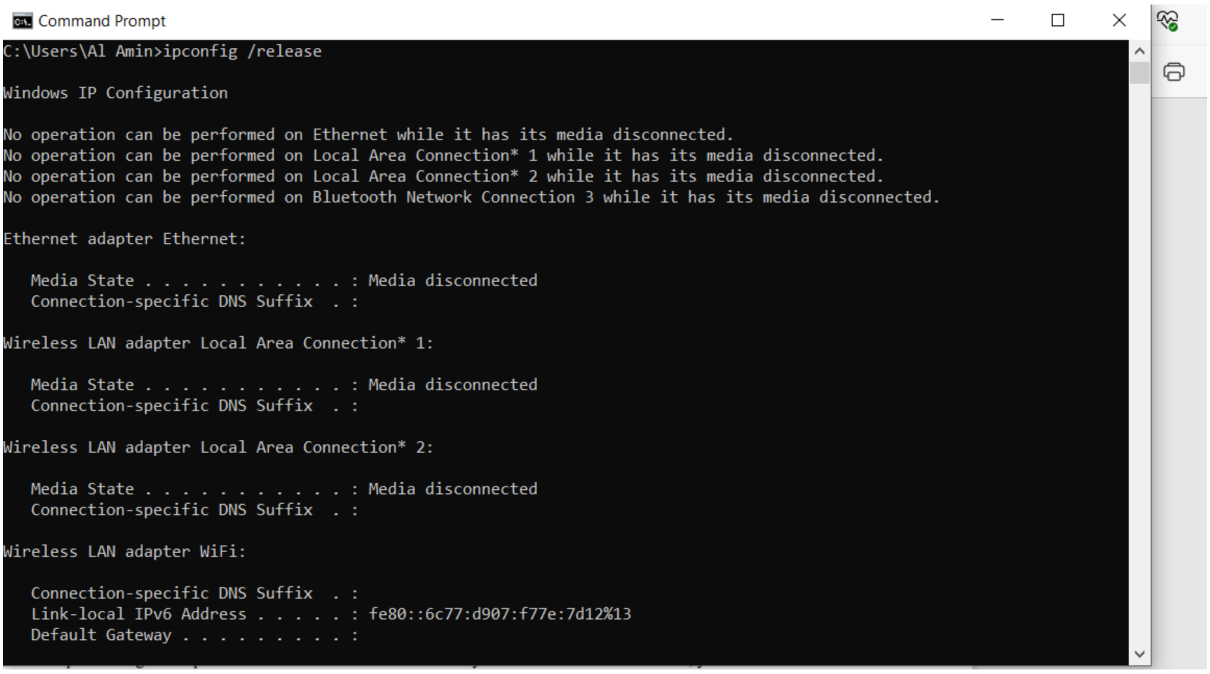
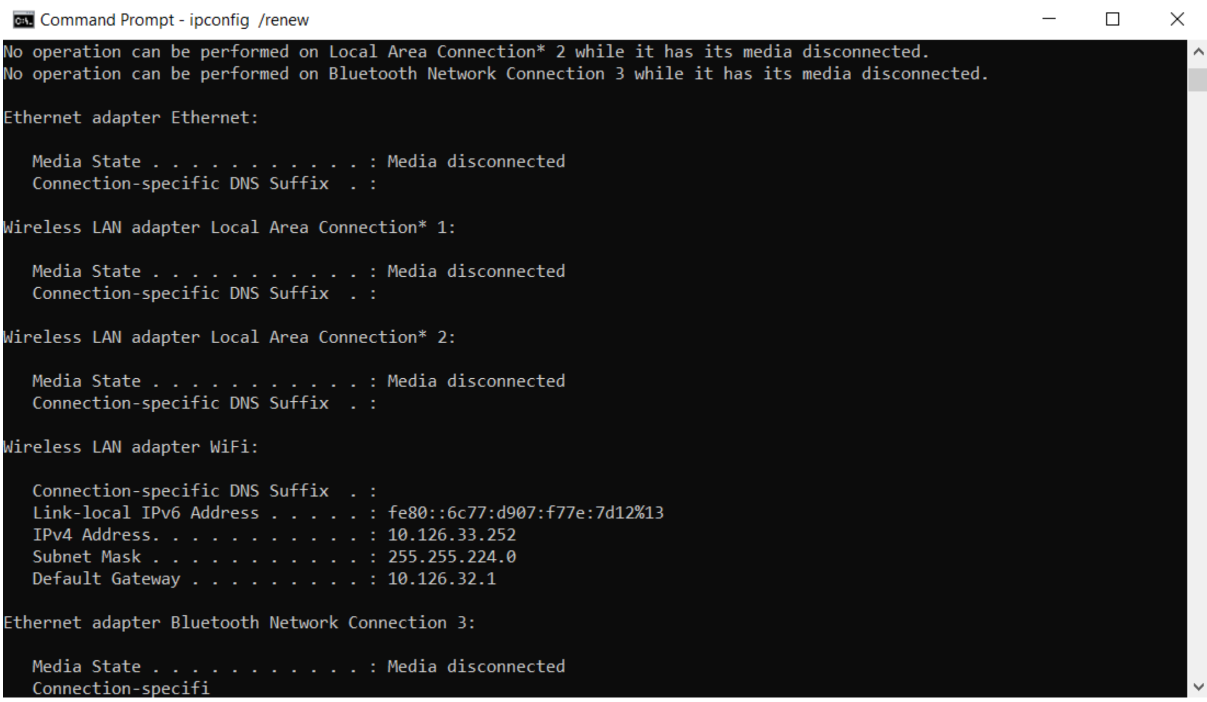
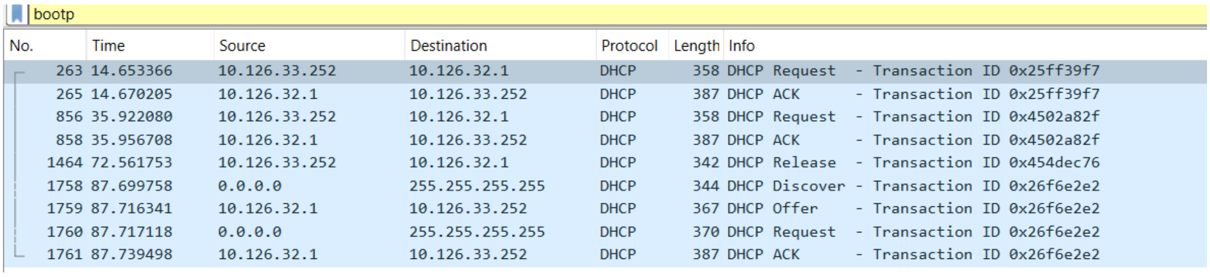


```
C:\Users\Al Amin>ipconfig /release

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* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection 3 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* 2:

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

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c77:d907:f77e:7d12%13
   Default Gateway . . . . . . . . . :
```



```
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection 3 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* 2:

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

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6c77:d907:f77e:7d12%13
   IPv4 Address. . . . . . . . . . . : 10.126.33.252
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Default Gateway . . . . . . . . . : 10.126.32.1

Ethernet adapter Bluetooth Network Connection 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specifi
```

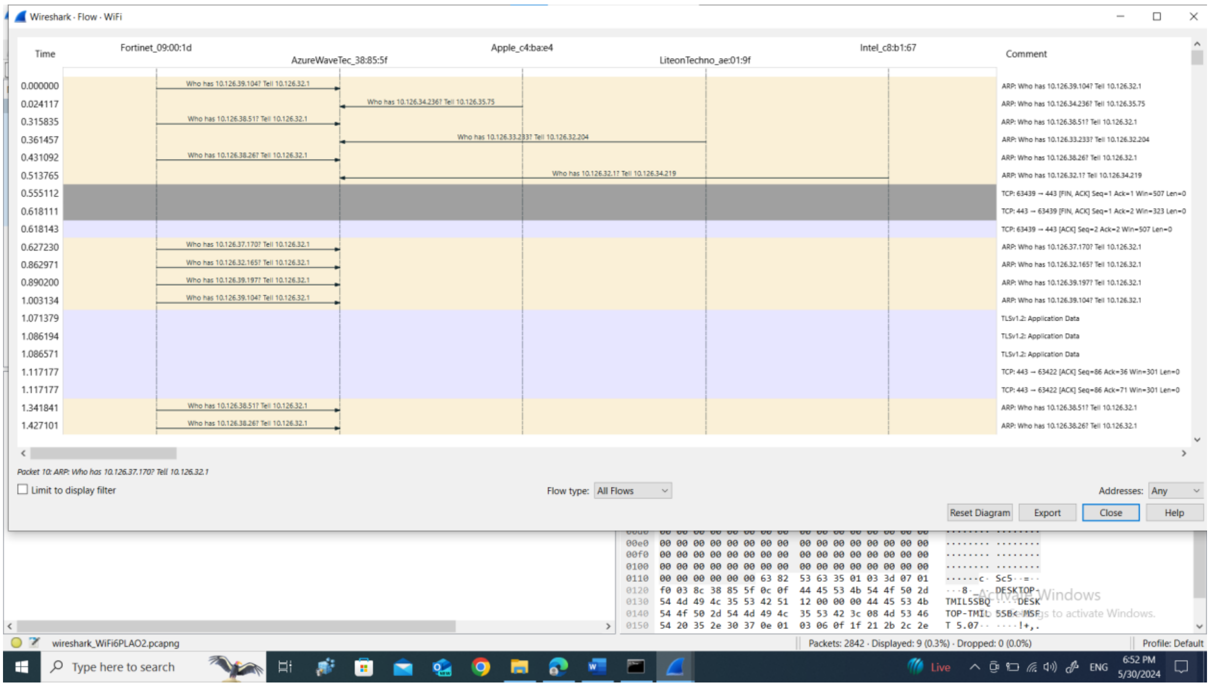
1. Are DHCP messages sent over UDP or TCP?



No.	Time	Source	Destination	Protocol	Length	Info
263	14.653366	10.126.33.252	10.126.32.1	DHCP	358	DHCP Request - Transaction ID 0x25ff39f7
265	14.670205	10.126.32.1	10.126.33.252	DHCP	387	DHCP ACK - Transaction ID 0x25ff39f7
856	35.922080	10.126.33.252	10.126.32.1	DHCP	358	DHCP Request - Transaction ID 0x4502a82f
858	35.956708	10.126.32.1	10.126.33.252	DHCP	387	DHCP ACK - Transaction ID 0x4502a82f
1464	72.561753	10.126.33.252	10.126.32.1	DHCP	342	DHCP Release - Transaction ID 0x454dec76
1758	87.699758	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x26f6e2e2
1759	87.716341	10.126.32.1	10.126.33.252	DHCP	367	DHCP Offer - Transaction ID 0x26f6e2e2
1760	87.717118	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x26f6e2e2
1761	87.739498	10.126.32.1	10.126.33.252	DHCP	387	DHCP ACK - Transaction ID 0x26f6e2e2

2. 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?


Wireshark · Flow · WiFi
Fortinet_09:00:1d
AzureWaveTec_38:85:5f
Apple_c4:ba:e4
LiteonTechno_ae:01:9f
Intel_c8:b1:67
Who has 10.126.39.104? Tell 10.126.32.1
Who has 10.126.34.236? Tell 10.126.35.75
Who has 10.126.38.51? Tell 10.126.32.1
Who has 10.126.33.233? Tell 10.126.32.204
Who has 10.126.38.26? Tell 10.126.32.1
Who has 10.126.32.1? Tell 10.126.34.219
Who has 10.126.37.170? Tell 10.126.32.1
Who has 10.126.32.165? Tell 10.126.32.1
Who has 10.126.39.197? Tell 10.126.32.1
Who has 10.126.39.104? Tell 10.126.32.1
Who has 10.126.38.51? Tell 10.126.32.1
Who has 10.126.38.26? Tell 10.126.32.1
Reset Diagram
Export
Close
Help
Type here to search
Live
ENG
6:52 PM
5/30/2024

```
Time      Comment
0.000000  ARP: Who has 10.126.39.104? Tell 10.126.32.1
0.024117  ARP: Who has 10.126.34.236? Tell 10.126.35.75
0.315835  ARP: Who has 10.126.38.51? Tell 10.126.32.1
0.361457  ARP: Who has 10.126.33.233? Tell 10.126.32.204
0.431092  ARP: Who has 10.126.38.26? Tell 10.126.32.1
0.513765  ARP: Who has 10.126.32.1? Tell 10.126.34.219
0.555112  TCP: 63439 → 443 [FIN, ACK] Seq=1 Ack=1 Win=507 Len=0
0.618111  TCP: 443 → 63439 [FIN, ACK] Seq=1 Ack=2 Win=323 Len=0
0.618143  TCP: 63439 → 443 [ACK] Seq=2 Ack=2 Win=507 Len=0
0.627230  ARP: Who has 10.126.37.170? Tell 10.126.32.1
0.862971  ARP: Who has 10.126.32.165? Tell 10.126.32.1
0.890200  ARP: Who has 10.126.39.197? Tell 10.126.32.1
1.003134  ARP: Who has 10.126.39.104? Tell 10.126.32.1
1.071379  TLSv1.2: Application Data
1.086194  TLSv1.2: Application Data
1.086571  TLSv1.2: Application Data
1.117177  TCP: 443 → 63422 [ACK] Seq=86 Ack=36 Win=301 Len=0
1.117177  TCP: 443 → 63422 [ACK] Seq=86 Ack=71 Win=301 Len=0
1.341841  ARP: Who has 10.126.38.51? Tell 10.126.32.1
1.427101  ARP: Who has 10.126.38.26? Tell 10.126.32.1
```

Packet 10: ARP: Who has 10.126.37.170? Tell 10.126.32.1

□ Limit to display filter

Flow type: All Flows

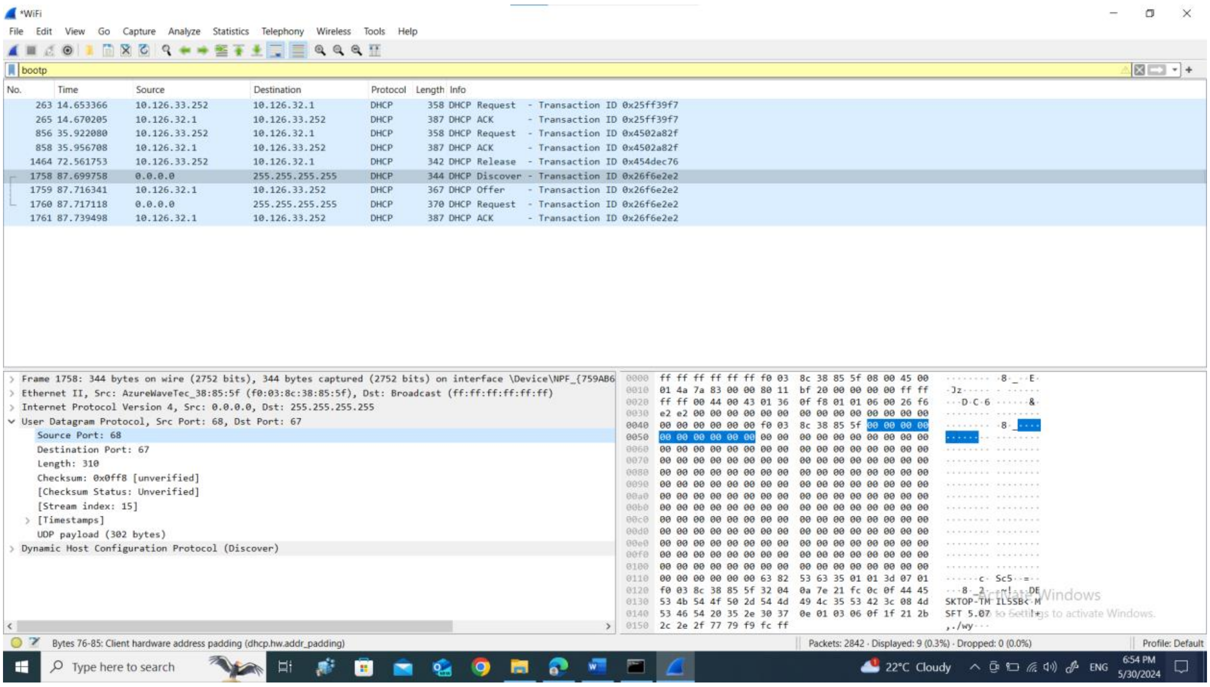
Addresses: Any

```
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  f0 03 8c 38 85 5f 0c 0f  44 45 53 4b 54 4f 50 2d   ···8·_·· DESKTOP-
0130  54 4d 49 4c 35 53 42 51  12 00 00 00 44 45 53 4b   TMIL5SBQ ····DESK
0140  54 4f 50 2d 54 4d 49 4c  35 53 42 3c 08 4d 53 46   TOP-TMIL 5SB<·MSF
0150  54 20 35 2e 30 37 0e 01  03 06 0f 1f 21 2b 2c 2e   T 5.07·· ····!+,.
```

wireshark_WiFi6PLAO2.pcapng

Packets: 2842 · Displayed: 9 (0.3%) · Dropped: 0 (0.0%)

Profile: Default



bootp

```
No.   Time       Source         Destination      Protocol Length Info
  263 14.653366  10.126.33.252  10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x25ff39f7
  265 14.670205  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x25ff39f7
  856 35.922080  10.126.33.252  10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x4502a82f
  858 35.956708  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x4502a82f
 1464 72.561753  10.126.33.252  10.126.32.1      DHCP     342 DHCP Release  - Transaction ID 0x454dec76
 1758 87.699758  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x26f6e2e2
 1759 87.716341  10.126.32.1    10.126.33.252    DHCP     367 DHCP Offer    - Transaction ID 0x26f6e2e2
 1760 87.717118  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x26f6e2e2
 1761 87.739498  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

```
> Frame 1758: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{759AB6
> Ethernet II, Src: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 310
    Checksum: 0x0ff8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
  > [Timestamps]
    UDP payload (302 bytes)
> Dynamic Host Configuration Protocol (Discover)
```

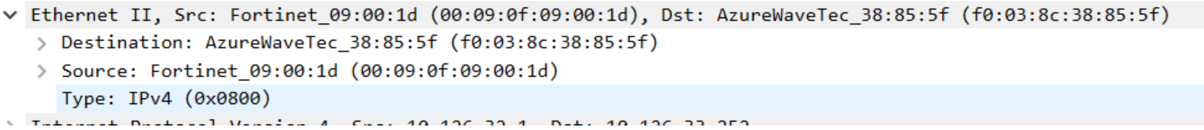
```
0000  ff ff ff ff ff ff f0 03  8c 38 85 5f 08 00 45 00   ······· ·8·_··E·
0010  01 4a 7a 83 00 00 80 11  bf 20 00 00 00 00 ff ff   ·Jz····· ·· ····
0020  ff ff 00 44 00 43 01 36  0f f8 01 01 06 00 26 f6   ···D·C·6 ······&·
0030  e2 e2 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 f0 03  8c 38 85 5f 00 00 00 00   ········ ·8·_····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ······c· Sc5··=··
0120  f0 03 8c 38 85 5f 32 04  0a 7e 21 fc 0c 0f 44 45   ···8·_2· ·~!···DE
0130  53 4b 54 4f 50 2d 54 4d  49 4c 35 53 42 3c 08 4d   SKTOP-TM IL5SB<·M
0140  53 46 54 20 35 2e 30 37  0e 01 03 06 0f 1f 21 2b   SFT 5.07 ······!+
0150  2c 2e 2f 77 79 f9 fc ff                            ,./wy···
```

Bytes 76-85: Client hardware address padding (dhcp.hw.addr_padding)

Packets: 2842 · Displayed: 9 (0.3%) · Dropped: 0 (0.0%)

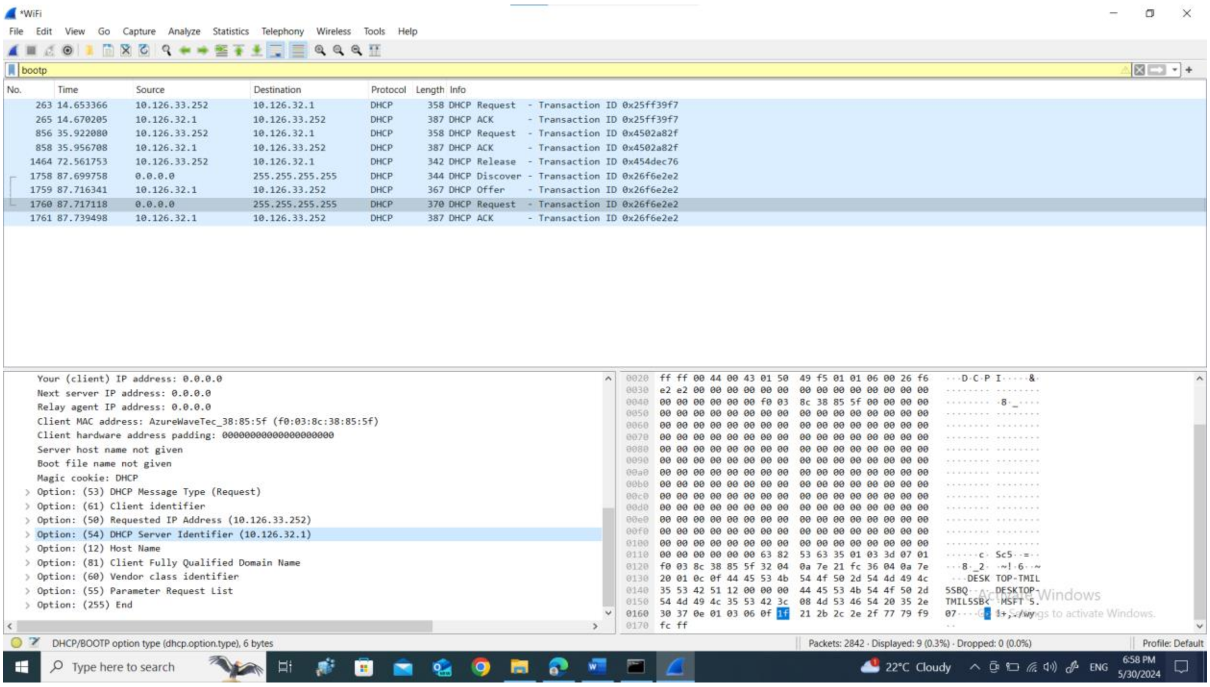
Profile: Default

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



```
v Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
  > Destination: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
  > Source: Fortinet_09:00:1d (00:09:0f:09:00:1d)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.126.32.1, Dst: 10.126.33.252
```

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



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
bootp
Type here to search
22°C Cloudy
ENG
6:58 PM
5/30/2024

```
No.   Time       Source          Destination      Protocol Length Info
  263 14.653366  10.126.33.252   10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x25ff39f7
  265 14.670205  10.126.32.1     10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x25ff39f7
  856 35.922080  10.126.33.252   10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x4502a82f
  858 35.956708  10.126.32.1     10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x4502a82f
 1464 72.561753  10.126.33.252   10.126.32.1      DHCP     342 DHCP Release  - Transaction ID 0x454dec76
 1758 87.699758  0.0.0.0         255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x26f6e2e2
 1759 87.716341  10.126.32.1     10.126.33.252    DHCP     367 DHCP Offer    - Transaction ID 0x26f6e2e2
 1760 87.717118  0.0.0.0         255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x26f6e2e2
 1761 87.739498  10.126.32.1     10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

```
    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: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
    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 (10.126.33.252)
  > Option: (54) DHCP Server Identifier (10.126.32.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

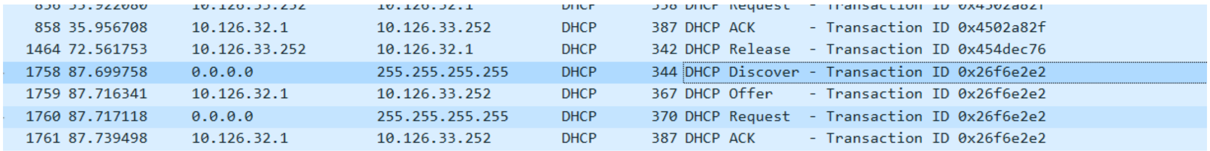
```
0020  ff ff 00 44 00 43 01 50  49 f5 01 01 06 00 26 f6   ···D·C·P I·····&·
0030  e2 e2 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 f0 03  8c 38 85 5f 00 00 00 00   ········ ·8·_····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  f0 03 8c 38 85 5f 32 04  0a 7e 21 fc 36 04 0a 7e   ···8·_2· ·~!·6··~
0130  20 01 0c 0f 44 45 53 4b  54 4f 50 2d 54 4d 49 4c    ···DESK TOP-TMIL
0140  35 53 42 51 12 00 00 00  44 45 53 4b 54 4f 50 2d   5SBQ···· DESKTOP-
0150  54 4d 49 4c 35 53 42 3c  08 4d 53 46 54 20 35 2e   TMIL5SB< ·MSFT 5.
0160  30 37 0e 01 03 06 0f 1f  21 2b 2c 2e 2f 77 79 f9   07······ !+,./wy·
0170  fc ff                                              ··
```

DHCP/BOOTP option type (dhcp.option.type), 6 bytes

Packets: 2842 · Displayed: 9 (0.3%) · Dropped: 0 (0.0%)

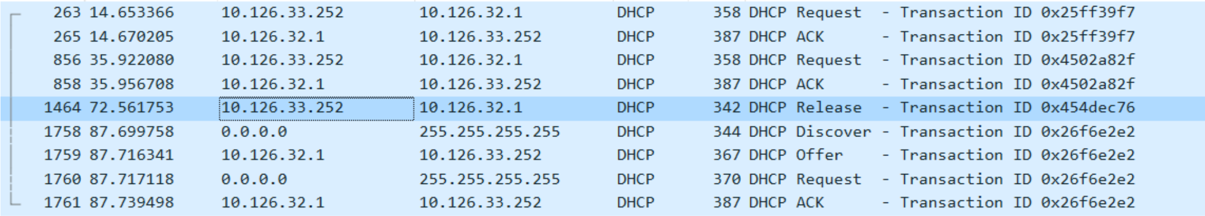
Profile: Default

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?



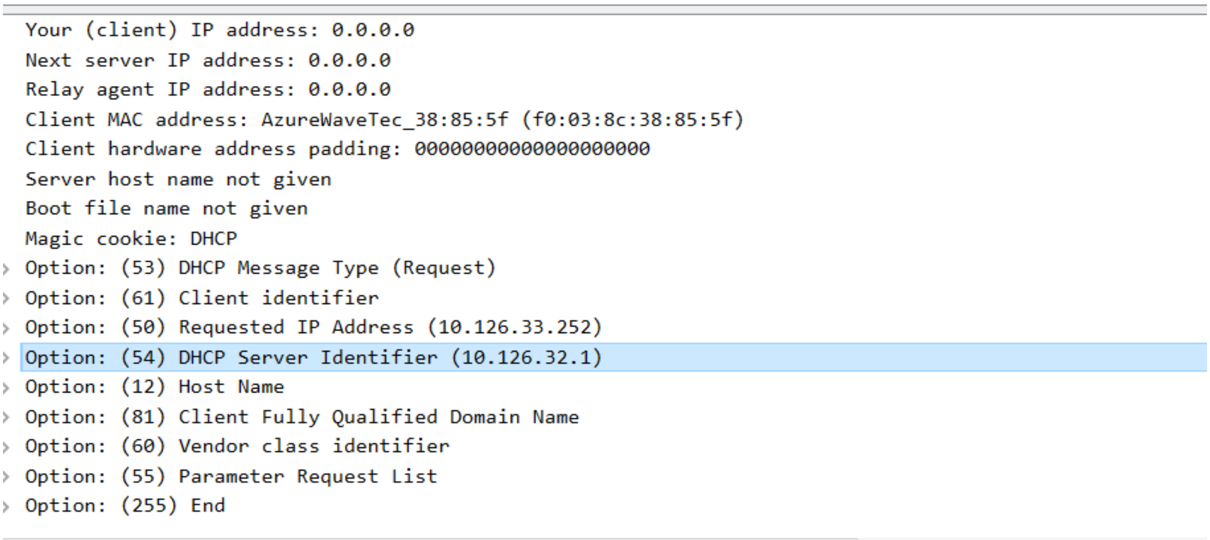
```
  856 35.922080  10.126.33.252  10.126.32.1      DHCP  358 DHCP Request  - Transaction ID 0x4502a82f
  858 35.956708  10.126.32.1    10.126.33.252    DHCP  387 DHCP ACK      - Transaction ID 0x4502a82f
 1464 72.561753  10.126.33.252  10.126.32.1      DHCP  342 DHCP Release  - Transaction ID 0x454dec76
 1758 87.699758  0.0.0.0        255.255.255.255  DHCP  344 DHCP Discover - Transaction ID 0x26f6e2e2
 1759 87.716341  10.126.32.1    10.126.33.252    DHCP  367 DHCP Offer    - Transaction ID 0x26f6e2e2
 1760 87.717118  0.0.0.0        255.255.255.255  DHCP  370 DHCP Request  - Transaction ID 0x26f6e2e2
 1761 87.739498  10.126.32.1    10.126.33.252    DHCP  387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

6. 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.



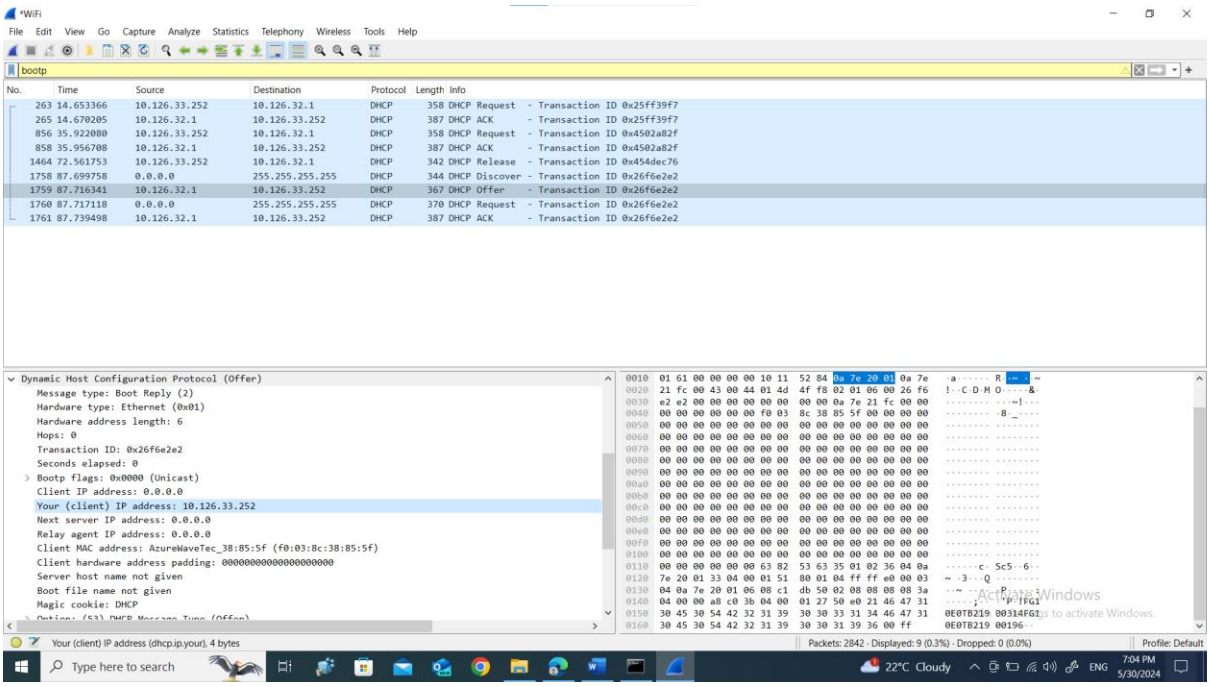
```
  263 14.653366  10.126.33.252  10.126.32.1      DHCP  358 DHCP Request  - Transaction ID 0x25ff39f7
  265 14.670205  10.126.32.1    10.126.33.252    DHCP  387 DHCP ACK      - Transaction ID 0x25ff39f7
  856 35.922080  10.126.33.252  10.126.32.1      DHCP  358 DHCP Request  - Transaction ID 0x4502a82f
  858 35.956708  10.126.32.1    10.126.33.252    DHCP  387 DHCP ACK      - Transaction ID 0x4502a82f
 1464 72.561753  10.126.33.252  10.126.32.1      DHCP  342 DHCP Release  - Transaction ID 0x454dec76
 1758 87.699758  0.0.0.0        255.255.255.255  DHCP  344 DHCP Discover - Transaction ID 0x26f6e2e2
 1759 87.716341  10.126.32.1    10.126.33.252    DHCP  367 DHCP Offer    - Transaction ID 0x26f6e2e2
 1760 87.717118  0.0.0.0        255.255.255.255  DHCP  370 DHCP Request  - Transaction ID 0x26f6e2e2
 1761 87.739498  10.126.32.1    10.126.33.252    DHCP  387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

7. What is the IP address of your DHCP server?



```
  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: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
  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 (10.126.33.252)
> Option: (54) DHCP Server Identifier (10.126.32.1)
> Option: (12) Host Name
> Option: (81) Client Fully Qualified Domain Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End
```

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.



bootp

```
No.   Time       Source         Destination      Protocol Length Info
  263 14.653366  10.126.33.252  10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x25ff39f7
  265 14.670205  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x25ff39f7
  856 35.922080  10.126.33.252  10.126.32.1      DHCP     358 DHCP Request  - Transaction ID 0x4502a82f
  858 35.956708  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x4502a82f
 1464 72.561753  10.126.33.252  10.126.32.1      DHCP     342 DHCP Release  - Transaction ID 0x454dec76
 1758 87.699758  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x26f6e2e2
 1759 87.716341  10.126.32.1    10.126.33.252    DHCP     367 DHCP Offer    - Transaction ID 0x26f6e2e2
 1760 87.717118  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x26f6e2e2
 1761 87.739498  10.126.32.1    10.126.33.252    DHCP     387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

```
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x26f6e2e2
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.126.33.252
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
```

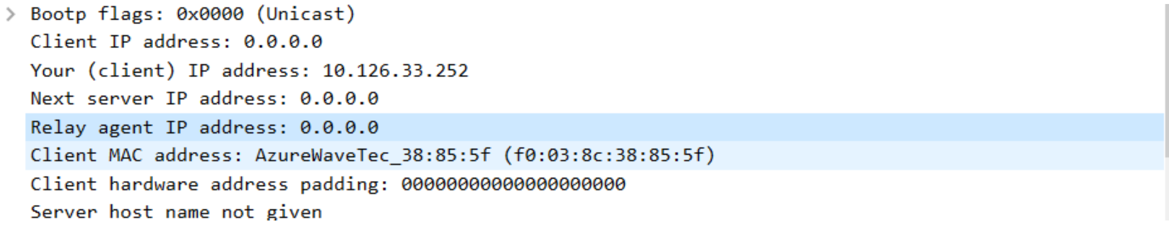
```
0010  01 61 00 00 00 00 10 11  52 84 0a 7e 20 01 0a 7e
0020  21 fc 00 43 00 44 01 4d  4f f8 02 01 06 00 26 f6
0030  e2 e2 00 00 00 00 00 00  00 00 0a 7e 21 fc 00 00
0040  00 00 00 00 00 00 f0 03  8c 38 85 5f 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 36 04 0a
0120  7e 20 01 33 04 00 01 51  80 01 04 ff ff e0 00 03
0130  04 0a 7e 20 01 06 08 c1  db 50 02 08 08 08 08 3a
0140  04 00 00 a8 c0 3b 04 00  01 27 50 e0 21 46 47 31
0150  30 45 30 54 42 32 31 39  30 30 33 31 34 46 47 31   0E0TB219 00314FG1
0160  30 45 30 54 42 32 31 39  30 30 31 39 36 00 ff      0E0TB219 00196
```

Your (client) IP address (dhcp.ip.your), 4 bytes

Packets: 2842 · Displayed: 9 (0.3%) · Dropped: 0 (0.0%)

Profile: Default

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?

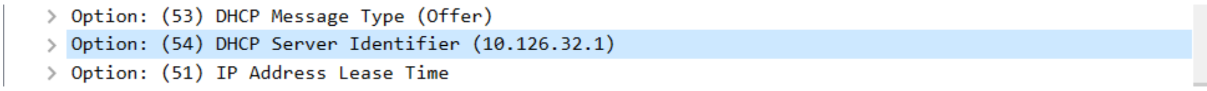


```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.126.33.252
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
  Client hardware address padding: 00000000000000000000
  Server host name not given
```

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

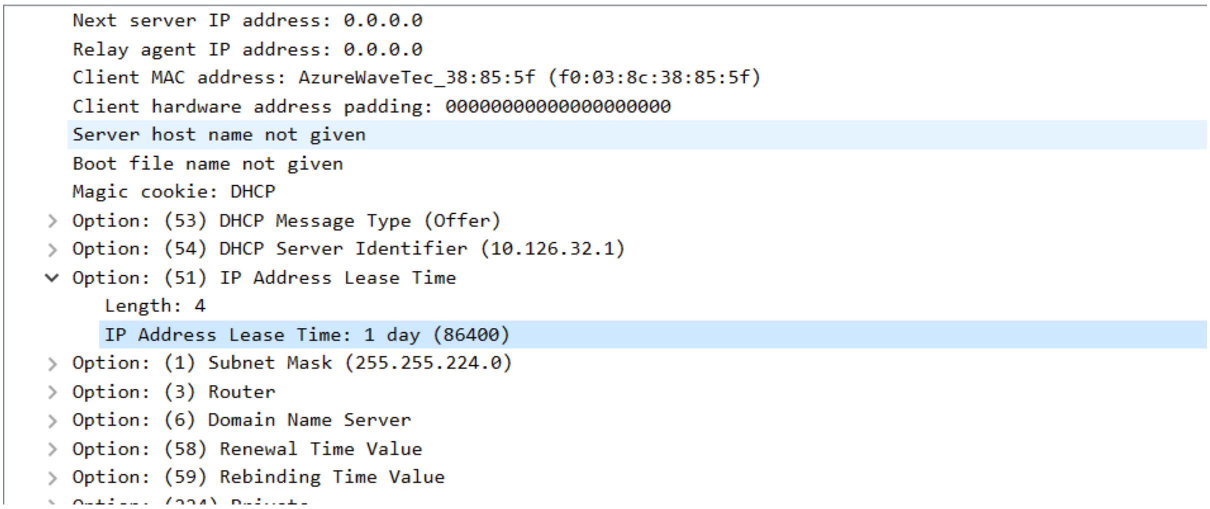
Ans. The router line indicates to the client which default router it should use to send messages while the subnet mask lines instruct the client on which subnet it should use.

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?



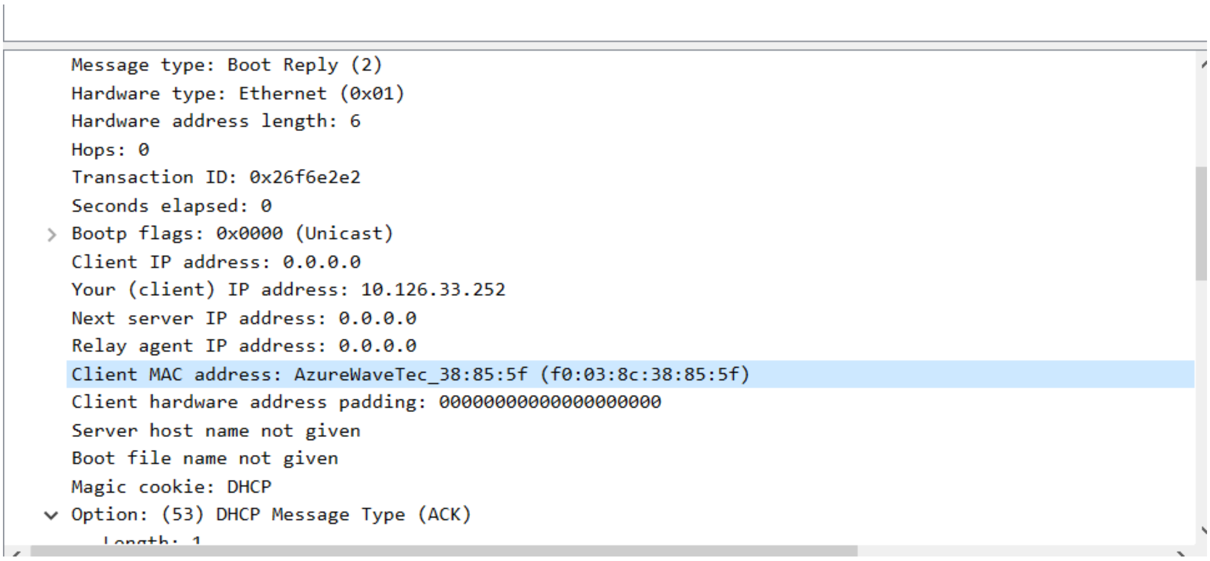
```
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (10.126.32.1)
  > Option: (51) IP Address Lease Time
```

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



```
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
    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 (10.126.32.1)
  v Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: 1 day (86400)
  > Option: (1) Subnet Mask (255.255.224.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (224) Private
```

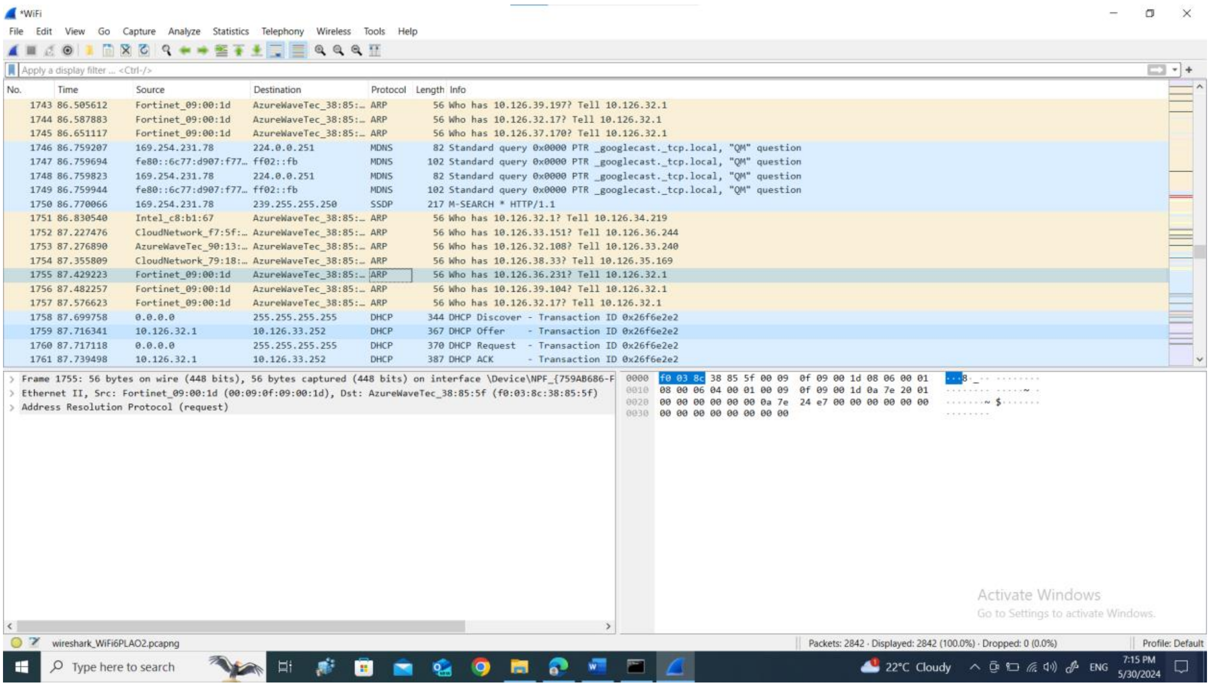
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?



```
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x26f6e2e2
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.126.33.252
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (ACK)
      Length: 1
```

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.



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time       Source                 Destination            Protocol Length Info
   1743 86.505612  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.39.197? Tell 10.126.32.1
   1744 86.587883  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.32.17? Tell 10.126.32.1
   1745 86.651117  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.37.170? Tell 10.126.32.1
   1746 86.759207  169.254.231.78         224.0.0.251            MDNS       82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
   1747 86.759694  fe80::6c77:d907:f77…   ff02::fb               MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
   1748 86.759823  169.254.231.78         224.0.0.251            MDNS       82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
   1749 86.759944  fe80::6c77:d907:f77…   ff02::fb               MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
   1750 86.770066  169.254.231.78         239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
   1751 86.830540  Intel_c8:b1:67         AzureWaveTec_38:85:…   ARP        56 Who has 10.126.32.1? Tell 10.126.34.219
   1752 87.227476  CloudNetwork_f7:5f:…   AzureWaveTec_38:85:…   ARP        56 Who has 10.126.33.151? Tell 10.126.36.244
   1753 87.276890  AzureWaveTec_90:13:…   AzureWaveTec_38:85:…   ARP        56 Who has 10.126.32.108? Tell 10.126.33.240
   1754 87.355809  CloudNetwork_79:18:…   AzureWaveTec_38:85:…   ARP        56 Who has 10.126.38.33? Tell 10.126.35.169
   1755 87.429223  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.36.231? Tell 10.126.32.1
   1756 87.482257  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.39.104? Tell 10.126.32.1
   1757 87.576623  Fortinet_09:00:1d      AzureWaveTec_38:85:…   ARP        56 Who has 10.126.32.17? Tell 10.126.32.1
   1758 87.699758  0.0.0.0                255.255.255.255        DHCP      344 DHCP Discover - Transaction ID 0x26f6e2e2
   1759 87.716341  10.126.32.1            10.126.33.252          DHCP      367 DHCP Offer    - Transaction ID 0x26f6e2e2
   1760 87.717118  0.0.0.0                255.255.255.255        DHCP      370 DHCP Request  - Transaction ID 0x26f6e2e2
   1761 87.739498  10.126.32.1            10.126.33.252          DHCP      387 DHCP ACK      - Transaction ID 0x26f6e2e2
```

```
> Frame 1755: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{759AB686-F
> Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
> Address Resolution Protocol (request)
```

```
0000  f0 03 8c 38 85 5f 00 09  0f 09 00 1d 08 06 00 01   ···8·_·· ········
0010  08 00 06 04 00 01 00 09  0f 09 00 1d 0a 7e 20 01   ········ ·····~ ·
0020  00 00 00 00 00 00 0a 7e  24 e7 00 00 00 00 00 00   ·······~ $·······
0030  00 00 00 00 00 00 00 00                            ········
```

Activate Windows
Go to Settings to activate Windows.
wireshark_WiFi6PLAO2.pcapng
Packets: 2842 · Displayed: 2842 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
22°C Cloudy
ENG
7:15 PM
5/30/2024

Ans. Purpose : the ARP is used to solve ip address to mac address within our local network.