**21CY681 - INTERNET PROTOCOL LAB - V**

Name: Akhil K J

Register Number: CB.EN.P2CYS22009

Date: 22th October 2022

Assignment Topic:  Understanding DHCP using Wireshark.

Aim :To analyse and study about DHCP using Wireshark

Tools Used: Wireshark, Command Prompt

***1. Perform the following steps to capture the DHCP traffic.***

Begin by opening the Windows Command Prompt application. Type “ipconfig /release”.

Start up the Wireshark packet sniffer.

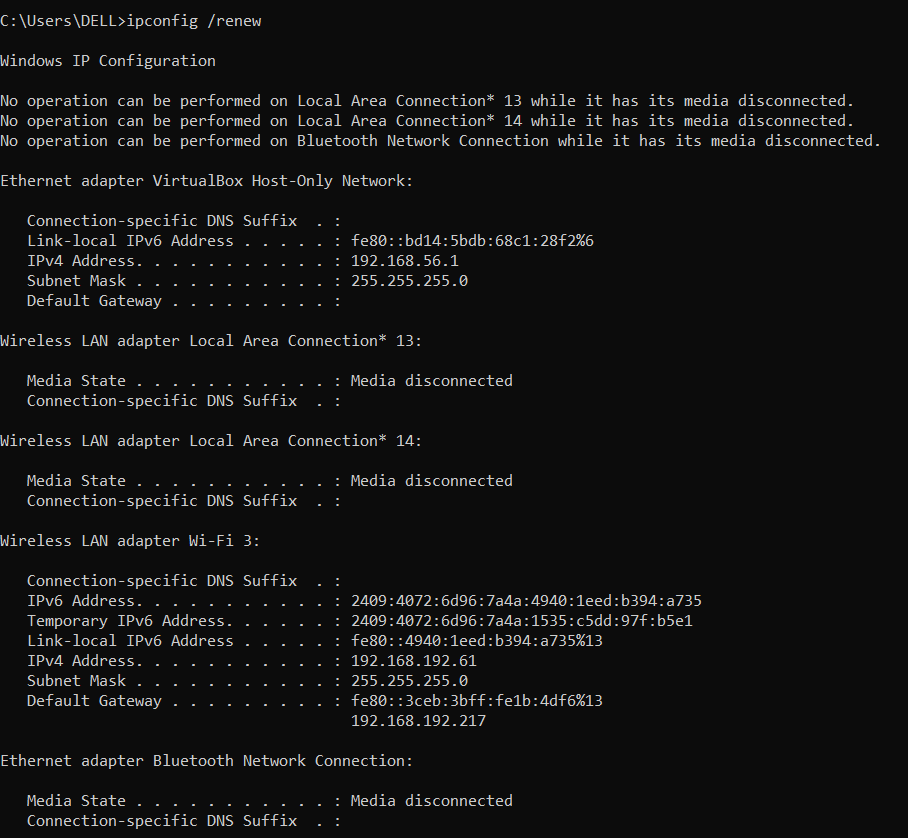
Now go back to the Windows Command Prompt and enter “ipconfig /renew”.

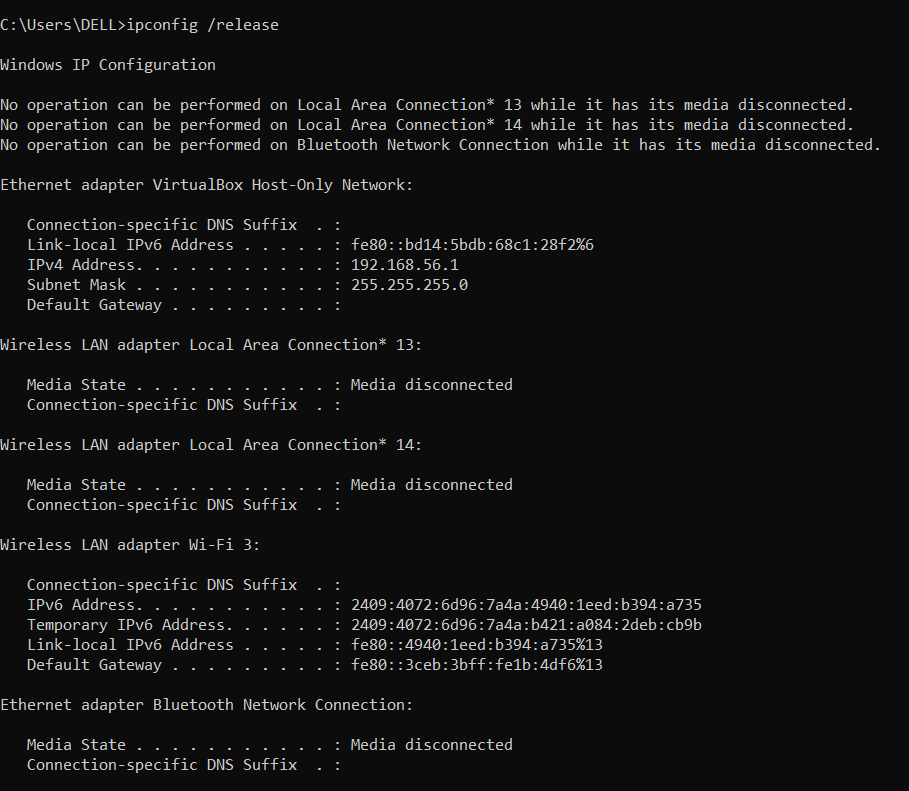
Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.

When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.

Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.

Stop Wireshark packet capture.

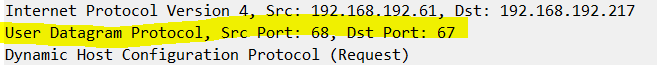




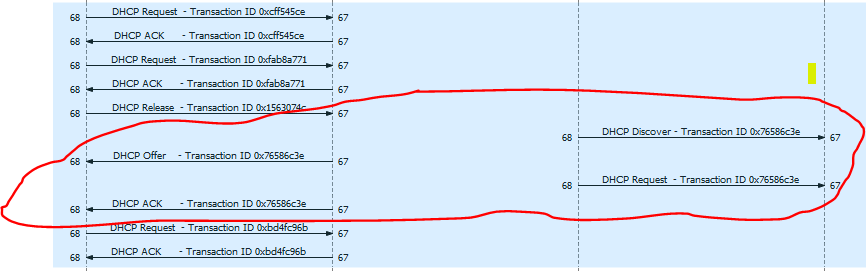
* 1. ***2. Open the captured traffic file and given pcap file “dhcp” in Wireshark to answer the following questions.***

1. Are DHCP messages sent over UDP or TCP?

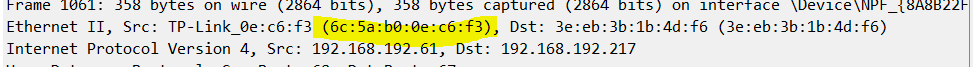
UDP



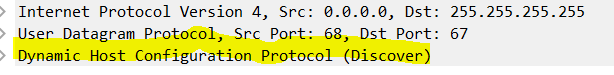
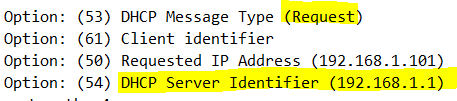
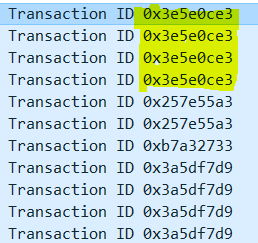
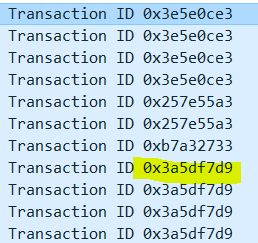
***b)*** Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers.

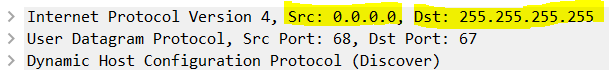
* 1. 
  2. Source number of client:68
  3. Source number of server: 67

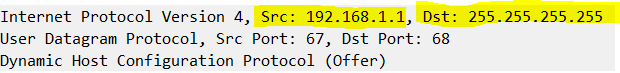
1. What is the link-layer (e.g., Ethernet) address of your host?

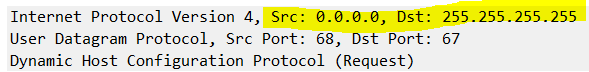


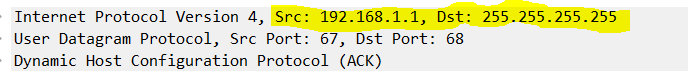
Link-layer address is:6c:5a:b0:0e:

* 1. ***d)*** What values in the DHCP discover message differentiate this message from the DHCP request message?
  2. 
  3. 
  4. Here, DHCP Request contains the DHCP Message type as Request and it has Server identifier.
  5. ***e)*** What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages?
  6. 
  7. 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?
  8. 
  9. Transaction Id is used to verify whether the transactions of packets are being done between the originals client or server or not.
  10. ***f)*** 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.
  11. Till the four transactions between client and server the IP Address of the client will be 0.0.0.0



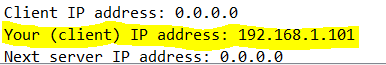






* 1. ***g)*** What is the IP address of your DHCP server?
  2. 

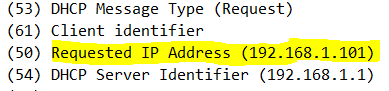
* 1. h) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.



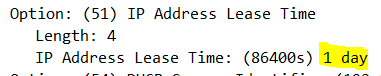
Offered IP Address: 192.168.1.101

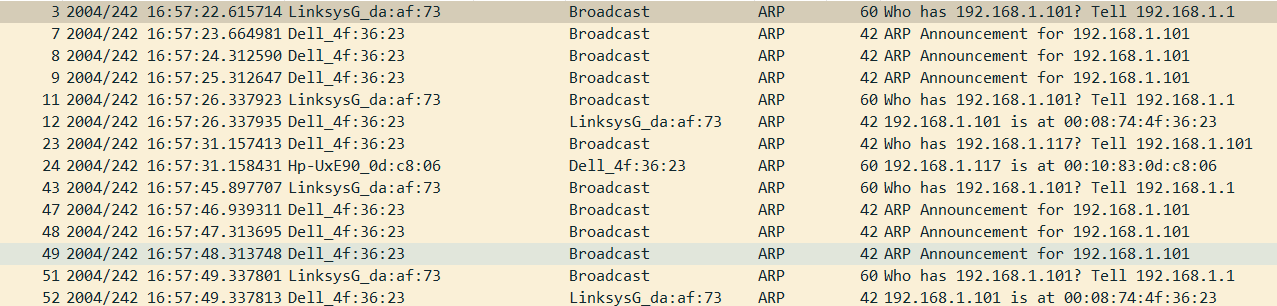
Offer and ACK

* 1. ***i)*** 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?
  2. 
  3. Is there a relay agent in your experiment? If so what is the IP address of the agent?
  4. NO
  5. ***j)*** Explain the purpose of the router and subnet mask lines in the DHCP offer message.
  6. When the DHCP server is not present in our network and if it is present in some other LAN then the DHCP DISCOVER message is sent to the router in its network. That router forwards the request packet to the network and it reaches the DHCP server in the other LAN network.
  7. ***k)*** In the DHCP trace file, the DHCP server offers a specific IP address to the client. 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?



The client accepts the offered IP Address

* 2. ***l)*** Explain the purpose of the lease time. How long is the lease time in your experiment?
  3. 
  4. An IP Address is given to a client for a certain period. This is called lease
  5. ***m)*** 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?
  6. DHCP Release Message is used to release the present IP Address provided. No, Acknowledgment is not provided. If client’s DHCP release message is lost the current IP will continue till the lease period.
  7. ***n)*** Clear the DHCP 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 , we can see many ARP packets that were transferred in the experiment since the server verifies whether the IP which is to be allocated to the requested computer is used already by any other other computer.

* 1. Result: Studied about DHCP using Wireshark