

### Lab 3 Assignment:

#### Command Line Execution screenshot:

```
Microsoft Windows [Version 10.0.22621.674]
(c) Microsoft Corporation. All rights reserved.

C:\Users\91890>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* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::7697:7afc:d38e:6ffa%14
    Default Gateway . . . . . :

C:\Users\91890>ipconfig/renew

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* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:
```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : dhost.uta.edu  
Link-local IPv6 Address . . . . . : fe80::7697:7afc:d38e:6ffa%14  
IPv4 Address. . . . . : 10.182.138.170  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.182.0.1

C:\Users\91890>ipconfig/renew

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\* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection\* 1:

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

Wireless LAN adapter Local Area Connection\* 2:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : dhost.uta.edu  
Link-local IPv6 Address . . . . . : fe80::7697:7afc:d38e:6ffa%14  
IPv4 Address. . . . . : 10.182.138.170  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.182.0.1

C:\Users\91890>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\* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection\* 1:

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

```

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . : fe80::7697:7afc:d38e:6ffa%14
Default Gateway . . . . . :

C:\Users\91890>ipconfig/renew

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* 2 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : dhost.uta.edu
Link-local IPv6 Address . . . . : fe80::7697:7afc:d38e:6ffa%14
IPv4 Address. . . . . : 10.182.138.170
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.182.0.1

C:\Users\91890>

```

Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?

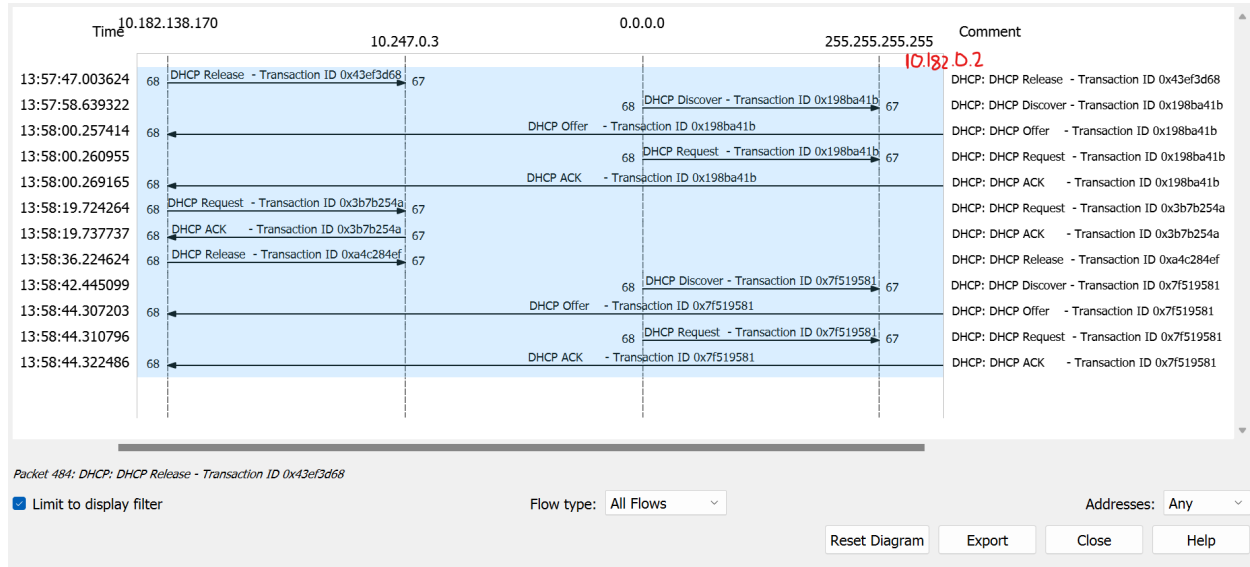
→ The DHCP messages are sent over UDP - User Datagram Protocol

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

> Frame 484: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{9E62E2A7-9AF2-4A6C-85B  
 > Ethernet II, Src: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: IETF-VRRP-VRID\_01 (00:00:5e:00:01:01)  
 > Internet Protocol Version 4, Src: 10.182.138.170, Dst: 10.247.0.3  
 > User Datagram Protocol, Src Port: 68, Dst Port: 67  
 > Dynamic Host Configuration Protocol (Release)

- 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, indicate the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

→ Yes the Port numbers are same as in the lab example ie 68 and 67



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

→ The link-layer address of my host is 00:d4:9e:53:8f:c2

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

> Frame 582: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874}

> Ethernet II, Src: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2), 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)

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

→ The option (53) : DHCP message Type differentiates both discover and request messages.

Request message has Option 54 DHCP server Identifier and Option (81) client fully qualified domain name. Screenshot attached below of Discover and request DHCP message

No.	Time	Source	Destination	Protocol	Length	Info
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b

Frame 582: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF\_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}, id 0

Interface id: 0 (\Device\NPF\_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057})

Encapsulation type: Ethernet (1)

Arrival Time: Nov 1, 2022 13:57:58.639322000 Central Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1667329078.639322000 seconds

[Time delta from previous captured frame: 0.072878000 seconds]

[Time delta from previous displayed frame: 11.635698000 seconds]

[Time since reference or first frame: 36.253766000 seconds]

Frame Number: 582

Frame Length: 342 bytes (2736 bits)

Capture Length: 342 bytes (2736 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:dhcp]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

Ethernet II, Src: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

Type: IPv4 (0x0800)

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)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x198ba41b

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)

Option: (61) Client identifier

Option: (50) Requested IP Address (10.182.138.170)

Option: (12) Host Name

Option: (60) Vendor class identifier

Option: (55) Parameter Request List

Option: (255) End

```

No.    Time                Source                Destination           Protocol Length Info
595 13:58:00.260955      0.0.0.0              255.255.255.255      DHCP      366    DHCP Request - Transaction ID 0x198ba41b
Frame 595: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057},
id 0
    Interface id: 0 (\Device\NPF_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 1, 2022 13:58:00.260955000 Central Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667329080.260955000 seconds
    [Time delta from previous captured frame: 0.003541000 seconds]
    [Time delta from previous displayed frame: 0.003541000 seconds]
    [Time since reference or first frame: 37.875399000 seconds]
    Frame Number: 595
    Frame Length: 366 bytes (2928 bits)
    Capture Length: 366 bytes (2928 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dhcp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
    Type: IPv4 (0x0800)
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)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x198ba41b
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_53:8f:c2 (00:d4:9e:53:8f:c2)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Request)
    Option: (61) Client identifier
    Option: (50) Requested IP Address (10.182.138.170)
    Option: (54) DHCP Server Identifier (10.247.0.3)
    Option: (12) Host Name
    Option: (81) Client Fully Qualified Domain Name
    Option: (60) Vendor class identifier
    Option: (55) Parameter Request List
    Option: (255) End

```

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?

→ The value of the Transaction-ID for all of the first four (Discover/Offer/Request/ACK) DHCP messages is 0x198ba41b.

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	<u>DHCP Discover</u> - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	<u>DHCP Offer</u> - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	<u>DHCP Request</u> - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	<u>DHCP ACK</u> - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

```

> [Timestamps]
  UDP payload (380 bytes)
Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x198ba41b
  Seconds elapsed: 0

```

→ The values of the Transaction-ID for all in the second set (Request/ACK) set of DHCP messages is 0x3b7b254a.

No.	Time	Source	Destination	Protocol	Length	Info
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a
4293	13:58:19.737737	10.247.0.3	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x3b7b254a
4494	13:58:36.224624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0xa4c284ef
4529	13:58:42.445099	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7f519581

Dynamic Host Configuration Protocol (Request)  
 Message type: Boot Request (1)  
 Hardware type: Ethernet (0x01)  
 Hardware address length: 6  
 Hops: 0  
 Transaction ID: 0x3b7b254a  
 Seconds elapsed: 0

→ The Transaction ID is different for every set of DHCP messages because the requesting device can differentiate between different requests made by it.

- 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.

→

Message type	Source Address	Destination Address
DHCP Discover	0.0.0.0	255.255.255.255
DHCP Offer	10.182.0.2	255.255.255.255
DHCP Request	0.0.0.0	255.255.255.255
DHCP Ack	10.182.0.2	255.255.255.255

- What is the IP address of your DHCP server?

→ The Ip address of DHCP server is 10.182.0.2

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

Frame 594: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface \Device\NPF\_{9E62E2A7-9AF2-4A6C-85B2-0FDA48}

Ethernet II, Src: JuniperN\_27:f3:f0 (d4:04:ff:27:f3:f0), Dst: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

Internet Protocol Version 4, Src: 10.182.0.2, Dst: 10.182.138.170

0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 403  
 Identification: 0x858e (34190)  
 Flags: 0x00



8. 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 offered by the DHCP server to my host in the DHCP offer message is 10.182.138.170  
The DHCP offer message contains the offered DHCP address.

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 10.182.138.170

Next server IP address: 10.247.0.3

Relay agent IP address: 0.0.0.0

Client MAC address: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

Client hardware address padding: 00000000000000000000

Server host name not given

9. 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?

→ The absence of a relay agent is indicated by a 0.0.0.0 value. There is no relay agent in my experiment.  
The IP address of my relay agent is 0.0.0.0

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

Client hardware address padding: 00000000000000000000

Server host name not given

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

→ The router line says where the client should send the message by default - default gateway

→ the subnet mask purpose is used to tell the client which subnet mask that is available to use

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). 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 request message has the IP address offered by the DHCP offer message. The client accepts the IP address. After the IP address being offered in the offer message, the request message is sent by the client to assign that IP address to itself.

No.	Time	Source	Destination	Protocol	Length	Info
484	13:57:47.003624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0x43ef3d68
582	13:57:58.639322	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x198ba41b
594	13:58:00.257414	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x198ba41b
595	13:58:00.260955	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x198ba41b
596	13:58:00.269165	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x198ba41b
4292	13:58:19.724264	10.182.138.170	10.247.0.3	DHCP	354	DHCP Request - Transaction ID 0x3b7b254a

Length: 7  
Hardware type: Ethernet (0x01)  
Client MAC address: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2)

- Option: (50) Requested IP Address (10.182.138.170)  
Length: 4  
Requested IP Address: 10.182.138.170
- Option: (54) DHCP Server Identifier (10.247.0.3)  
Length: 4  
DHCP Server Identifier: 10.247.0.3

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

→ The need for lease time is to know how long that particular IP address will be assigned to the client by the DHCP server. During this time, this IP address will not be assigned to another client.

→ The lease time is 1 day (86400s).

Screenshot attached below.

No.	Time	Source	Destination	Protocol	Length	Info
4293	13:58:19.737737	10.247.0.3	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x3b7b254a
4494	13:58:36.224624	10.182.138.170	10.247.0.3	DHCP	342	DHCP Release - Transaction ID 0xa4c284ef
4529	13:58:42.445099	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x7f519581
4543	13:58:44.307203	10.182.0.2	10.182.138.170	DHCP	417	DHCP Offer - Transaction ID 0x7f519581
4545	13:58:44.310796	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x7f519581
4546	13:58:44.322486	10.182.0.2	10.182.138.170	DHCP	422	DHCP ACK - Transaction ID 0x7f519581

- Option: (59) Rebinding Time Value  
Length: 4  
Rebinding Time Value: (75600s) 21 hours
- Option: (51) IP Address Lease Time  
Length: 4  
IP Address Lease Time: (86400s) 1 day
- Option: (54) DHCP Server Identifier (10.247.0.3)  
Length: 4  
DHCP Server Identifier: 10.247.0.3

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?

→ The purpose of DHCP release message is to release the Ip address or return back the Ip address to the dhcp server that was offered.

→ There is NO acknowledgment of the receipt of the client's DHCP request.

→ If the client's DHCP release message is lost, then the server will not assign that IP address until the lease Time on the address expires but the client releases the IP address.

14. Clear the bootp 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 the ARP packets were sent and received during the DHCP packet-exchange period.
  - They are the broadcast message sent out. Before offering an IP address to the client, the DHCP server checks whether the IP address is not in use by another client, hence DHCP server broadcast the ARP request message.

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
635	13:58:00.548306	10.182.138.170	40.86.187.166	TCP	54	58848 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
636	13:58:00.548617	10.182.138.170	40.86.187.166	TLSv1.2	281	Client Hello
637	13:58:00.563220	10.247.0.3	10.182.138.170	DNS	163	Standard query response 0x1a7b A trouter-azsc-u
638	13:58:00.568649	IntelCor_53:8f:c2	Broadcast	ARP	42	Who has 10.182.0.1? Tell 10.182.138.170
639	13:58:00.572654	IETF-VRRP-VRID_01	IntelCor_53:8f:c2	ARP	42	10.182.0.1 is at 00:00:5e:00:01:01
640	13:58:00.590485	40.86.187.166	10.182.138.170	TLSv1.2	195	Server Hello, Change Cipher Spec, Encrypted Han

> Frame 638: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{9E62E2A7-9AF2-4A6C-85B2-0FDA4874E057}

> Ethernet II, Src: IntelCor\_53:8f:c2 (00:d4:9e:53:8f:c2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)