ECE 455 Wireshark Lab

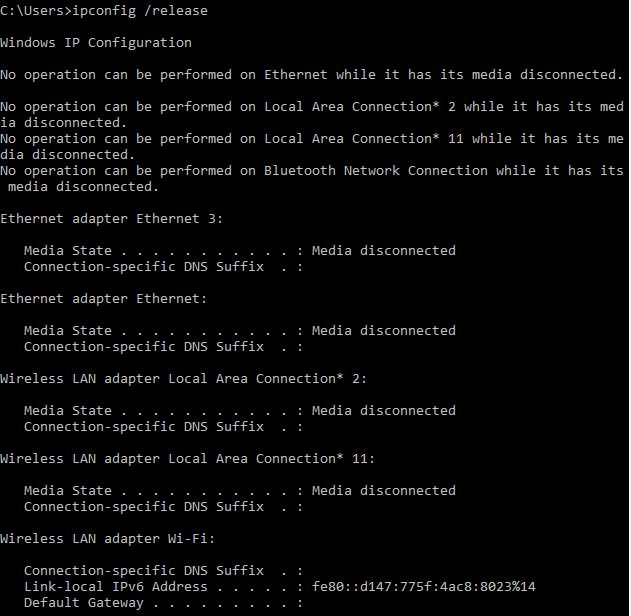
Wireshark DHCP

By: Katelynn Johnson

Due: 4/10/2019

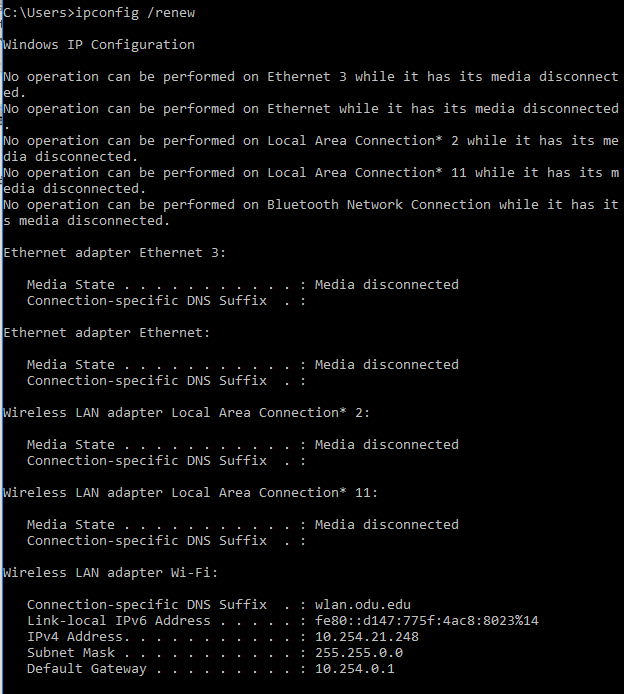
***Below are the screen captures of the “ipconfig /release” and the “ipconfig /renew” commands.***

**Command: ipconfig /release**



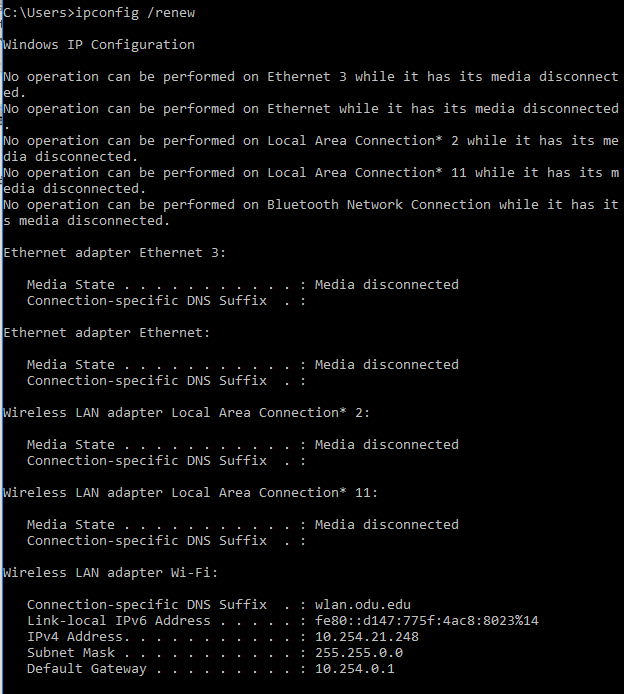
***Figure 1***

**Command: ipconfig /renew**



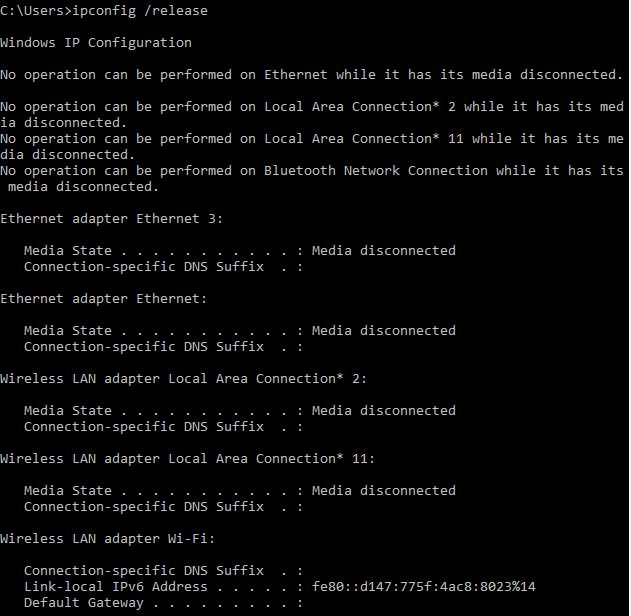
***Figure 2***

**Command: ipconfig /renew**



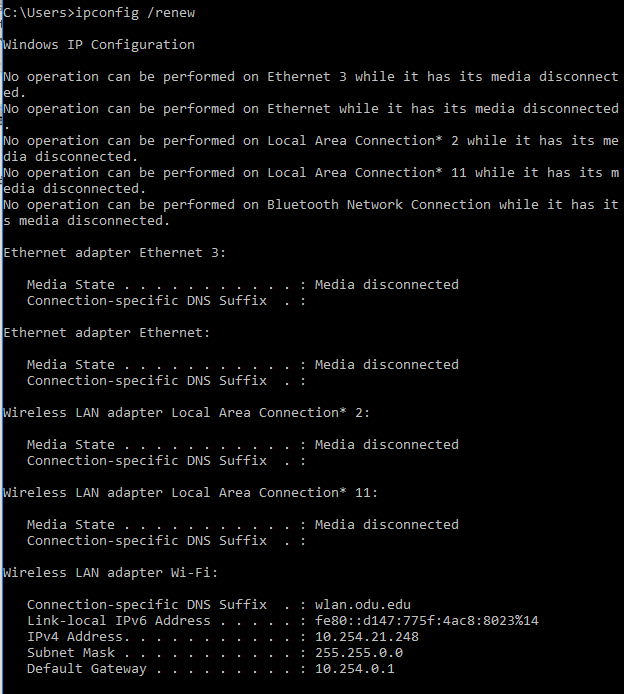
***Figure 3***

**Command: ipconfig /release**



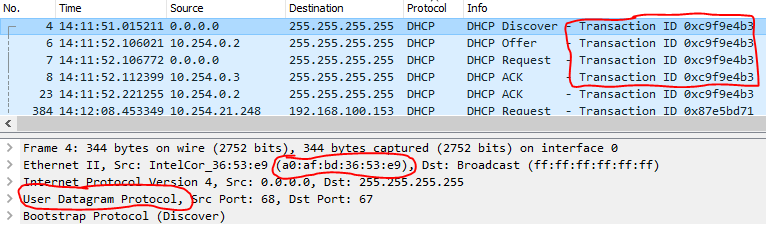
***Figure 4***

**Command: ipconfig /renew**



***Figure 5***

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

As shown in the photo below, DHCP messages 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?***

|  |  |
| --- | --- |
| ***Client*** | ***Server*** |
| ***DHCP Discover 🡪 source port: 68 dest port: 67*** | |
| ***source port: 67 dest port: 68 🡨 DHCP Offer*** | |
| ***DHCP Request 🡪 source port: 68 dest port: 67*** | |
| ***source port: 67 dest port: 68 🡨 DHCP Ack*** | |

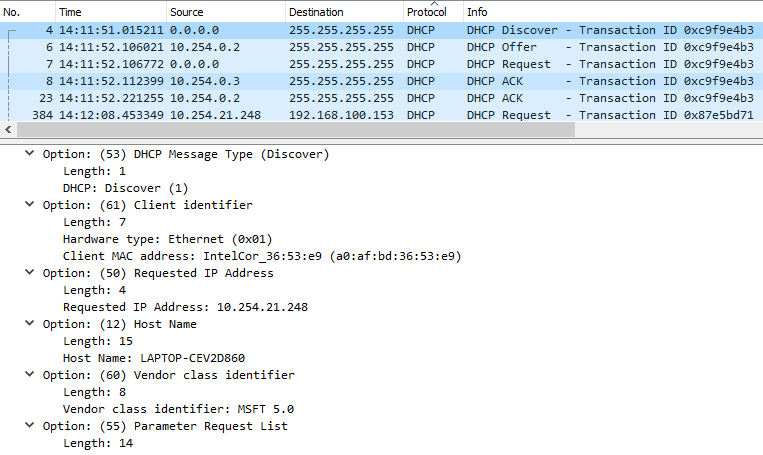
Yes, these port numbers are the same as the port numbers used in the example lab assignment given. This is because DHCP only uses the ports of UDP 67 and UDP 68.

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

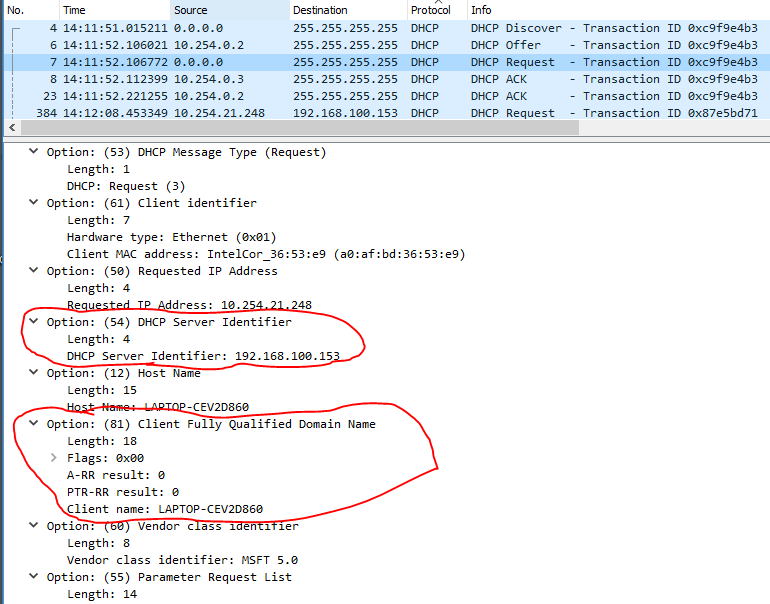
As shown in the photo from question 1, the MAC address of my host is: A0:AF:BD:36:53:E9

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

As shown by comparing the two photos below the differences in the DHCP discover message and the request message are that the DHCP request message has the sections of “DHCP Server Identifier” and “Client Fully Qualified Domain Name”

Discover message:

Request message:

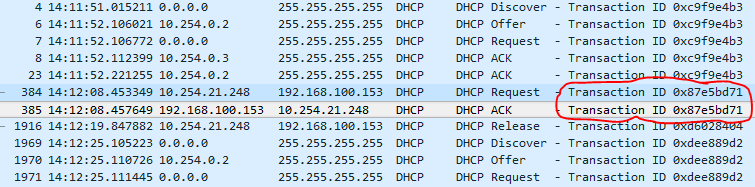


1. ***What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?***

As shown in the photo from question 1, the transaction ID for the first 4 DHCP messages is: 0xc9f9e4b3

As shown in the photo below the transaction ID for the second set of DHCP messages is: 0x87e5bd71

The purpose of these transaction ID’s is to keep track of the DHCP messages being sent and received. The Transaction ID groups the discover, offer, request, ack of a single sequence together.

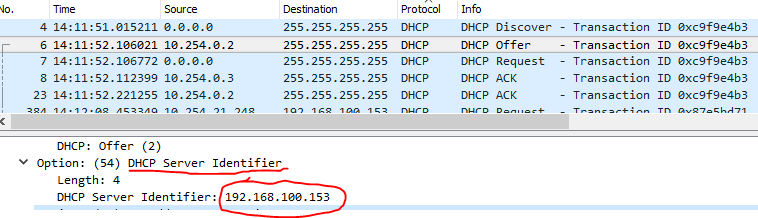


1. ***A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? 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 message type** | **Source IP address** | **Dest IP address** |
| Discover | 0.0.0.0 | 255.255.255.255 |
| Offer | 10.254.0.2 | 255.255.255.255 |
| Request | 0.0.0.0 | 255.255.255.255 |
| ACK | 10.254.0.3 | 255.255.255.255 |

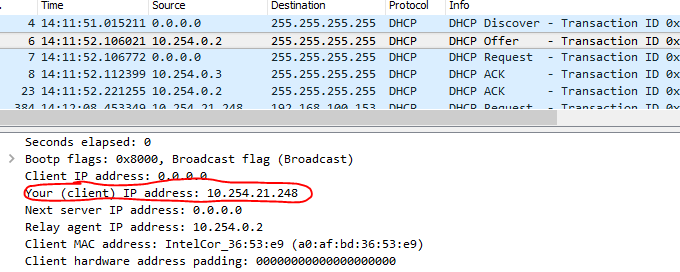


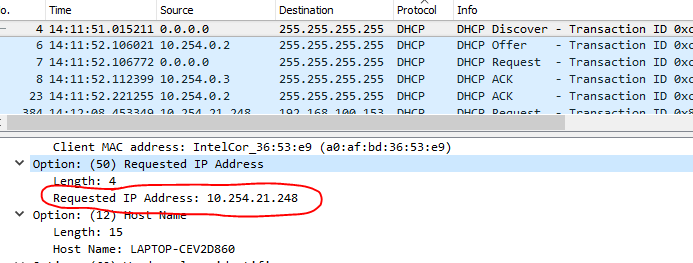
1. ***What is the IP address of your DHCP server?***

As shown in the photo below the IP address of my DHCP server is: 192.168.100.153

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.***

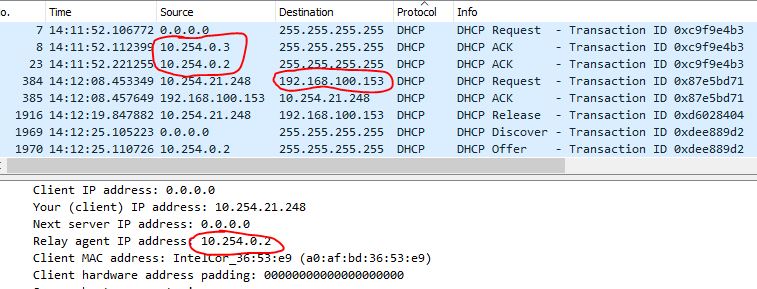
As shown in the first photo below the IP address that is being offered to my host in the DHCP offer message is: 10.254.21.248. This IP address is first seen being requested by my host in the DHCP discover message. My host is able to do this because this is the last known IP address that my host had and it is requesting it again. This is shown in the second picture below.





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?***

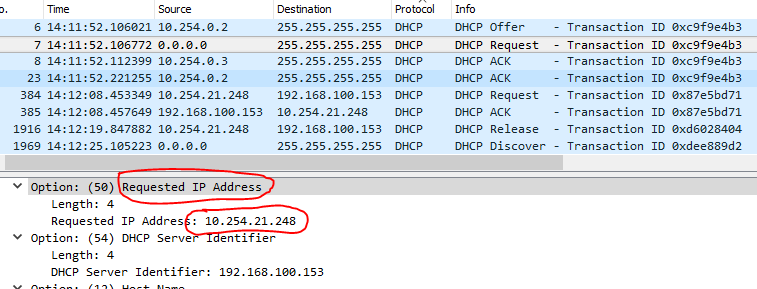
In the example screenshot for this lab the absence of a relay agent is indicated by the host receiving a direct response from the DHCP server from the beginning. This is known because when the host in the example does a second “ipconfig /renew” the destination IP address matches the course address in the first transaction. In the photo below, my experiment shows that in the first transaction there is a different IP address responding in the first transaction than in the second transaction. This is not due to multiple DHCP servers on the same subnet because the IP address are off different subnets. The relay agent IP address is: 10.254.0.3 and 10.254.0.2. All this information is shown in the photo below.



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

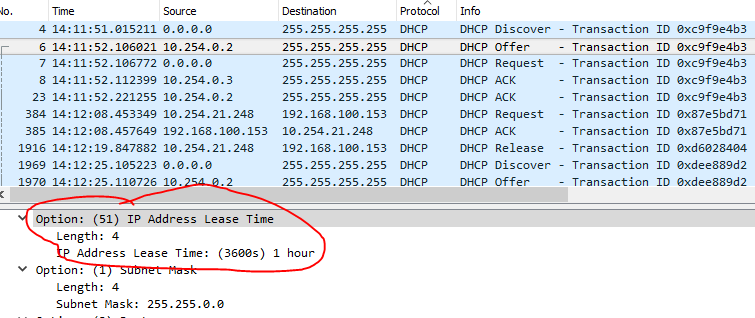
The purpose of these lines are to give the host the entire IPv4 information they will need in order to communicate on the network. The Router IP address will be the default gateway for the host.

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?***

Yes the host accepts this IP address. In the DHCP response under “Requested IP address” the IP address is: 10.254.21.248. This is shown in the photo below.

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

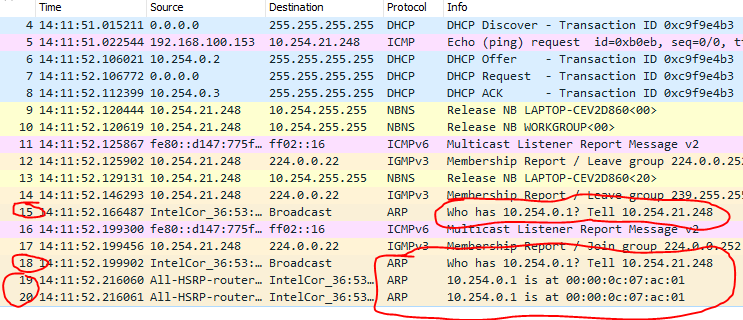
As shown in the photo below, the lease time for my experiment is 1 hour. The purpose of the lease time is so that the IP address that is leased out to your host can be recycled back into the DHCP pool. The reason this is necessary is so that IP addresses can become available when they are no longer needed.



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 purpose of the DHCP release message is for the client to inform the DHCP server that they are no longer needing the DHCP lease that they were given. No, the DHCP does not send and ACK for the DHCP release message. If the DHCP message got lost, then the DHCP server would not know that the client who sent the release no longer needed/wanted that IP address. Therefore, the IP address would not go back into the DHCP pool and it would not go back into the pool until the lease was 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.***

I did not see any ARP messages in-between the 4-way DHCP process. I did see ARP messages sent after the 4-way DHCP process was completed. This ARP message is looking for the MAC address of “10.254.0.1”, which is the IP address of the default gateway given to my host through the DHCP process.