CS 315: Computer Networks Lab
Spring 2023-24, IIT Dharwad
Assignment-9

Wireshark Lab: DHCP

March 17, 2025

Chidurala Tejaswini
(220010012/CS22BT012)

Introduction

In this lab, we'll take a quick look at the Dynamic Host Configuration Protocol, 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.

As we've done in earlier Wireshark labs, you'll perform a few actions on your computer that will cause DHCP to spring into action, and then use Wireshark to collect and then the packet trace containing DHCP protocol messages.

Part 0: Paste a screenshot of your system IP address, using `ipconfig` (on Windows) or `ifconfig` (on Mac and Linux), and fill out this Google form to submit the details of your system. The same system must be used to attempt all exercises of this lab.

```
user@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.240.118.97  netmask 255.255.248.0  broadcast 10.240.119.255
        inet6 fe80::1d6b:1bfb:2bd6:ef0d  prefixlen 64  scopeid 0x20<link>
        ether e0:73:e7:0a:99:9a  txqueuelen 1000  (Ethernet)
        RX packets 355117  bytes 395639432 (395.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 84233  bytes 10880630 (10.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4716  bytes 523190 (523.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4716  bytes 523190 (523.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Gathering a Packet Trace

In order to collect a trace that will contain all four DHCP message types, we'll need to take a few command line actions on a Mac, Linux or PC.

On a Mac:

1. In a terminal window/shell enter the following command:

```
% sudo ipconfig set en0 none
```

   Where `en0` (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture->options. This command will de-configure network interface `en0`.

2. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
3. In the terminal window/shell enter the following command:

```
% sudo ipconfig set en0 dhcp
```

   This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

On a Linux machine:

1. In a terminal window/shell, enter the following commands:

```
sudo ip addr flush en0
sudo dhclient -r
```

   where en0 (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture -> Options. This command will remove the existing IP address of the interface, and release any existing DHCP address leases.

2. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
3. In the terminal window/shell, enter the following command:

```
sudo dhclient en0
```

   where, as with above, `en0` is the interface on which you are currently capturing packets. This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

On a Windows:

1. In a command-line window enter the following command:

```
> ipconfig /release
```

   This command will cause your PC to give up its IP address.

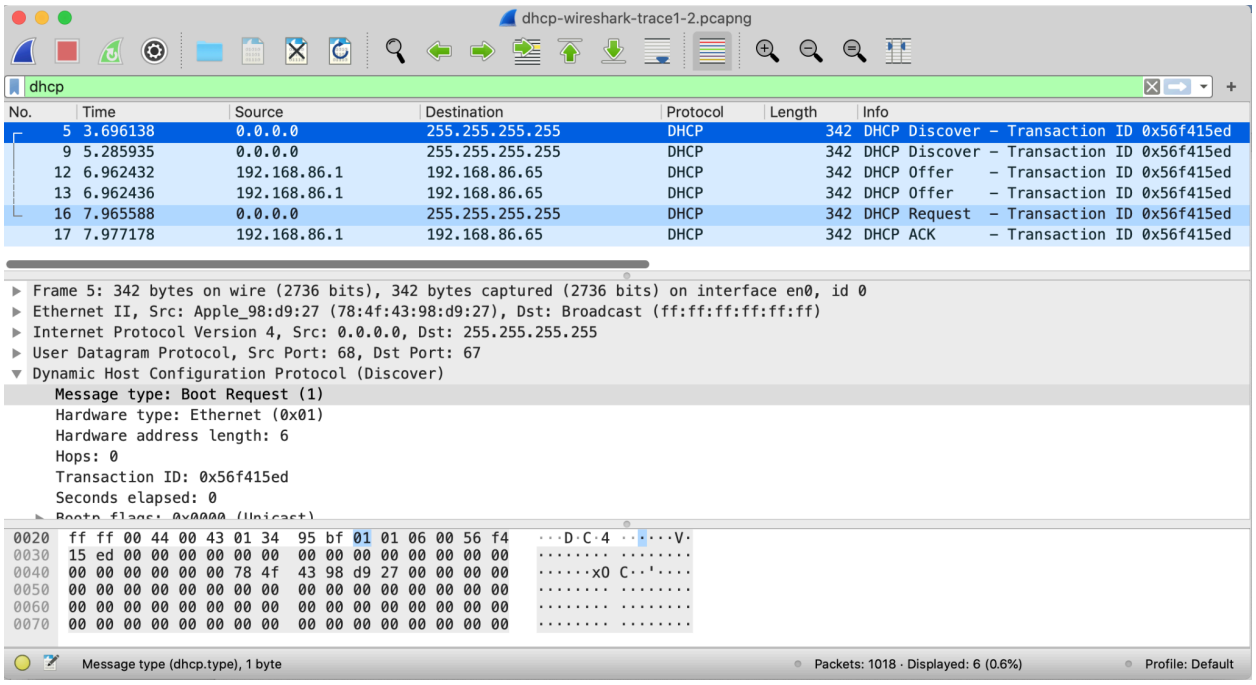
2. Start up Wireshark.
3. In the command-line window enter the following command:

   ```
   > ipconfig /renew
   ```

   This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.

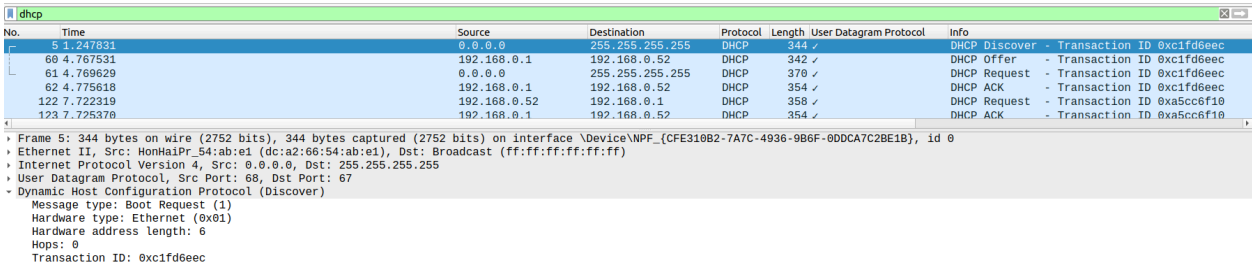
4. After waiting for a few seconds, stop Wireshark capture.

After stopping Wireshark capture in step 4, take a peek in your Wireshark window to make sure you've actually captured the packets that we're looking for. If you enter "dhcp" into the display filter field (as shown in the light green field in the top left of Figure 1), your screen (on a Mac) should look similar to Figure 1.



Part 1: DHCP Questions

1. **What is the Transaction ID in a DHCP Discover message? Which system generates this identifier? What is its significance?**



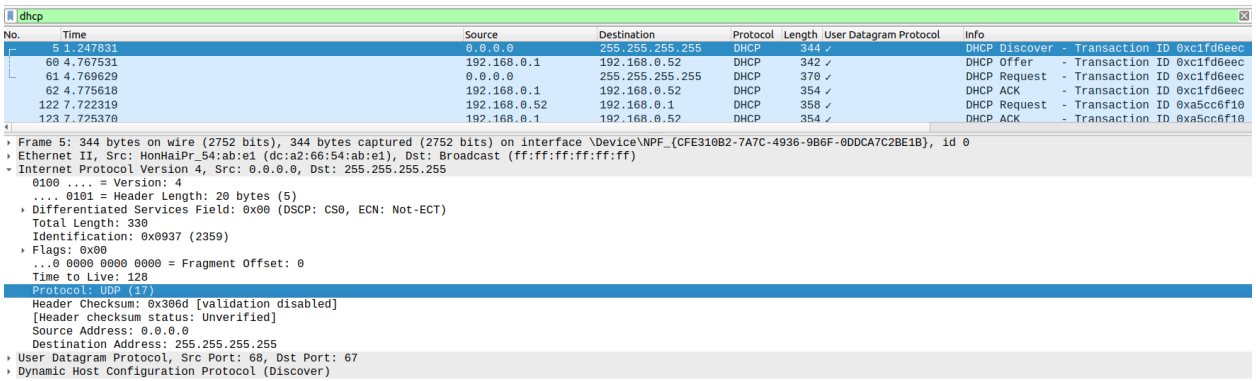
Transaction ID: 0xc1fd6eec
The **DHCP client** generates the Transaction ID before sending a **DHCP Discover message.** This ID remains the same for the entire DHCP transaction, allowing the client to identify responses from the DHCP server that correspond to its request.

Significance of the Transaction ID (XID)

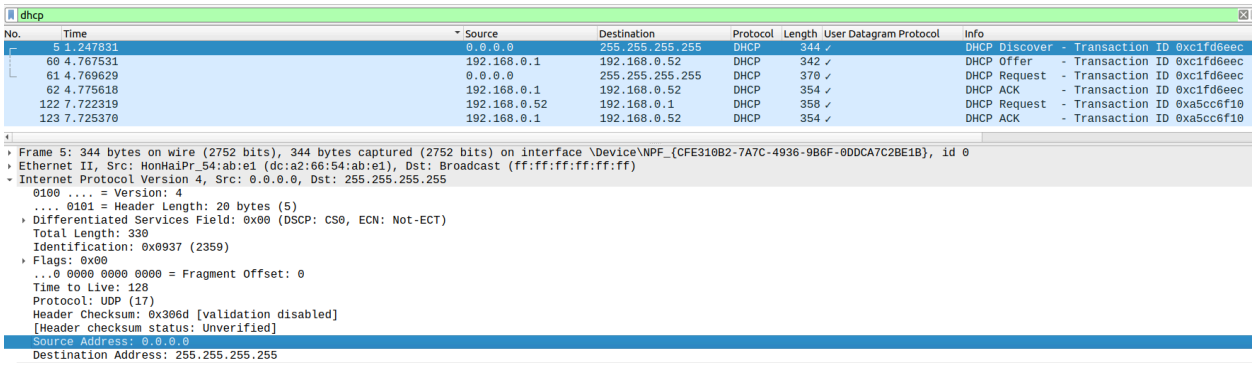
1. Uniquely Identifies a DHCP Session
    - The XID helps the client match incoming DHCP Offer, ACK, or NAK responses to its original Discover request.
2. Ensures No Confusion in Multi-Client Environments
    - Since multiple clients might request IP addresses simultaneously, each client uses a unique XID to distinguish its responses from others.
3. Prevents Misassociation of Responses
    - DHCP servers use the XID in replies (Offer, ACK, or NAK) so that the client can recognize which response belongs to its request.

2. **Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?**

A DHCP Discover message is sent out using **UDP** as the underlying transport protocol.



3. **What are the source and destination IP addresses in a DHCP Discover message? Why are they this way?**

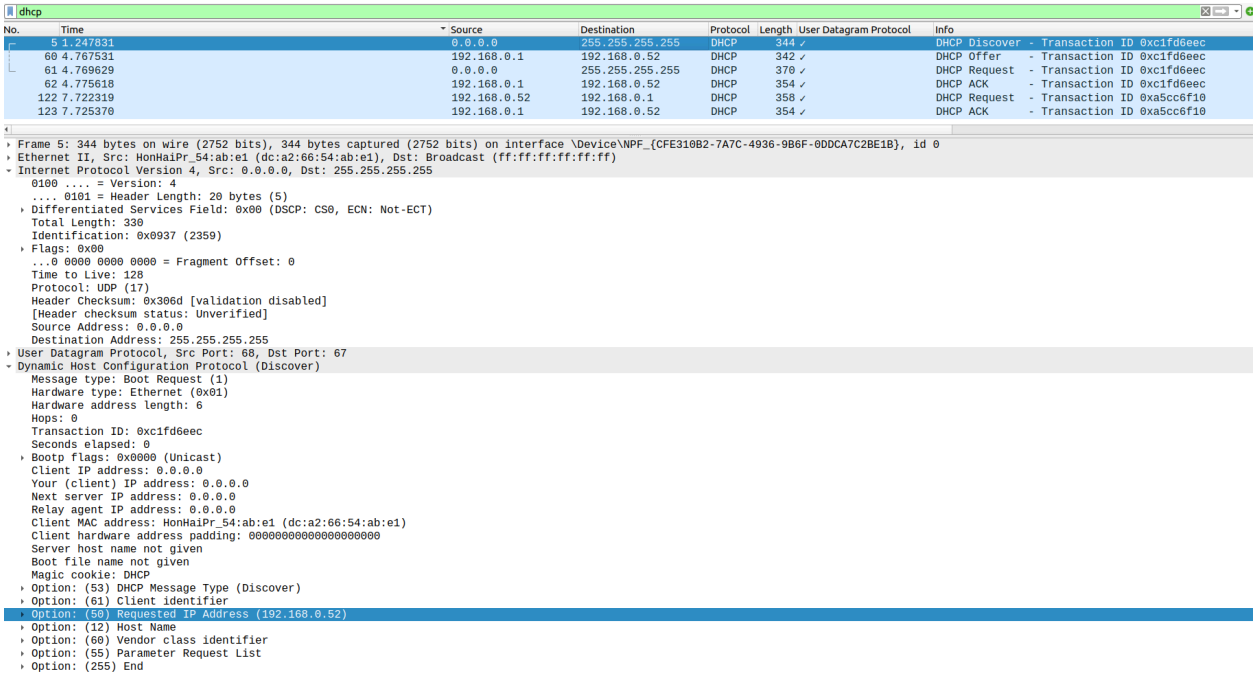


- Source IP Address : 0.0.0.0
- Destination IP Address : 255.255.255.255

1. **Source IP Address: `0.0.0.0`**
   - The DHCP client **does not yet have an IP address** assigned.
   - It uses `0.0.0.0` as a placeholder until the DHCP server assigns an IP.
2. **Destination IP Address: `255.255.255.255` (Broadcast Address)**
   - The client does not know the DHCP server's IP address.
   - It sends the Discover message as a **broadcast** so that all DHCP servers on the network can receive it.

This mechanism ensures that the DHCP client can communicate with a DHCP server **even without an initial IP address**.

4. **What is the "Requested IP address" field in a DHCP Discover packet, and how does it impact the DHCP Offer?**



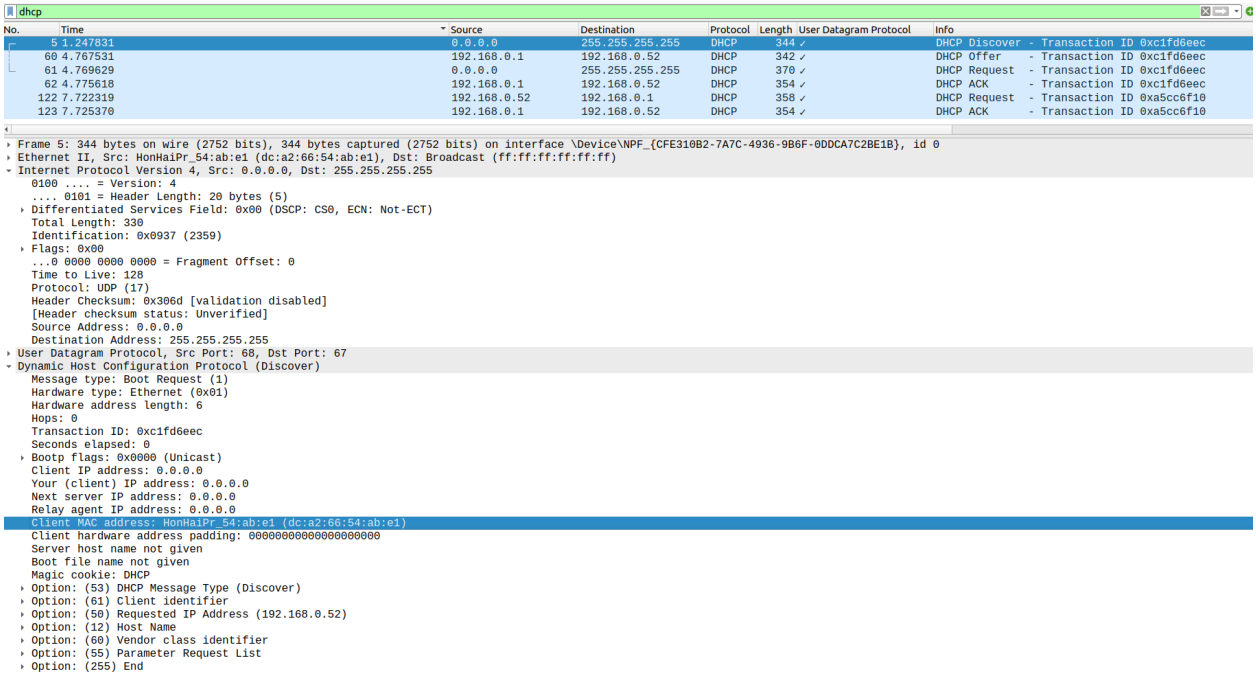
In a DHCP Discover packet, the Requested IP Address field (Option 50) allows the client to request a specific IP address from the DHCP server.

- Option (50): Requested IP Address: **192.168.0.52**

Impact on the DHCP Offer:

1. **If the Requested IP Address is Available:**
   - The DHCP server includes the requested IP address in the DHCP Offer message.
2. **If the Requested IP Address is Not Available:**
   - If the requested IP is already assigned to another client or is reserved, the DHCP server will not offer that IP address.
   - Instead, the server assigns and offers a different available IP address from its DHCP pool.
3. **If the Requested IP Address is Absent ("Requested IP Address" field is missing in the request):**
   - The DHCP server dynamically assigns an available IP address from its pool and includes it in the DHCP Offer.
4. **If the Requested IP Address is Invalid (Outside the server's range):**
   - The server ignores the invalid request.
   - It responds with a DHCP Offer containing a valid IP address from its configured DHCP pool.

5. **What is the MAC address in the DHCP Discover packet, and why is it crucial in the DHCP process?**

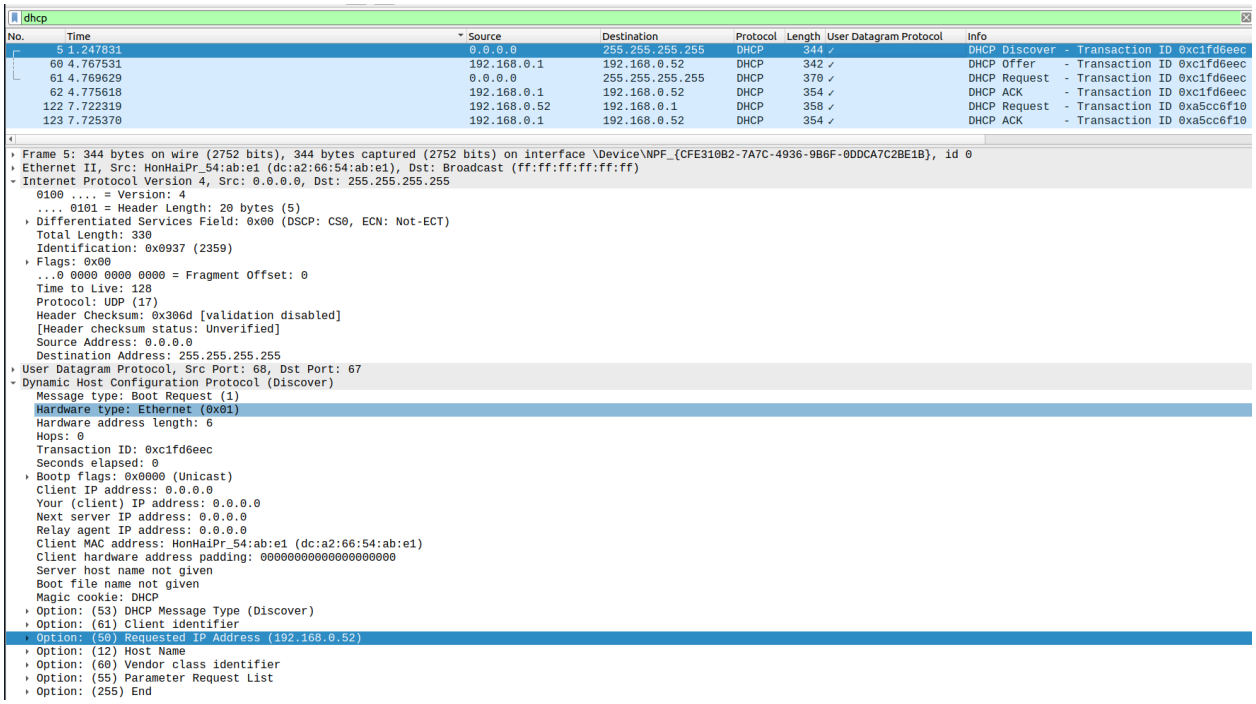


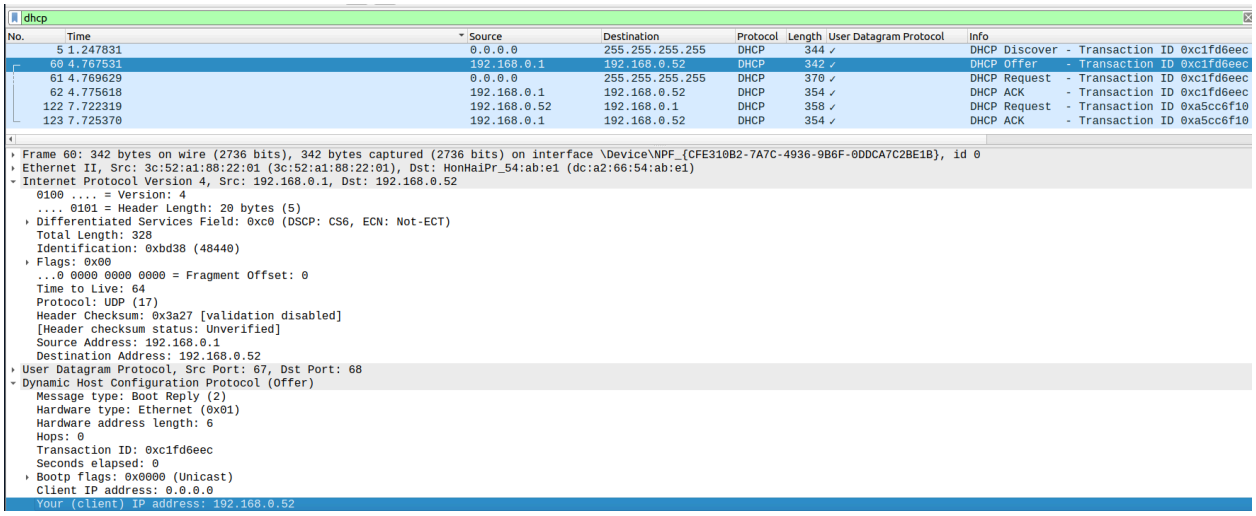
The MAC address in the DHCP Discover packet is **dc:a2:66:54:ab:e1.**

Why is the MAC address crucial in the DHCP process?

1. **Client Identification:**
   - The DHCP server uses the MAC address to uniquely identify the client device, since the client does not yet have an IP address.
2. **IP Lease Assignment:**
   - The server maps the client's MAC address to an IP address and assigns the IP accordingly. This ensures proper IP management.
3. **Address Reservation:**
   - If configured, the DHCP server can reserve and consistently assign a specific IP address to a known MAC address for predictable assignments.
4. **DHCP Binding Table Maintenance:**
   - The server maintains a MAC-to-IP binding table to track active leases and avoid IP conflicts in the network.
5. **Reply Routing:**
   - The MAC address allows the server to correctly route DHCP Offer, ACK, and other responses back to the requesting device.
6. **Local Network Communication:**
   - Since DHCP messages operate at the network layer, the MAC address ensures that these messages are delivered accurately to the correct interface on the local network.

6. **How do you know that this Offer message is being sent in response to the DHCP Discover message?**

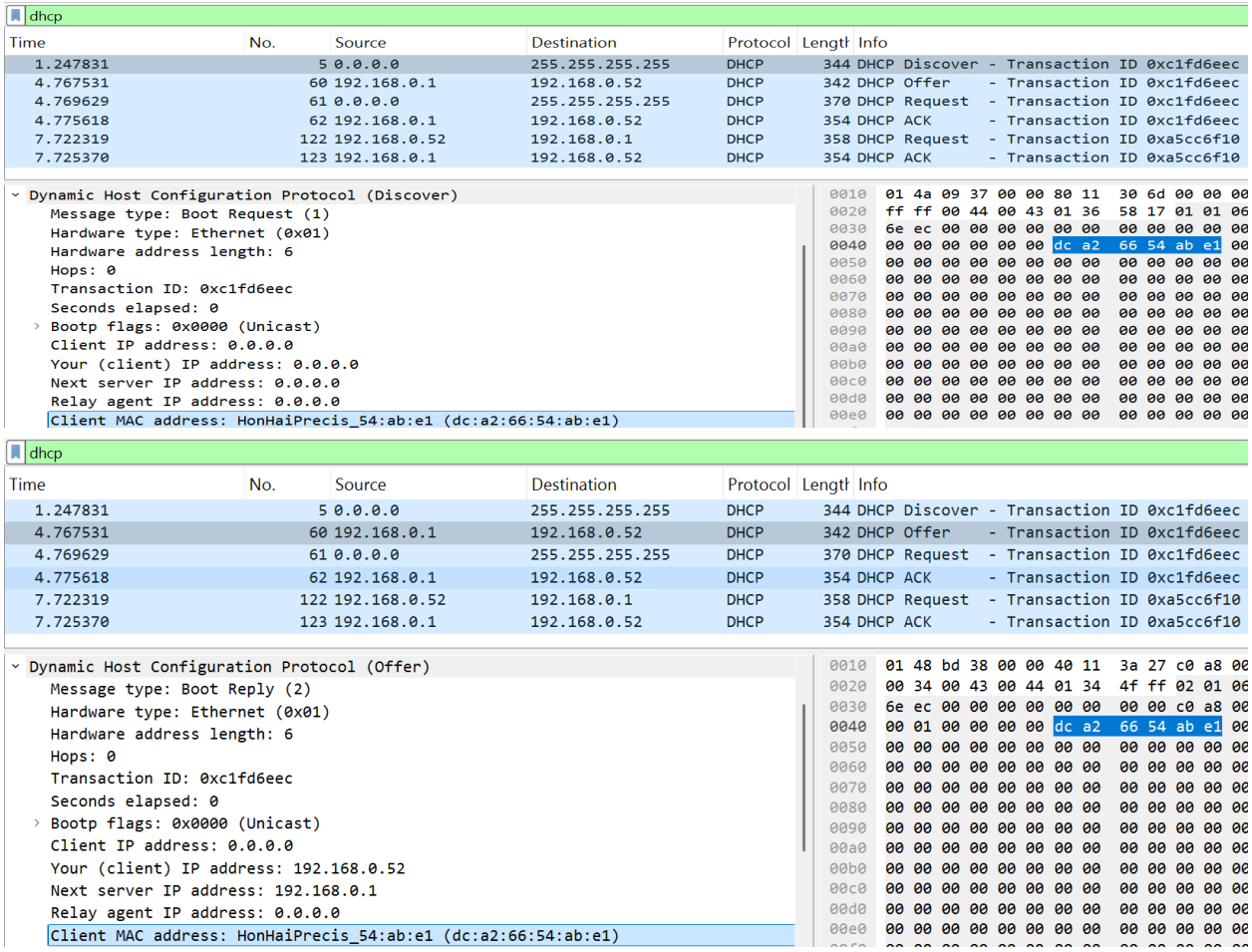




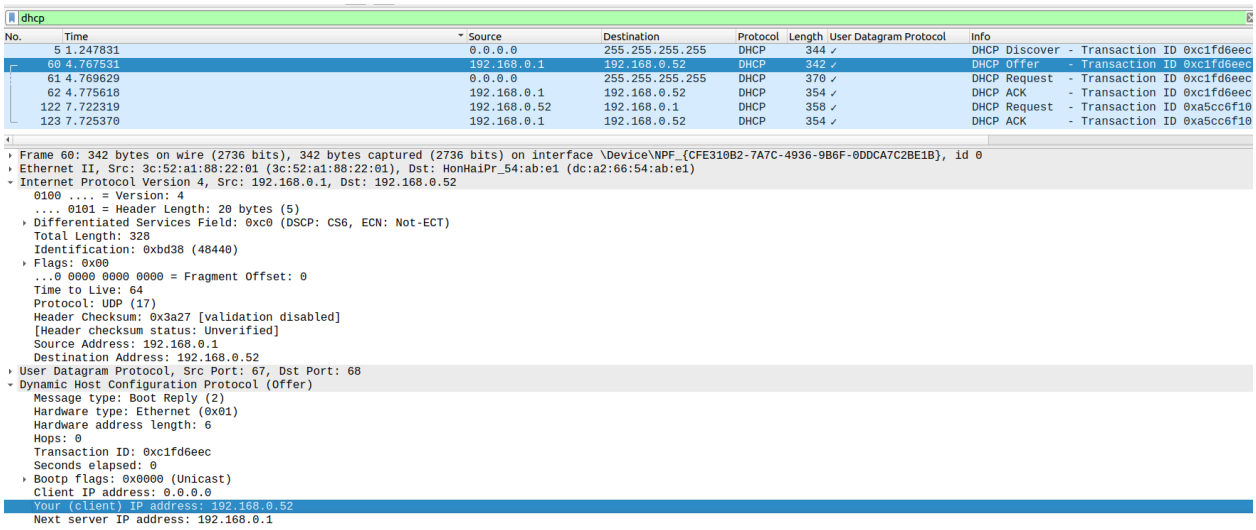
The DHCP Offer message is sent in response to the DHCP Discover message.

1. **Matching Transaction ID:**
    - The DHCP Offer message contains the same **Transaction ID** as the DHCP Discover message (e.g., `0xc1fd6eec`).
    - This ensures that the Offer is directly linked to the Discover request from the correct client.
2. **Message Sequence in DHCP Process (DORA):**
    - The DHCP Discover message is followed by a DHCP Offer message from the server.
    - This sequence follows the standard **DORA process**: Discover → Offer → Request → Acknowledge.

3. **Server's Response IP:**
    - The Offer message originates from a valid DHCP server IP address (e.g., `192.168.0.1`), indicating that the server is responding to the client's Discover request.
4. **Proposed IP Address in Offer:**
    - The DHCP Offer message contains the IP address (e.g., `192.168.0.52`) that the server proposes to assign to the client, often matching the requested or suggested IP in the Discover message.
5. **Matching Client MAC Address:**
    - The **Client MAC address** in the DHCP Offer message matches the **Client MAC address** in the DHCP Discover message.
    - This confirms that the Offer is intended for the correct client device.



7. **What is the client-assigned and next-hop IP address in the DHCP Offer packet, and how do they assist in routing?**



In the DHCP Offer packet:

Client-assigned IP Address: 192.168.0.52

- This is the offered IP address for the client.
- The client will confirm it in a DHCP Request message.

Next-Hop IP Address (Next Server IP Address): 192.168.0.1

- This is typically the default gateway provided by the DHCP server.
- It allows the client to communicate with other networks (including the internet).

How They Assist in Routing:

1. Client-assigned IP (192.168.0.52)

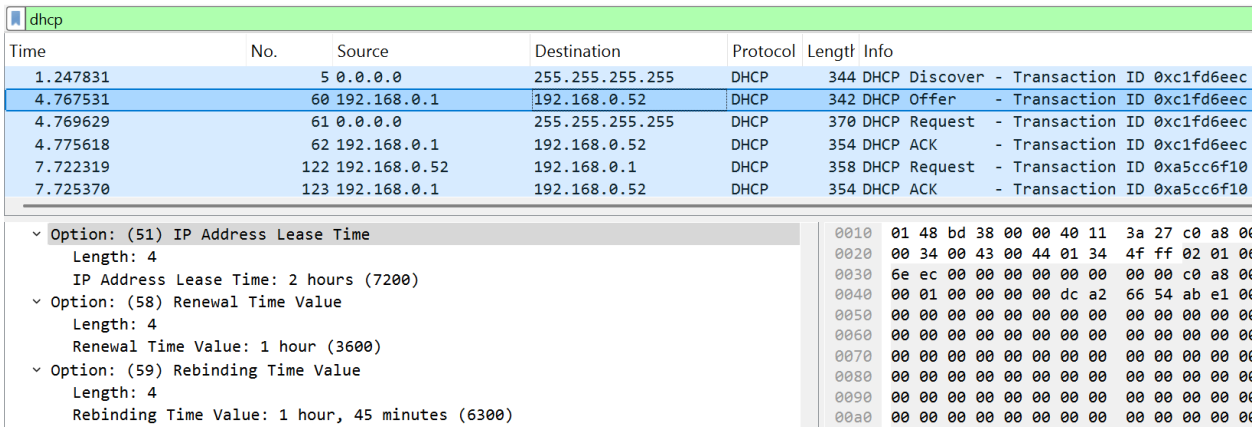
- Enables communication within the local subnet (in this case, 192.168.0.52).
- Allows the client to send and receive packets within the LAN.

2. Next-Hop IP (192.168.0.1)

- Serves as the default gateway for the client.
- Routes traffic to external networks, including the internet.

Thus, the **client IP allows local network access, while the next-hop ensures external routing.**

8. Explain the Lease time, Renewal time, and Rebinding time in DHCP. How do they ensure IP continuity?



DHCP assigns dynamic IP addresses to clients for a limited period, ensuring efficient IP management. These three timers help maintain IP continuity while preventing conflicts.

1. Lease Time (T1)

- The total duration for which the DHCP server grants an IP address to the client.
- If the lease expires and is not renewed, the IP is returned to the DHCP pool.
- Example: If Lease Time = 2 hours, the client can use the IP for that duration.

Ensures: Temporary IP assignment to optimize address usage.

2. Renewal Time (T1)

- The client attempts to renew its lease (at 50% of the lease time) by sending a DHCP Request to the DHCP server.
- If the server responds with a DHCP ACK, the lease is extended.
- Example: If Lease Time = 2 hours, the client tries renewing at 1 hour.

Ensures: Continuous use of the same IP if the client remains connected.

3. Rebinding Time (T2)

- If renewal fails, the client enters the rebinding phase(at 87.5% of the lease time).
- The client broadcasts a DHCP Request to any available DHCP server.
- If there is no response, the lease expires, and the client must request a new IP.
- Example: If Lease Time = 2 hours, rebinding starts at 1 hour 45 minutes.

Ensures: The client can get a new IP before lease expiration, preventing connectivity loss.

How DHCP Timers (T1 and T2) Ensure IP Continuity?

1. Early Renewal (T1 Timer)

- **T1** is the time at which the client attempts to **renew its lease directly with the original DHCP server**, well before the lease expires (typically at 50% of the lease duration).
- This prevents sudden disconnections and ensures that the client can continue using the same IP address without interruption.
- If the renewal is successful, the lease is refreshed without any changes or downtime.

2. Rebinding (T2 Timer) as a Backup

- If the T1 renewal attempt fails (server unresponsive), the client waits until **T2 (usually at 87.5% of the lease duration)** and then attempts to rebind.
- Rebinding allows the client to **request lease renewal from any available DHCP server** on the network, not just the original one.
- This provides a fallback mechanism and avoids IP conflicts or disconnection in case the original DHCP server is unavailable.

3. Graceful Lease Expiry Management

- The client continues to use its IP address during the renewal and rebinding periods without disruption.

- Only if both T1 and T2 fail, and the lease fully expires, the client will release the IP and restart the DHCP process.
- This structured mechanism ensures a **smooth transition** and seamless connectivity.

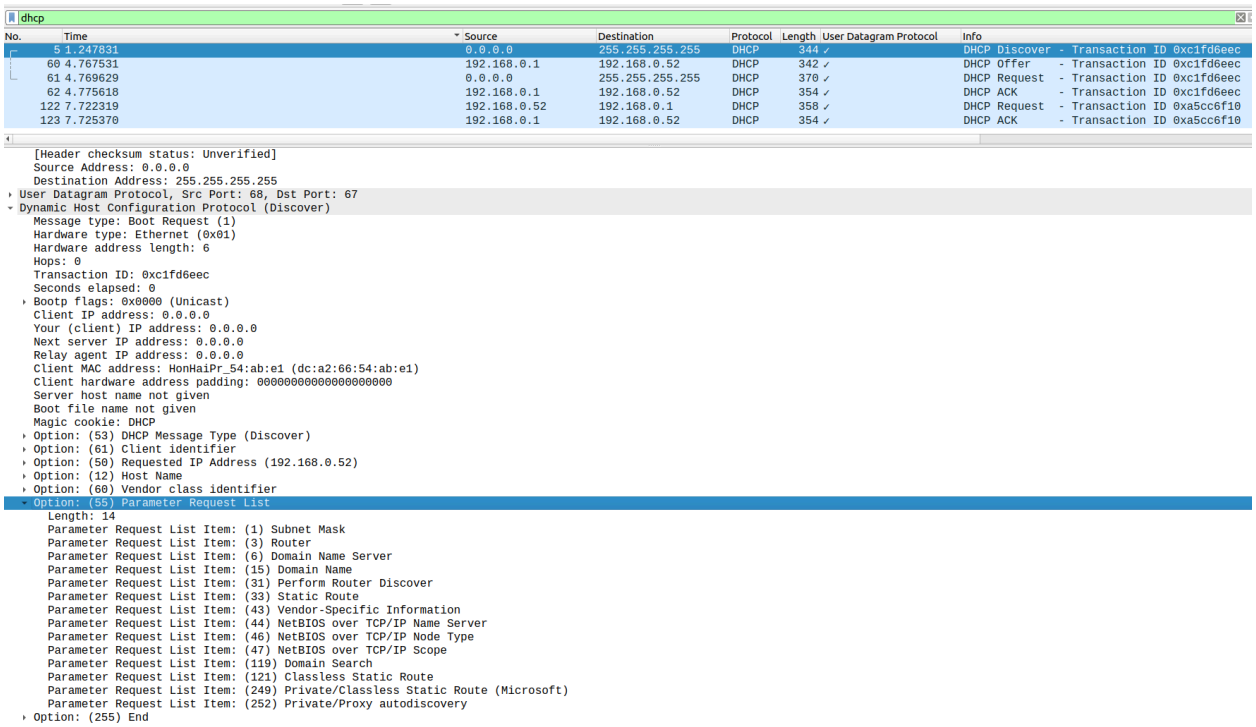
The T1 and T2 timers, as seen in DHCP communication (e.g., Wireshark captures), demonstrate **efficient lease management**, ensuring the client:

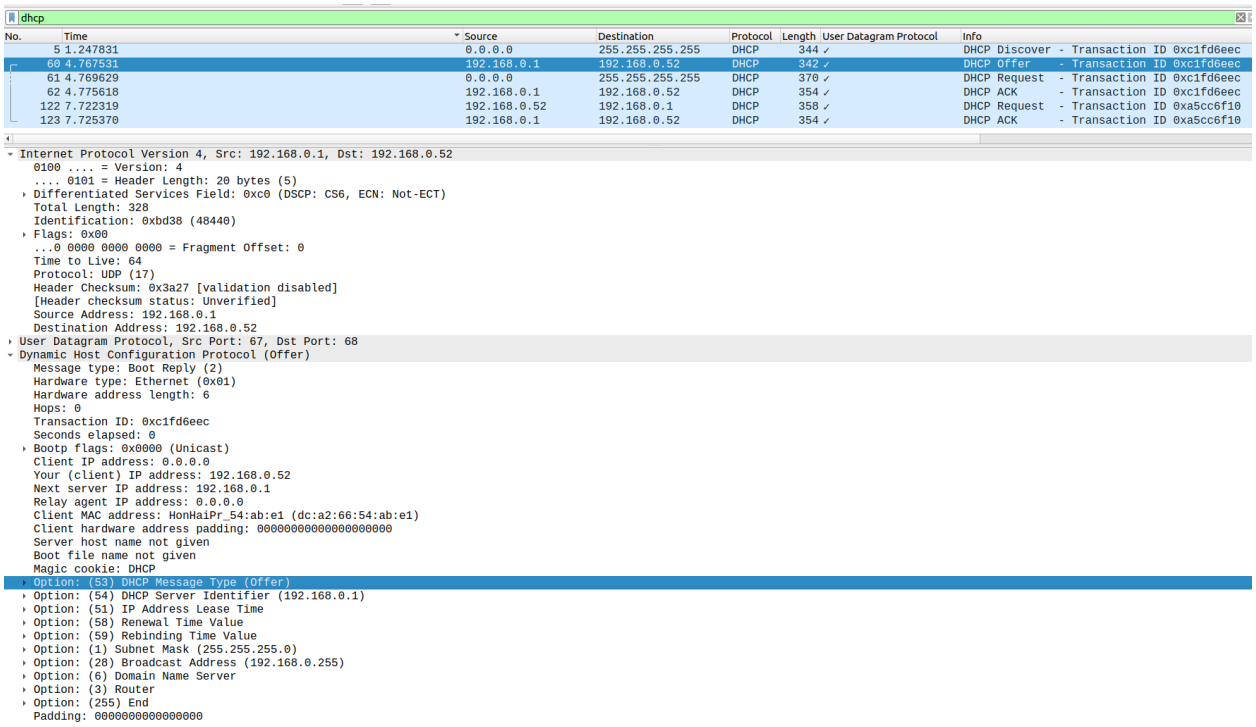
- Renews IP addresses early.
- Has backup mechanisms via rebinding.
- Experiences continuous and conflict-free network connectivity without sudden disruptions.

9. Which DHCP options are included in the 'Parameter Request Lists' of a DHCP Discover packet, and answered in the DHCP Offer packet?

The DHCP options that are included in the **'Parameter Request List'** of the **DHCP Discover** packet and are **answered** in the **DHCP Offer** packet are:

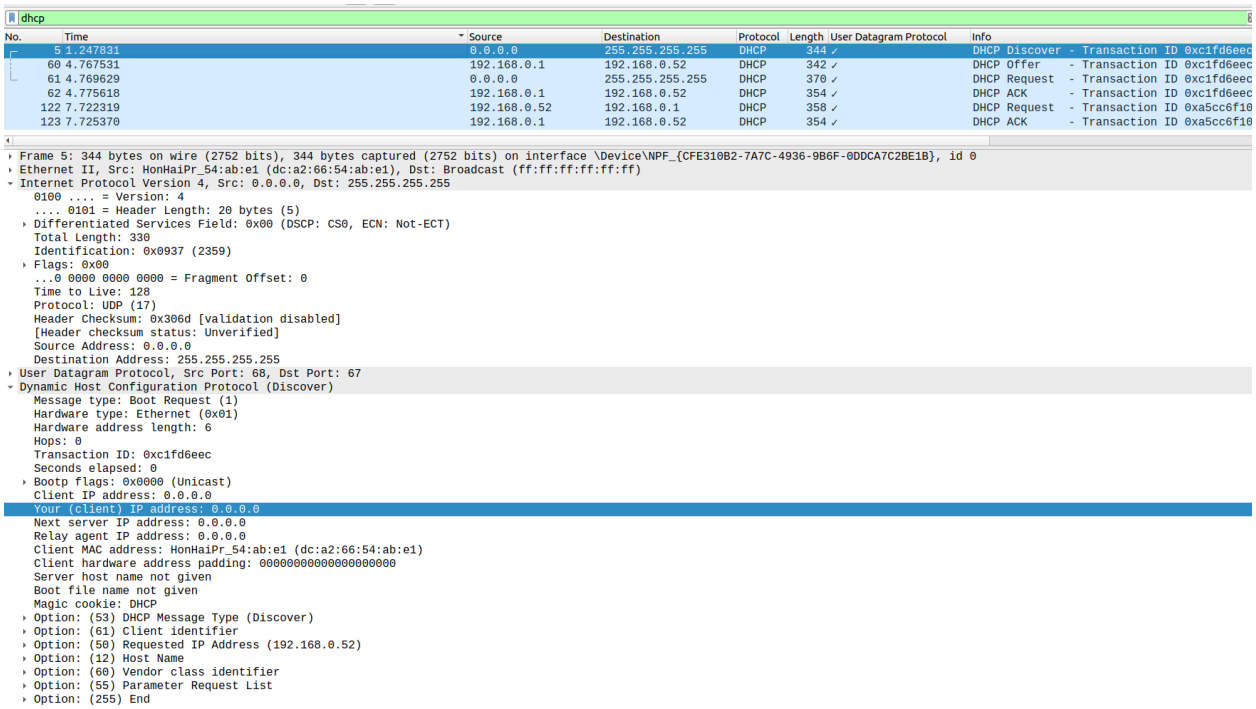
1. **Subnet Mask (Option 1)**
2. **Router (Option 3)**
3. **Domain Name Server (Option 6)**

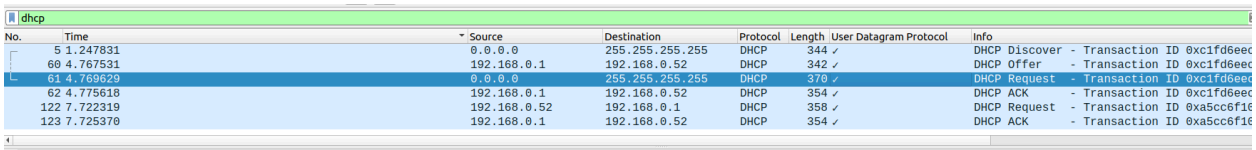


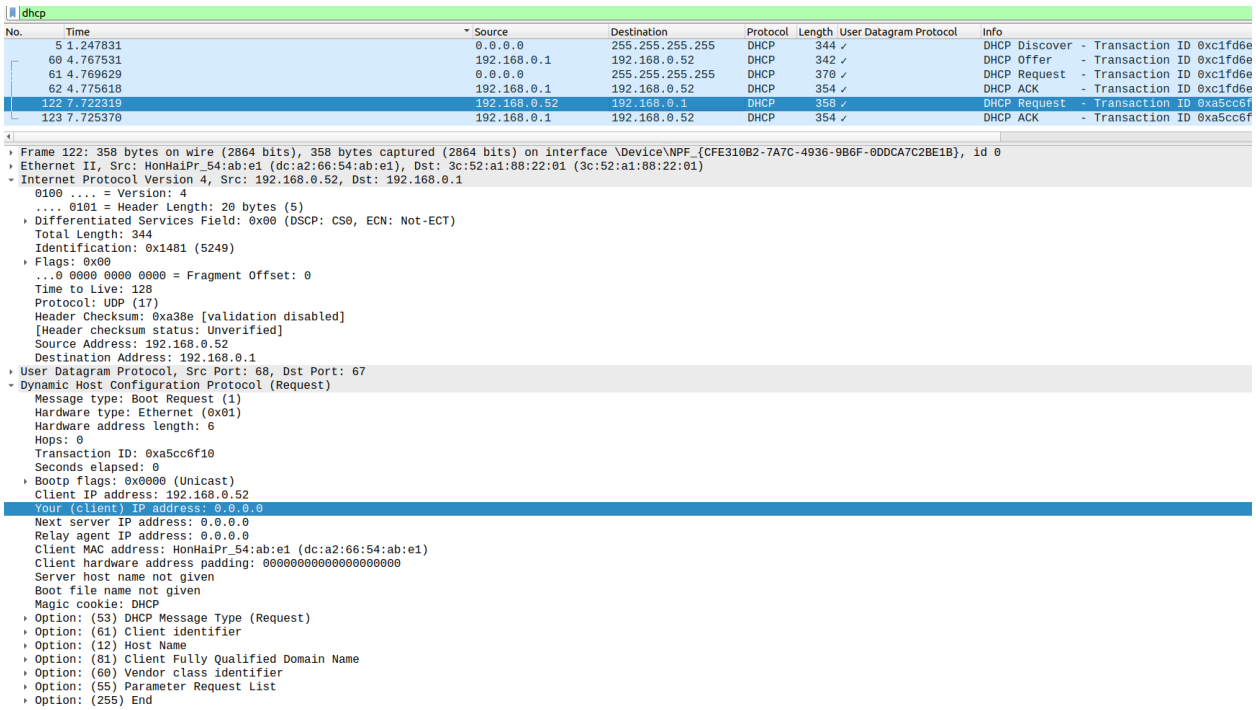


These options are explicitly requested in the **Parameter Request List (Option 55)** of the DHCP Discover packet and are provided in the DHCP Offer packet as part of the server's response.

10. In the DHCP Discover and Request packets, the client IP address is 0.0.0.0, so on what basis does the DHCP server know from where the request has been raised?







In both DHCP Discover and DHCP Request packets, the client IP address is set to **0.0.0.0** because the client has not yet been assigned an IP address. However, the DHCP server identifies the client and knows where the request comes from based on the following factors:

1. Client MAC Address (Hardware Address)

- The client's **MAC address** is included in the **Client Hardware Address** field of the DHCP packet.
- This MAC address is a unique identifier for the client's network interface card (NIC).
- The DHCP server uses this MAC address to track the request, identify the client, and assign an IP address.

2. Transaction ID

- Each DHCP Discover packet includes a unique **Transaction ID**.
- This allows the DHCP server to distinguish between multiple requests and track the request-response cycle for each client.

3. Broadcast Mechanism

- The DHCP Discover message is sent as a **broadcast (255.255.255.255)** since the client does not yet have an IP address to directly target the server.
- The server receives this broadcast and identifies the requesting client using the MAC address provided in the message.

4. Server's Network Interface Context

- The DHCP server receives the request on a particular **network interface or subnet**, helping it determine from which network segment the request has originated.
- This is particularly useful when the DHCP server is connected to multiple networks.

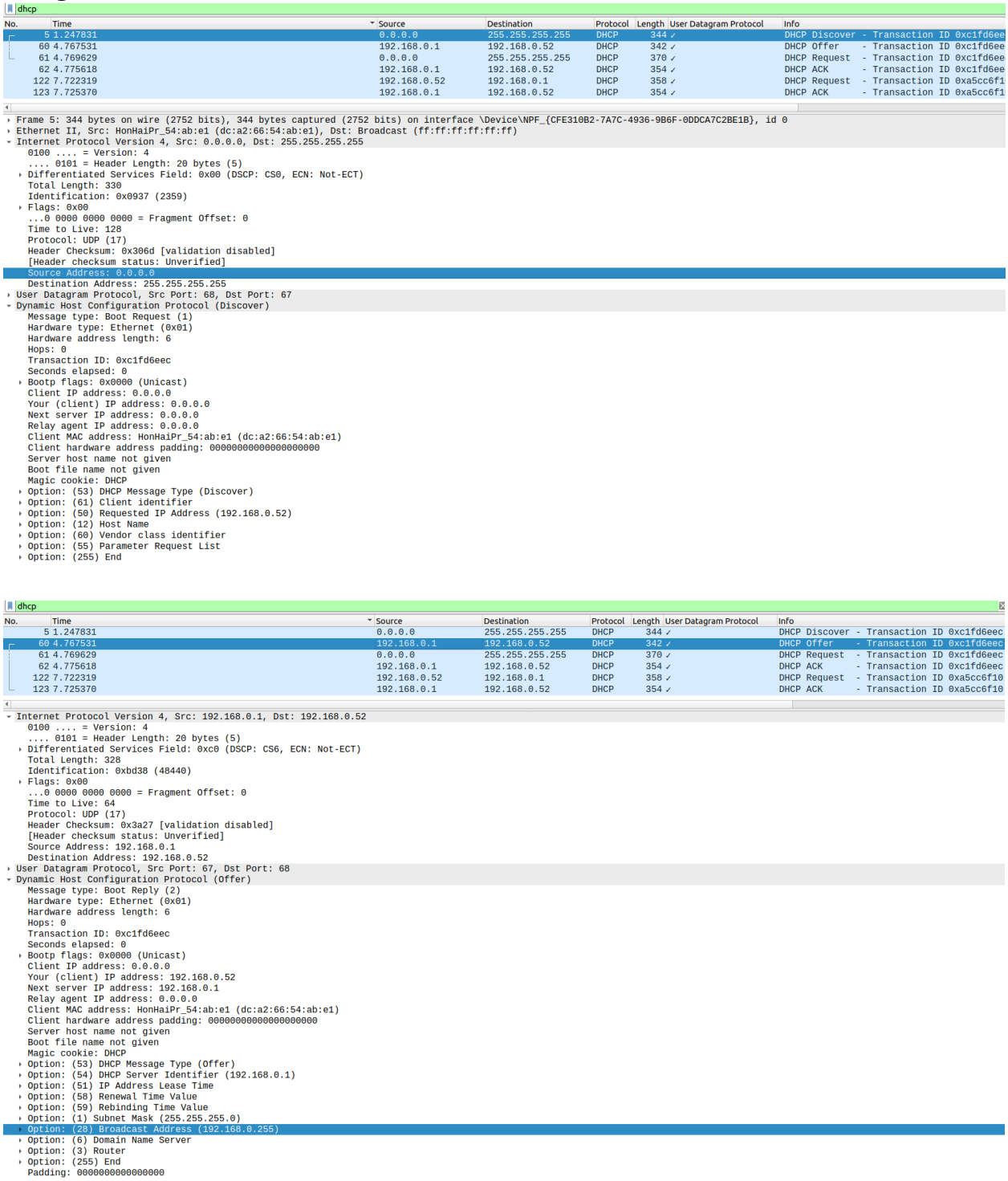
5. Relay Agent IP Address (If Applicable)

- If a **DHCP relay agent** is used, it sets the **Relay Agent IP Address (giaddr field)** in the DHCP packet.
- This indicates the network or subnet from where the request was raised, allowing the server to respond appropriately.

How the Server Knows Where to Respond:

- The server uses the Client MAC address in the packet to know which device made the request.
- The DHCP Offer message is either broadcasted or directed to that MAC address, ensuring the client receives the response, even though its IP address is 0.0.0.0.

11. What is the broadcast IP address used in the DHCP communication, and why is it significant?



dhcp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
5	1.247831	0.0.0.0	255.255.255.255	DHCP	344 ✓		DHCP Discover - Transaction ID 0xc1fd6ee
60	4.767531	192.168.0.1	192.168.0.52	DHCP	342 ✓		DHCP Offer - Transaction ID 0xc1fd6ee
61	4.769629	0.0.0.0	255.255.255.255	DHCP	370 ✓		DHCP Request - Transaction ID 0xc1fd6ee
62	4.775618	192.168.0.1	192.168.0.52	DHCP	354 ✓		DHCP ACK - Transaction ID 0xc1fd6ee
122	7.722319	192.168.0.52	192.168.0.1	DHCP	358 ✓		DHCP Request - Transaction ID 0xa5cc6f1
123	7.725370	192.168.0.1	192.168.0.52	DHCP	354 ✓		DHCP ACK - Transaction ID 0xa5cc6f1

```
▸ Frame 5: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{CFE310B2-7A7C-4936-9B6F-0DDCA7C2BE1B}, id 0
▸ Ethernet II, Src: HonHaiPr_54:ab:e1 (dc:a2:66:54:ab:e1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▾ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 330
    Identification: 0x0937 (2359)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x306d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 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: 0xc1fd6eec
    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: HonHaiPr_54:ab:e1 (dc:a2:66:54:ab:e1)
    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 (192.168.0.52)
  ▸ Option: (12) Host Name
  ▸ Option: (60) Vendor class identifier
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
```


dhcp

No.	Time	Source	Destination	Protocol	Length	User Datagram Protocol	Info
5	1.247831	0.0.0.0	255.255.255.255	DHCP	344 ✓		DHCP Discover - Transaction ID 0xc1fd6eec
60	4.767531	192.168.0.1	192.168.0.52	DHCP	342 ✓		DHCP Offer - Transaction ID 0xc1fd6eec
61	4.769629	0.0.0.0	255.255.255.255	DHCP	370 ✓		DHCP Request - Transaction ID 0xc1fd6eec
62	4.775618	192.168.0.1	192.168.0.52	DHCP	354 ✓		DHCP ACK - Transaction ID 0xc1fd6eec
122	7.722319	192.168.0.52	192.168.0.1	DHCP	358 ✓		DHCP Request - Transaction ID 0xa5cc6f10
123	7.725370	192.168.0.1	192.168.0.52	DHCP	354 ✓		DHCP ACK - Transaction ID 0xa5cc6f10

```
▾ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.52
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xbd38 (48440)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x3a27 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.52
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc1fd6eec
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.0.52
    Next server IP address: 192.168.0.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: HonHaiPr_54:ab:e1 (dc:a2:66:54:ab:e1)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (54) DHCP Server Identifier (192.168.0.1)
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (28) Broadcast Address (192.168.0.255)
  ▸ Option: (6) Domain Name Server
  ▸ Option: (3) Router
  ▸ Option: (255) End
    Padding: 0000000000000000
```

Broadcast IP Address Used:

- The broadcast IP address used by the client in DHCP communication is **255.255.255.255** (limited broadcast).
- Additionally, the DHCP server provides the **subnet broadcast address** (e.g., **192.168.0.255**) in the DHCP Offer packet (Option 28).

Significance:

1. 255.255.255.255 (Limited Broadcast)

- **Used in DHCP Discover and Request packets.**
- Since the client does not yet have an IP address, it uses this broadcast address to send the Discover message.
- This ensures that **all DHCP servers on the local network** receive the request, even though the client does not know their IPs.
- **Source IP:** 0.0.0.0 | **Destination IP:** 255.255.255.255 in Discover and Request.

2. 192.168.0.255 (Subnet Broadcast Address)

- Provided by the server in the DHCP Offer (via **Option 28**).
- Indicates the broadcast address of the subnet (in this case, **192.168.0.255**).
- Helps the client know the correct broadcast address for that subnet, which will be used after the IP is assigned.

3. Ensures Server Reachability

- The use of 255.255.255.255 guarantees that any DHCP server on the network will receive the client's Discover packet.
- The server responds with a DHCP Offer, often broadcasted as well if the client is still without an IP.

4. DHCP Relay and Cross-Subnet Communication

- If a **DHCP relay agent** is present (giaddr field), it forwards the client's broadcast to the server via **unicast**.
- This allows DHCP to function across different subnets, while the client's initial request still uses **255.255.255.255**.

5. Pre-Assignment Communication

- Before IP assignment, the client cannot send unicast packets.
- **Broadcasting** allows communication with the DHCP server without needing an IP address.

Wireshark Confirmation:

- **DHCP Discover & Request:**
  - Source IP: 0.0.0.0
  - Destination IP: 255.255.255.255
- **DHCP Offer:**
  - Contains **Option 28: Broadcast Address = 192.168.0.255**

Result:

- **255.255.255.255** is crucial for initial DHCP communication, ensuring server reachability without an assigned client IP.
- The **subnet broadcast address** (e.g., 192.168.0.255) is used for subnet-specific broadcasts after assignment.

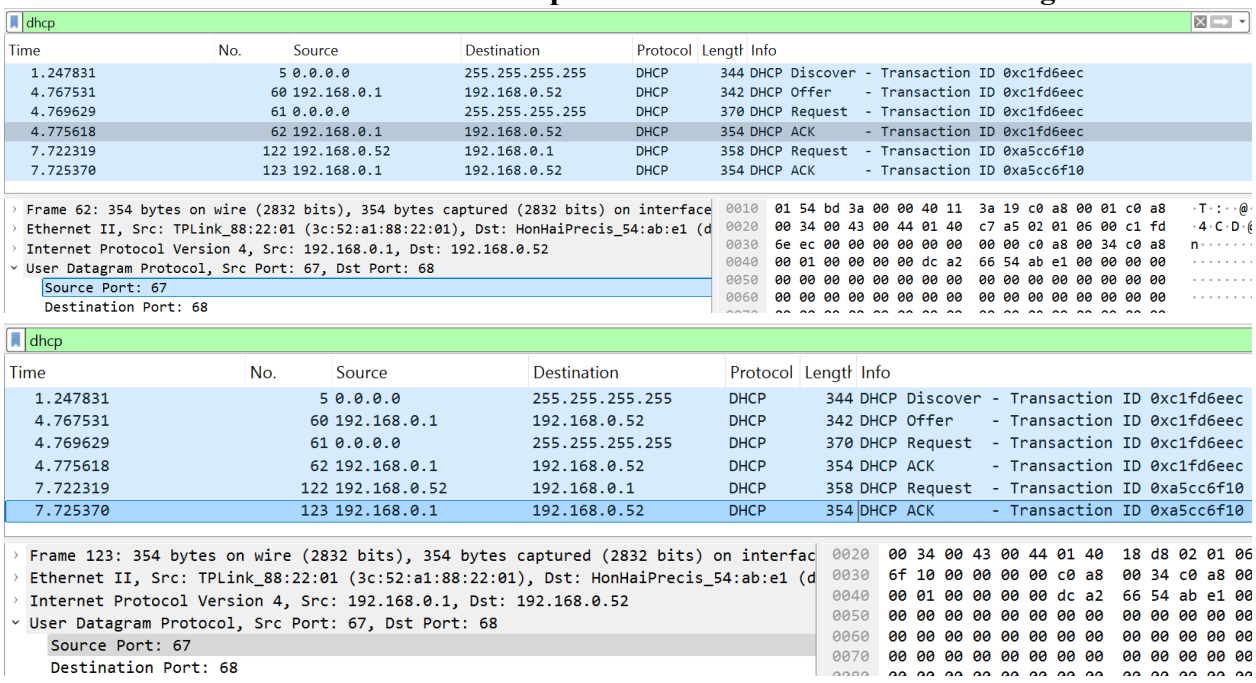
12. Which transport layer protocol and its standard port number is used for DHCP ACK message exchange?

The transport layer protocol used for DHCP ACK message exchange is **UDP (User Datagram Protocol).**
The standard port numbers used in DHCP communication are:

- **UDP Port 67 (Source - DHCP Server)**
- **UDP Port 68 (Destination - DHCP Client)**

Thus, DHCP uses UDP on ports 67 and 68 for message exchange, including the DHCP ACK message.

13. What are the source and destination port numbers in DHCP ACK message?



- **Source Port Number: 67**
  The DHCP server uses port 67 as its source port when sending a DHCP ACK message. This is the standard port for DHCP servers.
- **Destination Port Number: 68**
  The DHCP client listens on port 68 and receives the DHCP ACK message on this port. This is the standard port for DHCP clients.

14. What is unique about the source and destination IP addresses in the DHCP ACK message?

Unique Aspects of the IP Addresses in a DHCP ACK Message:

1. Source IP Address (DHCP Server IP)

- The source IP address in the DHCP ACK message is the **IP address of the DHCP server** (e.g., **192.168.0.1** in Wireshark capture).
- This confirms that the message is authoritative and originates from the server that has assigned the IP lease.
- It helps the client identify the DHCP server it is communicating with.

2. Destination IP Address (Client IP Address)

- The destination IP address is **either the newly assigned IP address of the client** (e.g., **192.168.0.52**) or, in some cases, **255.255.255.255 (broadcast)** if the client is not yet fully configured.
- This is unique because:
  - Earlier in the process, the client had **0.0.0.0** as its IP address.
  - Now, the DHCP server communicates directly with the client using the IP address it just assigned, or via broadcast to ensure the client receives the ACK before configuration is complete.

Significance of This Uniqueness:

- The DHCP ACK message is the **final step** in the **DORA (Discover, Offer, Request, Acknowledge)** process.
- By sending the ACK with the client's assigned IP as the destination, the server confirms that the IP lease is granted and finalized.
- If broadcast is used (255.255.255.255), it ensures that the client, even without fully applying the assigned IP, can still receive the acknowledgment.
- After receiving the ACK, the client configures its network stack with the assigned IP address.

Result: The DHCP ACK message is unique because it comes from the **server's IP** and is directed to either the **newly assigned client IP** or **broadcast address**, marking the official completion of the IP address assignment process.

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).

References

- https://superuser.com/questions/1614467/why-does-dhcp-server-prefer-unicasting-over-broadcasting-and-at-what-cost
- https://forum.networklessons.com/t/introduction-to-dhcp/970/71?u=lagapidis
- https://networkengineering.stackexchange.com/questions/11120/how-dhcp-offer-unicast-works?rq=1
- https://notes.networklessons.com/dhcp-offer-message-sent-as-broadcast