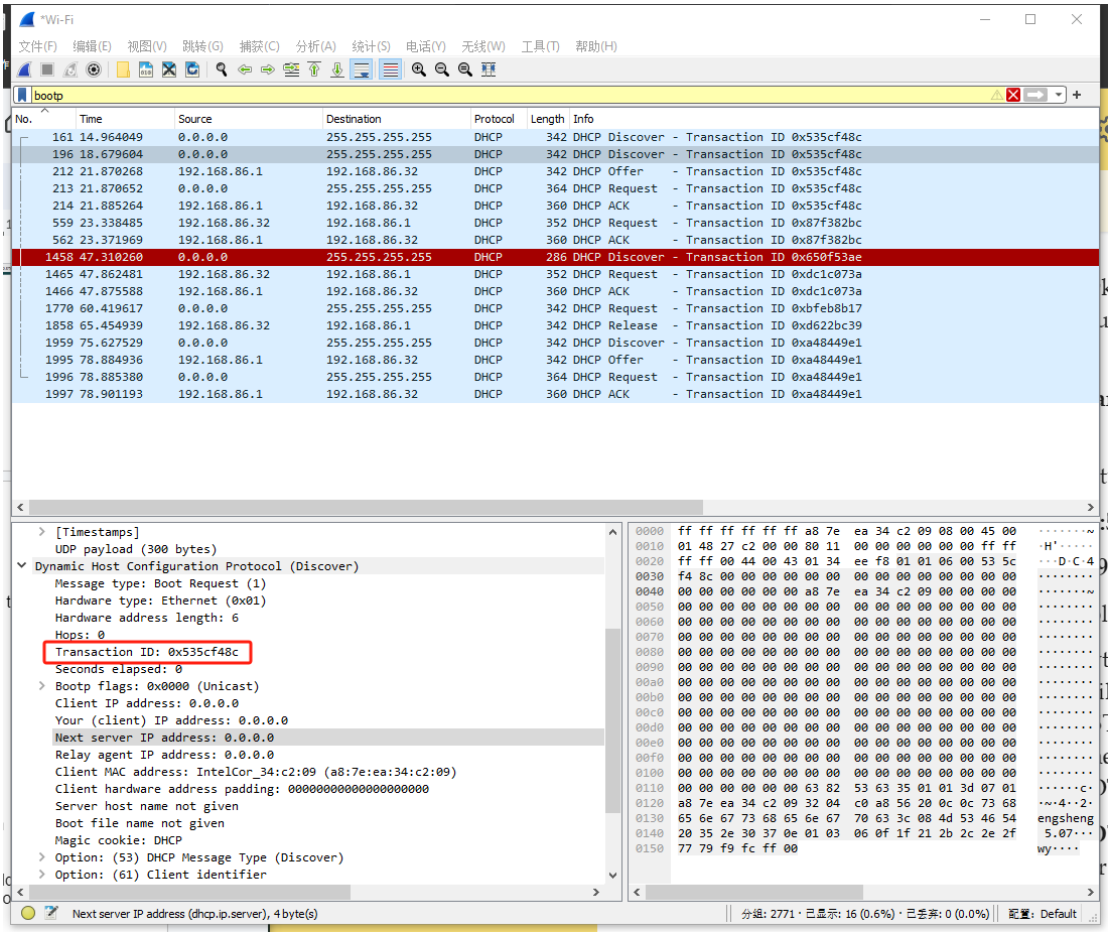
4. What values in the DHCP discover message differentiate this message from the DHCP request message?



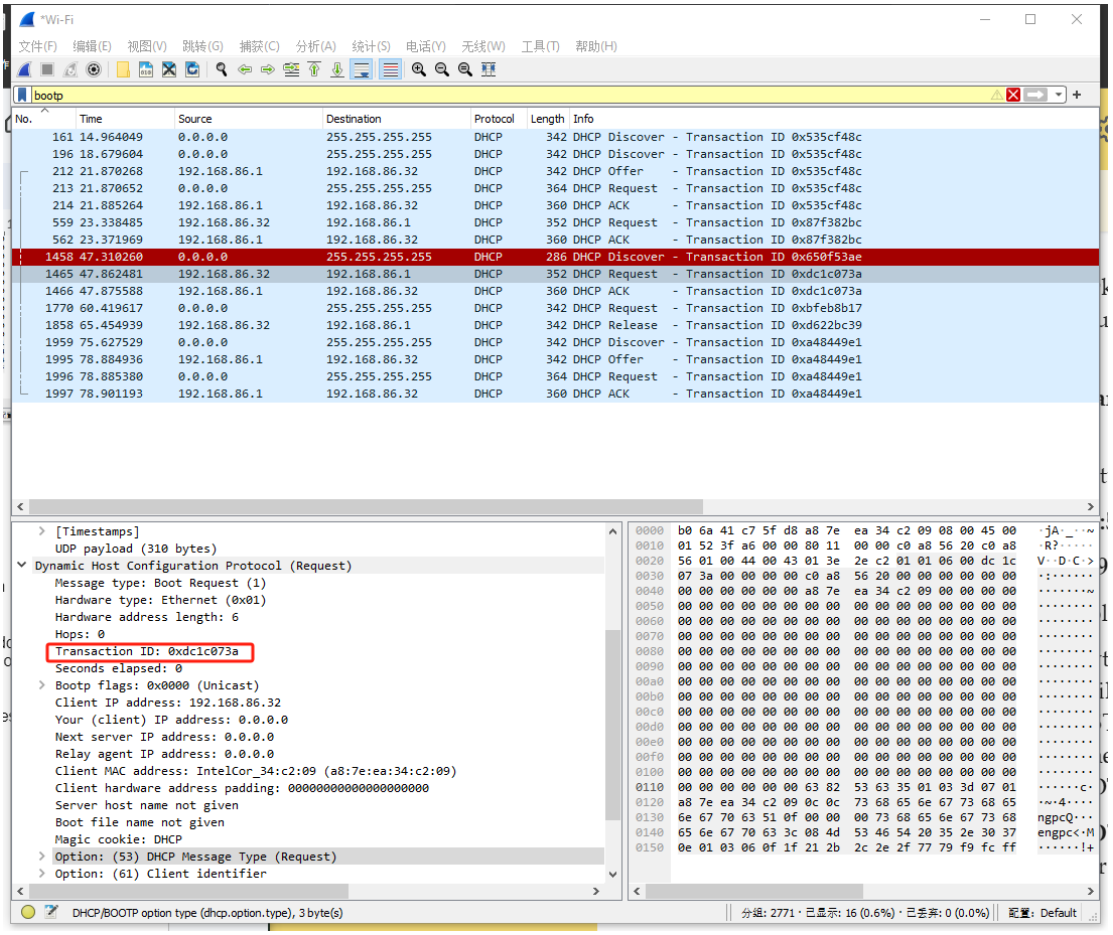
DHCP Message Type and DHCP Server Identifier

5. 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?



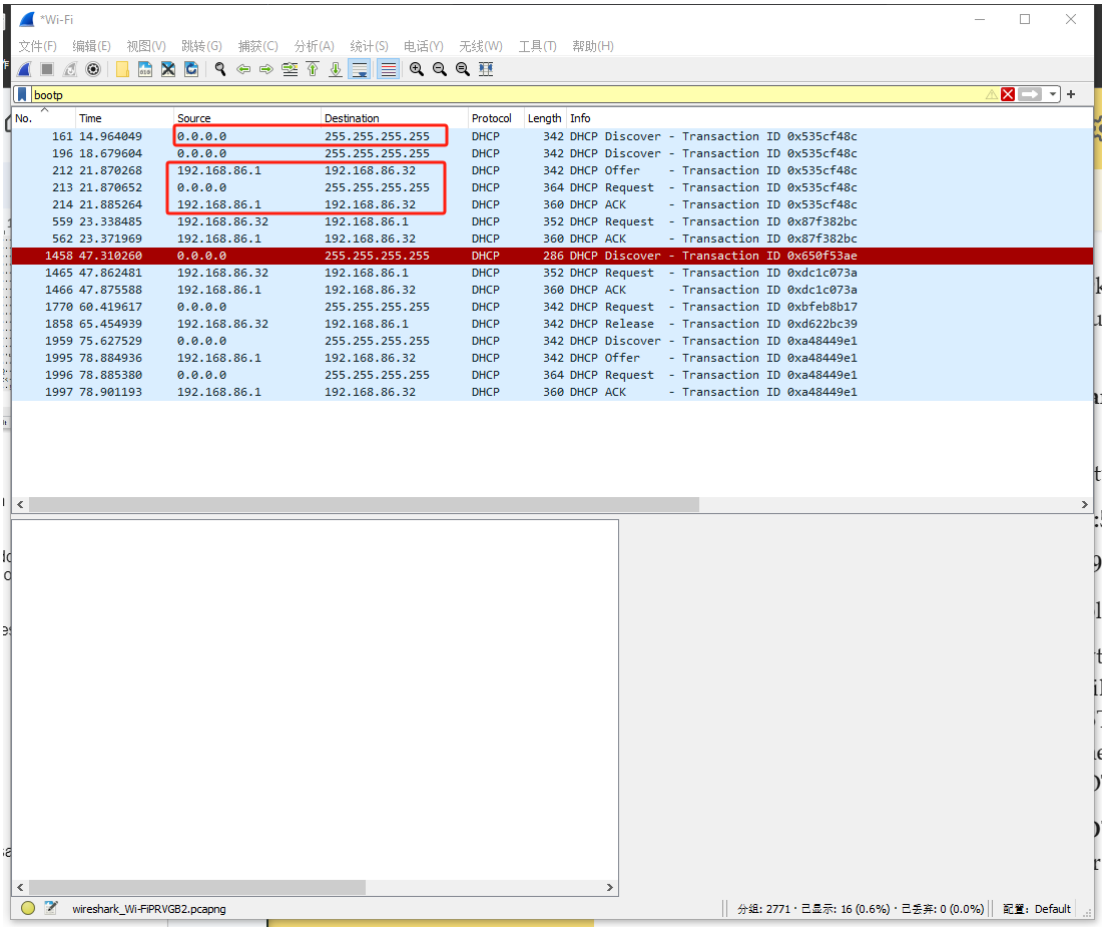
first Discover: 0x535cf48c
first Offer: 0x535cf48c
first Request: 0x535cf48c
first ACK: 0x535cf48c



Second Request: 0xdc1c073a
Second ACK: 0xdc1c073a

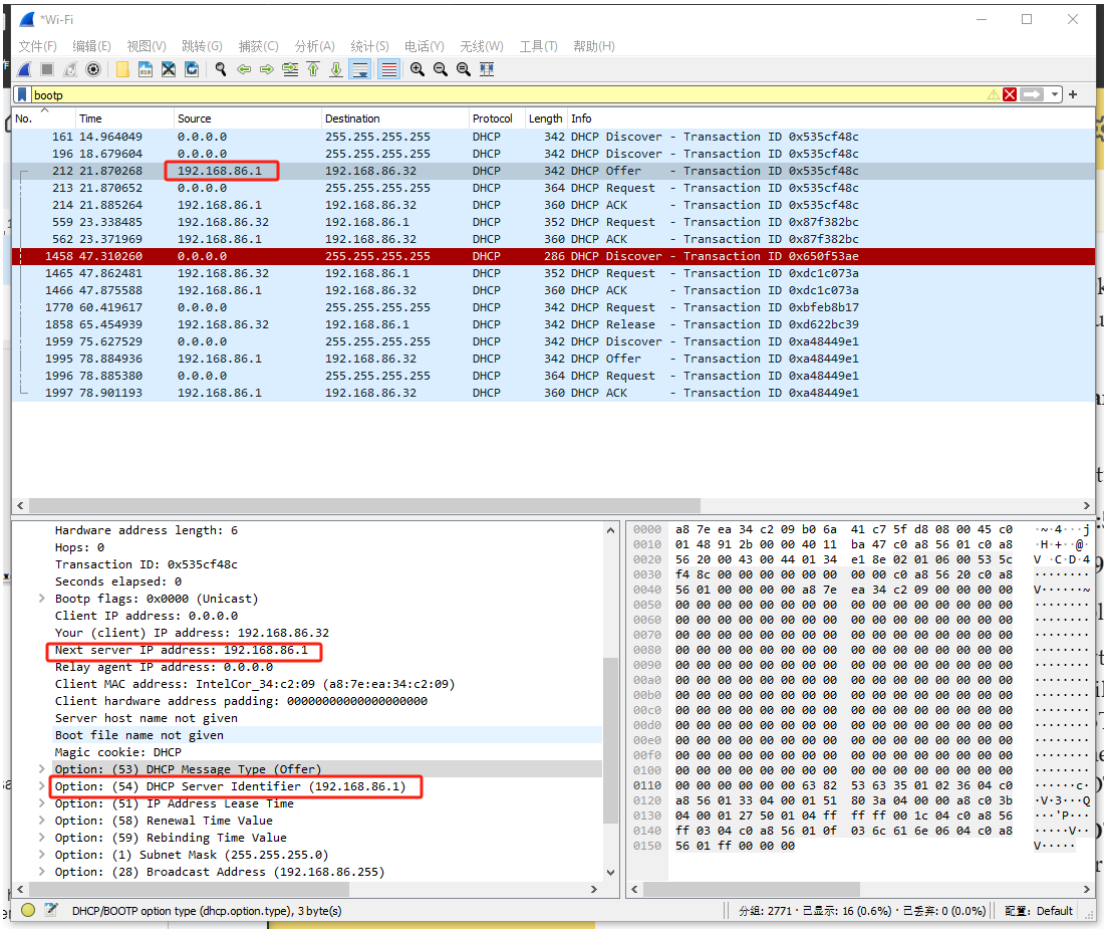
The purpose of the transaction ID is used to distinguish the different requests from clients.

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.



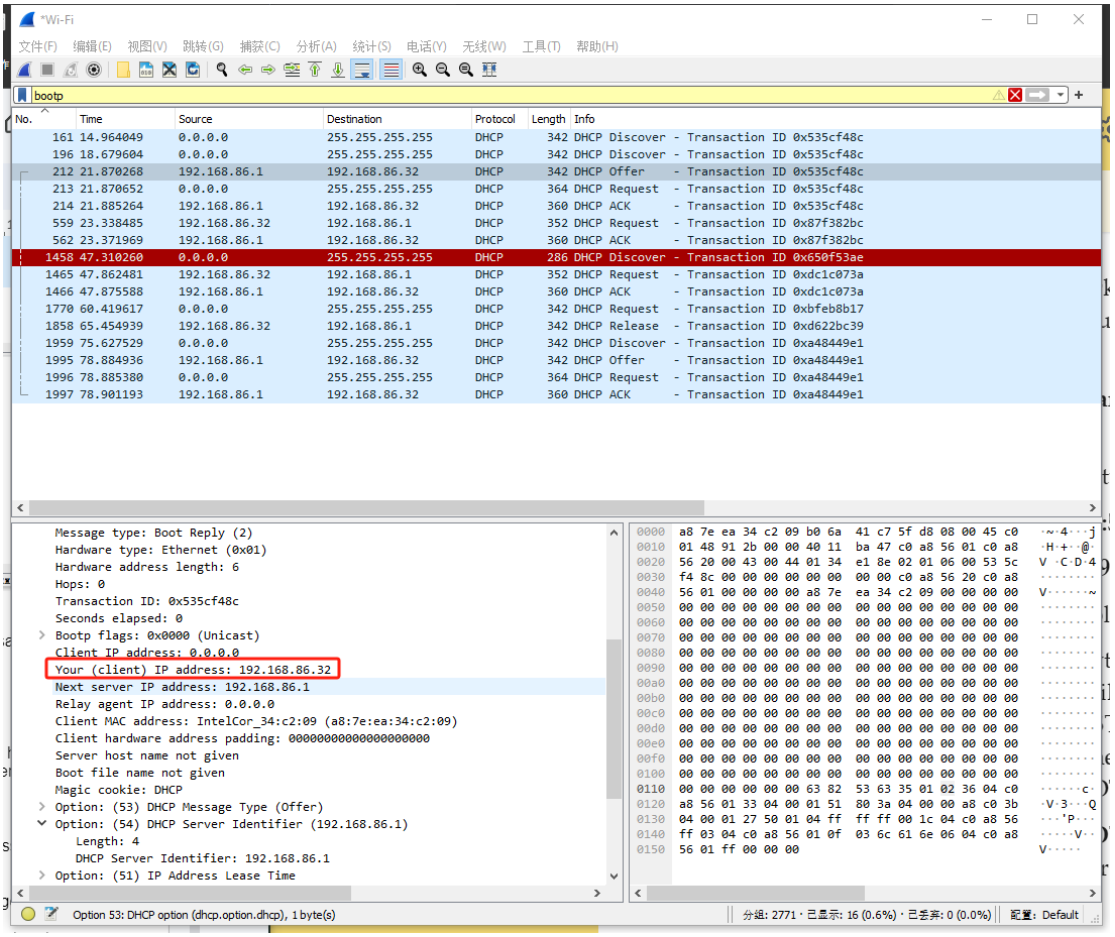
Discover: Src: 0.0.0.0, Dst: 255.255.255.255
Offer: Src: 192.168.86.1, Dst: 192.168.86.32
Request: Src: 0.0.0.0, Dst: 255.255.255.255
ACK: Src: 192.168.86.1, Dst: 192.168.86.32

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



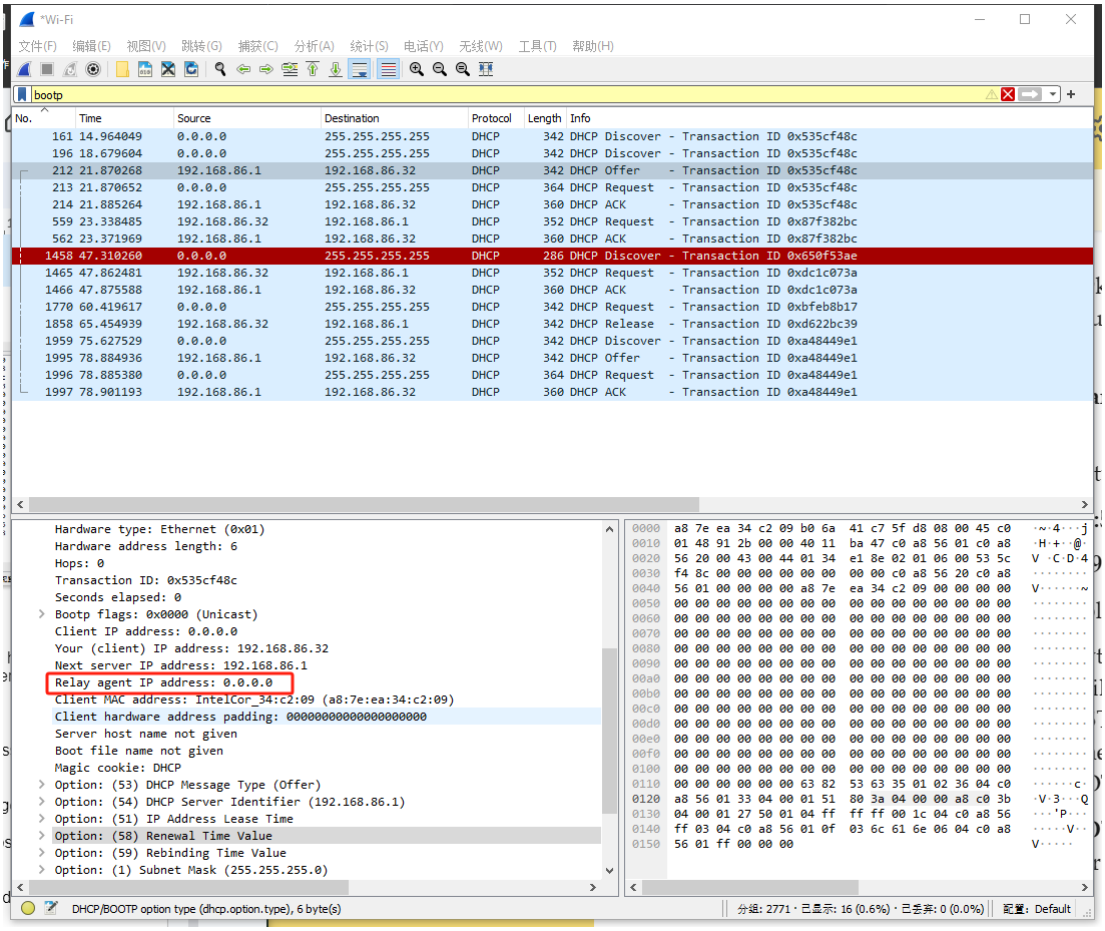
192.168.86.1

8. 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.



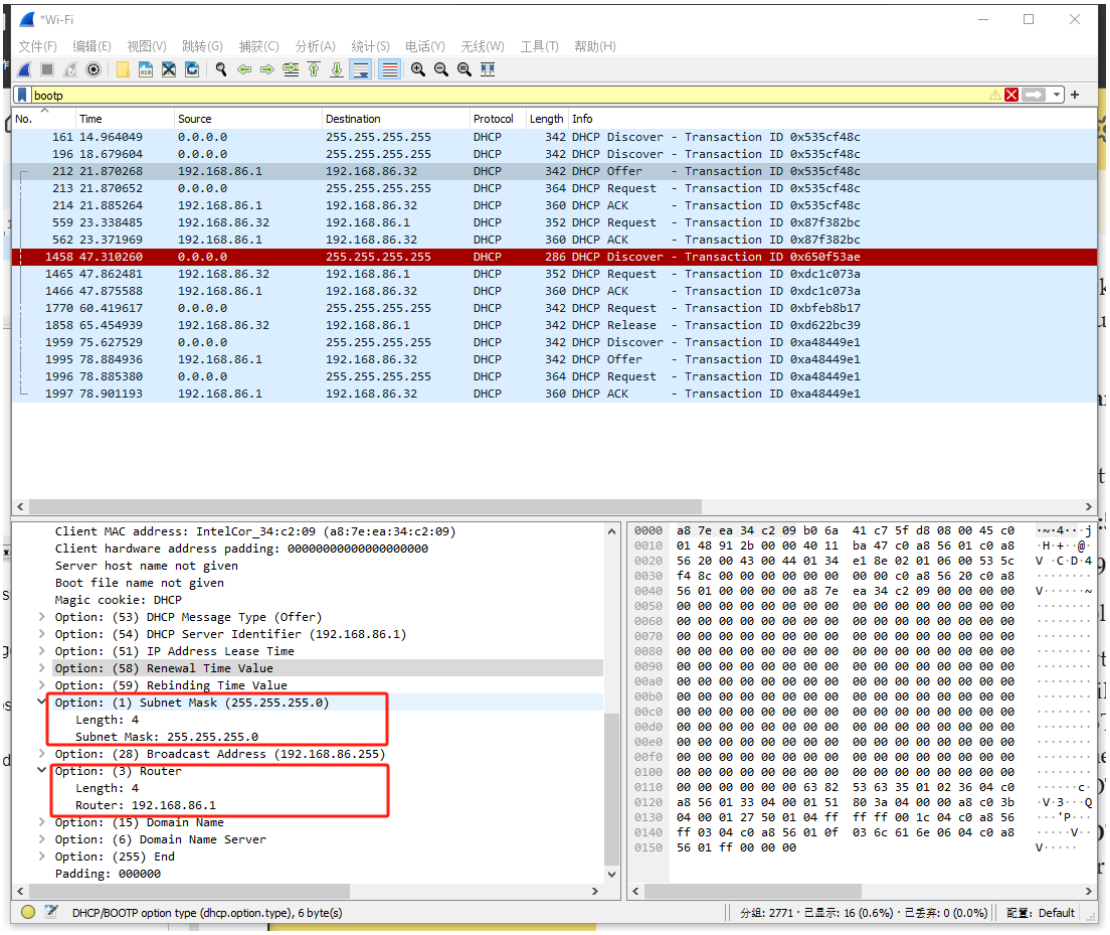
192.168.86.32
Offer DHCP message contain the offered DHCP address

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?



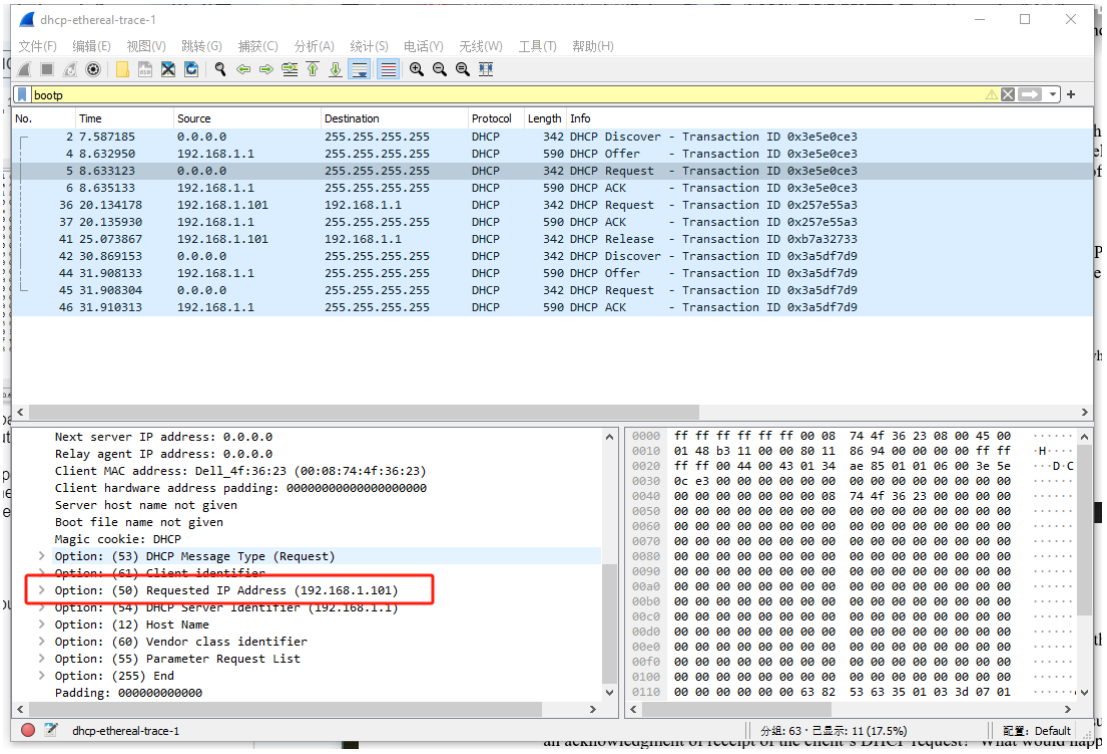
The “Relay agent IP address” indicates the absence of a relay agent.
There is no relay agent in my lab, due to the value of this is “Relay agent IP address: 0.0.0.0”

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



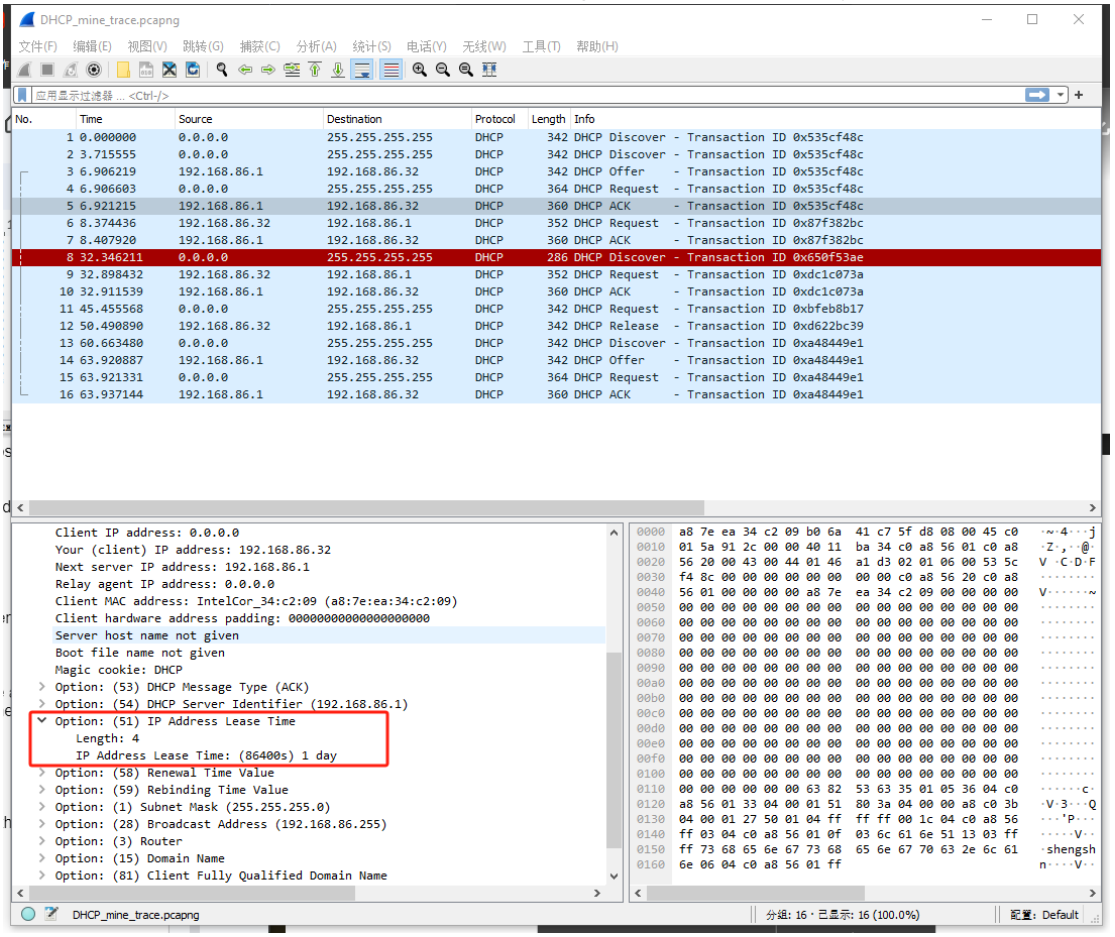
The subnet mask tells the client which part is the internet part, which part is the host part. The router line tells the clients what is the ip address of the default router.

11. 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 serve OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?



The client accepts this ip address, due to it sending a request message for this ip address.

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



The purpose of the lease time is to provide the expiration date for the offered ip address.

The number of the ip address is limited. Thus, the ip address will be returned when you do not need to use your ip address.

The lease time of my ip address is 1 day.

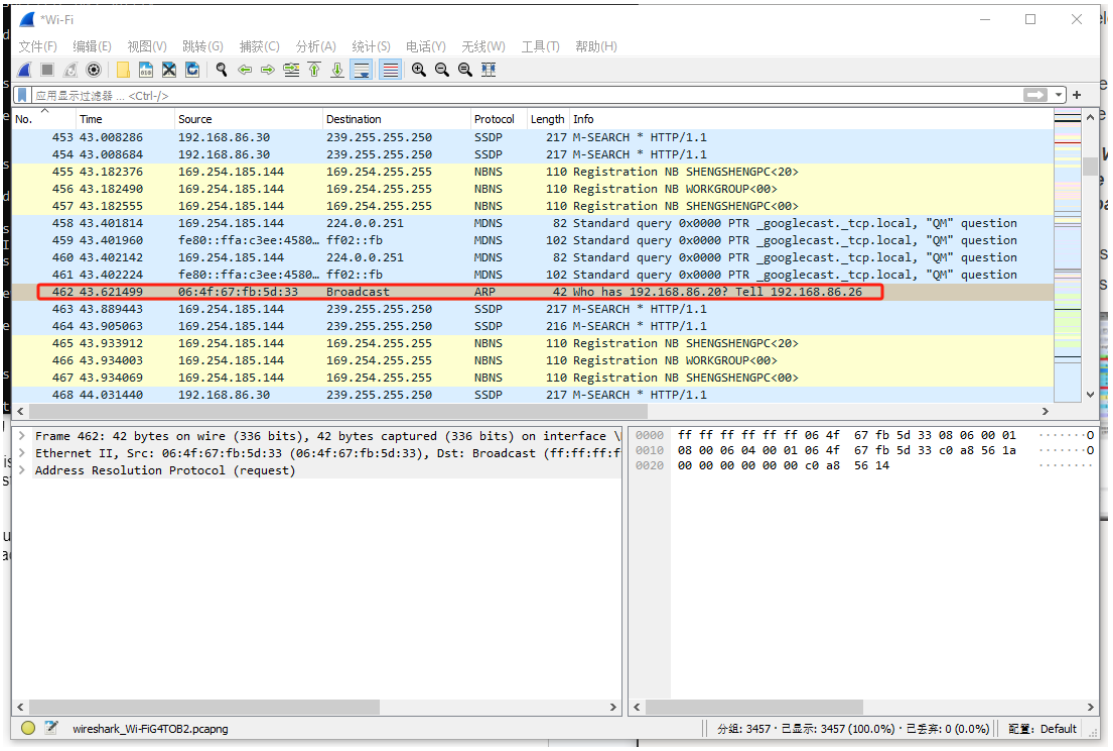
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

    The purpose of the DHCP release message is telling the DHCP server that the client is releasing its current ip address. Then the DHCP server can distribute this ip address later.

    There is no ACK for DHCP release request, but there is ACK for DHCP ip request. I am not sure what you are asking here.

    If a DHCP release message is lost, the DHCP server will not distribute this ip address to others, it will think someone still uses this ip address until it reaches its lease time.

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.



Yes, there is one ARP packet in my Lab

The purpose of those ARP packets is to ask the MAC address of the specified ip address.