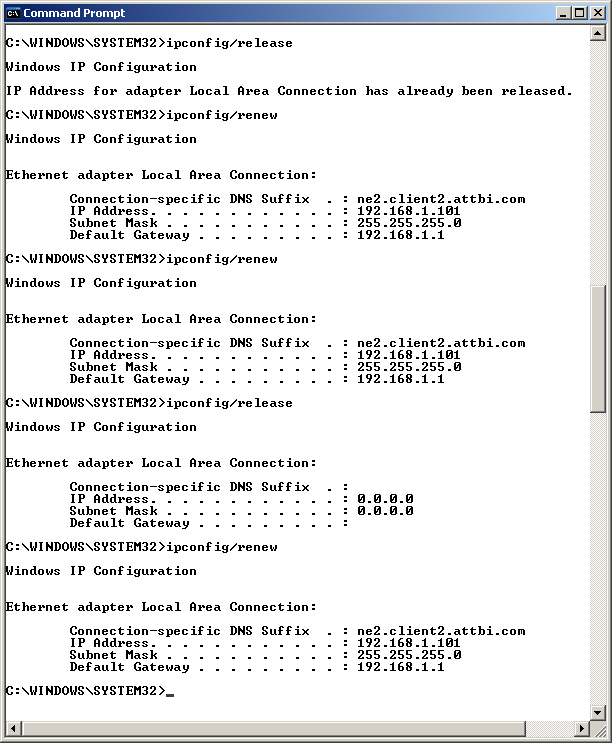
Nathan Flack

Wireshark Lab #5

**Note: using provided trace (dhcp-ethereal-trace-1)**

### What to Hand In:

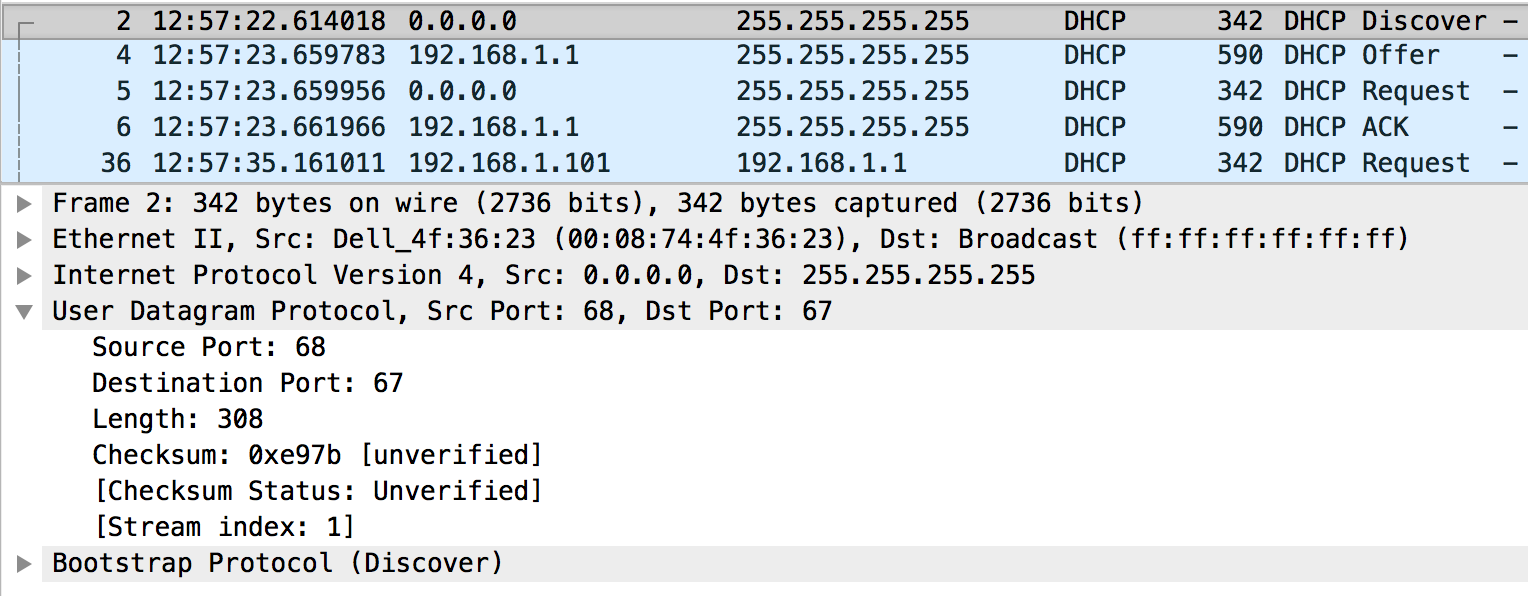
You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Since I am using the provided trace, I copied the screenshot of the commands that they ran for the lab.



Answer the following questions:

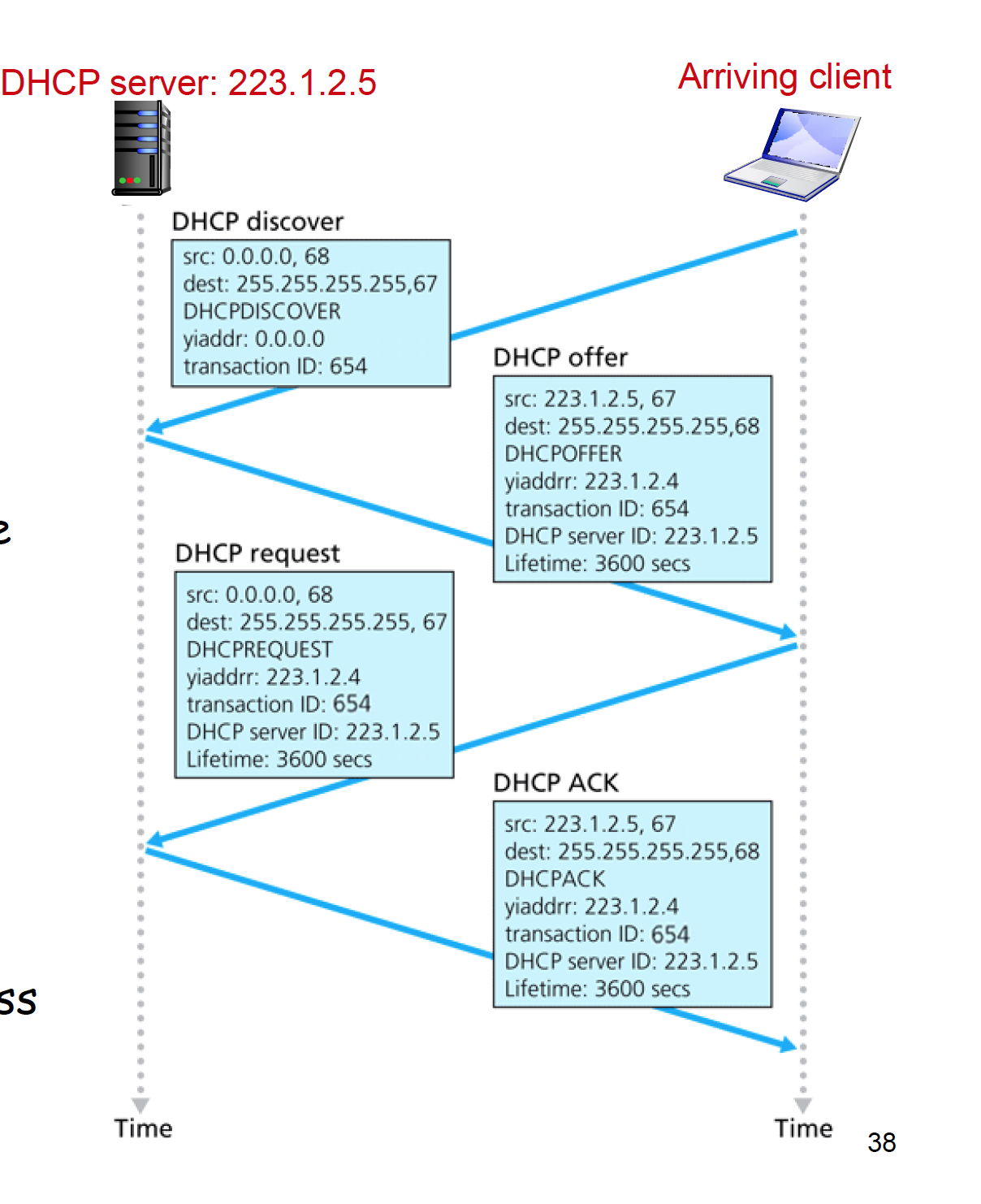
1. Are DHCP messages sent over UDP or TCP?

Message are sent using 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?

**Timing diagram taken from Dr. Mullins’ lecture slides (slide 38). Annotations added by me to show what is specifically taking place within the lab. If something is not covered up by my response, it was the same on the original diagram.**



**Yes, the port numbers (67 and 68) are the same as those given in the example provided in the lab assignment.**

1 Day

192.168.1.1

192.168.1.1

0x3E5E0CE3

192.168.1.101

192.168.1.1

0x3E5E0CE3

192.168.1.101

192.168.1.1

1 Day

0x3E5E0CE3

192.168.1.101

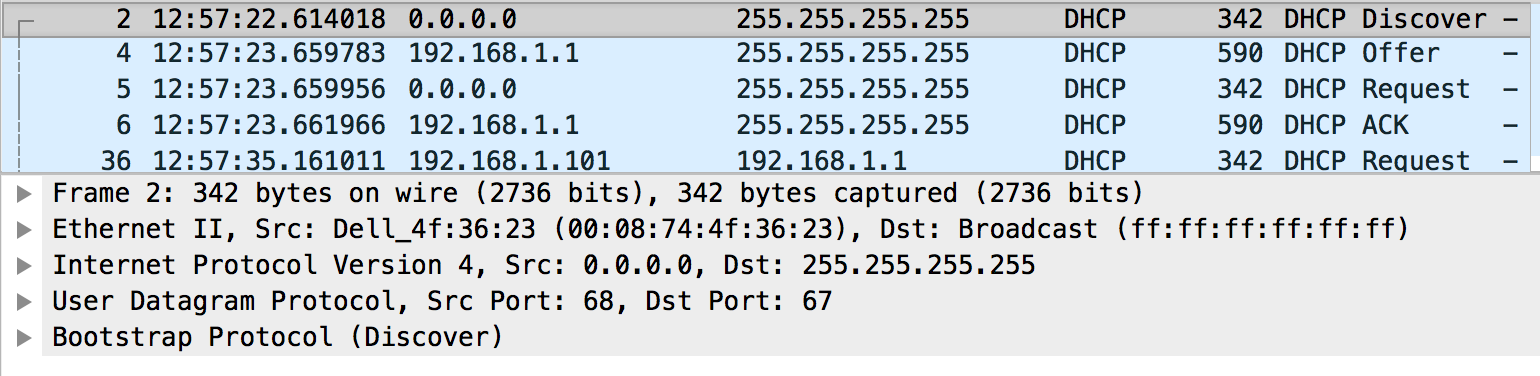
192.168.1.1

0x3E5E0CE3

192.168.1.1

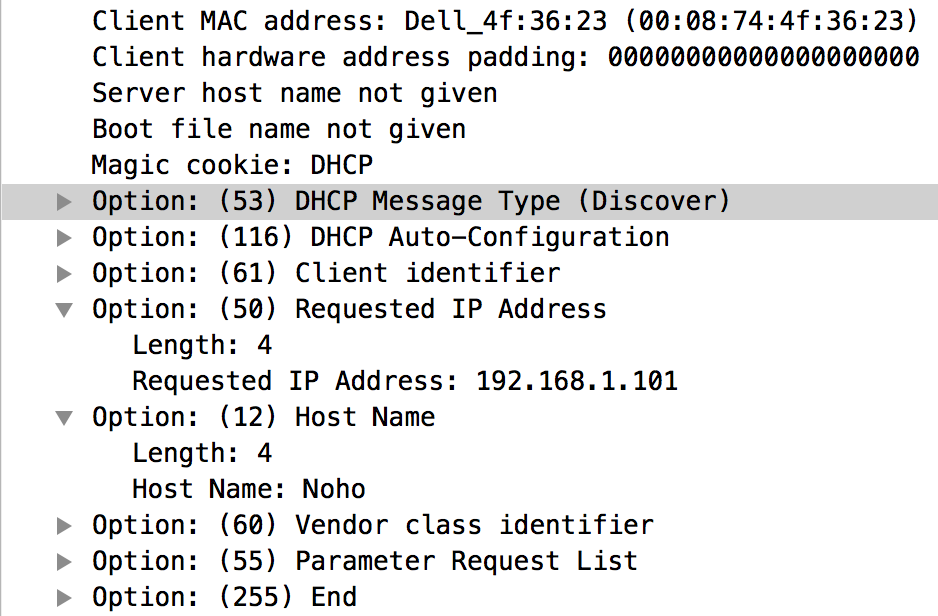
1. What is the link-layer (e.g., Ethernet) address of your host?

**MAC Address for Ethernet: 00:08:74:4F:36:23**



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

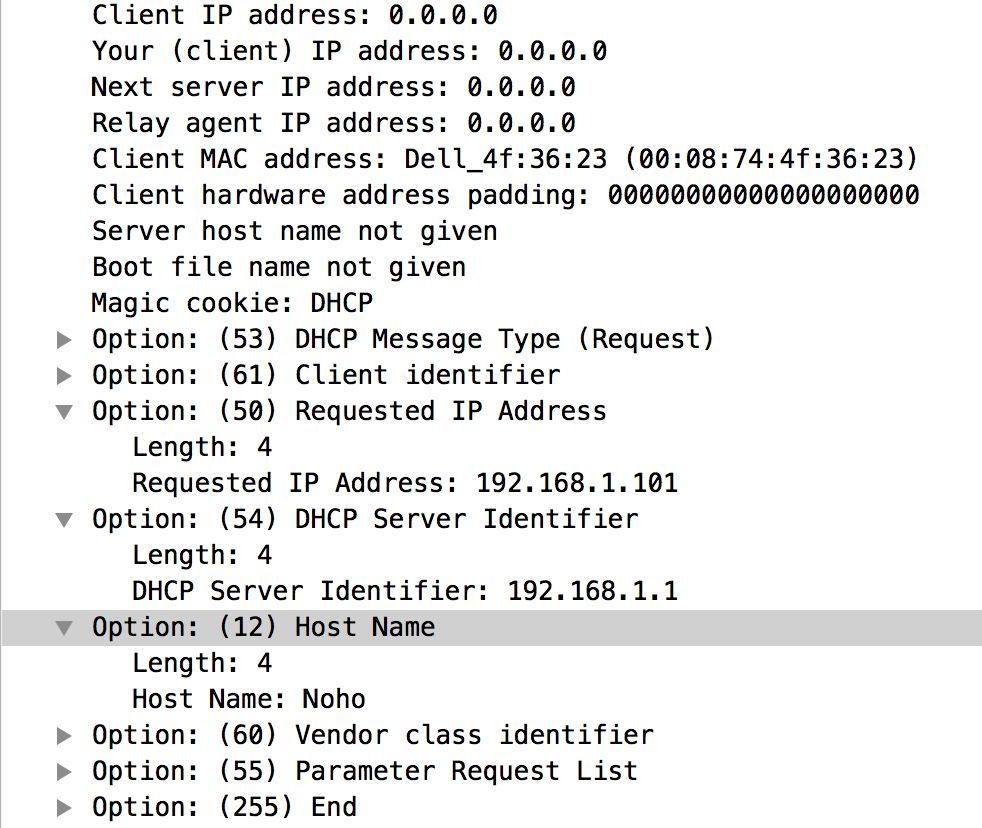
**Discover Message:**



Differences:

* The request message is showing the value of the DHCP server Identifier
* The discover message does not show Option 116: DHCP auto-configuration option

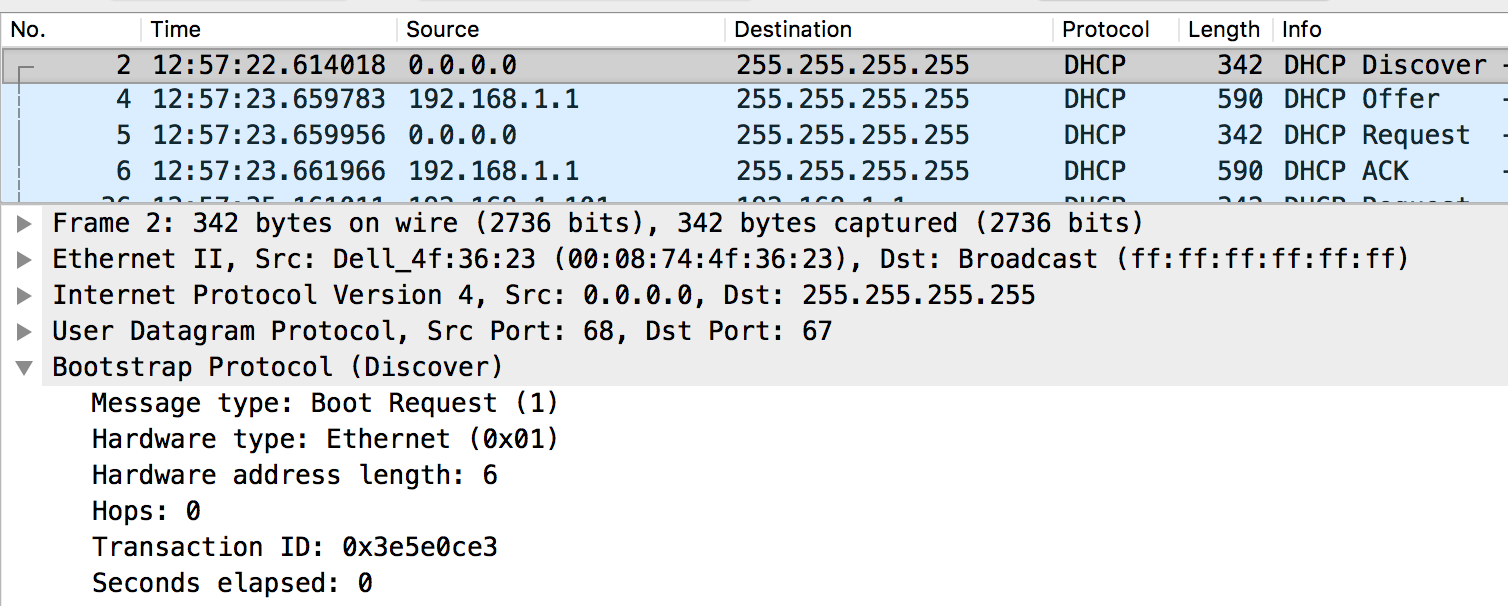
**Request Message:**



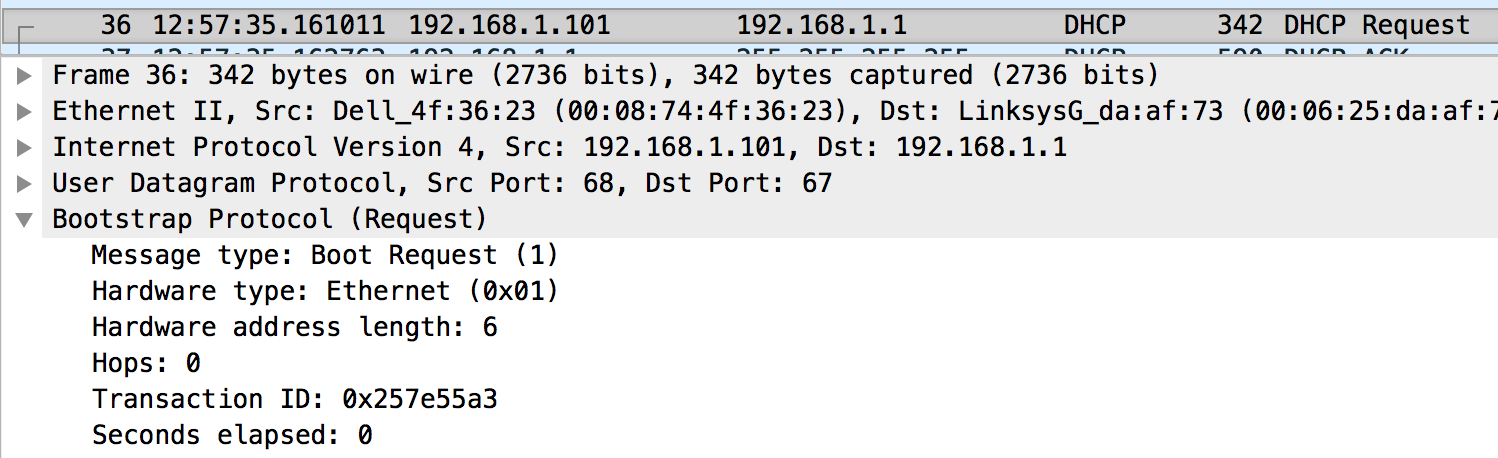
1. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

**The purpose of the transaction ID is to let the DHCP server to differentiate between two sets of requests (either from different computers at the same time or the same computer at different times).**

**First set of messages: “0x3E5E0CE3”**

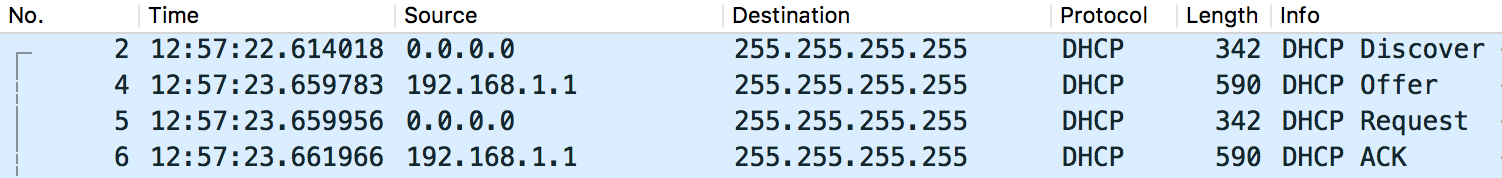


**Second set of messages: “0x257E55A3”**



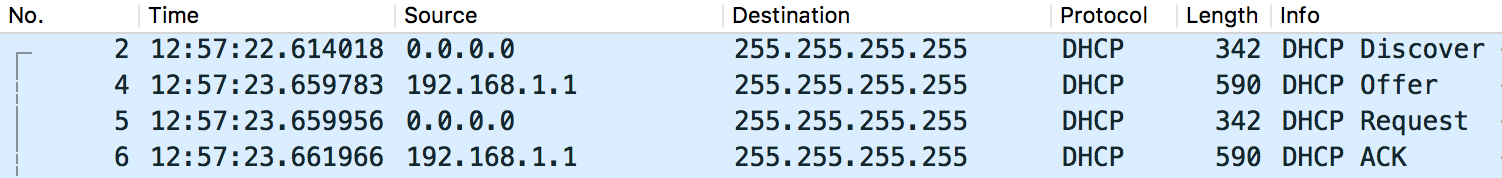
1. A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For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

|  |  |  |
| --- | --- | --- |
| Type of Message | Source IP | Destination IP |
| Discover | 0.0.0.0 | 255.255.255.255 |
| Offer | 192.168.1.1 | 255.255.255.255 |
| Request | 0.0.0.0 | 255.255.255.255 |
| ACK DHCP | 192.168.1.1 | 255.255.255.255 |



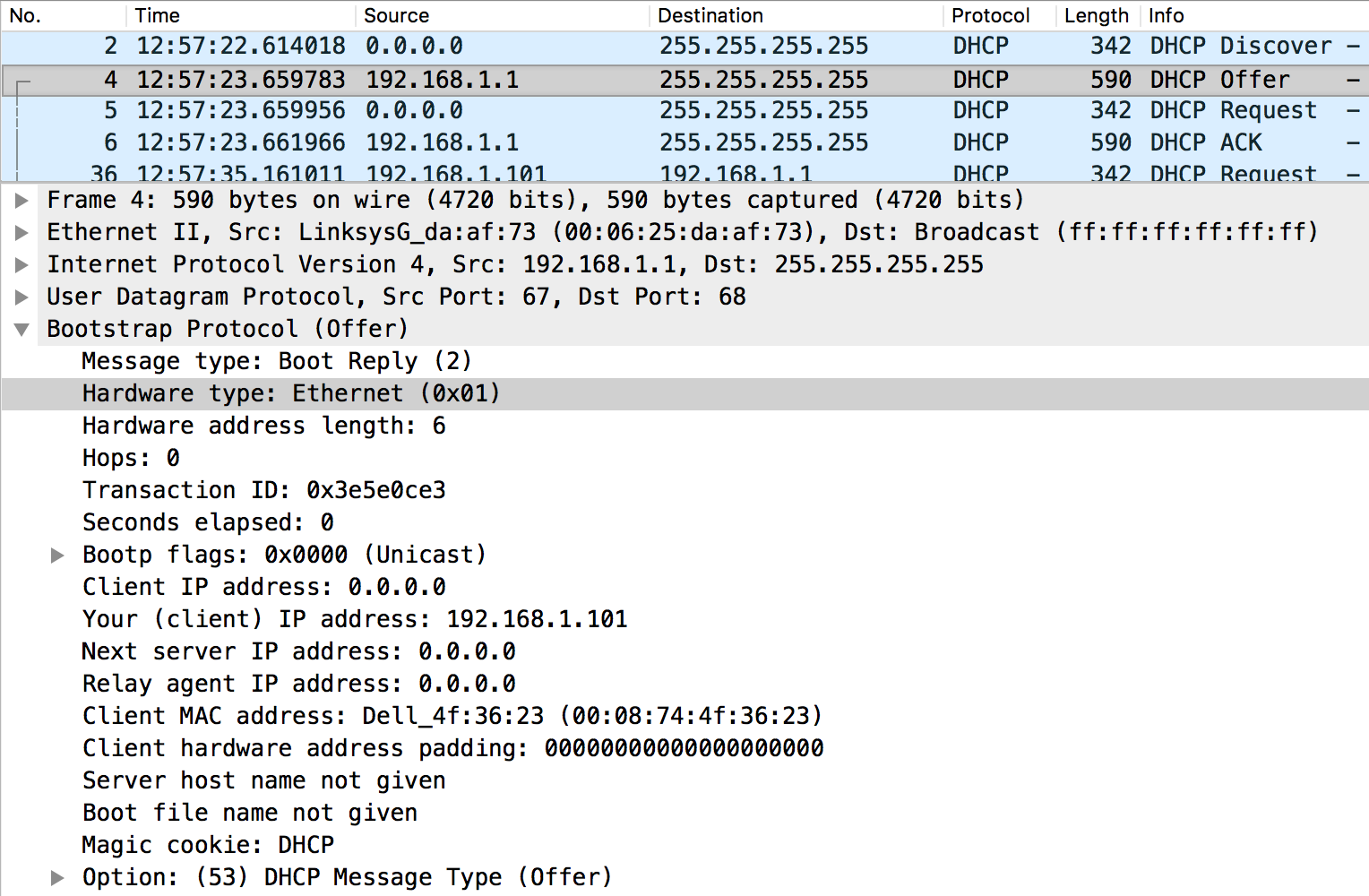
1. What is the IP address of your DHCP server?

**192.168.1.1**



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.

**The “DHCP Offer” message sent from the DHCP server contains the IP address**



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?

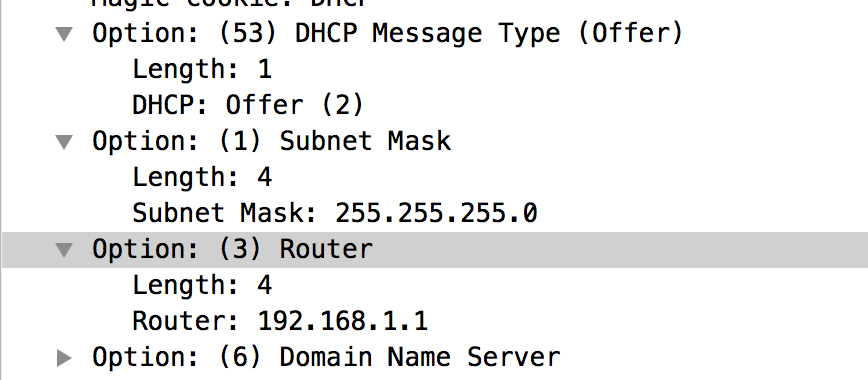
**There is no relay agent in my experiment (I used the downloaded trace).**

**You know there is not relay agent because the DHCP server is sending the traffic directly to the new client.**

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

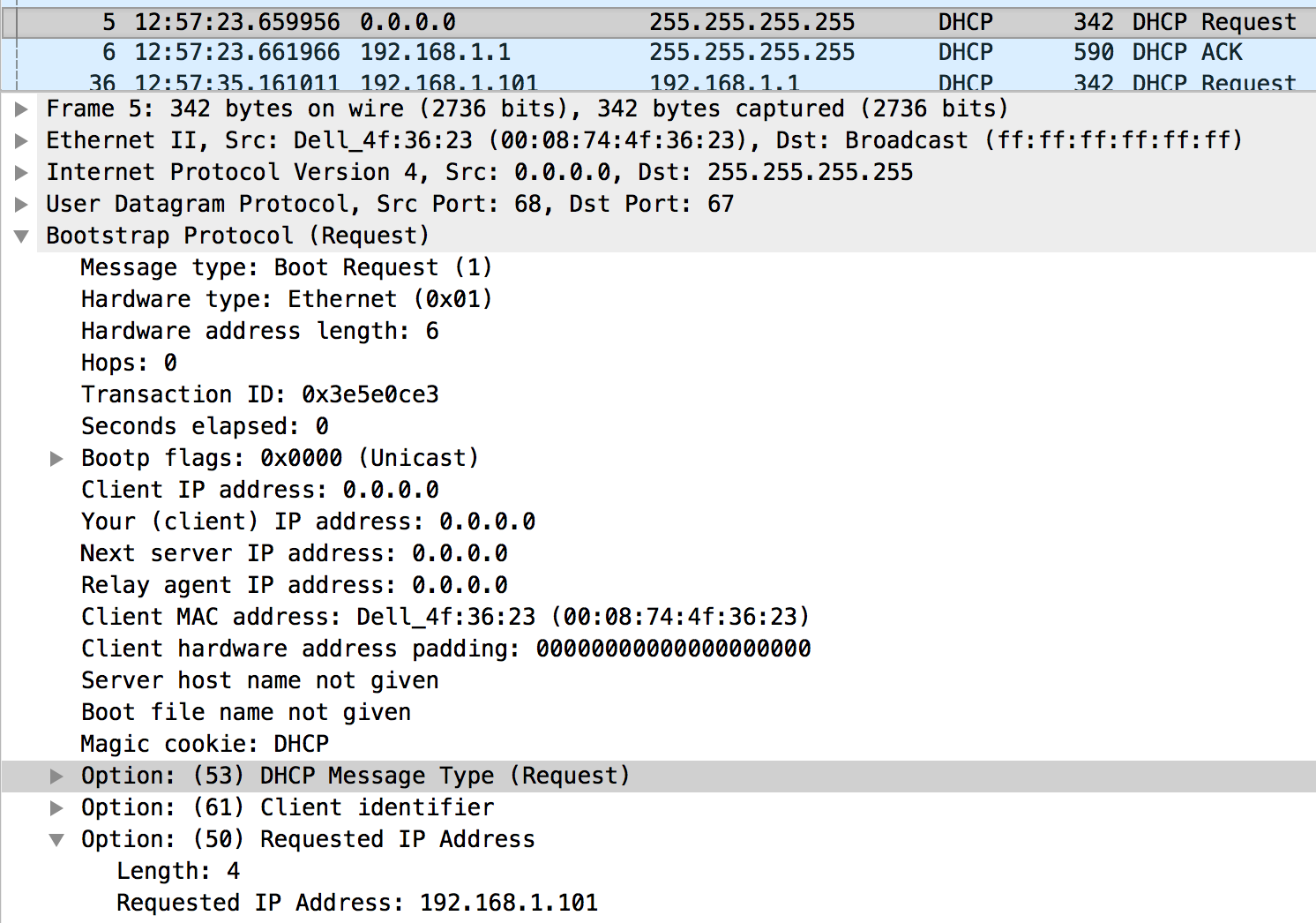
**The subnet mask tells the client the size of its subnet. Specifically, this subnet mask is a /24, meaning there is space for 255 other addresses in the subnet.**

**The router is given so the client knows where to send its outbound packets.**



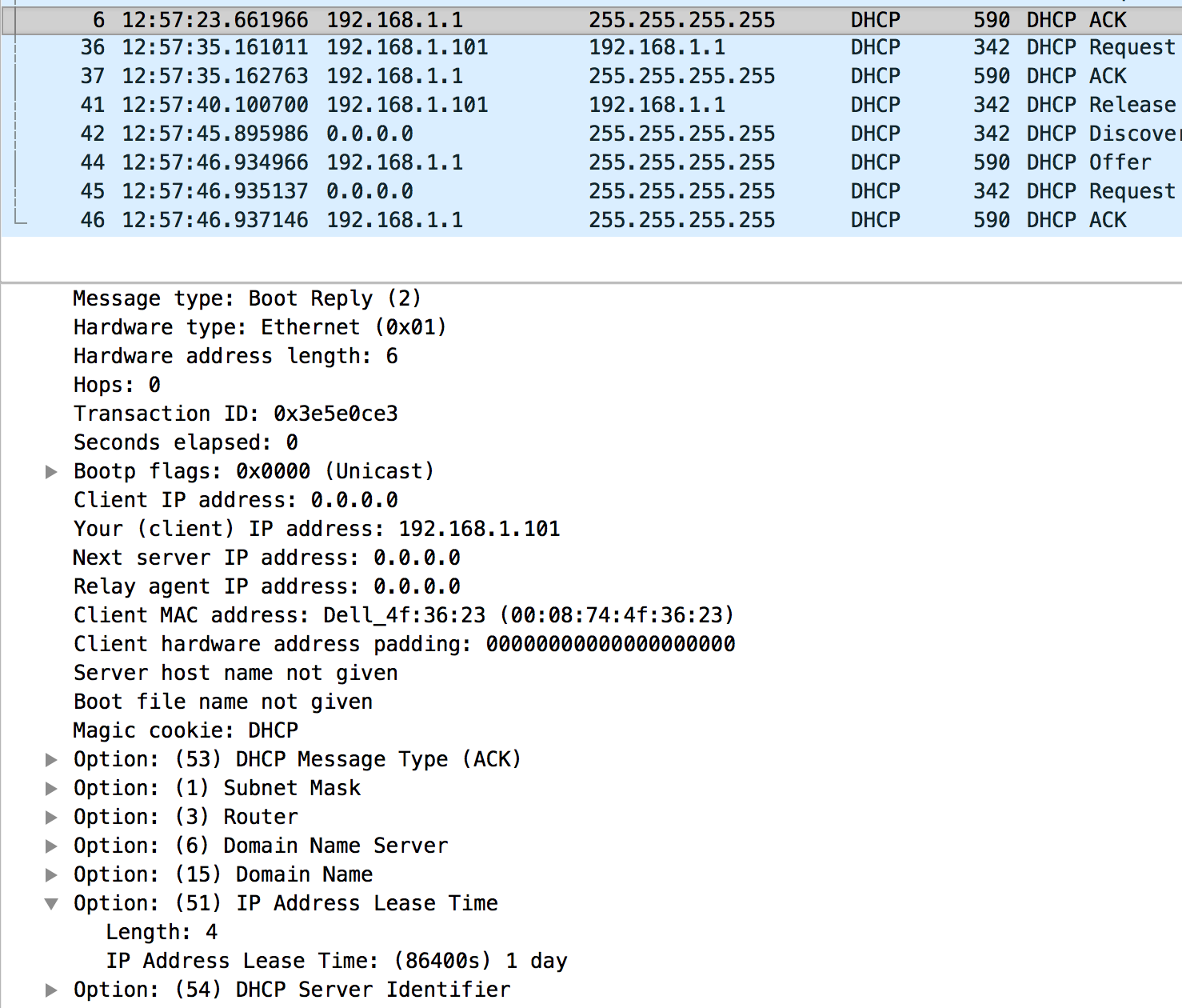
1. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client’s response to the first server OFFER message, does the client accept this IP address? Where in the client’s RESPONSE is the client’s requested address?

No, in the first response to the DHCP server, the client does not accept the IP address. We know this because the client lists their own IP address as 0.0.0.0 and lists 192.168.1.101 in the “Requested IP Address” field.



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

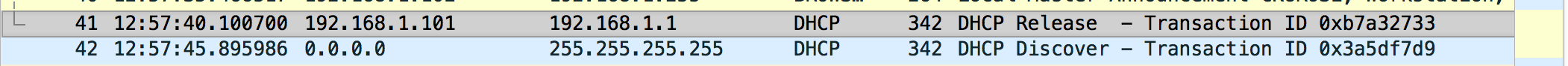
**The lease time in this experiment is 1 day. The purpose is that if the client does not renew the lease on the IP address or the server does not automatically reset the lease time, the DHCP server will take the IP address back from the client to be (potentially) assigned to a different client.**



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?

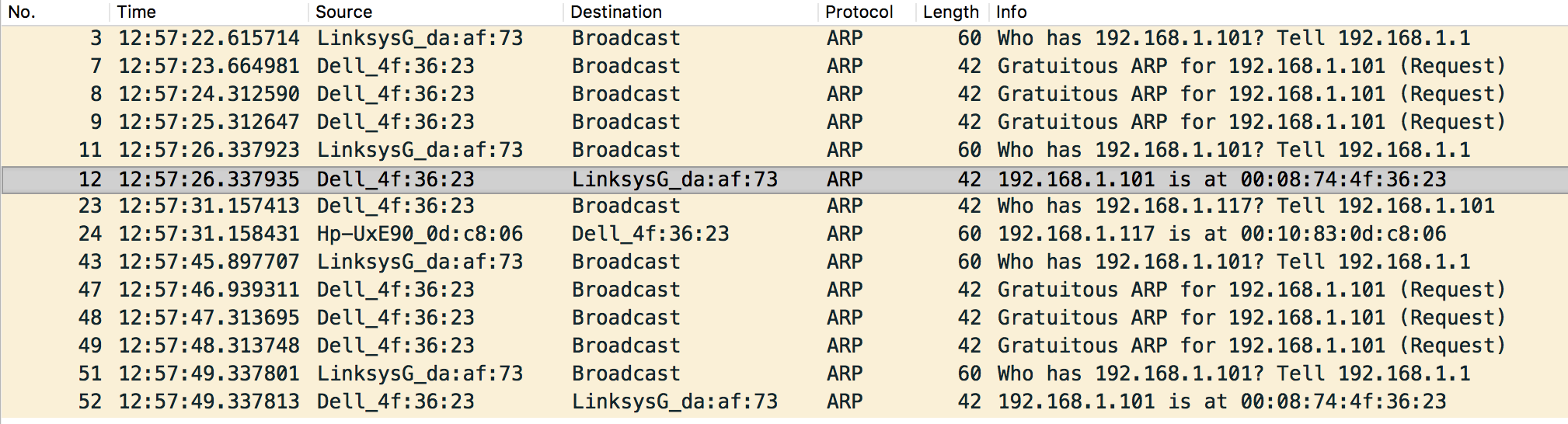
**The DHCP release message is used by the client to tell the DHCP server that it does not want to have its IP assigned. This means the DHCP server immediately puts that clients IP address back into its address bank of those IP addresses that could be allocated.**

**No, there is no ACK by the DHCP server. You can see from this screenshot that the next packet in the trace is sent by the client to the DHCP server with the IP address of 0.0.0.0 meaning the DHCP server did drop the assignment in its records.**

****

**If the client’s DHCP release message is lost, then the DHCP server will maintain the association of that client to the IP address. If the client does leave the network, then the DHCP server will have to wait until the timeout to reallocate that IP address to a new 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.

****

**Packet 3 – The router is telling everyone that if they are 192.168.1.101 (the IP address requested by the new client) that they should tell the DHCP router, so that they are not bumped from the network if the DHCP server assigns 192.168.1.101 to the new client**

**Packet 7, 8 & 9 – The new client is announcing to everyone that it is 192.168.1.101**

**Packet 12 – the new client is announcing its MAC address to the router so that it can receive messages and the router/switch can associate its MAC Address and IP.**

**Other messages are versions similar to those described above.**