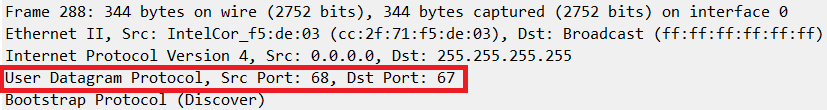
**Wireshark Lab 5 DHCP**

**Marvin Newlin**

**CSCE 560**

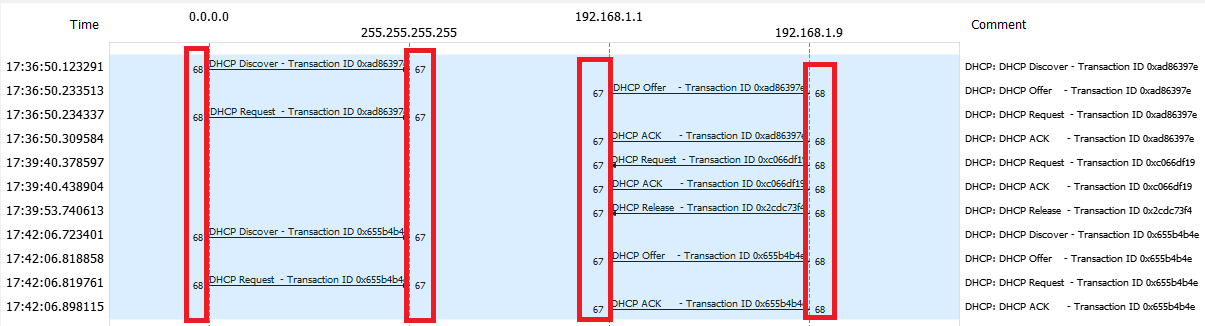
**19 Nov 18**

1. Are DHCP messages sent over UDP or TCP?



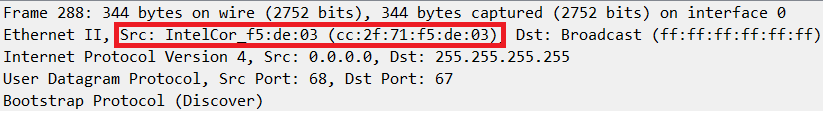
**Sol’n:** As we can see from the red box, DHCP uses UDP.

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?



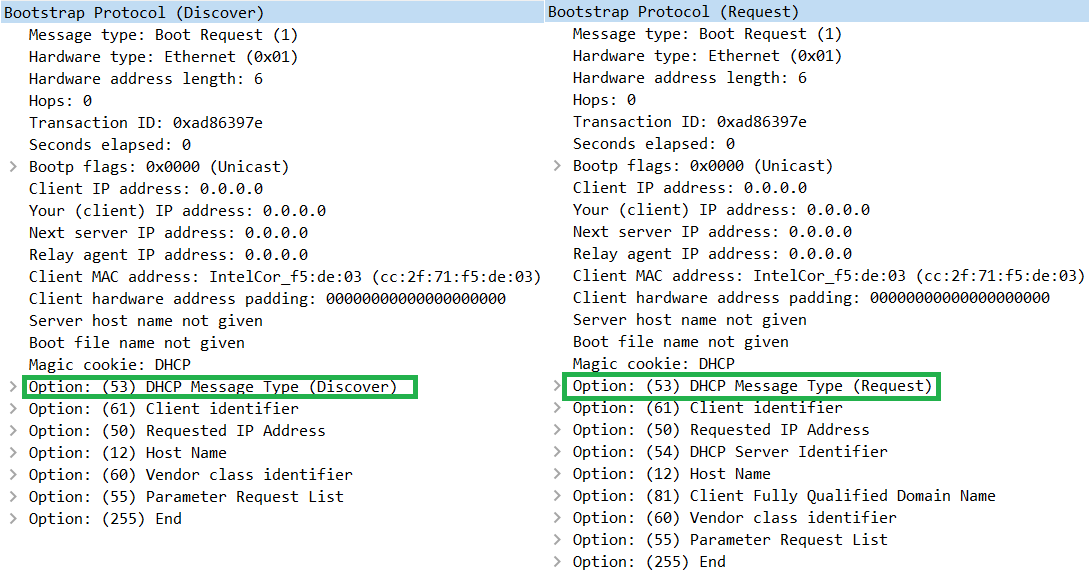
**Sol’n:** As we can see from the red boxes, DHCP uses UDP ports 67 and 68 which is the same as the example.

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



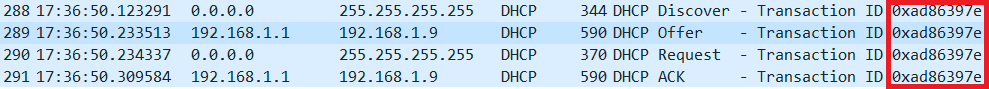
**Sol’n:** The Ethernet address is cc:2f:71:f5:de:03 as shown in the red box.

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



**Sol’n:** As we can see from the green boxes, the Option 53 DHCP Message Type is the only field that changes.

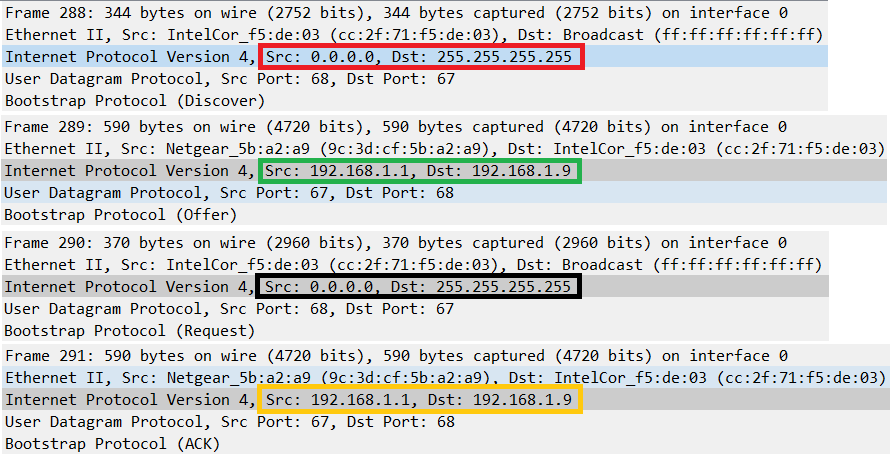
1. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?





**Sol’n:** As we can see from the red box, the transaction ID field for the first set is 0xad86397e. From the yellow box we see that the transaction ID for the second set is 0xc066df19. The purpose of the transaction ID is to differentiate between the sets of DHCP handshakes.

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.



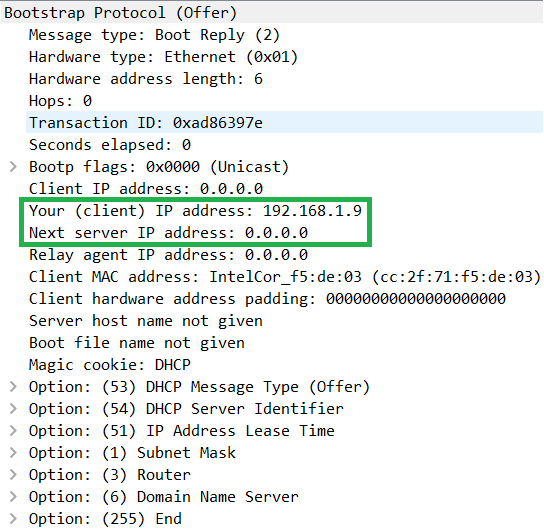
**Sol’n:**

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

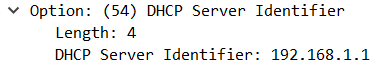
**Sol’n:** In the Green box we see the source of the DHCP Offer is 192.168.1.1 is my device’s default gateway (my router).

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.

**Sol’n:** The DHCP Offer message contains the IP address offered by the DNS Server (Green box above). The picture below shows in the green box that my device is being offered 192.168.1.9.

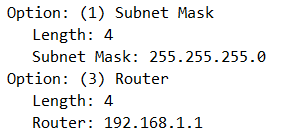


1. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?



**Sol’n:** In the Offer message above, we see that there is no relay agent since the offer is coming directly from my default gateway (picture above). If there was a relay agent, then Option 82 would be enabled, and we can see that it is not.

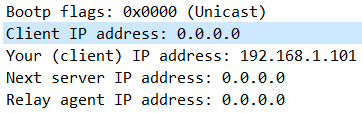
1. Explain the purpose of the router and subnet mask lines in the DHCP offer message.



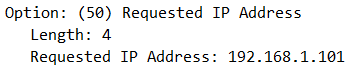
**Sol’n:** The router field tells the host what its default gateway address should be and the subnet mask tells the host what its subnet mask should be.

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?

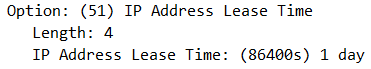
**Sol’n:** In the offer message below the server offers 192.168.1.101 to the client.



In the request message after the offer, the client does accept the offered IP address and does so with the requested IP address Option, the client requests 192.168.1.101

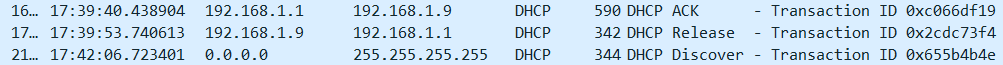


1. Explain the purpose of the lease time. How long is the lease time in your experiment?



**Sol’n:** The lease time tells the host how long they have the offered IP address for. As we can see above the lease time is one day.

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?



**Sol’n:** The DHCP release message tells the DHCP server that the host is no longer using the leased IP address. The DHCP server does not acknowledge the DHCP release message (as seen above). If the DHCP release message is lost, then the DHCP server would not be able to re-lease that IP address to another device until the lease expired.

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.



**Sol’n:** These are the Address Resolution Protocol (ARP) packets sent by my machine during the DHCP process. The purpose of these ARP packets is for my device to find out the MAC (Link Layer) address of the default gateway (device that has IP address of 192.168.1.1).