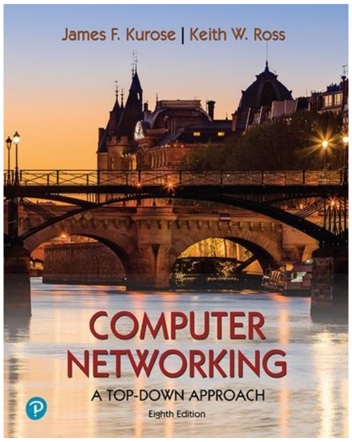
# Wireshark Lab: DHCP v8.1

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



**Name:** Urooba Gohar
**Roll No:** 22P-9216
**Section:** BSCS-5A

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.

[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.

On a Mac:

2. 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`.
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.

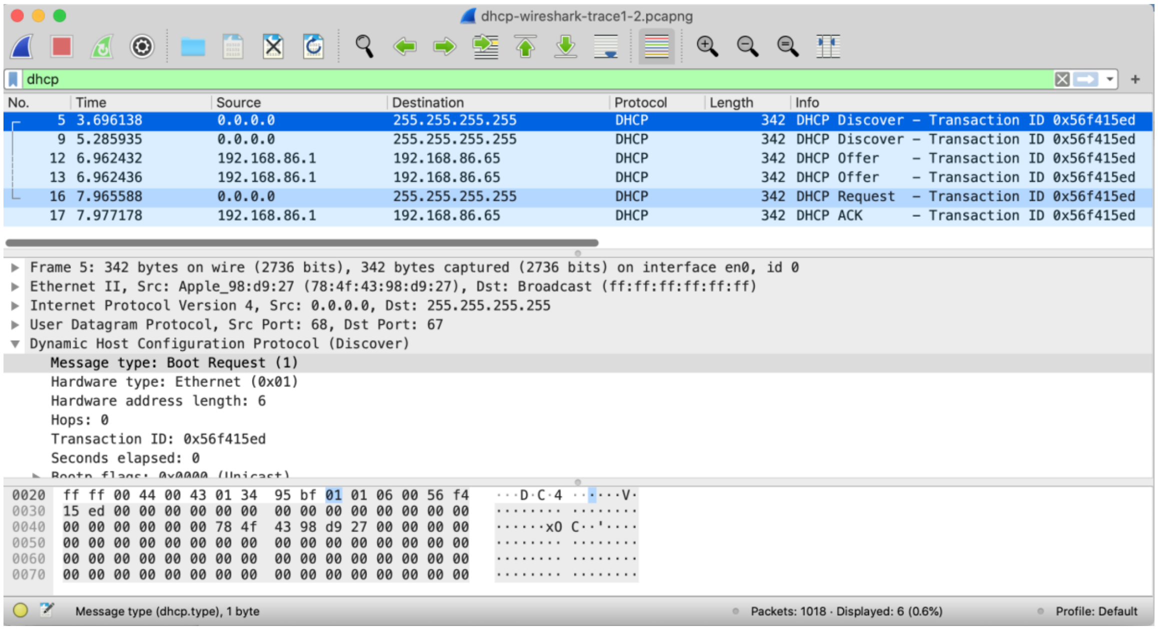
On a Linux machine:

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.

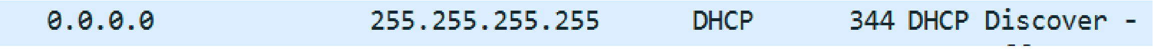
[2] You can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces-8.1.zip and extract the trace file *dhcp-wireshark-trace1-1.pcapng.* These trace files can be used to answer these Wireshark lab questions without actually capturing packets on your own. Each trace was made using 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

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

1. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain. (0.5 marks)

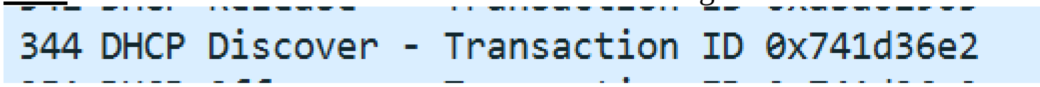
**Ans:** The source IP address used in the Discover message is: 0.0.0.0. It is special because the client has not been assigned an IP address yet. The destination IP address in the Discover message is: 255.255.255.255. It is special because it reaches all DHCP serves in the local network.



```
0.0.0.0             255.255.255.255      DHCP      344 DHCP Discover -
```

2. What is the value in the transaction ID field of this DHCP Discover message? (0.5 marks)

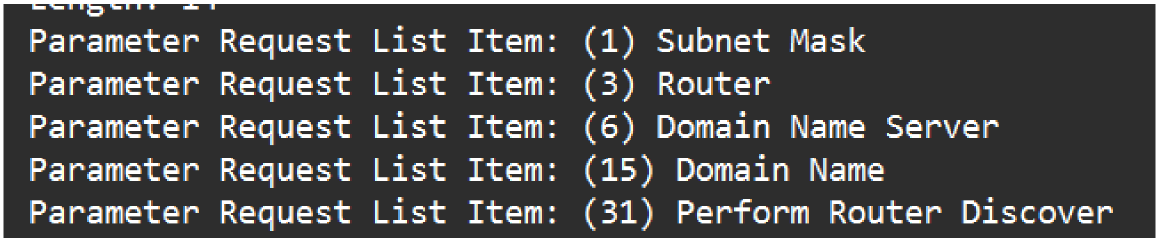
**Ans:** The transaction ID of the DHCP Discover message is: 0x741d36e2.



```
344 DHCP Discover - Transaction ID 0x741d36e2
```

3. 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? (1 marks)

**Ans:** The five pieces of information are:
1. Subnet Mask
2. Router
3. Domain Name Server
4. Domain Name
5. Perform Router Discover



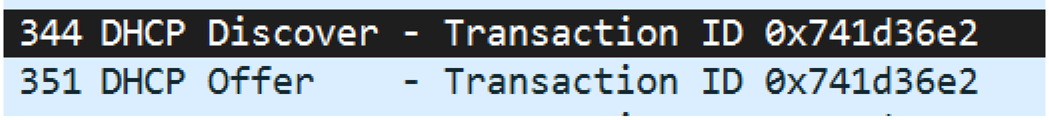
```
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
```

questions online and have answers auto-graded for these Wireshark labs at http://gaia.cs.umass.edu/kurose_ross/lms.htm

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.

4. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-3 above? (1 marks)

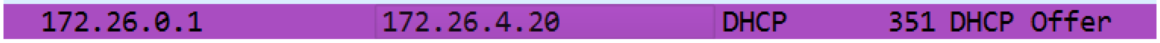
**Ans:** The Offer message sent in response to the Discover message can be proved by the transaction ID which is the same for both, i-e: 0x741d36e2.



```
344 DHCP Discover - Transaction ID 0x741d36e2
351 DHCP Offer    - Transaction ID 0x741d36e2
```

5. What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain. What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. (1 marks)

**Ans:** The source IP address of the Offer message is: 172.26.0.1. It is special because it assigns the client its configuration details. The destination IP address of the Offer message is: 172.26.4.20. It is special because it is used for direct communication.

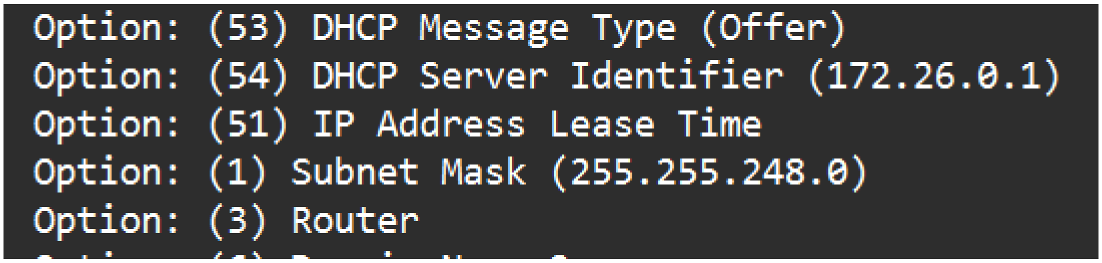


```
172.26.0.1          172.26.4.20          DHCP       351 DHCP Offer
```

6. 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? (1 marks)

**Ans:** The DHCP Offer message provides the following five pieces of information:

1. DHCP Message Type (Offer)
2. DHCP Server Identifier
3. IP Address Lease Time
4. Subnet Mask
5. Router



```
Option: (53) DHCP Message Type (Offer)
Option: (54) DHCP Server Identifier (172.26.0.1)
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask (255.255.248.0)
Option: (3) Router
```

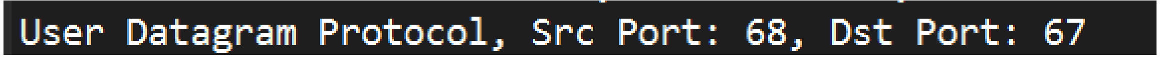
It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request 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.

7. 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? (1 marks)

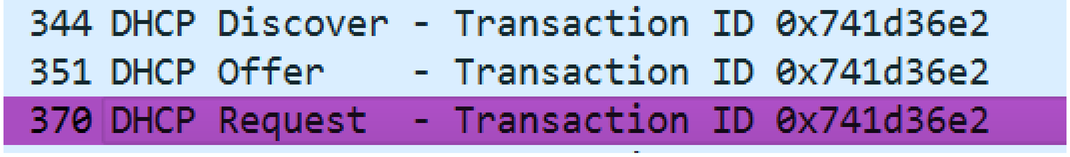
**Ans:** The UDP source port number is: 68 and the UDP destination port number is: 67.



```
User Datagram Protocol, Src Port: 68, Dst Port: 67
```

8. 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? (1 marks)

**Ans:** The transaction ID of the DHCP Request message is: 0x741d36e2. Yes, it matches the transaction IDs of the Discover and Offer messages.



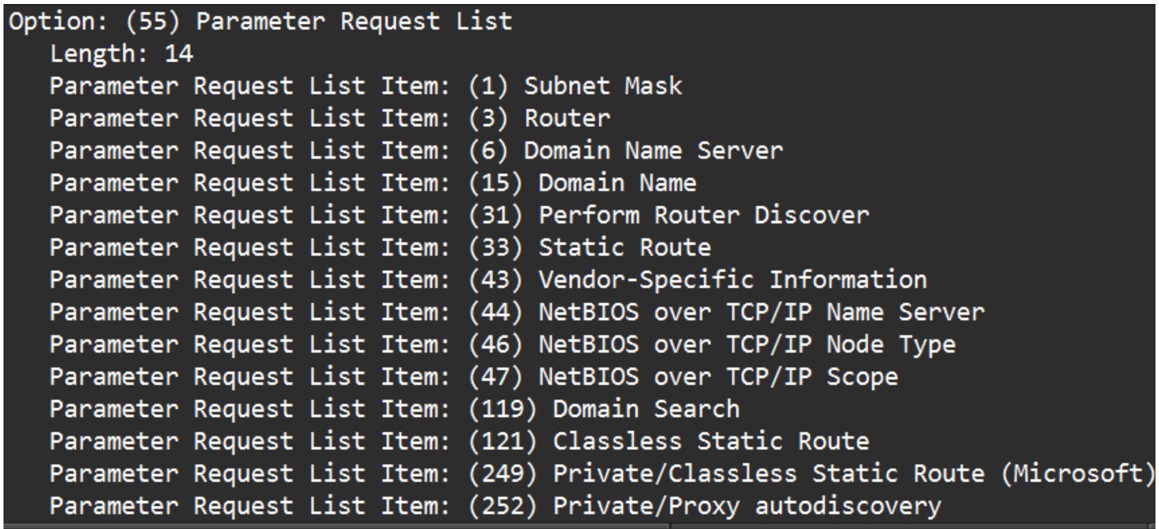
```
344 DHCP Discover - Transaction ID 0x741d36e2
351 DHCP Offer    - Transaction ID 0x741d36e2
370 DHCP Request  - Transaction ID 0x741d36e2
```

9. 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

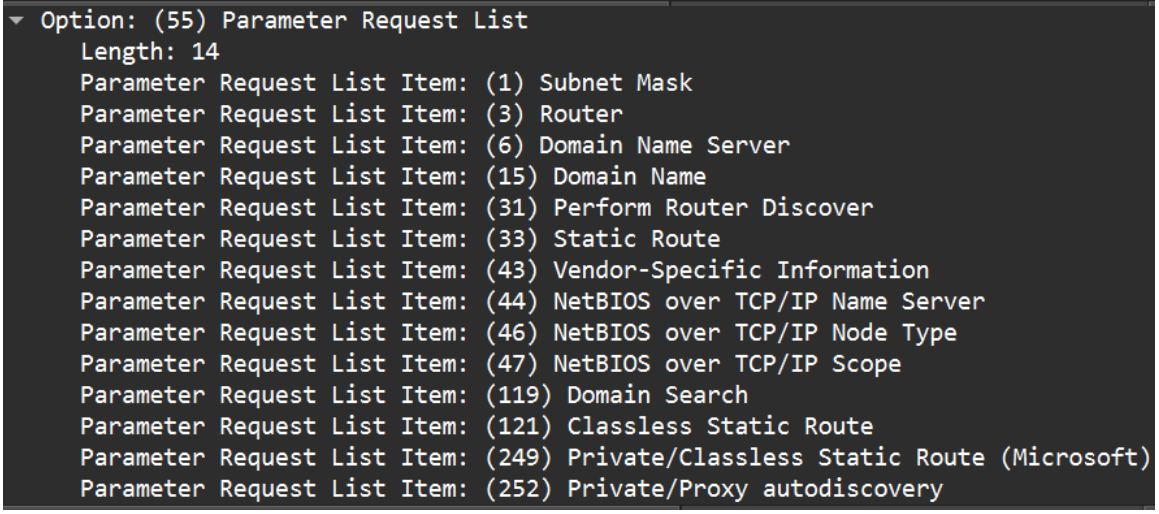
   > “The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number.”

   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? (1 marks)

**Ans:** There are no clear differences in the parameter request list of the Request and Discover messages.



```
Option: (55) Parameter Request List
   Length: 14
   Parameter Request List Item: (1) Subnet Mask
   Parameter Request List Item: (3) Router
   Parameter Request List Item: (6) Domain Name Server
   Parameter Request List Item: (15) Domain Name
   Parameter Request List Item: (31) Perform Router Discover
   Parameter Request List Item: (33) Static Route
   Parameter Request List Item: (43) Vendor-Specific Information
   Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
   Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
   Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
   Parameter Request List Item: (119) Domain Search
   Parameter Request List Item: (121) Classless Static Route
   Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
   Parameter Request List Item: (252) Private/Proxy autodiscovery
```

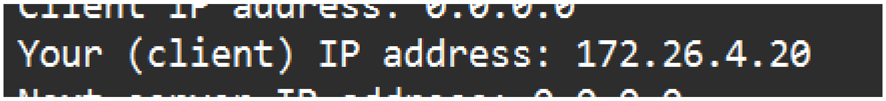


```
▾ Option: (55) Parameter Request List
     Length: 14
     Parameter Request List Item: (1) Subnet Mask
     Parameter Request List Item: (3) Router
     Parameter Request List Item: (6) Domain Name Server
     Parameter Request List Item: (15) Domain Name
     Parameter Request List Item: (31) Perform Router Discover
     Parameter Request List Item: (33) Static Route
     Parameter Request List Item: (43) Vendor-Specific Information
     Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
     Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
     Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
     Parameter Request List Item: (119) Domain Search
     Parameter Request List Item: (121) Classless Static Route
     Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
     Parameter Request List Item: (252) Private/Proxy autodiscovery
```

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

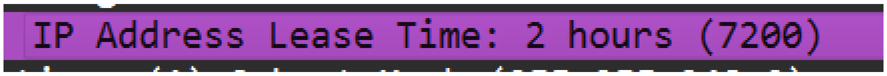
10. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address? For how long a time (the so-called "lease time") has the DHPC server assigned this IP address to the client? (1 marks)

**Ans:** The field with the assigned client IP address is named as: Your (client) IP address.



```
Client IP address: 0.0.0.0
Your (client) IP address: 172.26.4.20
```

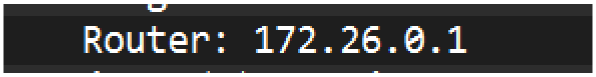
The lease time is: 2 hours.



```
IP Address Lease Time: 2 hours (7200)
```

11. 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? (1 marks)

Ans: The IP address is: 172.26.0.1.



```
    Router: 172.26.0.1
```