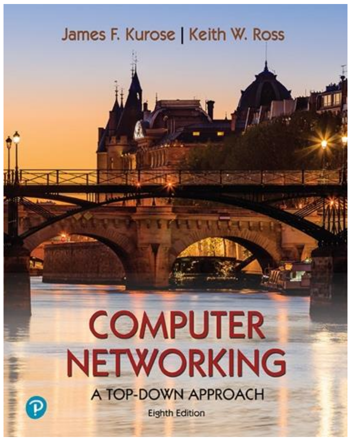
2151013087

Wireshark Lab: DHCP v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



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.

Before getting started, you'll probably want to review the coverage of DHCP in Section 4.4.3 in the text[1]. In particular, you'll want to pay close attention to Figure 4.24, since we'll be studying the DHCP Discover, Offer, Request and ACK messages shown in Figure 4.24.

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.

Gathering a Packet Trace

The first two steps in the DHCP protocol in Figure 4.24 (using the Discover and Offer messages) are optional (in the sense that they need not always be used when, for example, a new IP address is needed, or an existing DHCP address is to be renewed); the Request and ACK messages are not. 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:

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

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

[1] References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8h ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.* Our website for this book is http://gaia.cs.umass.edu/kurose_ross You'll find lots of interesting open material there.

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`.

3. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
4. 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 in 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 PC:

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

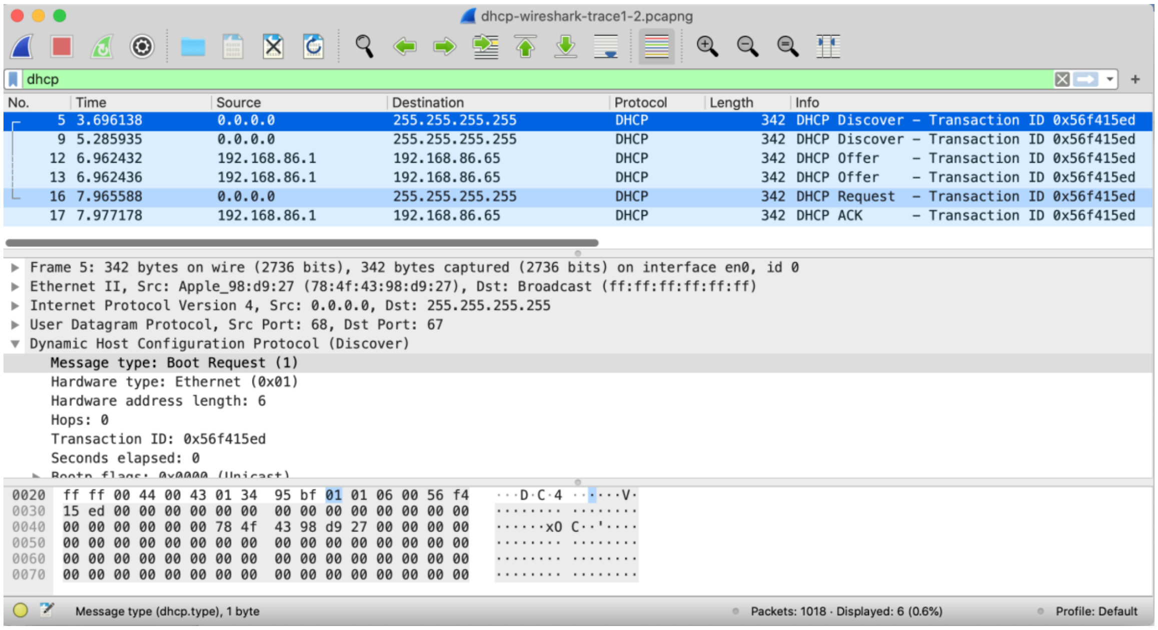
   ```
   > ipconfig /release
   ```

   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, you should 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.



```
No.   Time       Source          Destination        Protocol  Length  Info
  5   3.696138   0.0.0.0         255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x56f415ed
  9   5.285935   0.0.0.0         255.255.255.255    DHCP         342  DHCP Discover - Transaction ID 0x56f415ed
 12   6.962432   192.168.86.1    192.168.86.65      DHCP         342  DHCP Offer    - Transaction ID 0x56f415ed
 13   6.962436   192.168.86.1    192.168.86.65      DHCP         342  DHCP Offer    - Transaction ID 0x56f415ed
 16   7.965588   0.0.0.0         255.255.255.255    DHCP         342  DHCP Request  - Transaction ID 0x56f415ed
 17   7.977178   192.168.86.1    192.168.86.65      DHCP         342  DHCP ACK      - Transaction ID 0x56f415ed
```

```
▶ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), 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)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x56f415ed
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
```

```
0020  ff ff 00 44 00 43 01 34  95 bf 01 01 06 00 56 f4   ···D·C·4 ······V·
0030  15 ed 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 78 4f  43 98 d9 27 00 00 00 00   ······xO C··'····
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   ········ ········
```

```
Message type (dhcp.type), 1 byte          Packets: 1018 · Displayed: 6 (0.6%)          Profile: Default
```

Figure 1: Wireshark display, showing the capture of DHCP Discover, Offer, Request and ACK messages

If you're unable to run Wireshark on a live network connection, are unable to capture all four DHCP messages, or are assigned to do so by your instructor, you can use the Wireshark trace file, *dhcp-wireshark-trace1-1.pcapng*[2] that we've gathered following the steps above on one of the author's computers. You may well find it valuable to download this trace even if you've captured your own trace and use it, as well as your own trace, as you explore the questions below.

DHCP Questions

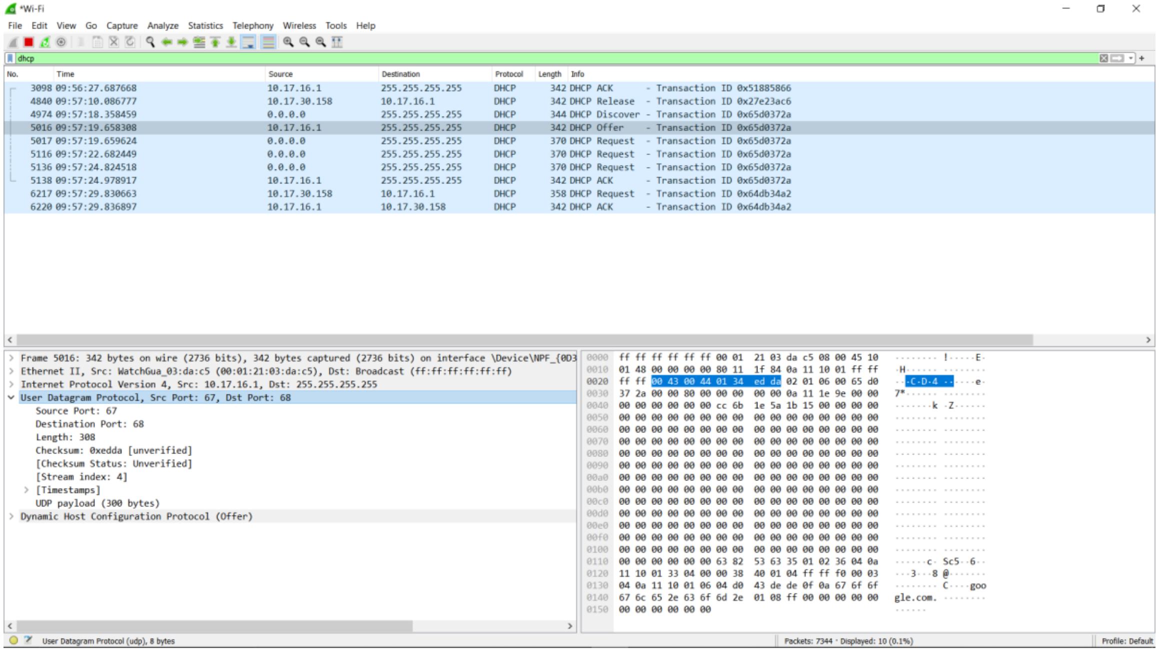
Answer the following questions[3]. If you're doing this lab as part of class, your teacher will provide details about how to hand in assignments, whether written or in an LMS.

[2] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file *dhcp-wireshark-trace1-1.pcapng*. These trace files can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you've downloaded a trace file, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the trace file name.

[3] For the author's class, when answering the following questions with hand-in assignments, students sometimes need to print out specific packets (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the packet they've found the information that answers a question. They do this by marking paper copies with a pen or annotating electronic copies with text in a colored font. There are also learning management system (LMS) modules for teachers that allow students to answer these questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

Let's start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace.

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



```
*Wi-Fi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
dhcp

No.   Time             Source         Destination      Protocol Length Info
3098 09:56:27.687668   10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x51885866
4840 09:57:10.086777   10.17.30.158   10.17.16.1       DHCP     342 DHCP Release  - Transaction ID 0x27e23ac6
4974 09:57:18.358459   0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x65d0372a
5016 09:57:19.658308   10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x65d0372a
5017 09:57:19.659624   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5116 09:57:22.682449   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5136 09:57:24.824518   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5138 09:57:24.978917   10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x65d0372a
6217 09:57:29.830663   10.17.30.158   10.17.16.1       DHCP     358 DHCP Request  - Transaction ID 0x64db34a2
6220 09:57:29.836897   10.17.16.1     10.17.30.158     DHCP     342 DHCP ACK      - Transaction ID 0x64db34a2
```

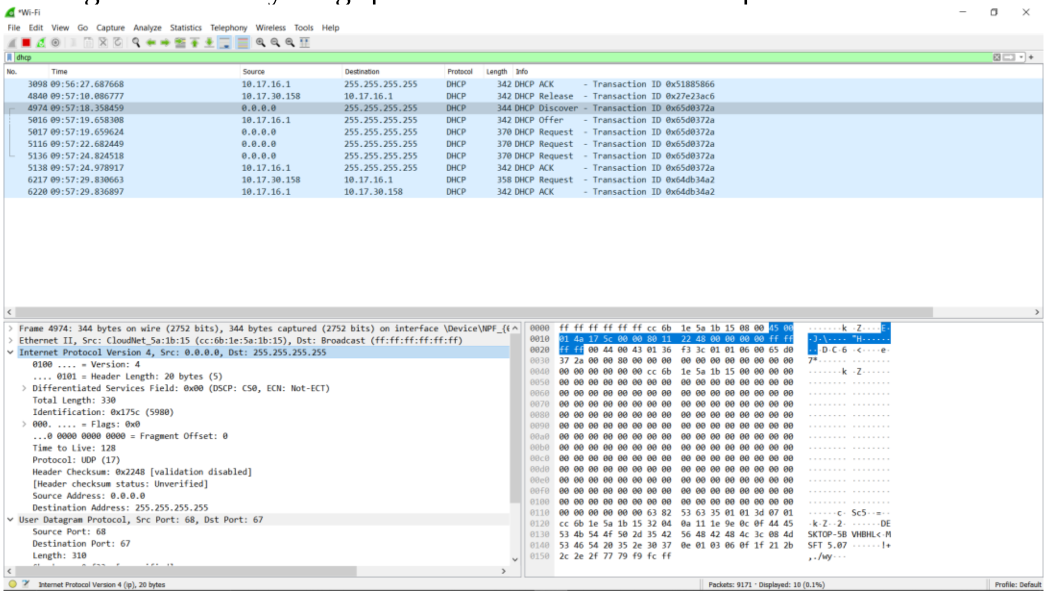
```
> Frame 5016: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{0D3
> Ethernet II, Src: WatchGua_03:da:c5 (00:01:21:03:da:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.17.16.1, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source Port: 67
    Destination Port: 68
    Length: 308
    Checksum: 0xedda [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  > [Timestamps]
    UDP payload (300 bytes)
> Dynamic Host Configuration Protocol (Offer)
```

```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ........ !.....E.
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   .H...... ........
0020  ff ff 00 43 00 44 01 34  ed da 02 01 06 00 65 d0   ...C.D.4 ......e.
0030  37 2a 00 00 80 00 00 00  00 00 0a 11 1e 9e 00 00   7*...... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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   ......c. Sc5..6..
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ...3...8 @.......
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ........ C....goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ........
0150  00 00 00 00 00 00                                  ......
```

User Datagram Protocol (udp), 8 bytes | Packets: 7344 · Displayed: 10 (0.1%) | Profile: Default

this DHCP Discover message sent out using UDP

2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.



```
*Wi-Fi
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
dhcp

No.   Time             Source         Destination      Protocol Length Info
3098 09:56:27.687668   10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x51885866
4840 09:57:10.086777   10.17.30.158   10.17.16.1       DHCP     342 DHCP Release  - Transaction ID 0x27e23ac6
4974 09:57:18.358459   0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x65d0372a
5016 09:57:19.658308   10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x65d0372a
5017 09:57:19.659624   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5116 09:57:22.682449   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5136 09:57:24.824518   0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
5138 09:57:24.978917   10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x65d0372a
6217 09:57:29.830663   10.17.30.158   10.17.16.1       DHCP     358 DHCP Request  - Transaction ID 0x64db34a2
6220 09:57:29.836897   10.17.16.1     10.17.30.158     DHCP     342 DHCP ACK      - Transaction ID 0x64db34a2
```

```
> Frame 4974: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{6
> Ethernet II, Src: CloudNet_5a:1b:15 (cc:6b:1e:5a:1b:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v 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: 0x175c (5980)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x2248 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 310
```

```
0000  ff ff ff ff ff ff cc 6b  1e 5a 1b 15 08 00 45 00   .......k .Z....E.
0010  01 4a 17 5c 00 00 80 11  22 48 00 00 00 00 ff ff   .J.\.... "H......
0020  ff ff 00 44 00 43 01 36  f3 3c 01 01 06 00 65 d0   ...D.C.6 .<....e.
0030  37 2a 00 00 80 00 00 00  00 00 00 00 00 00 00 00   7*...... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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  cc 6b 1e 5a 1b 15 32 04  0a 11 1e 9e 0c 0f 44 45   .k.Z..2. ......DE
0130  53 4b 54 4f 50 2d 35 42  56 48 42 48 4c 3c 08 4d   SKTOP-5B VHBHL<.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...
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 9171 · Displayed: 10 (0.1%) | Profile: Default

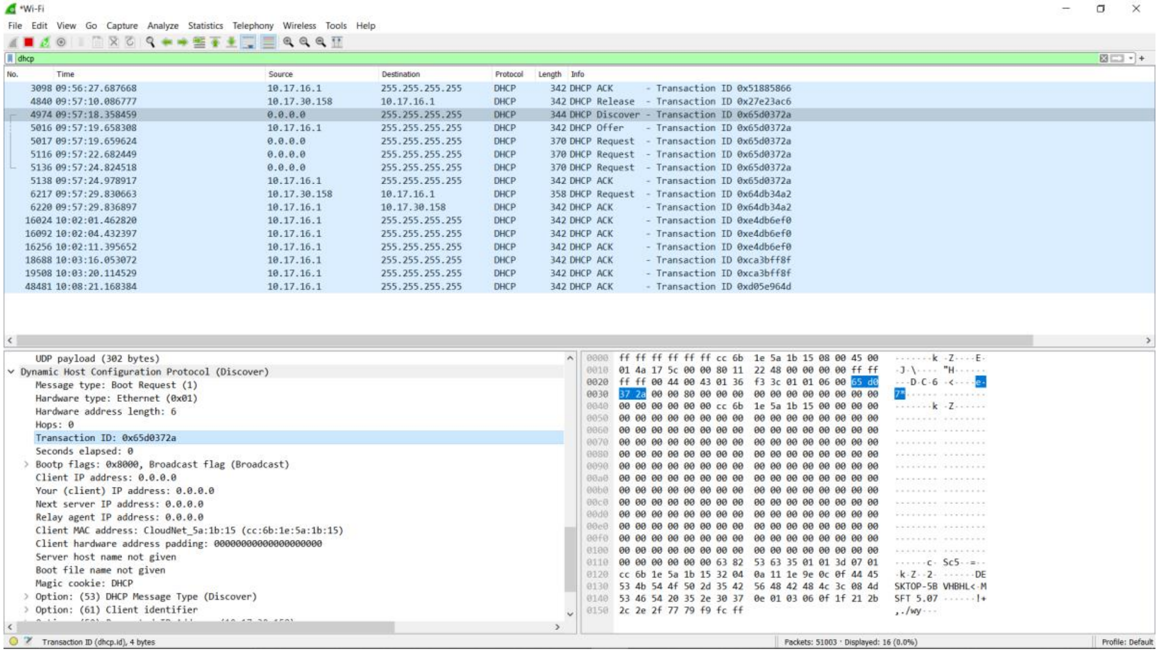
the source IP address used in the IP datagram containing the Discover message:0.0.0.0

This is because the host does not yet have an IP address assigned to it, and is broadcasting its request for an IP address to all DHCP servers on the network.

3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.
   the destination IP address used in the datagram containing the Discover message:255.255.255.255

The broadcast flag actually determines which address the server sends it's responses to. When DHCP starts the client has no idea about the network it's currently on. Some clients may store the IP address they were previously on and send this out with the Discovery and Request packets, but the network is not truly set up until after the server has sent it's final Ack message.
Because of this the server does not know the network's true broadcast address, however there is an address mapped for this very purpose.

4. What is the value in the transaction ID field of this DHCP Discover message?


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time             Source         Destination      Protocol Length Info
 3098 09:56:27.687668  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x51885866
 4840 09:57:10.086777  10.17.30.158   10.17.16.1       DHCP     342 DHCP Release  - Transaction ID 0x27e23ac6
 4974 09:57:18.358459  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x65d0372a
 5016 09:57:19.658308  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x65d0372a
 5017 09:57:19.659624  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
 5116 09:57:22.682449  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
 5136 09:57:24.824518  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x65d0372a
 5138 09:57:24.978917  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x65d0372a
 6217 09:57:29.830663  10.17.30.158   10.17.16.1       DHCP     358 DHCP Request  - Transaction ID 0x64db34a2
 6220 09:57:29.836897  10.17.16.1     10.17.30.158     DHCP     342 DHCP ACK      - Transaction ID 0x64db34a2
16024 10:02:01.462820  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe4db6ef0
16092 10:02:04.432397  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe4db6ef0
16256 10:02:11.395652  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe4db6ef0
18688 10:03:16.053072  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xca3bff8f
19508 10:03:20.114529  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xca3bff8f
48481 10:08:21.168384  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xd05e964d
```

```
    UDP payload (302 bytes)
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x65d0372a
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    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: CloudNet_5a:1b:15 (cc:6b:1e:5a:1b:15)
    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
```

```
0000  ff ff ff ff ff ff cc 6b  1e 5a 1b 15 08 00 45 00   ······k ·Z····E·
0010  01 4a 17 5c 00 00 80 11  22 48 00 00 00 00 ff ff   ·J·\···· "H······
0020  ff ff 00 44 00 43 01 36  f3 3c 01 01 06 00 65 d0   ···D·C·6 ·<····e·
0030  37 2a 00 00 80 00 00 00  00 00 00 00 00 00 00 00   7*······ ········
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   ······k ·Z······
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  cc 6b 1e 5a 1b 15 32 04  0a 11 1e 9e 0c 0f 44 45   ·k·Z··2· ······DE
0130  53 4b 54 4f 50 2d 35 42  56 48 42 48 4c 3c 08 4d   SKTOP-5B VHBHL<·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···
```

Transaction ID (dhcp.id), 4 bytes
Packets: 51003 · Displayed: 16 (0.0%)
Profile: Default

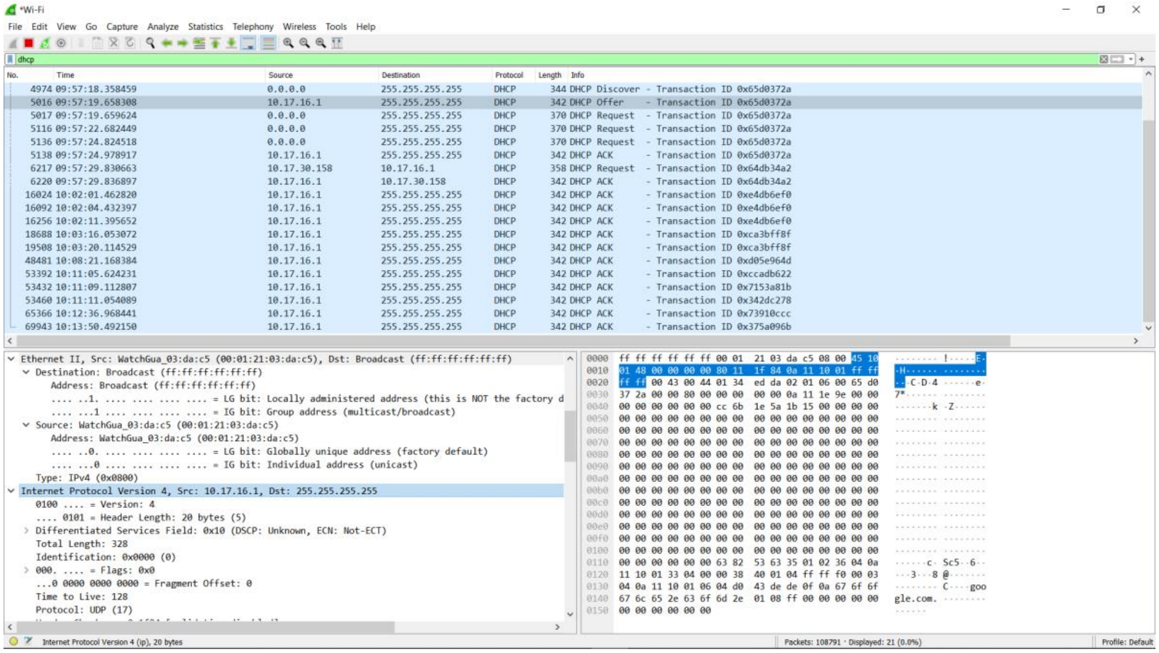
the transaction ID field of this DHCP Discover message :0x65d0372a

5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?

client IP address, host name, default gateway IP address, DNS IP address, IP request time and DHCP server IP address.

Now let's look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-5 above.

6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?
   Broadcast or unicast response of a server to a discover message with configuration parameters for the client.
7. What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time               Source          Destination       Protocol  Length Info
 4974 09:57:18.358459    0.0.0.0         255.255.255.255   DHCP      344 DHCP Discover - Transaction ID 0x65d0372a
 5016 09:57:19.658308    10.17.16.1      255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0x65d0372a
 5017 09:57:19.659624    0.0.0.0         255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0x65d0372a
 5116 09:57:22.682449    0.0.0.0         255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0x65d0372a
 5136 09:57:24.824518    0.0.0.0         255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0x65d0372a
 5138 09:57:24.978917    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x65d0372a
 6217 09:57:29.830663    10.17.30.158    10.17.16.1        DHCP      358 DHCP Request  - Transaction ID 0x64db34a2
 6220 09:57:29.836897    10.17.16.1      10.17.30.158      DHCP      342 DHCP ACK      - Transaction ID 0x64db34a2
16024 10:02:01.462820    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xe4db6ef0
16092 10:02:04.432397    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xe4db6ef0
16256 10:02:11.395652    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xe4db6ef0
18688 10:03:16.053072    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xca3bff8f
19508 10:03:20.114529    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xca3bff8f
48481 10:08:21.168384    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xd05e964d
53392 10:11:05.624231    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xccadb622
53432 10:11:09.112807    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x7153a81b
53460 10:11:11.054089    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x342dc278
65366 10:12:36.968441    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x73910ccc
69943 10:13:50.492150    10.17.16.1      255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x375a096b
```

```
v Ethernet II, Src: WatchGua_03:da:c5 (00:01:21:03:da:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory d
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: WatchGua_03:da:c5 (00:01:21:03:da:c5)
      Address: WatchGua_03:da:c5 (00:01:21:03:da:c5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.17.16.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
```

```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ........ !.....E.
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   .H...... ........
0020  ff ff 00 43 00 44 01 34  ed da 02 01 06 00 65 d0   ...C.D.4 ......e.
0030  37 2a 00 00 80 00 00 00  00 00 0a 11 1e 9e 00 00   7*...... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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   ......c. Sc5..6..
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ...3...8 @.......
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ........ C....goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ........
0150  00 00 00 00 00 00                                  ......
```

Internet Protocol Version 4 (ip), 20 bytes
Packets: 108791 · Displayed: 21 (0.0%)
Profile: Default

the *source* IP address used in the IP datagram containing the Offer message:10.17.16.1.
use Default Gateway

8. What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [Hint: Look at your trace carefully. The answer to this question may differ from what you see in Figure 4.24 in the textbook. If you really want to dig into this, consult the DHCP RFC, page 24.]
   the *destination* IP address used in the datagram containing the Offer message:255.255.255.255

Because of this the server does not know the network's true broadcast address, however there is an address mapped for this very purpose.

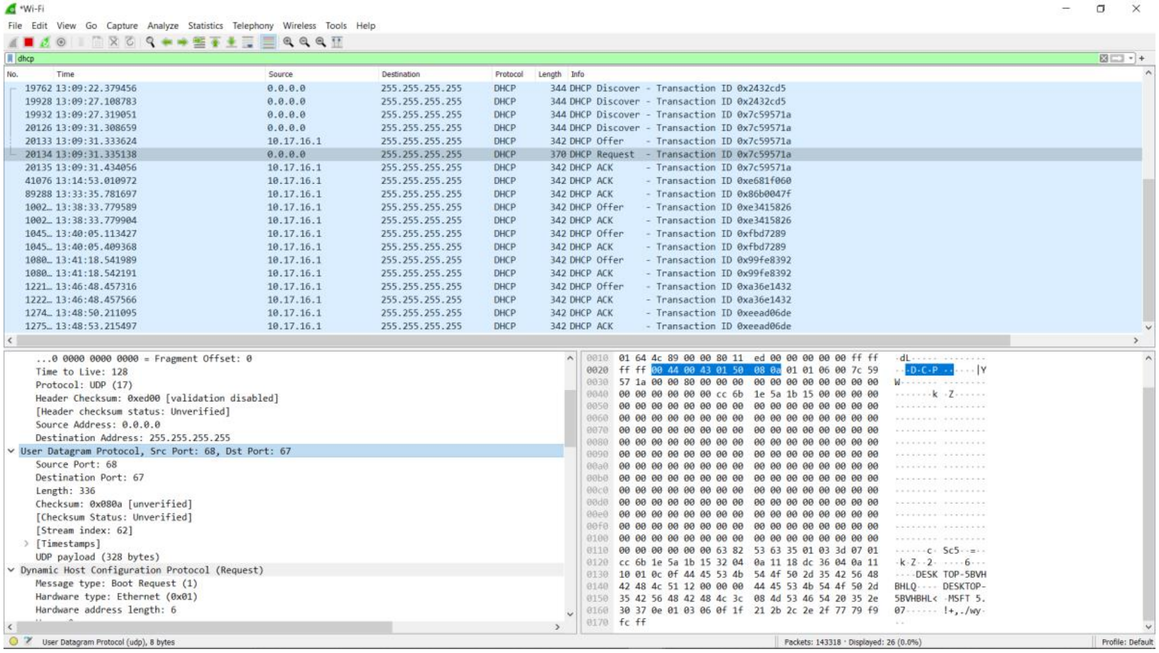
9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?

client IP address, subnet mask, default gateway IP address, DNS IP address, IP lease time and DHCP server IP address.

It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! Let's take a look at the DHCP Request message, remembering that although we've already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent.

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.

10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time                Source        Destination       Protocol  Length Info
19762 13:09:22.379456     0.0.0.0       255.255.255.255   DHCP      344 DHCP Discover - Transaction ID 0x2432cd5
19928 13:09:27.108783     0.0.0.0       255.255.255.255   DHCP      344 DHCP Discover - Transaction ID 0x2432cd5
19932 13:09:27.319051     0.0.0.0       255.255.255.255   DHCP      344 DHCP Discover - Transaction ID 0x7c59571a
20126 13:09:31.308659     0.0.0.0       255.255.255.255   DHCP      344 DHCP Discover - Transaction ID 0x7c59571a
20133 13:09:31.333624     10.17.16.1    255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0x7c59571a
20134 13:09:31.335138     0.0.0.0       255.255.255.255   DHCP      370 DHCP Request  - Transaction ID 0x7c59571a
20135 13:09:31.434056     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x7c59571a
41076 13:14:53.010972     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xe681f060
89288 13:33:35.781697     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x86b0047f
1002… 13:38:33.779589     10.17.16.1    255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0xe3415826
1002… 13:38:33.779904     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xe3415826
1045… 13:40:05.113427     10.17.16.1    255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0xfbd7289
1045… 13:40:05.409368     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xfbd7289
1080… 13:41:18.541989     10.17.16.1    255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0x99fe8392
1080… 13:41:18.542191     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x99fe8392
1221… 13:46:48.457316     10.17.16.1    255.255.255.255   DHCP      342 DHCP Offer    - Transaction ID 0xa36e1432
1222… 13:46:48.457566     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xa36e1432
1274… 13:48:50.211095     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xeead06de
1275… 13:48:53.215497     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0xeead06de
```

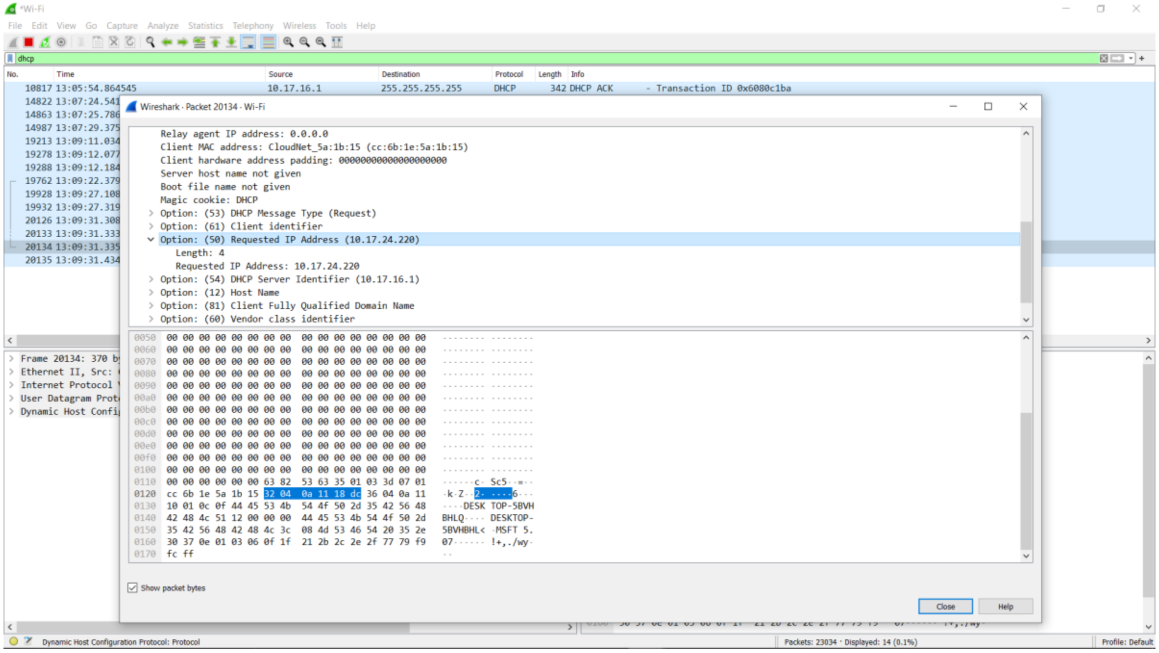
```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xed00 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 336
    Checksum: 0x080a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 62]
  > [Timestamps]
    UDP payload (328 bytes)
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
```

```
0010  01 64 4c 89 00 00 80 11  ed 00 00 00 00 00 ff ff   ·dL····· ········
0020  ff ff 00 44 00 43 01 50  08 0a 01 01 06 00 7c 59   ···D·C·P ······|Y
0030  57 1a 00 00 80 00 00 00  00 00 00 00 00 00 00 00   W······· ········
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   ·······k ·Z······
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  cc 6b 1e 5a 1b 15 32 04  0a 11 18 dc 36 04 0a 11   ·k·Z··2· ····6···
0130  10 01 0c 0f 44 45 53 4b  54 4f 50 2d 35 42 56 48   ····DESK TOP-5BVH
0140  42 48 4c 51 12 00 00 00  44 45 53 4b 54 4f 50 2d   BHLQ···· DESKTOP-
0150  35 42 56 48 42 48 4c 3c  08 4d 53 46 54 20 35 2e   5BVHBHL< ·MSFT 5.
0160  30 37 0e 01 03 06 0f 1f  21 2b 2c 2e 2f 77 79 f9   07······ !+,./wy·
0170  fc ff                                              ··
```

User Datagram Protocol (udp), 8 bytes
Packets: 143318 · Displayed: 26 (0.0%)
Profile: Default

68 is source port number, 67 is destination port number

11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
Wireshark · Packet 20134 · Wi-Fi

```
No.   Time                Source        Destination       Protocol  Length Info
10817 13:05:54.864545     10.17.16.1    255.255.255.255   DHCP      342 DHCP ACK      - Transaction ID 0x6080c1ba
14822 13:07:24.541
14863 13:07:25.786
14987 13:07:29.375
19213 13:09:11.034
19278 13:09:12.077
19288 13:09:12.184
19762 13:09:22.379
19928 13:09:27.108
19932 13:09:27.319
20126 13:09:31.308
20133 13:09:31.333
20134 13:09:31.335
20135 13:09:31.434
```

```
> Frame 20134: 370 by
> Ethernet II, Src: 
> Internet Protocol 
> User Datagram Prot
> Dynamic Host Confi
```

```
    Relay agent IP address: 0.0.0.0
    Client MAC address: CloudNet_5a:1b:15 (cc:6b:1e:5a:1b:15)
    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
  v Option: (50) Requested IP Address (10.17.24.220)
      Length: 4
      Requested IP Address: 10.17.24.220
  > Option: (54) DHCP Server Identifier (10.17.16.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
```

```
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  cc 6b 1e 5a 1b 15 32 04  0a 11 18 dc 36 04 0a 11   ·k·Z··2· ····6···
0130  10 01 0c 0f 44 45 53 4b  54 4f 50 2d 35 42 56 48   ····DESK TOP-5BVH
0140  42 48 4c 51 12 00 00 00  44 45 53 4b 54 4f 50 2d   BHLQ···· DESKTOP-
0150  35 42 56 48 42 48 4c 3c  08 4d 53 46 54 20 35 2e   5BVHBHL< ·MSFT 5.
0160  30 37 0e 01 03 06 0f 1f  21 2b 2c 2e 2f 77 79 f9   07······ !+,./wy·
0170  fc ff                                              ··
```

☑ Show packet bytes
Close
Help
Dynamic Host Configuration Protocol: Protocol
Packets: 23034 · Displayed: 14 (0.1%)
Profile: Default

Ip:10.17.24.220

12. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?

0.0.0.0 match. The transaction ID should match the transaction ID of the DHCP Offer message that the client has accepted.

13. Now inspect the options field in the DHCP Discover message and take a close look at the "Parameter Request List". The [DHCP RFC] notes that

    > "The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number."

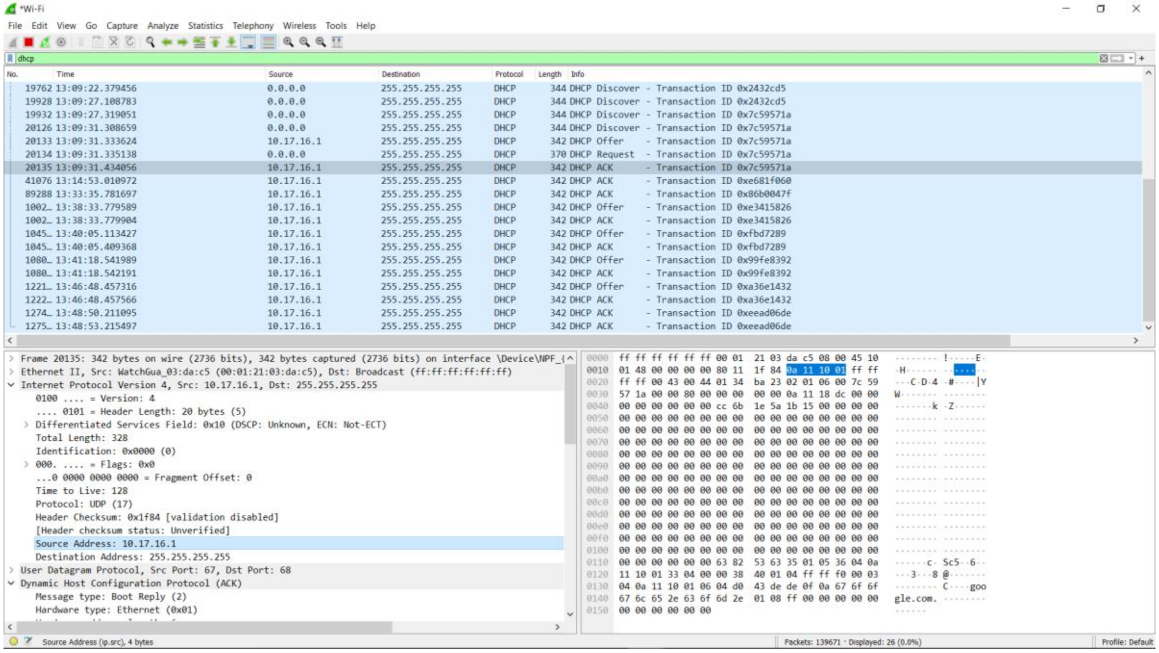
    What differences do you see between the entries in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message?

the main difference between the entries in the "Parameter Request List" option in the DHCP Discover and Request messages would be any changes made by the client based on the options offered by the server in the DHCP Offer message. The client may add or remove options from the list based on its preferences and the options available from the server.

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.

14. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

The source IP address is an important component of the IP datagram, as it is used by routers to determine the path that the packet should take through the network. Additionally, the source IP address is used by the recipient device to send a response back to the original sender.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

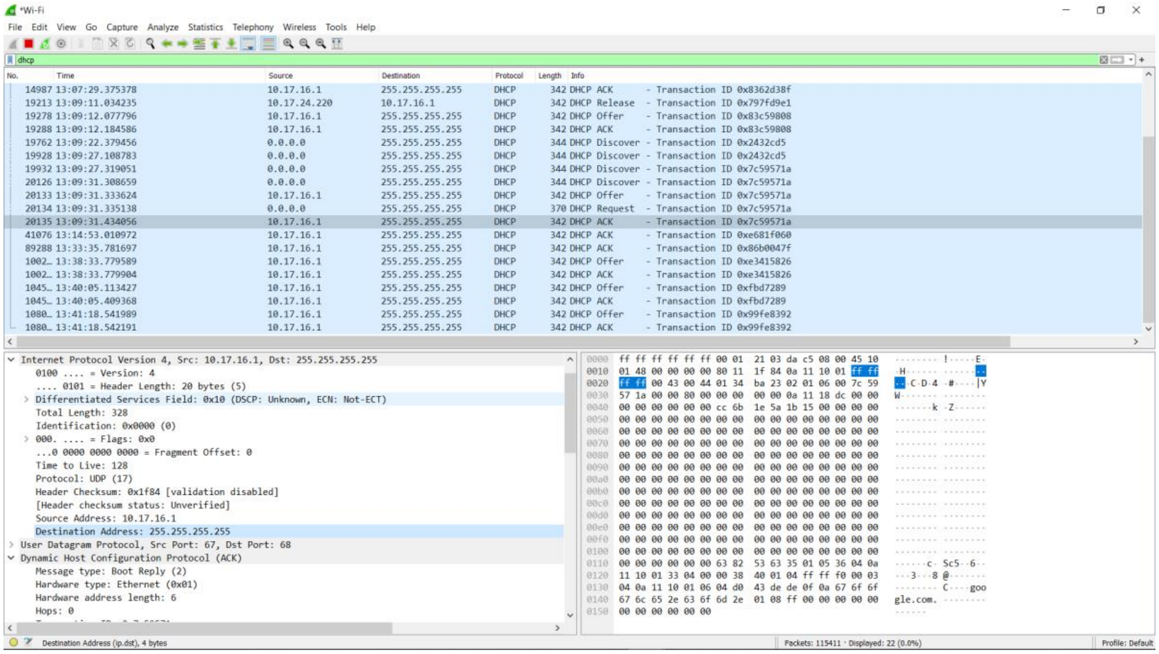
```
No.    Time                Source        Destination        Protocol  Length Info
19762 13:09:22.379456      0.0.0.0       255.255.255.255    DHCP      344 DHCP Discover - Transaction ID 0x2432cd5
19928 13:09:27.108783      0.0.0.0       255.255.255.255    DHCP      344 DHCP Discover - Transaction ID 0x2432cd5
19932 13:09:27.319051      0.0.0.0       255.255.255.255    DHCP      344 DHCP Discover - Transaction ID 0x7c59571a
20126 13:09:31.308659      0.0.0.0       255.255.255.255    DHCP      344 DHCP Discover - Transaction ID 0x7c59571a
20133 13:09:31.333624      10.17.16.1    255.255.255.255    DHCP      342 DHCP Offer    - Transaction ID 0x7c59571a
20134 13:09:31.335138      0.0.0.0       255.255.255.255    DHCP      370 DHCP Request  - Transaction ID 0x7c59571a
20135 13:09:31.434056      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x7c59571a
41076 13:14:53.010972      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xe681f060
89288 13:33:35.781697      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x86b0047f
1002… 13:38:33.779589      10.17.16.1    255.255.255.255    DHCP      342 DHCP Offer    - Transaction ID 0xe3415826
1002… 13:38:33.779904      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xe3415826
1045… 13:40:05.113427      10.17.16.1    255.255.255.255    DHCP      342 DHCP Offer    - Transaction ID 0xfbd7289
1045… 13:40:05.409368      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xfbd7289
1080… 13:41:18.541989      10.17.16.1    255.255.255.255    DHCP      342 DHCP Offer    - Transaction ID 0x99fe8392
1080… 13:41:18.542191      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x99fe8392
1221… 13:46:48.457316      10.17.16.1    255.255.255.255    DHCP      342 DHCP Offer    - Transaction ID 0xa36e1432
1222… 13:46:48.457566      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xa36e1432
1274… 13:48:50.211095      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xeead06de
1275… 13:48:53.215497      10.17.16.1    255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0xeead06de
```

```
> Frame 20135: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{
> Ethernet II, Src: WatchGua_03:da:c5 (00:01:21:03:da:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Internet Protocol Version 4, Src: 10.17.16.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x1f84 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.17.16.1
    Destination Address: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
```

```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ........ !.....E.
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   .H...... ........
0020  ff ff 00 43 00 44 01 34  ba 23 02 01 06 00 7c 59   ...C.D.4 .#....|Y
0030  57 1a 00 00 80 00 00 00  00 00 0a 11 18 dc 00 00   W....... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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 05 36 04 0a   ......c. Sc5..6..
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ...3...8 @.......
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ........ C....goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ........
0150  00 00 00 00 00 00                                  ......
```

Source Address (ip.src), 4 bytes   Packets: 139671 · Displayed: 26 (0.0%)   Profile: Default

16. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time             Source         Destination      Protocol Length Info
14987 13:07:29.375378  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x8362d38f
19213 13:09:11.034235  10.17.24.220   10.17.16.1       DHCP     342 DHCP Release  - Transaction ID 0x797fd9e1
19278 13:09:12.077796  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x83c59808
19288 13:09:12.184586  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x83c59808
19762 13:09:22.379456  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x2432cd5
19928 13:09:27.108783  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x2432cd5
19932 13:09:27.319051  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x7c59571a
20126 13:09:31.308659  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x7c59571a
20133 13:09:31.333624  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x7c59571a
20134 13:09:31.335138  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x7c59571a
20135 13:09:31.434056  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x7c59571a
41076 13:14:53.010972  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe681f060
89288 13:33:35.781697  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x86b0047f
1002… 13:38:33.779589  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xe3415826
1002… 13:38:33.779904  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe3415826
1045… 13:40:05.113427  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xfbd7289
1045… 13:40:05.409368  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xfbd7289
1080… 13:41:18.541989  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x99fe8392
1080… 13:41:18.542191  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x99fe8392
```

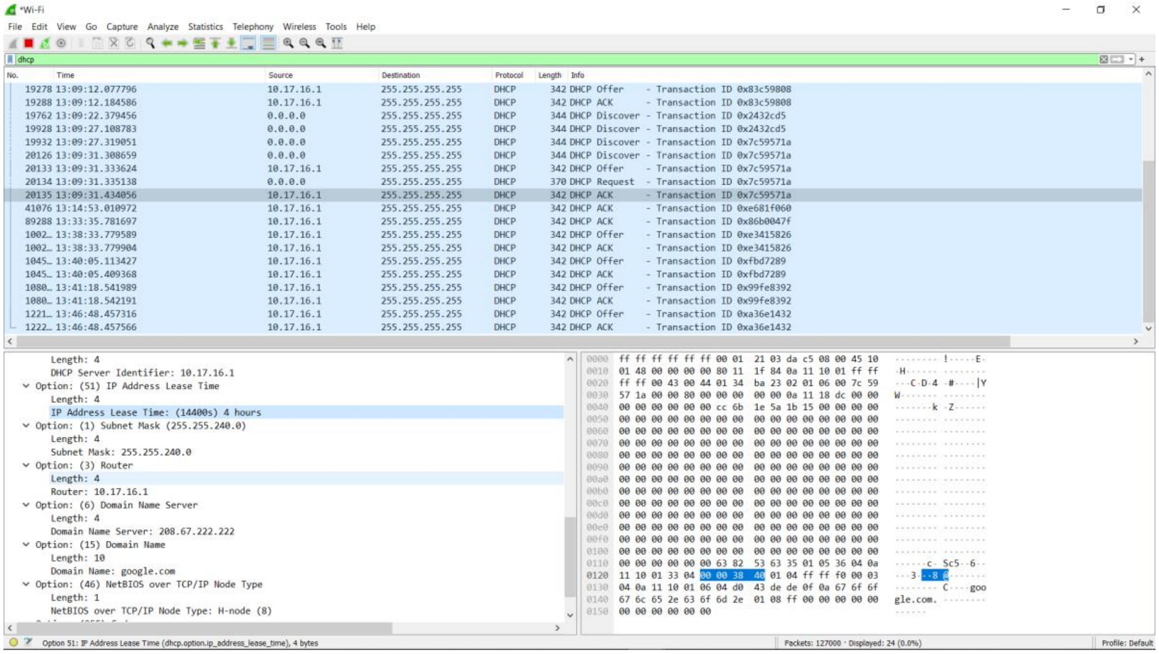
```
Internet Protocol Version 4, Src: 10.17.16.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x1f84 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.17.16.1
    Destination Address: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
```

```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ........ !.....E.
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   .H...... ........
0020  ff ff 00 43 00 44 01 34  ba 23 02 01 06 00 7c 59   ...C.D.4 .#....|Y
0030  57 1a 00 00 80 00 00 00  00 00 0a 11 18 dc 00 00   W....... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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 05 36 04 0a   ......c. Sc5..6..
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ...3...8 @.......
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ........ C....goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ........
0150  00 00 00 00 00 00                                  ......
```

Destination Address (ip.dst), 4 bytes | Packets: 115411 · Displayed: 22 (0.0%) | Profile: Default

255.255.255.255

17. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?
The name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address is "10.17.24.220".
18. For how long a time (the so-called “lease time”) has the DHPC server assigned this IP address to the client?


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time             Source         Destination      Protocol Length Info
19278 13:09:12.077796  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x83c59808
19288 13:09:12.184586  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x83c59808
19762 13:09:22.379456  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x2432cd5
19928 13:09:27.108783  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x2432cd5
19932 13:09:27.319051  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x7c59571a
20126 13:09:31.308659  0.0.0.0        255.255.255.255  DHCP     344 DHCP Discover - Transaction ID 0x7c59571a
20133 13:09:31.333624  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x7c59571a
20134 13:09:31.335138  0.0.0.0        255.255.255.255  DHCP     370 DHCP Request  - Transaction ID 0x7c59571a
20135 13:09:31.434056  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x7c59571a
41076 13:14:53.010972  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe681f060
89288 13:33:35.781697  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x86b0047f
1002… 13:38:33.779589  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xe3415826
1002… 13:38:33.779904  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xe3415826
1045… 13:40:05.113427  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xfbd7289
1045… 13:40:05.409368  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xfbd7289
1080… 13:41:18.541989  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x99fe8392
1080… 13:41:18.542191  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0x99fe8392
1221… 13:46:48.457316  10.17.16.1     255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xa36e1432
1222… 13:46:48.457566  10.17.16.1     255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xa36e1432
```

```
      Length: 4
      DHCP Server Identifier: 10.17.16.1
  Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (14400s) 4 hours
  Option: (1) Subnet Mask (255.255.240.0)
      Length: 4
      Subnet Mask: 255.255.240.0
  Option: (3) Router
      Length: 4
      Router: 10.17.16.1
  Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 208.67.222.222
  Option: (15) Domain Name
      Length: 10
      Domain Name: google.com
  Option: (46) NetBIOS over TCP/IP Node Type
      Length: 1
      NetBIOS over TCP/IP Node Type: H-node (8)
```

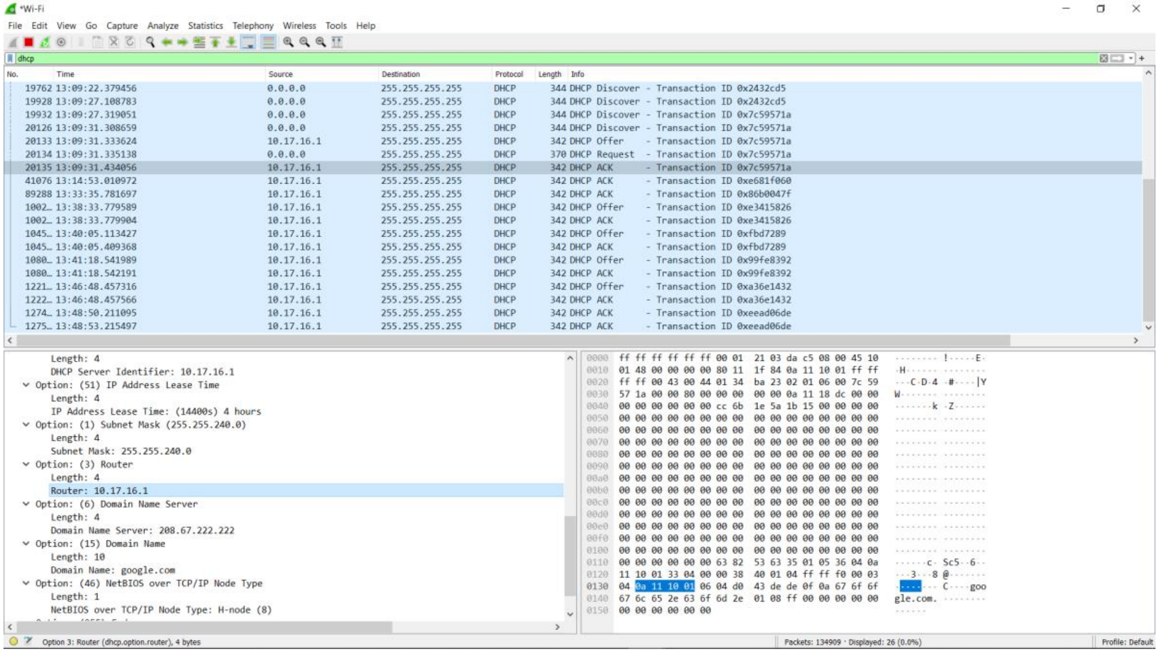
```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ........ !.....E.
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   .H...... ........
0020  ff ff 00 43 00 44 01 34  ba 23 02 01 06 00 7c 59   ...C.D.4 .#....|Y
0030  57 1a 00 00 80 00 00 00  00 00 0a 11 18 dc 00 00   W....... ........
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   .......k .Z......
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 05 36 04 0a   ......c. Sc5..6..
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ...3...8 @.......
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ........ C....goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ........
0150  00 00 00 00 00 00                                  ......
```

Option 51: IP Address Lease Time (dhcp.option.ip_address_lease_time), 4 bytes | Packets: 127000 · Displayed: 24 (0.0%) | Profile: Default

4 hours

19. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?

The IP address of the first-hop router on the default path from the client to the rest of the Internet is typically included in the DHCP ACK message sent by the DHCP server to the client. This IP address is known as the default gateway, and it is used by the client to forward packets to destinations outside of the local network.



dhcp

No.	Time	Source	Destination	Protocol	Length	Info
19762	13:09:22.379456	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x2432cd5
19928	13:09:27.108783	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x2432cd5
19932	13:09:27.319051	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x7c59571a
20126	13:09:31.308659	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x7c59571a
20133	13:09:31.333624	10.17.16.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x7c59571a
20134	13:09:31.335138	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x7c59571a
20135	13:09:31.434056	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x7c59571a
41076	13:14:53.010972	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe681f060
89288	13:33:35.781697	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x86b0047f
1002…	13:38:33.779589	10.17.16.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe3415826
1002…	13:38:33.779904	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe3415826
1045…	13:40:05.113427	10.17.16.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xfbd7289
1045…	13:40:05.409368	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xfbd7289
1080…	13:41:18.541989	10.17.16.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x99fe8392
1080…	13:41:18.542191	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x99fe8392
1221…	13:46:48.457316	10.17.16.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa36e1432
1222…	13:46:48.457566	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xa36e1432
1274…	13:48:50.211095	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xeead06de
1275…	13:48:53.215497	10.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xeead06de

```
      Length: 4
      DHCP Server Identifier: 10.17.16.1
  ˅ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (14400s) 4 hours
  ˅ Option: (1) Subnet Mask (255.255.240.0)
      Length: 4
      Subnet Mask: 255.255.240.0
  ˅ Option: (3) Router
      Length: 4
      Router: 10.17.16.1
  ˅ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 208.67.222.222
  ˅ Option: (15) Domain Name
      Length: 10
      Domain Name: google.com
  ˅ Option: (46) NetBIOS over TCP/IP Node Type
      Length: 1
      NetBIOS over TCP/IP Node Type: H-node (8)
```

```
0000  ff ff ff ff ff ff 00 01  21 03 da c5 08 00 45 10   ········ !·····E·
0010  01 48 00 00 00 00 80 11  1f 84 0a 11 10 01 ff ff   ·H······ ········
0020  ff ff 00 43 00 44 01 34  ba 23 02 01 06 00 7c 59   ···C·D·4 ·#····|Y
0030  57 1a 00 00 80 00 00 00  00 00 0a 11 18 dc 00 00   W······· ········
0040  00 00 00 00 00 00 cc 6b  1e 5a 1b 15 00 00 00 00   ·······k ·Z······
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 05 36 04 0a   ······c· Sc5··6··
0120  11 10 01 33 04 00 00 38  40 01 04 ff ff f0 00 03   ···3···8 @·······
0130  04 0a 11 10 01 06 04 d0  43 de de 0f 0a 67 6f 6f   ········ C····goo
0140  67 6c 65 2e 63 6f 6d 2e  01 08 ff 00 00 00 00 00   gle.com. ········
0150  00 00 00 00 00 00                                  ······
```

Option 3: Router (dhcp.option.router), 4 bytes

Packets: 134909 · Displayed: 26 (0.0%)

Profile: Default

Router : 10.17.16.1