IP LAB EXPERIMENT – 5 [CYS 2022 - 2024] 31-10-2022

(Note: Total 25 marks for this lab assignment which includes 20 marks + 5 marks for your report)

For each of the following steps, describe your results, give the syntax of the command you used, and, where appropriate, the output produced. Include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and answer each question in your report.

1. ***Perform the following steps to capture the DHCP traffic.***
    a) Begin by opening the Windows Command Prompt application. Type "ipconfig /release".
    b) Start up the Wireshark packet sniffer.
    c) Now go back to the Windows Command Prompt and enter "ipconfig /renew".
    d) Wait until the "ipconfig /renew" has terminated. Then enter the same command "ipconfig /renew" again.
    e) When the second "ipconfig /renew" terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
    f) Finally, enter "ipconfig /renew" to again be allocated an IP address for your computer.
    g) Stop Wireshark packet capture.

2. ***Open the captured traffic file and given pcap file "dhcp" in Wireshark to answer the following questions.***
    a) Are DHCP messages sent over UDP or TCP?
    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.
    c) What is the link-layer (e.g., Ethernet) address of your host?
    d) What values in the DHCP discover message differentiate this message from the DHCP request message?
    e) 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?
    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.
    g) What is the IP address of your DHCP server?
    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.

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? Is there a relay agent in your experiment? If so what is the IP address of the agent?

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

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?

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

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?

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.