**Wireshark Lab DHCP**

**LAB # 07**



**Spring 2025**

Submitted by: **Mohsin Sajjad**

Registration No: **22pwsce2149**

Class Section: **A**

“On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work.”



Student Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submitted to:

**Dr. Yasir Saleem Afridi**

Month Day, Year (06 05, 2025)

Department of Computer Systems Engineering

University of Engineering and Technology, Peshawar

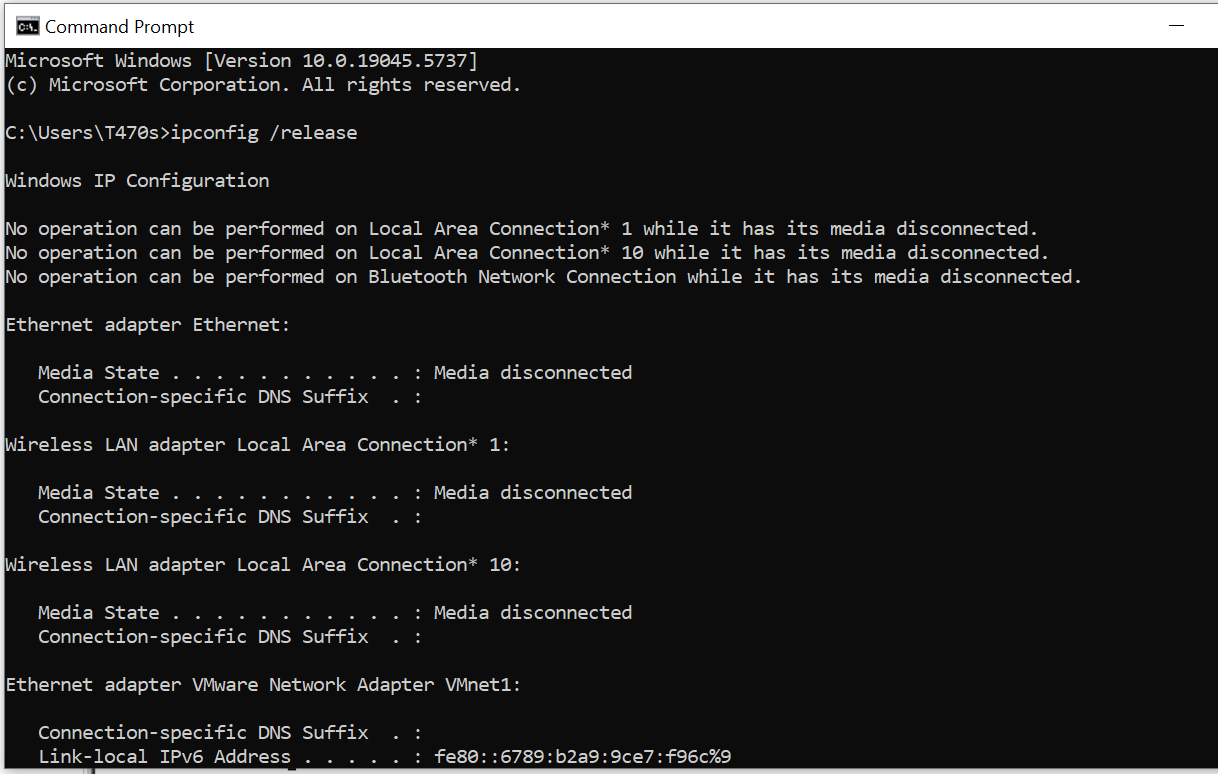
**CSE 303L: Data Communication and Computer Networks**

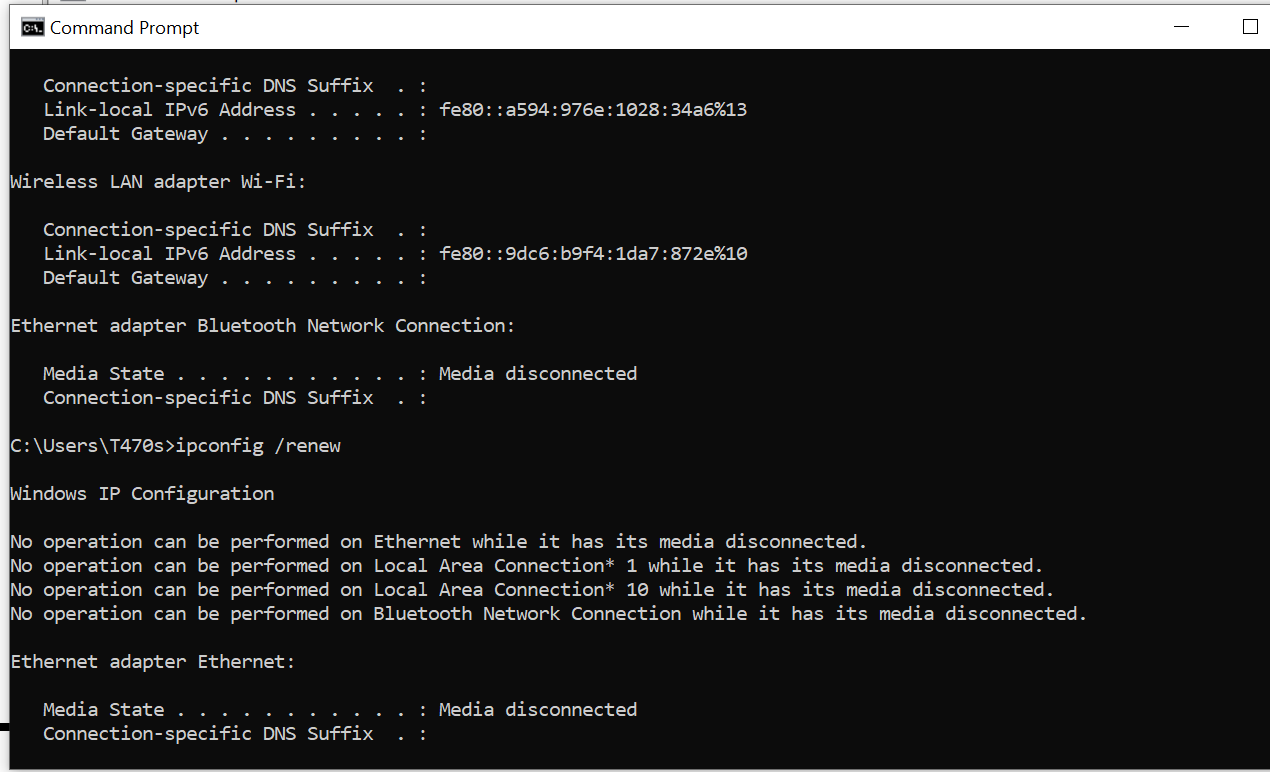
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Demonstration of Concepts** | **Poor (Does not meet expectation (1))**  The student failed to demonstrate a clear understanding of the assignment concepts | **Fair (Meet Expectation (2-3))**  The student demonstrated a clear understanding of some of the assignment concepts | **Good (Exceeds Expectation (4-5)**  The student demonstrated a clear understanding of the assignment concepts | **Score**  **30%** |
| **Accuracy** | The student mis-configured enough network settings that the lab computer couldn't function properly on the network | The student configured enough network settings that the lab computer partially functioned on the network | The student configured the network settings that the lab computer fully functioned on the network | **30%** |
| **Following Directions** | The student clearly failed to follow the verbal and written instructions to successfully complete the lab | The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab | The student followed the verbal and written instructions to successfully complete requirements of the lab | **20%** |
| **Time Utilization** | The student failed to complete even part of the lab in the allotted amount of time | The student failed to complete the entire lab in the allotted amount of time | The student completed the lab in its entirety in the al | **20%** |

**Credit Hours: 1**

# **Objectives**

1. 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).
2. DHCP Experiment
3. In order to observe DHCP in action, we’ll perform several DHCP-related commands and
4. capture the *DHCP messages* exchanged as a result of executing these commands. Do the following:
5. 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.
6. 2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark
7. lab and begin Wireshark packet capture.
8. 3. Now go back to the Windows Command Prompt and enter “*ipconfig /renew*”.
9. 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
10. 4. Wait until the “ipconfig /renew” has terminated. Then enter the same command
11. “ipconfig /renew” again.
12. 5. When the second “ipconfig /renew” terminates, enter the command
13. “ipconfig/release” to release the previously-allocated IP address to your computer.
14. 6. Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.
15. 7. Stop Wireshark packet capture.





Now let’s take a look at the resulting Wireshark window. To see only the DHCP packets,

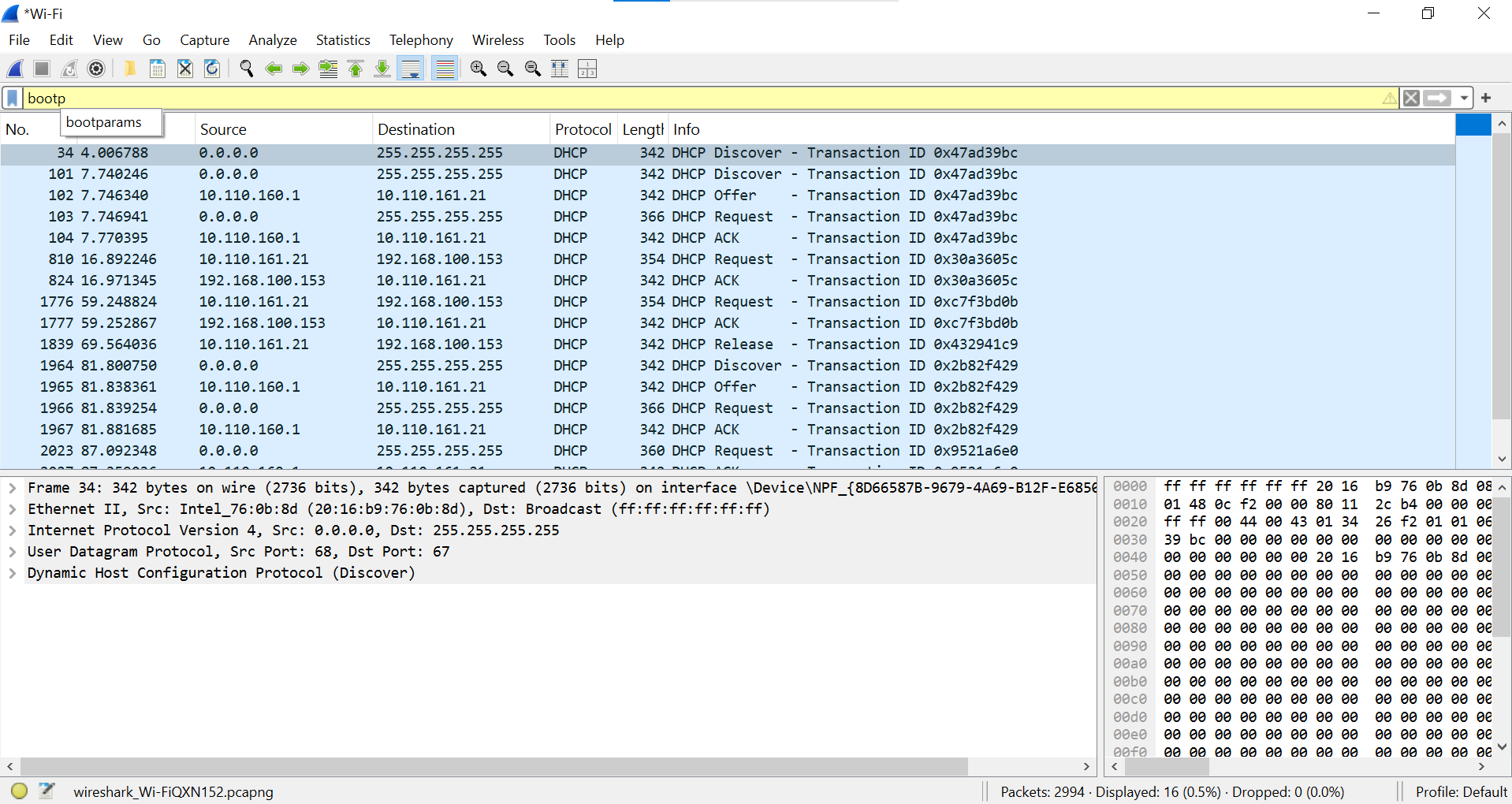
enter into the filter field “bootp”. (DHCP derives from an older protocol called BOOTP.

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 “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.***



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

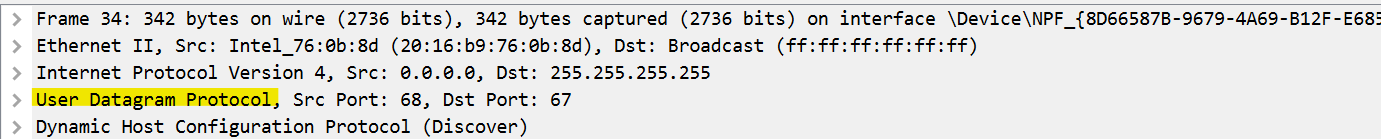
Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

Answer the following questions:

**Question 01:**

Are DHCP messages sent over UDP or TCP?

**Answer:**  
UDP



**Question 02:**

Draw a timing datagram illustrating the sequence of the first four-packet

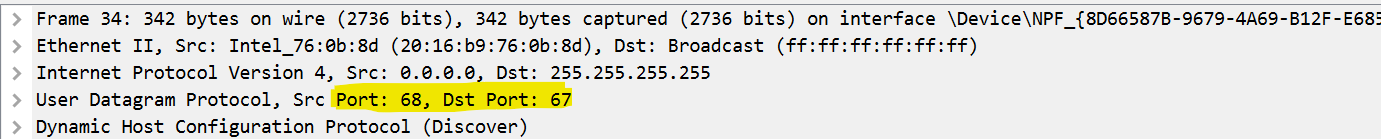
Discover/Offer/Request/ACK DHCP exchange between the client and server. For

each packet, indicated the source and destination port numbers. Are the port

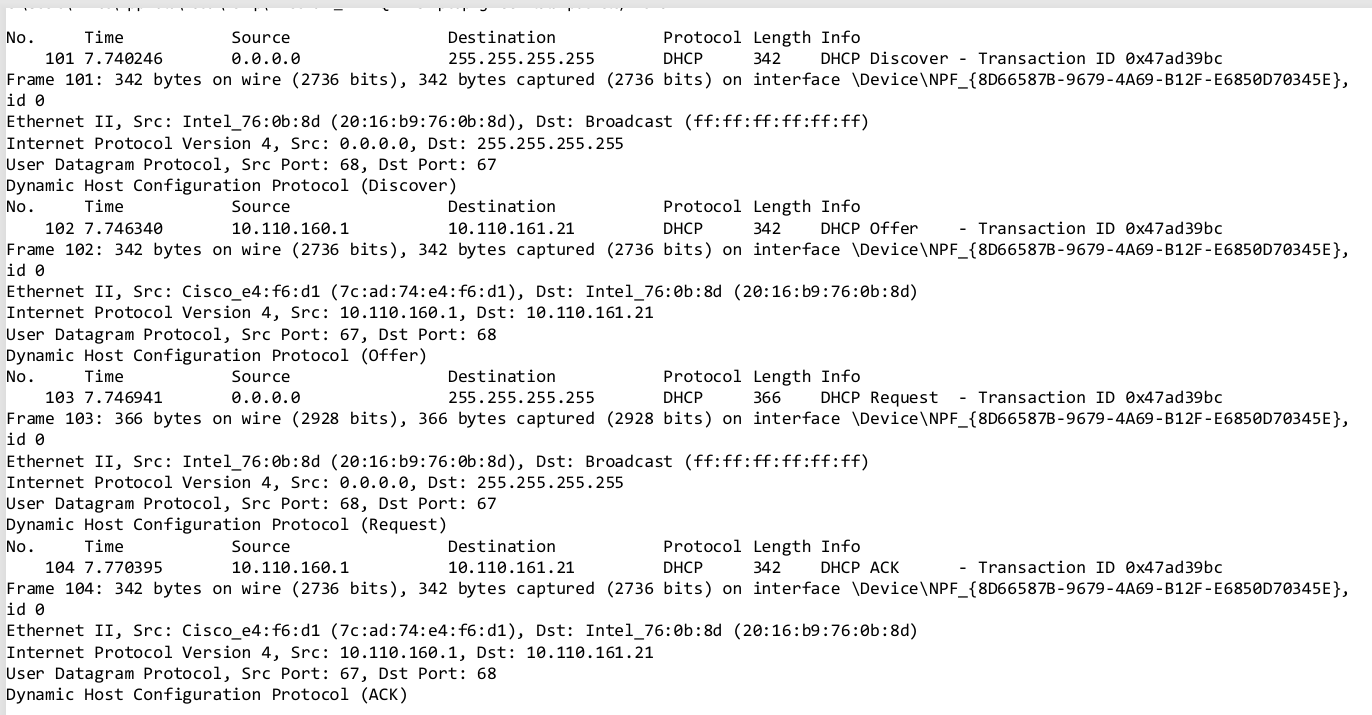
numbers the same as in the example given in this lab assignment?

**Answer:**

Yes, the port number is same 67,68.



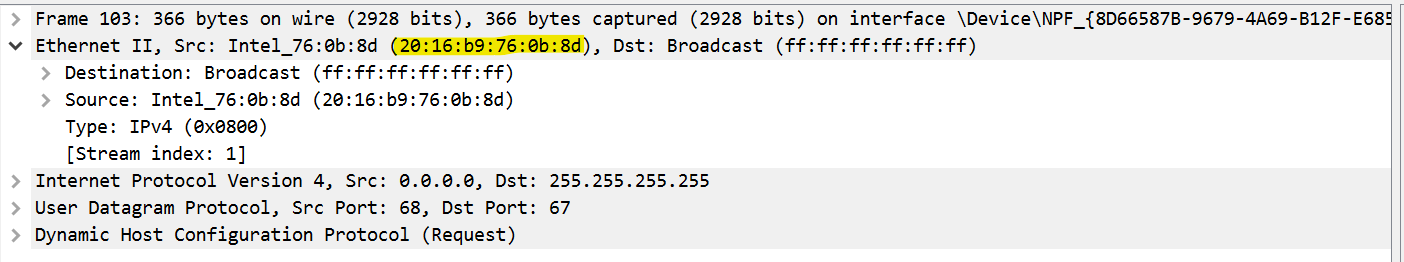
**Timing diagram of first four packets:**



**Question 03:**

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

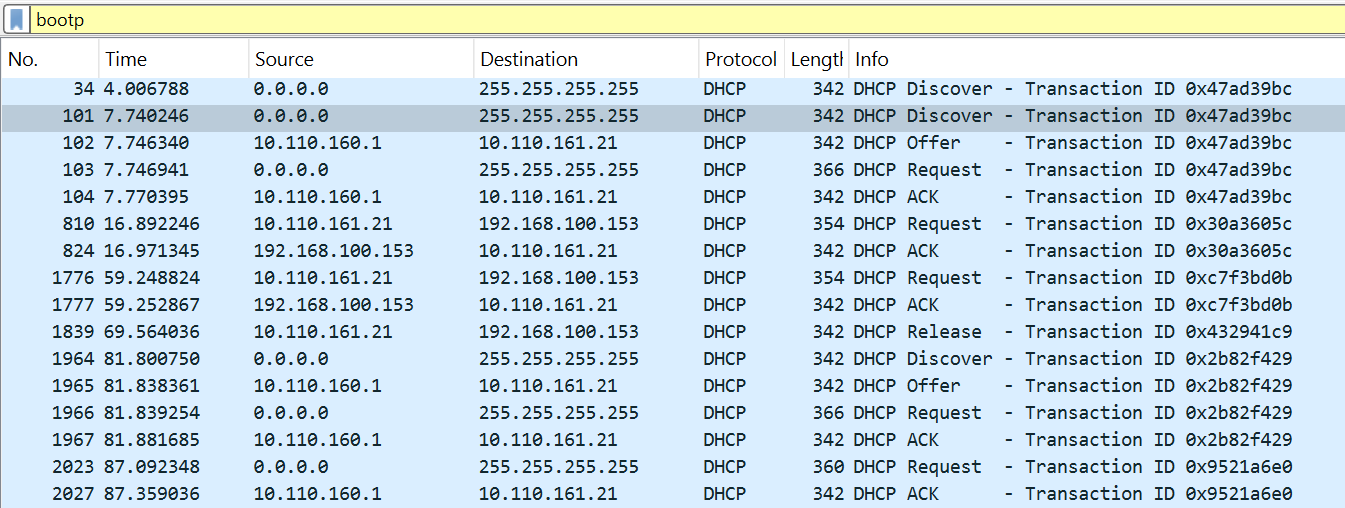
**Answer:**

****

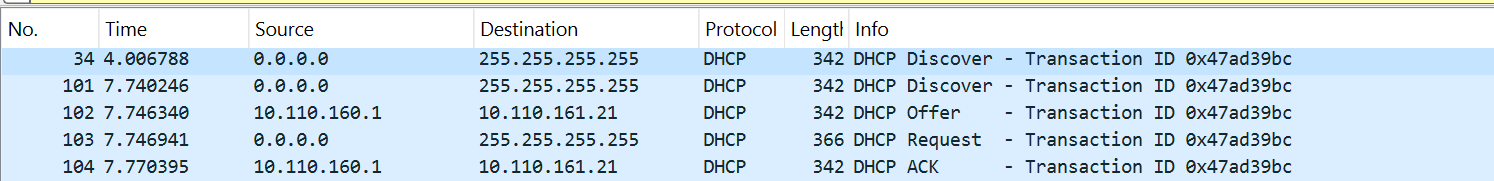
**Question 04:**

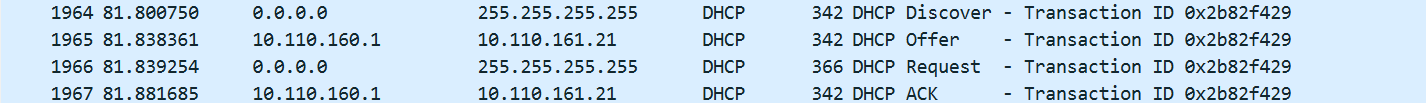
What values in the DHCP discover message differentiate this message from the DHCP request message?

**Answer:**

****

**Question 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?

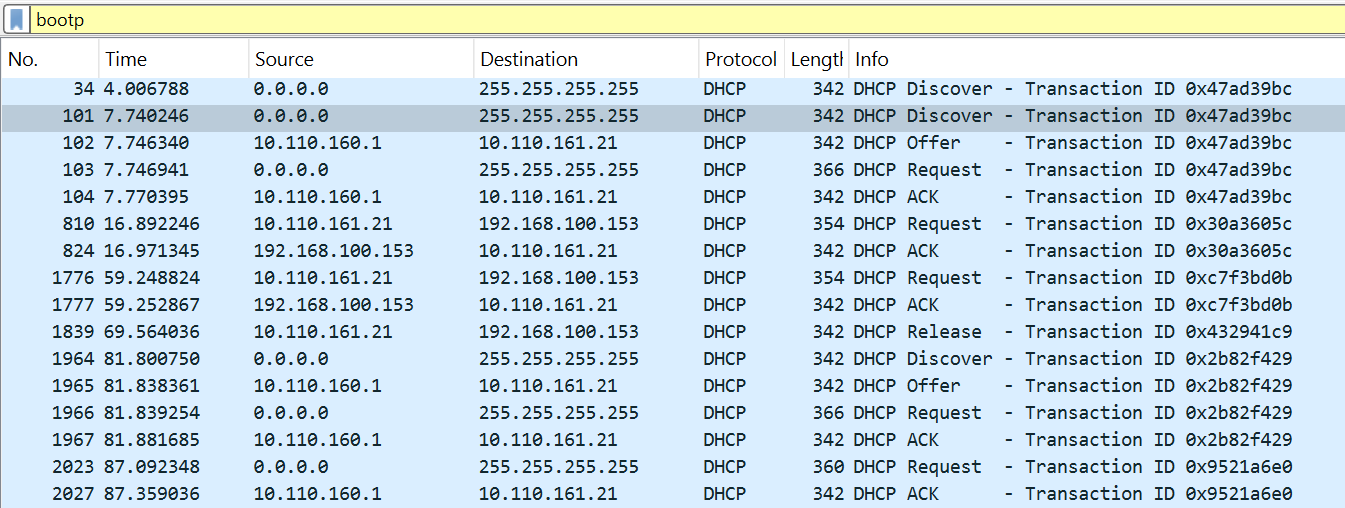
**Answer:  
**

****

**Purpose:**The **Transaction-ID** is a random number chosen by the client to help **match its request with the correct response** from the DHCP server. It avoids confusion when multiple clients are talking to the server at the same time.

**Question 06:**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.

**Answer:**

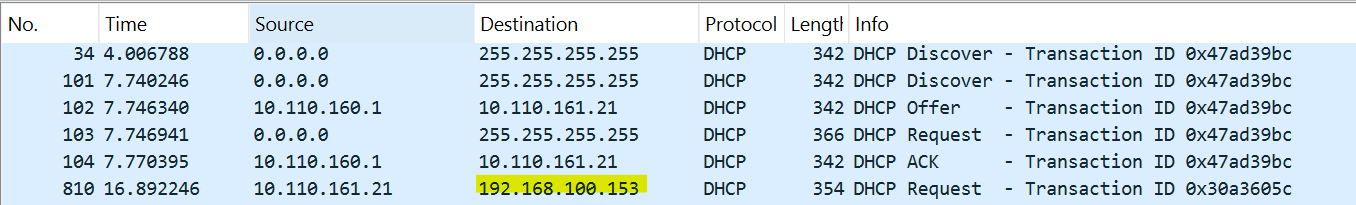
****The client starts with no IP address, so it uses 0.0.0.0 as source.

It sends to broadcast (255.255.255.255) to reach any DHCP server.

The server responds via broadcast (or unicast if the client supports it).

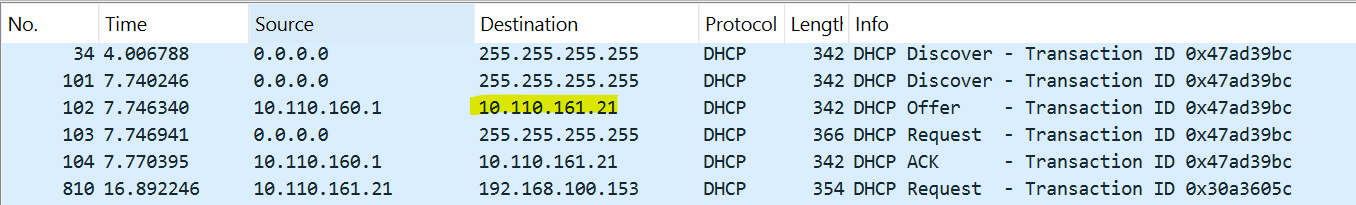
**Question 07:**

What is the IP address of your DHCP server?

**Answer:  
**

**Question 08:**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.

**Answer:**

****

**Question 09:**Explain the purpose of the router and subnet mask lines in the DHCP offer message.

**Answer:**

* **Router:** Provides the gateway address for the client to access external networks.
* **Subnet Mask:** Defines the client's local network range, helping it identify local and remote addresses.

**Question 10:**

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

**Answer:**The **lease time** is how long a client can use an IP address before renewing it, and its duration depends on the DHCP server settings.

****

**Question 11:**

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?

**Answer:**The **DHCP release message** tells the server the client is giving up the IP address; the server doesn't acknowledge it, and if lost, the server may keep the address until the lease expires.