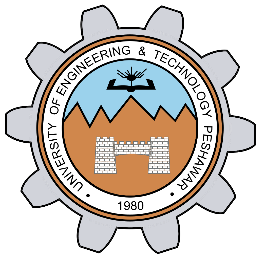
**“Wire shark lab DHCP”**

**LAB REPORT # 06**



# Spring 2023

Submitted by:

**Maaz Habib**

Registration:

**20PWCSE1952**

Class Section:  
C

Submitted to:

**Engr. Yair Saleem Afridi**

**Dated:**

05-06-2023

**Department of Computer Systems Engineering**

**University of Engineering and Technology, Peshawar.**



**Lab 06**

# Wireshark Lab: DHCP

i) In this lab, we’ll take a **quick look at DHCP**. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).

This lab is brief, as we’ll only examine the DHCP packets captured by a host. If you also have administrative access to your DHCP server, you may want to repeat this lab after making some configuration changes (such as the lease time). If you have a router at home, you most likely can configure your DHCP server. Because many linux/Unix machines (especially those that serve many users) have a static IP address and because manipulating DHCP on such machines typically requires super-user privileges, we’ll only present a Windows version of this lab below.

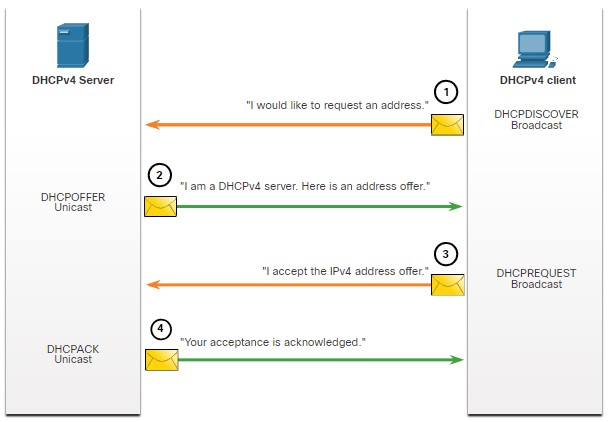
Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically. Because desktop clients typically make up the bulk of network nodes, DHCPv4 is an extremely useful and timesaving tool for network administrators. The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address.

Clients lease the information from the server for an administratively defined period.

Administrators configure DHCPv4 servers to set the leases to time out at different intervals. The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.

DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client.

* The client connects to the network with that leased IPv4 address until the lease expires. The client must contact the DHCP server periodically to extend the lease.
* This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need.
* When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.



DHCP Experiment

In order to observe DHCP in action, we’ll perform several DHCP-related commands and capture the *DHCP messages* exchanged as a result of executing these commands. Do the following:

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter **“*ipconfig /release*”.** The executable for *ipconfig* is in C:\windows\system32. This command releases your current IP address, so that your host’s IP address becomes 0.0.0.0.
2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture. 3. Now go back to the Windows Command Prompt and enter “*ipconfig /renew*”.

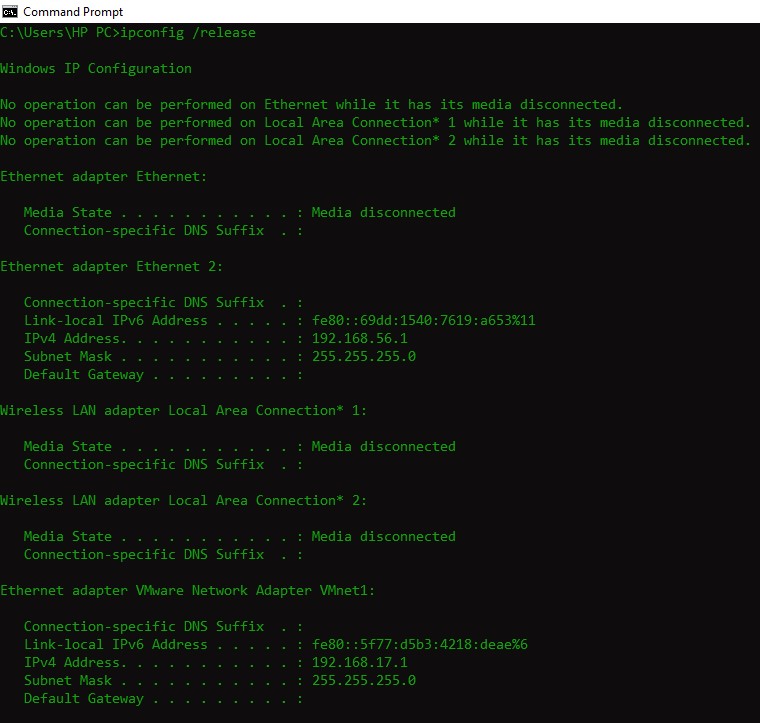
This instructs your host to obtain a network configuration, including a new IP address. In Figure

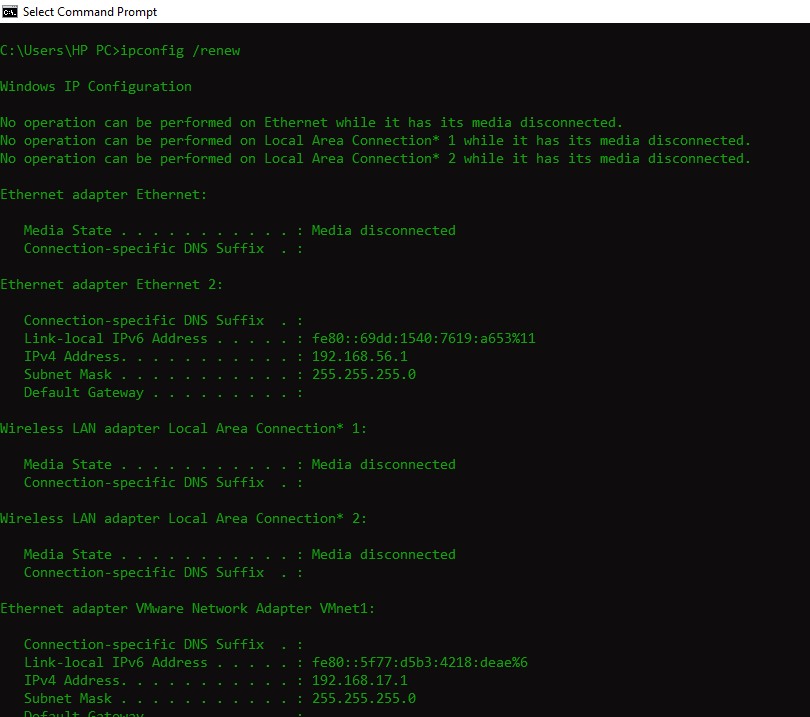
1, the host obtains the IP address 192.168.1.101

1. Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.
2. When the second “ipconfig /renew” terminates, enter the command

“ipconfig/release” to release the previously-allocated IP address to your computer.

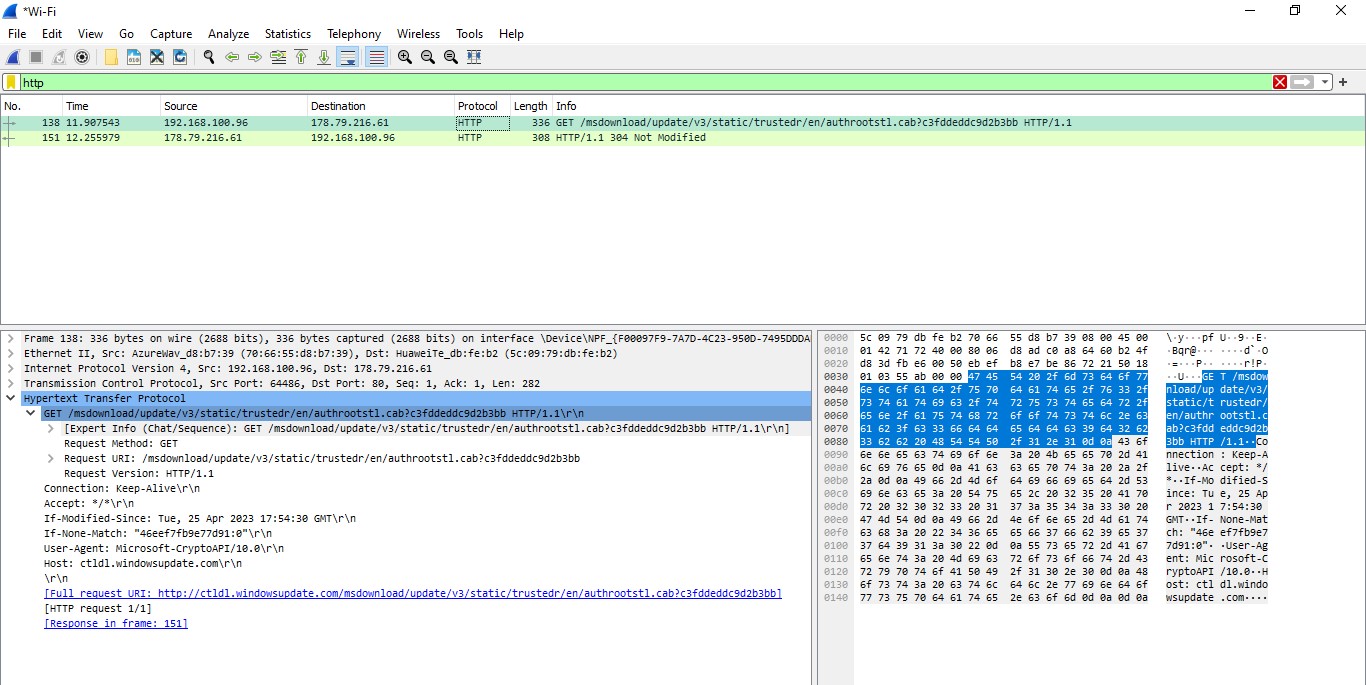
1. Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.
2. Stop Wireshark packet capture.





**Figure 1** Command Prompt window showing sequence of *ipconfig* commands that you should enter.

Now let’s take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field “bootp”. (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter “bootp” and not “dhcp” in the filter.) We see from Figure 2 that the first *ipconfig* renew command caused four DHCP packets to be generated: ***a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.***



**[I used http because BOOTP wasn’t available in the filter options]**

**Figure 2** Wireshark windows with first DHCP packet – the DHCP Discover packet – expanded.

What to Hand In:

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked.

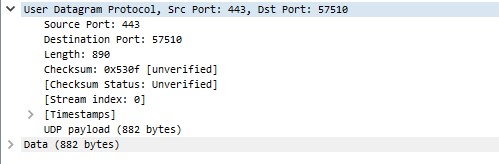
Annotate the printout3 to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

**CMD Screenshots:**

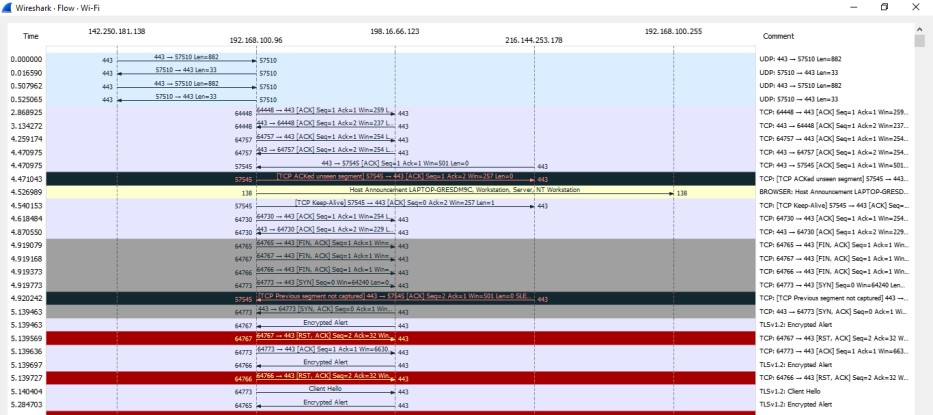
**Answer the following questions:**

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

DHCP (Dynamic Host Configuration Protocol) messages are sent over UDP (User Datagram Protocol).



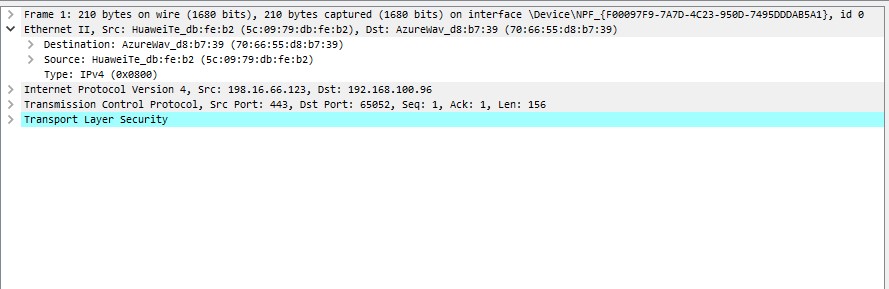
1. **Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?**



REMARKS: Can’t able to differentiate it much.

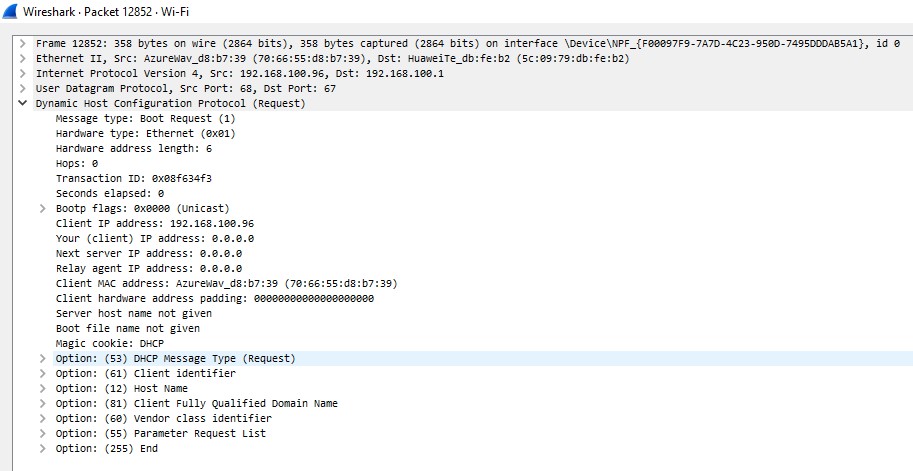
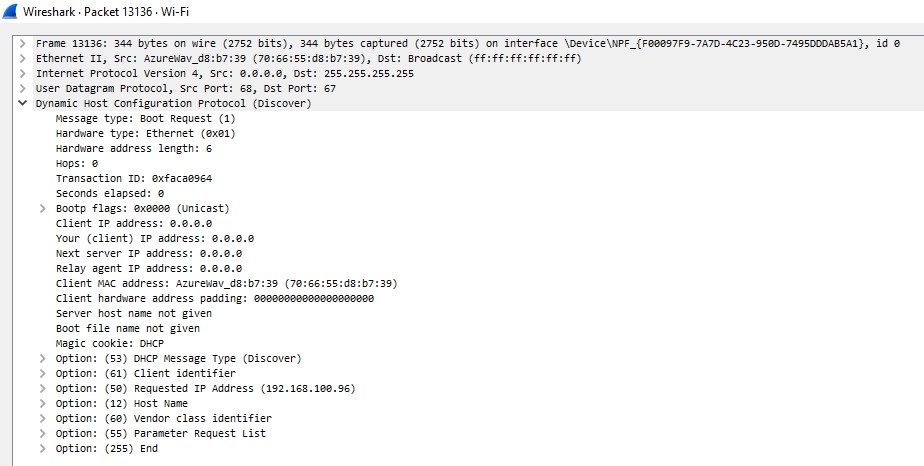
1. **What is the link-layer (e.g., Ethernet) address of your host?**

Link-layer address: **5c:09:79:db:fe:b2**



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

**Answer:** The “Option 53” in both DHCP discover and DHCP request messages differentiate each other.



**5. 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?**

**(First Four)**

**Transation-ID of Discover DHCP message** “0xfaca0964”

**Transation-ID of Offer DHCP message** “0xfaca0964”

**Transation-ID of Request DHCP message** “0x8f634f3”

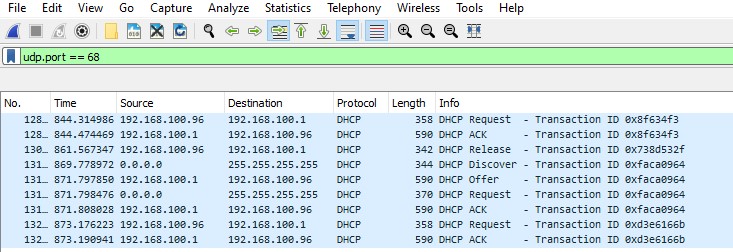
**Transation-ID of ACK DHCP message** “0x8f634f3”

**(Second set)**

**Transation-ID of Request DHCP message** “0xfaca0964”

**Transation-ID of ACK DHCP message** “0xfaca0964”

**Purpose** to associate and match DHCP messages that belong to the same transaction.



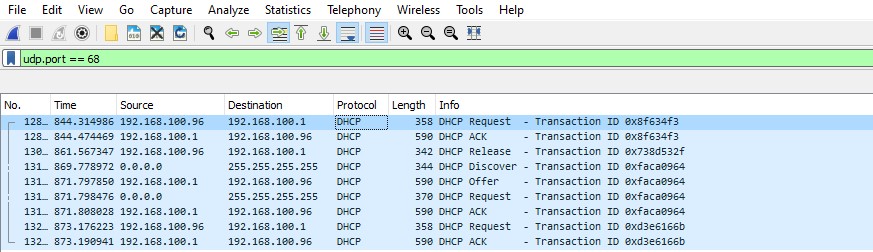
1. **A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange?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

Discover IP address = 255.255.255.255

Offer IP address = 192.168.100.96

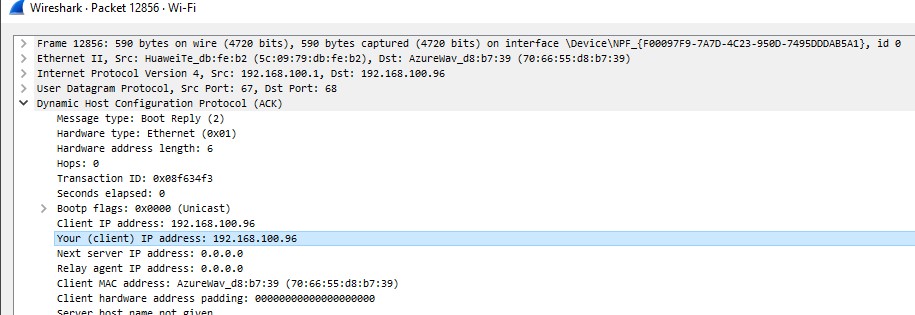
Request IP address = 192.168.100.1

ACK IP address = 192.168.100.96



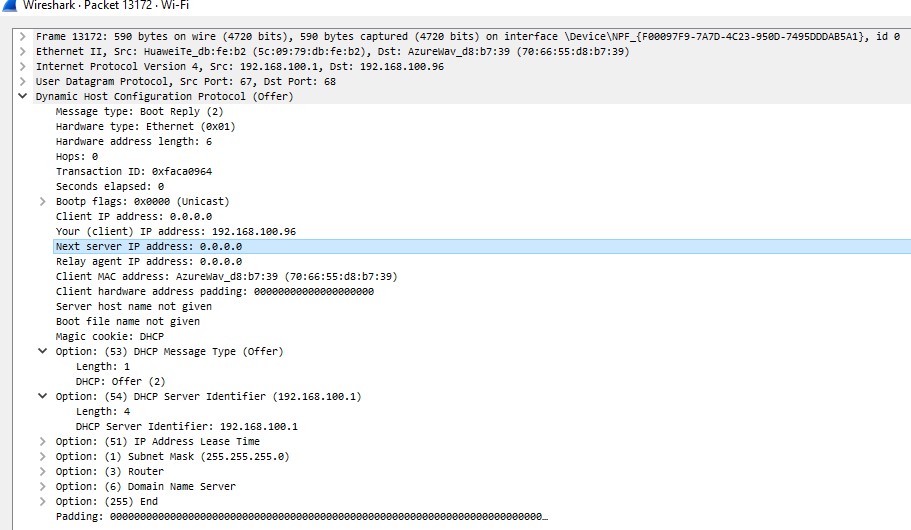
1. **What is the IP address of your DHCP server?**

**IP Address of DHCP server:** 192.168.100.96



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 IP Address being offered to the host in DHCP Offer message is “0.0.0.0”. The “Option 53” contains the DHCP message type with length of 1 and DHCP Offer is 2.

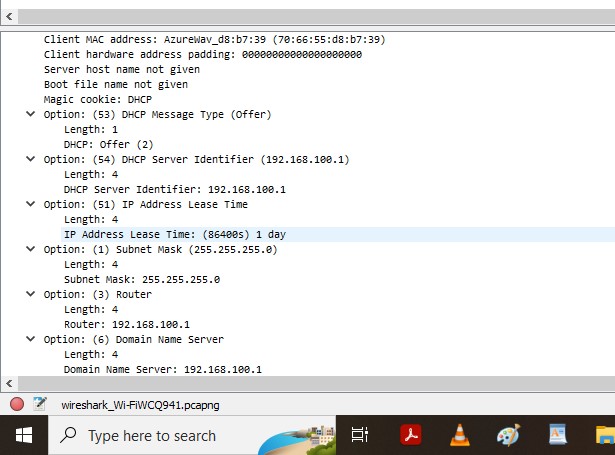


1. **Explain the purpose of the router and subnet mask lines in the DHCP offer message.**

The subnet mask line tells the client which subnet mask should be used.

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

The purpose of lease time in DHCP (Dynamic Host Configuration Protocol), is used to limit a client to use an IP Address and other network configuration parameters provided by the DHCP server. I had been assigned with 1 day equivalent Lease Time.



**13. 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?**

A DHCP release message is for the client to inform the DHCP server that it no longer requires the IP address lease and associated network configuration.

Yes, the DHCP server issues an acknowledgement of receipt of the client’s DHCP request by sending a DHCP ACK message for confirmation of successful allocation of the requested IP address.

If a client’s DHCP release message is lost, the server remains unaware that the client has released the IP Address by acknowledging the IP Address as leased to the client.