

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.”

A handwritten signature in black ink that reads "Mohsin Sajjad".

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

Credit Hours: 1

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%

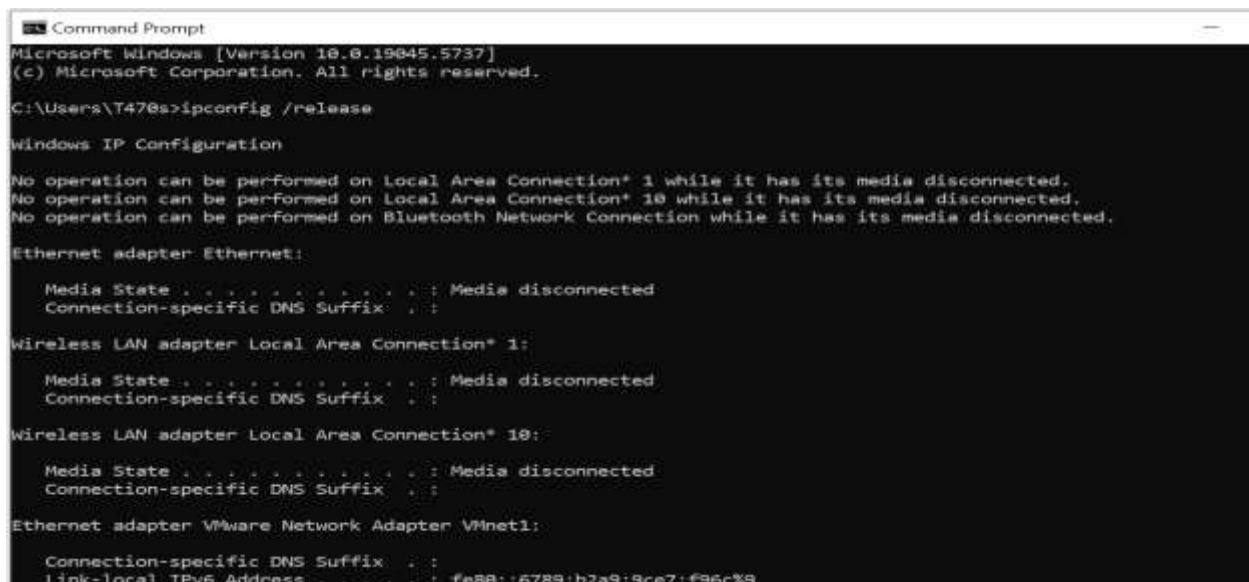
Objectives

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).

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
4. Wait until the "ipconfig /renew" has terminated. Then enter the same command "ipconfig /renew" again.
5. When the second "ipconfig /renew" terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.
6. Finally, enter "ipconfig /renew" to again be allocated an IP address for your computer.
7. Stop Wireshark packet capture.



```
Microsoft Windows [Version 10.0.19045.5737]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T478s>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6789:b2a9:9ce7:f96c%9
```

```

Command Prompt

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::a594:976e:1028:34a6%13
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe88::9dc6:b9f4:1da7:872e%10
Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\T470s>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

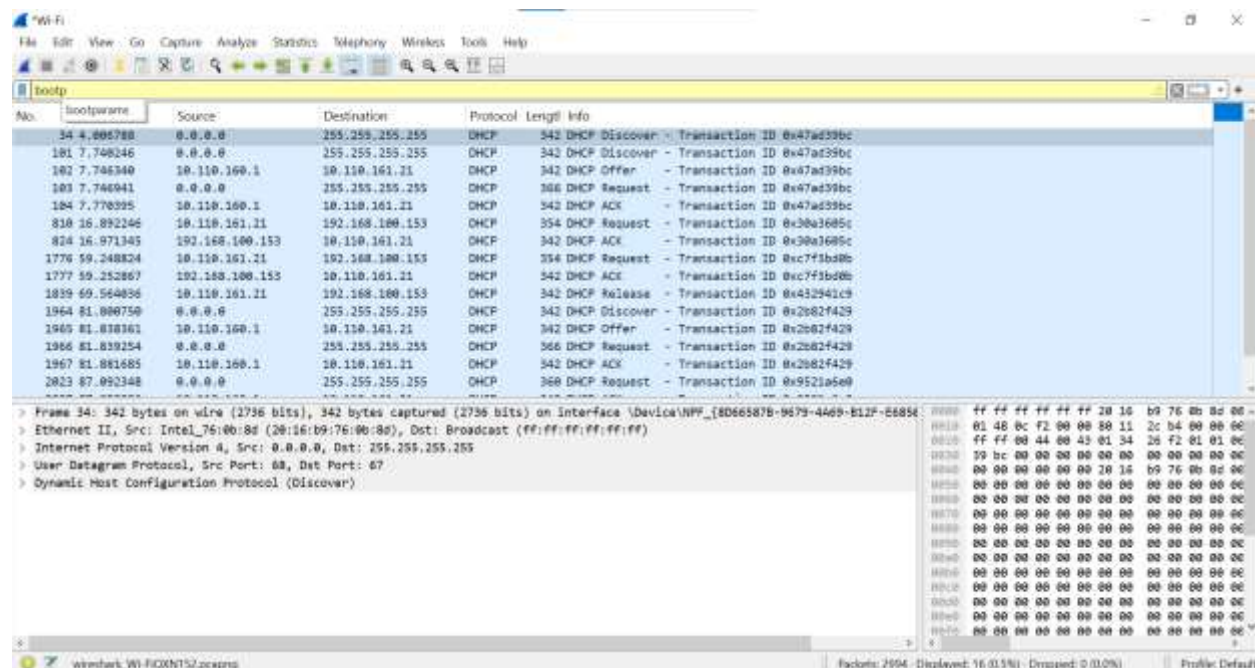
Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

```

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

```
> Frame 34: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E681}
> Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

Question 02:

Draw a timing diagram 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.

```
> Frame 34: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E681}
> Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

Timing diagram of first four packets:

```

No.    Time          Source           Destination      Protocol Length Info
 101 7.740246      0.0.0.0          255.255.255.255  DHCP           342    DHCP Discover - Transaction ID 0x47ad39bc
Frame 101: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70345E},
id 0
Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
No.    Time          Source           Destination      Protocol Length Info
 102 7.746340      10.110.160.1     10.110.161.21    DHCP           342    DHCP Offer - Transaction ID 0x47ad39bc
Frame 102: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70345E},
id 0
Ethernet II, Src: Cisco_e4:f6:d1 (7c:ad:74:e4:f6:d1), Dst: Intel_76:0b:8d (20:16:b9:76:0b:8d)
Internet Protocol Version 4, Src: 10.110.160.1, Dst: 10.110.161.21
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (Offer)
No.    Time          Source           Destination      Protocol Length Info
 103 7.746941      0.0.0.0          255.255.255.255  DHCP           366    DHCP Request - Transaction ID 0x47ad39bc
Frame 103: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70345E},
id 0
Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
No.    Time          Source           Destination      Protocol Length Info
 104 7.770395      10.110.160.1     10.110.161.21    DHCP           342    DHCP ACK - Transaction ID 0x47ad39bc
Frame 104: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70345E},
id 0
Ethernet II, Src: Cisco_e4:f6:d1 (7c:ad:74:e4:f6:d1), Dst: Intel_76:0b:8d (20:16:b9:76:0b:8d)
Internet Protocol Version 4, Src: 10.110.160.1, Dst: 10.110.161.21
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)

```

Question 03:

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

Answer:

```

> Frame 103: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70345E}
  Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: Intel_76:0b:8d (20:16:b9:76:0b:8d)
    > Type: IPv4 (0x0800)
    [Stream index: 1]
  > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  > User Datagram Protocol, Src Port: 68, Dst Port: 67
  > Dynamic Host Configuration Protocol (Request)

```

Question 04:

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

Answer:

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
34	4.006788	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
101	7.740246	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
102	7.746340	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x47ad39bc
103	7.746941	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x47ad39bc
104	7.770395	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x47ad39bc
810	16.892246	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0x30a3605c
824	16.971345	192.168.100.153	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x30a3605c
1776	59.248824	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0xc7f3bd0b
1777	59.252867	192.168.100.153	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0xc7f3bd0b

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:

No.	Time	Source	Destination	Protocol	Length	Info
34	4.006788	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
101	7.740246	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
102	7.746340	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x47ad39bc
103	7.746941	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x47ad39bc
104	7.770395	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x47ad39bc
1964	81.800750	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x2b82f429
1965	81.838361	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x2b82f429
1966	81.839254	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x2b82f429
1967	81.881685	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x2b82f429

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:

No.	Time	Source	Destination	Protocol	Length	Info
34	4.006788	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
101	7.740246	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
102	7.746340	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x47ad39bc
103	7.746941	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x47ad39bc
104	7.770395	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x47ad39bc
810	16.892246	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0x30a3605c
824	16.971345	192.168.100.153	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x30a3605c
1776	59.248824	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0xc7f3bd0b
1777	59.252867	192.168.100.153	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0xc7f3bd0b

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:

No.	Time	Source	Destination	Protocol	Length	Info
34	4.006788	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
101	7.740246	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
102	7.746340	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x47ad39bc
103	7.746941	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x47ad39bc
104	7.770395	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x47ad39bc
810	16.892246	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0x30a3605c

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:

No.	Time	Source	Destination	Protocol	Length	Info
34	4.006788	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
101	7.740246	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x47ad39bc
102	7.746340	10.110.160.1	10.110.161.21	DHCP	342	DHCP Offer - Transaction ID 0x47ad39bc
103	7.746941	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x47ad39bc
104	7.770395	10.110.160.1	10.110.161.21	DHCP	342	DHCP ACK - Transaction ID 0x47ad39bc
810	16.892246	10.110.161.21	192.168.100.153	DHCP	354	DHCP Request - Transaction ID 0x30a3605c

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.

```
Lease Obtained. . . . . : Tuesday, 6 May 2025 8:13:25 pm
Lease Expires . . . . . : Thursday, 5 June 2025 8:37:55 pm
```

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.