EE450 – Lab2 Report
XINYUE LIU
1332044343

Part 1: DHCP

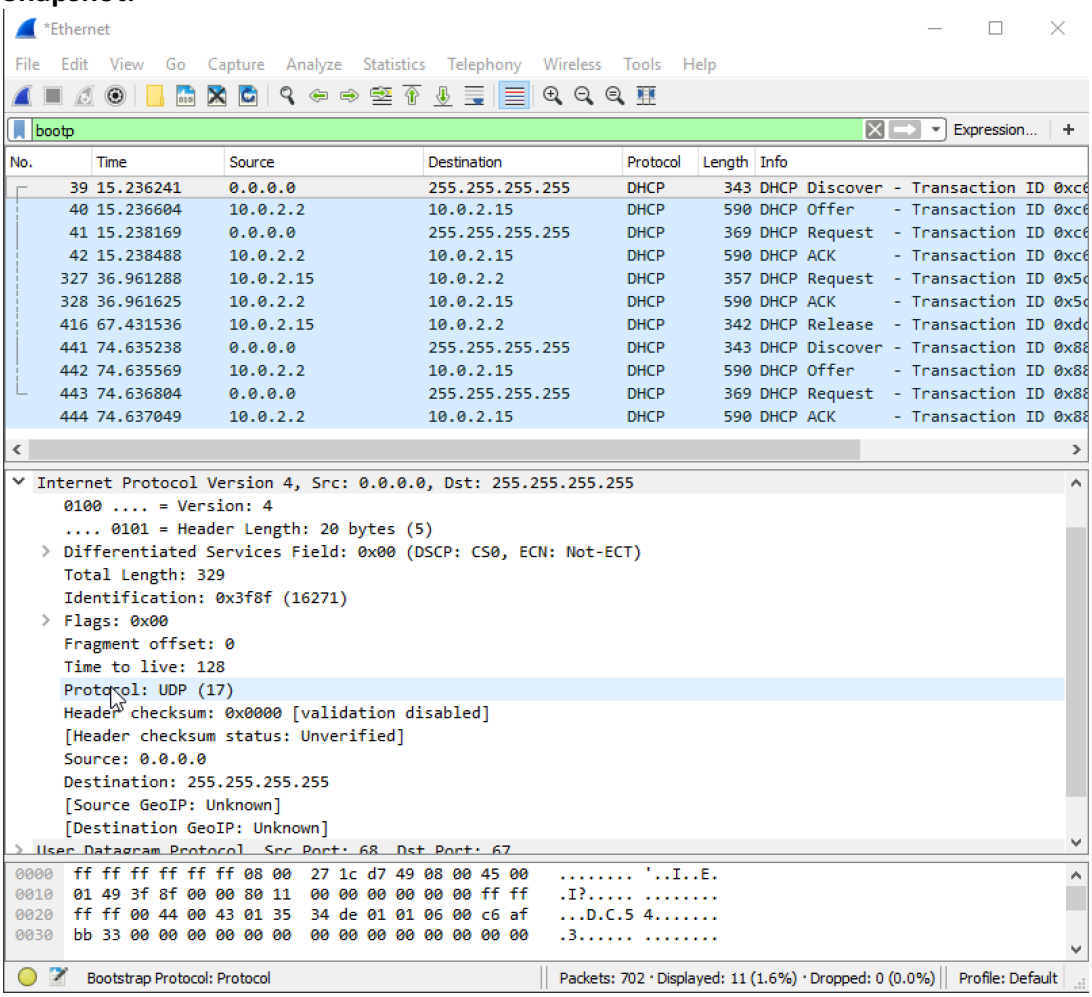
Screen shot of the Command Prompt window:

```
Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\XinyueLiu>ipconfig/release

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d883:7346:a8e5:e570%2
   Default Gateway . . . . . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:303a:349f:f5ff:fdf0
   Link-local IPv6 Address . . . . . : fe80::303a:349f:f5ff:fdf0%7
   Default Gateway . . . . . . . . . : ::

C:\Users\XinyueLiu>ipconfig/renew

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d883:7346:a8e5:e570%2
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:14cd:aca:f5ff:fdf0
   Link-local IPv6 Address . . . . . : fe80::14cd:aca:f5ff:fdf0%7
   Default Gateway . . . . . . . . . : ::

C:\Users\XinyueLiu>ipconfig/renew
```

1. Are DHCP messages sent over TCP or UDP? Provide a snapshot.

Answer: UDP

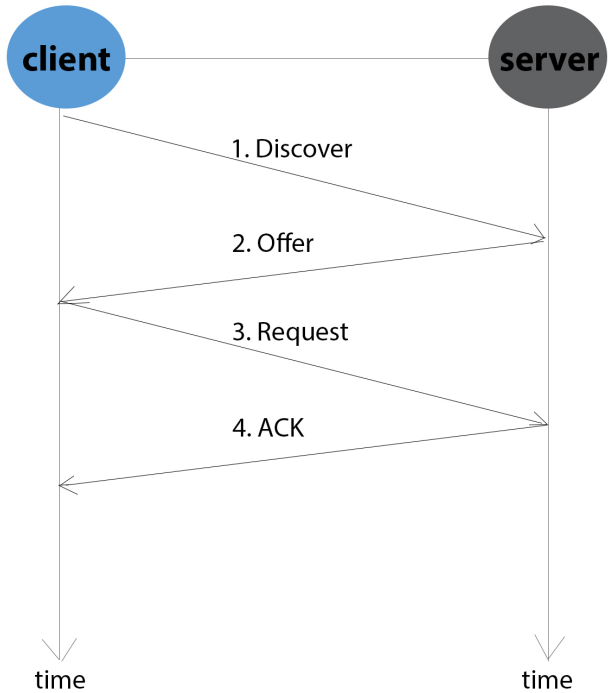
Snapshot:



2. Does DHCP use client-server or peer to peer architecture? No snapshot needed.

Answer: Client-server architecture

3. 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 and IP addresses.



1. Discover
Source port number: **68**
Source IP Address: **0.0.0.0**
Destination port #: **67**
Destination IP Addr: **255.255.255.255**

2. Offer
Source port number: **67**
Source IP Address: **10.0.2.2**
Destination port #: **68**
Destination IP Addr: **10.0.2.15**

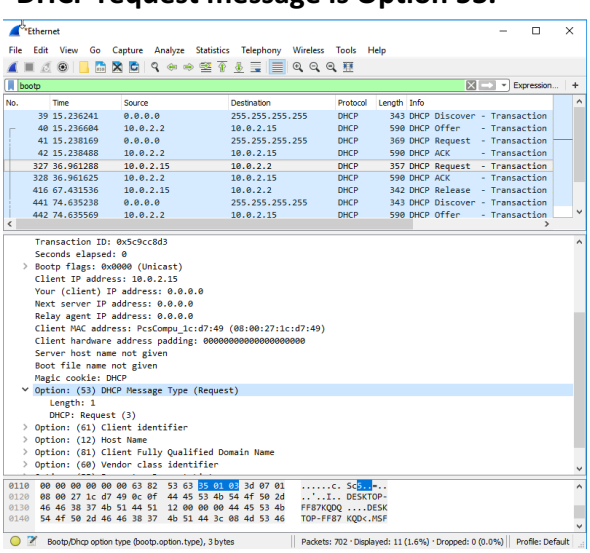
3. Request
Source port number: **68**
Source IP Address: **0.0.0.0**
Destination port #: **67**
Destination IP Addr: **255.255.255.255**

4. ACK
Source port number: **67**
Source IP Address: **10.0.2.2**
Destination port #: **68**
Destination IP Addr: **10.0.2.15**

4. What is the link-layer (e.g., Ethernet) address of your host in hex format?
Answer: The link-layer address of my host is (08:00:27:1c:d7:49)

```
Ethernet II, Src: PcsCompu_1c:d7:49 (08:00:27:1c:d7:49)
```

5. What values in the DHCP Discover message differentiate this message from the DHCP Request message?
Answer: The value in the DHCP discover message that differentiates this message from the DHCP request message is Option 53.



6. What is the value of the Transaction-ID in each of the first four DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? Why do we need the Transaction-ID field?

Answer:

In the first four DHCP messages, the transaction-IDs are the same.

First four messages' transaction-ID (Discover/Offer/Request/ACK): 0xc6afbb33

```
Transaction ID: 0xc6afbb33
```

The second set's (Request/ACK) Transaction-ID: 0x5c9cc8d3

```
Transaction ID: 0x5c9cc8d3
```

Purpose: The transaction ID is different so that the host can differentiate between different requests made by the user.

7. 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 first four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP packet.

Answer:

Discover: 0.0.0.0/255.255.255.255
Offer: 10.0.2.2/255.255.255.255
Request: 0.0.0.0/255.255.255.255
ACK: 10.0.2.2/255.255.255.255

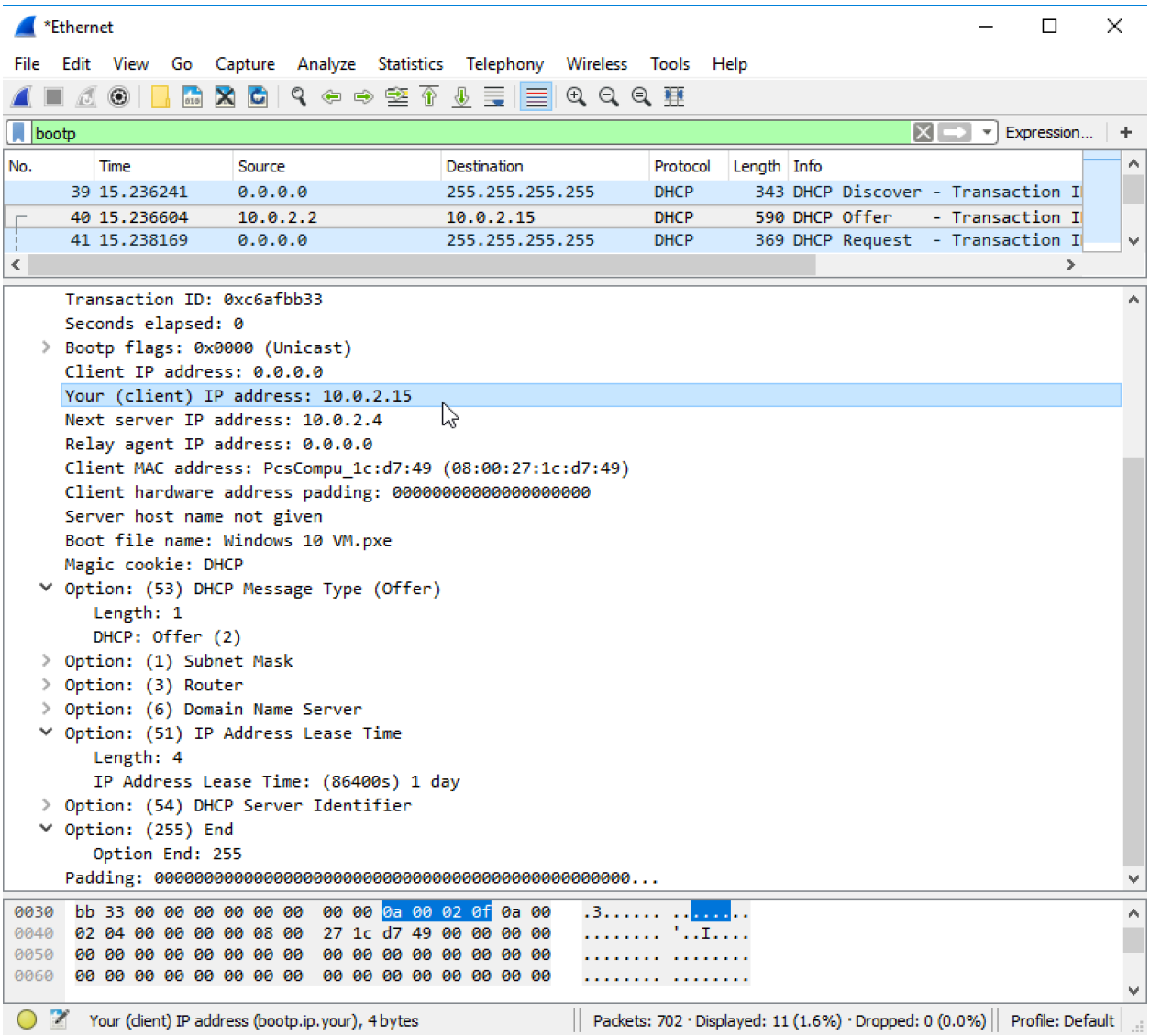
8. What is the IP address of your DHCP server?

```
42 15.238488    10.0.2.2        10.0.2.15        DHCP    590 DHCP ACK    - Transaction
```

Answer:

The IP address of my DHCP server is 10.0.2.2

9. What IP address is the DHCP server offering to your host in the DHCP Offer message and what is the lease time? Which DHCP messages have this IP Address in them?

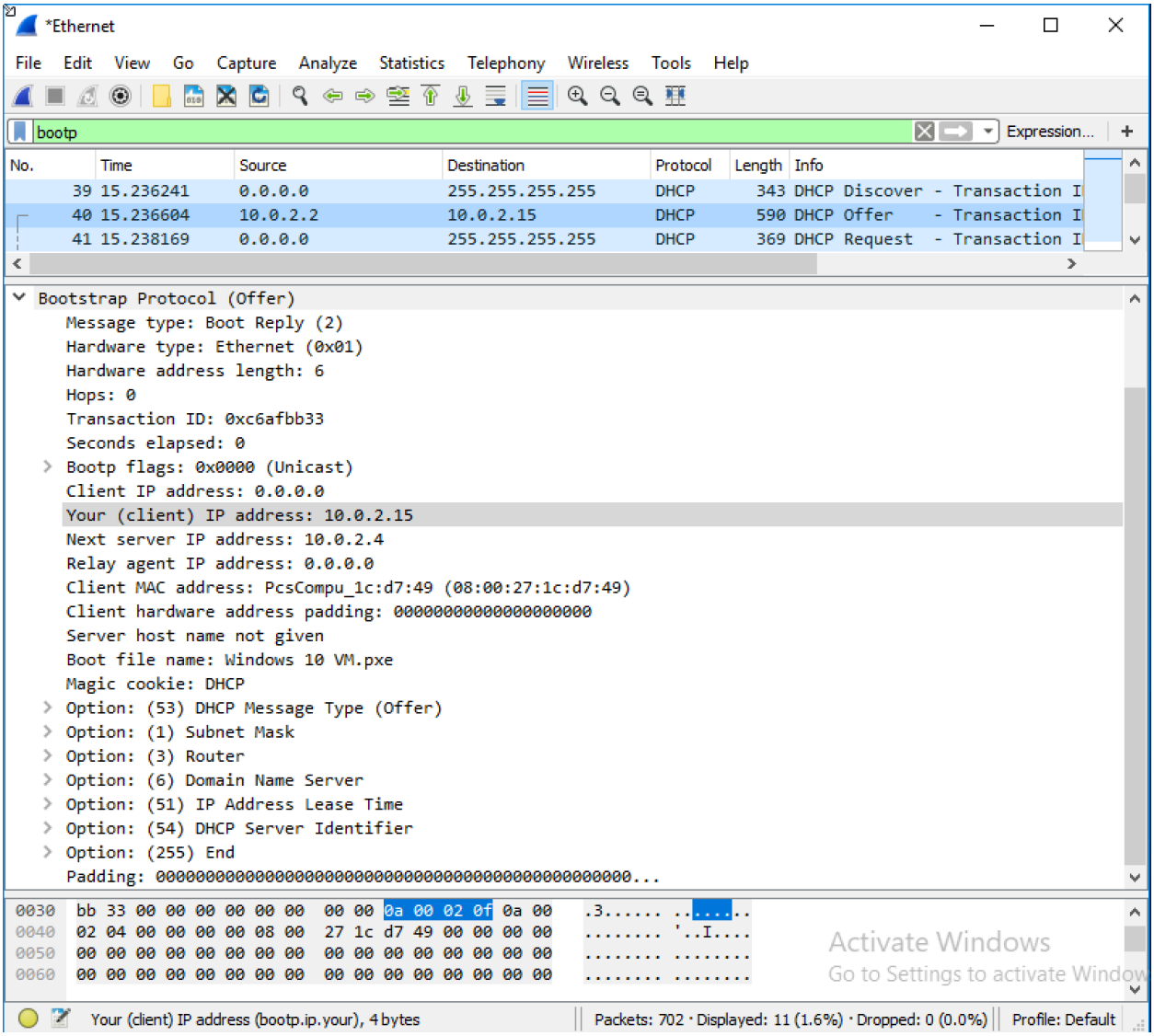


Answer:

The IP address in which the DHCP server is offering to my host in the DHCP Offer message is 10.0.2.15. The IP Address Lease Time is (86400s) 1 day (Option 51).

DHCP Offer message and DHCP ACK message have this IP Address in them.

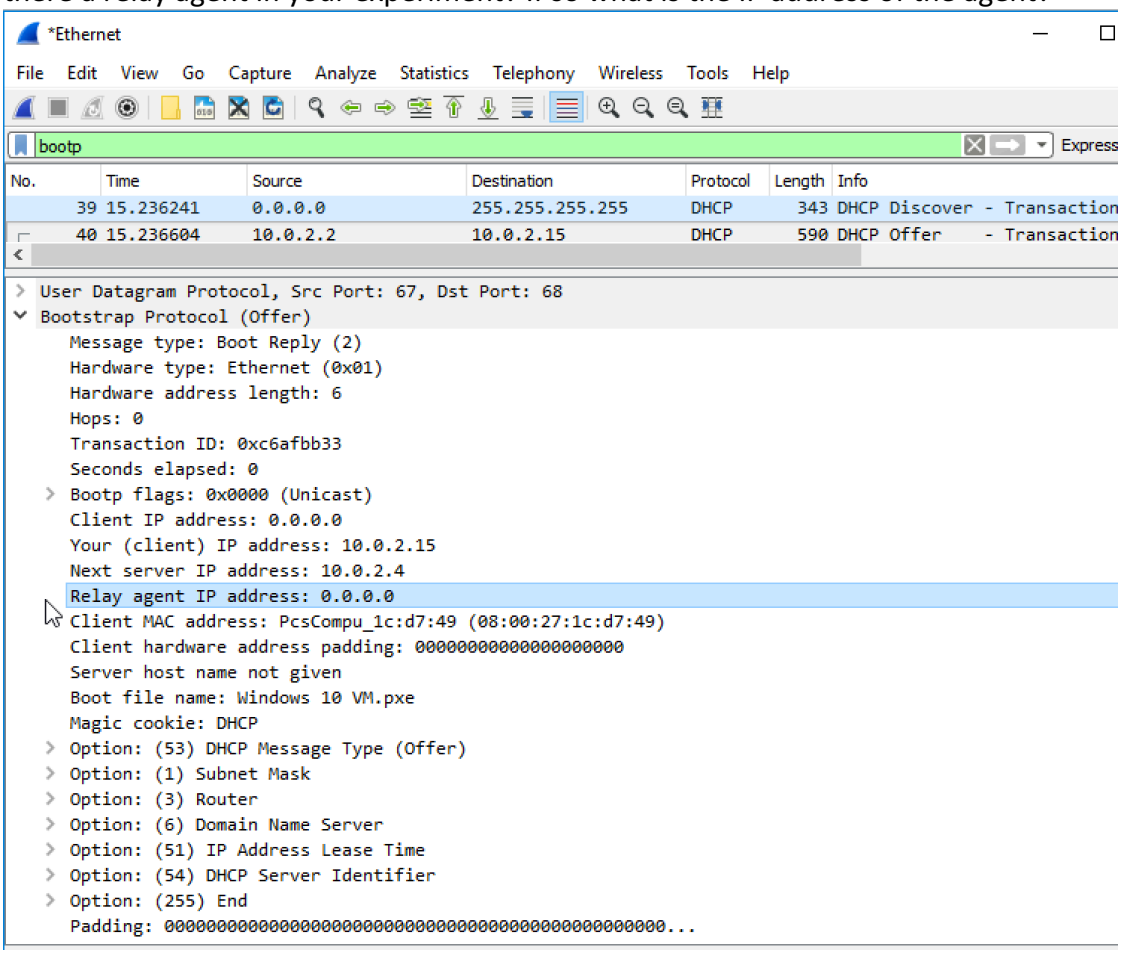
10. Apart from IP Address, what other information does DHCP server provide to the client?



Answer:

Besides IP address, there are IP address of the next server, the DHCP Message Type (Length & offer), the subnet mask (including length), router (including length), DNS server info, IP address lease time, DHCP server identifier.

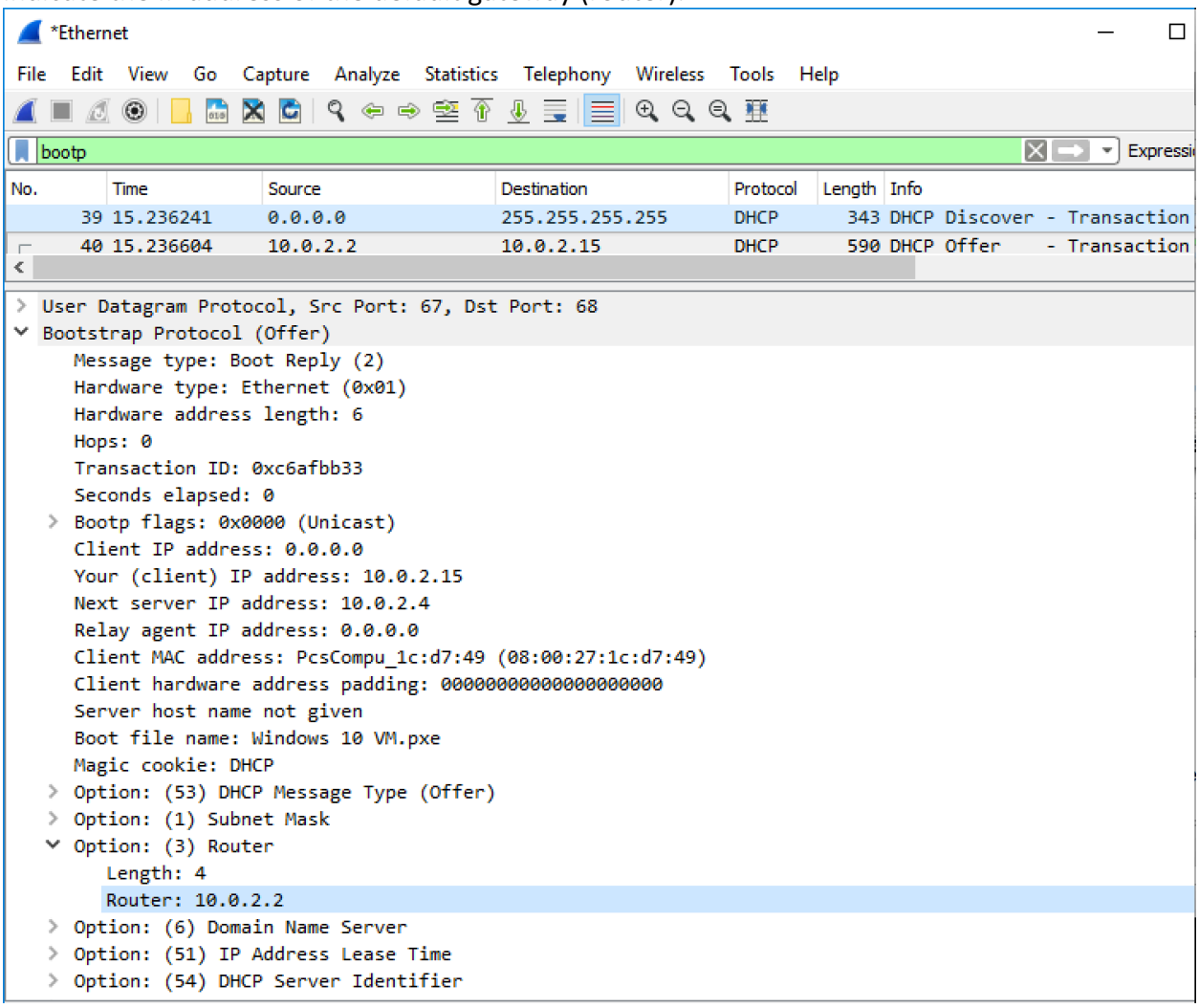
11. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?



Answer:

In the example given, the value that indicates there is no relay agent is 0.0.0.0, in the case of my capture, I also have a value for the relay agent of 0.0.0.0 indicating that I did not have a relay agent either.

12. Explain the purpose of the router and subnet mask lines in the DHCP offer message and indicate the IP address of the default gateway (router).



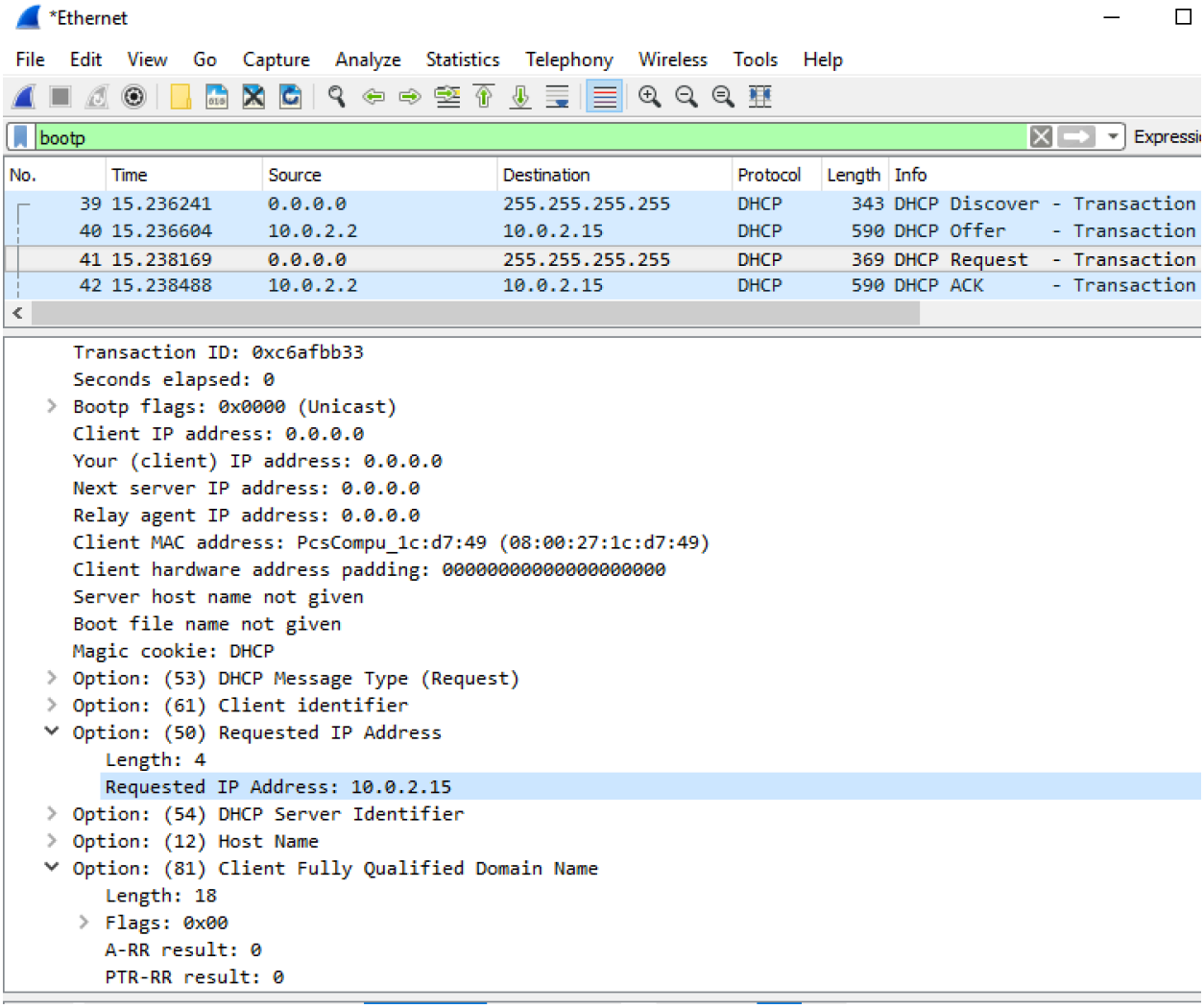
Answer:

The subnet mask line tells the client which subnet mask to use.

The router line indicates where the client should send messages by default.

The IP address of the default gateway (router): 10.0.2.2

13. In the client's response to the first server DHCP Offer message, does the client accept this IP address? Where in the DHCP Request is the client's requested IP address?



Answer:

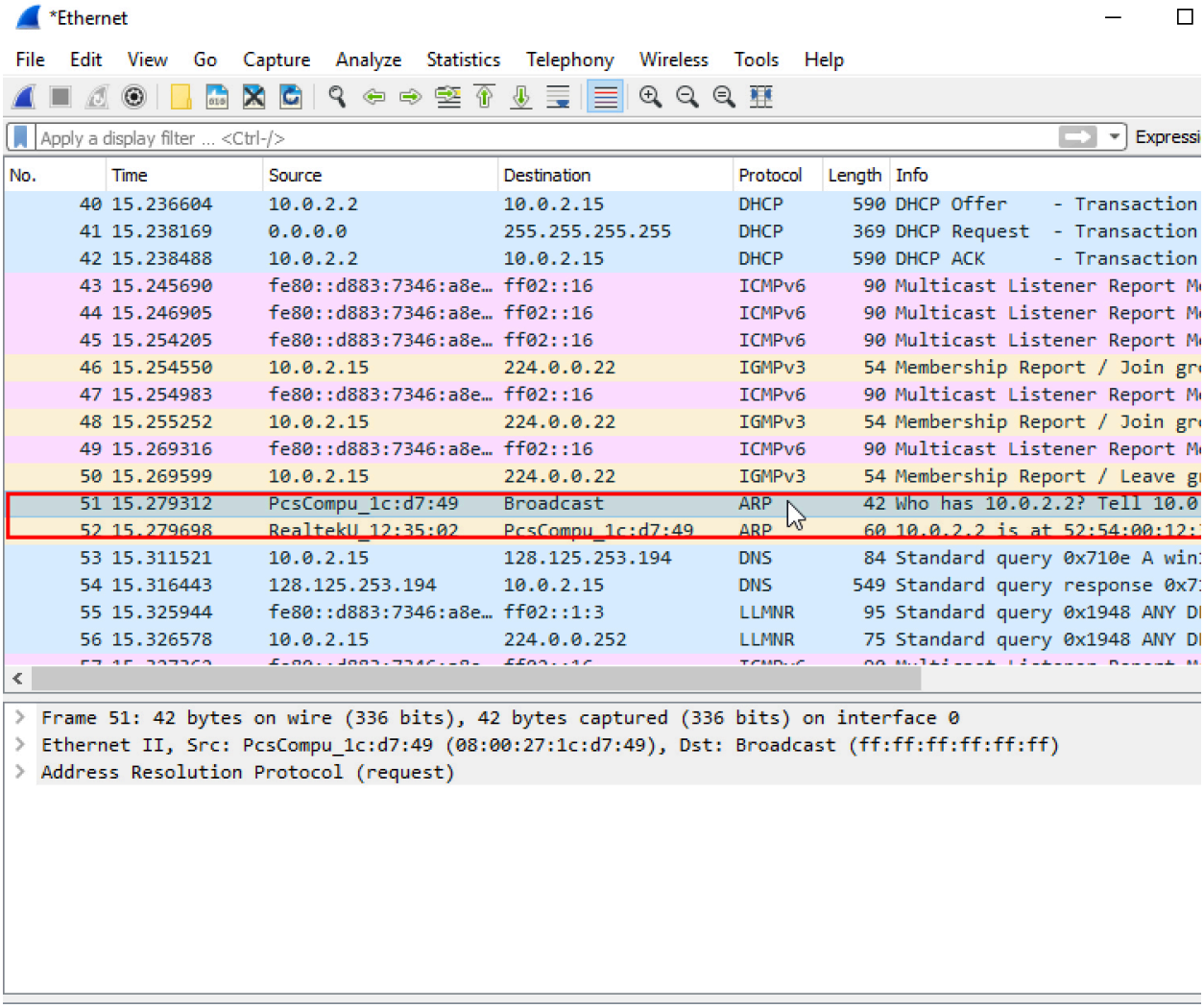
The client accepts the IP address given in the offer message within the request message. After being offered the IP address 10.0.2.15 in the offer message, my client sent back a message further requesting that specific IP address in Option 50 of the request message.

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

Answer:

The purpose of the release message is to release the IP address back to the server.
There is no verification that the release message has been received by the server.
If the message is lost, the client releases the IP address, but the server will not reassign that address until the clients lease on the address expires.

15. 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.



Answer:

Yes, they appear to be broadcasts sent out by the network to build up the known IP addresses by the clients network.

Part 2: Address Resolution Protocol

16. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

```
C:\Users\XinyueLiu>arp -a

Interface: 10.0.2.15 --- 0x2
  Internet Address      Physical Address      Type
  10.0.2.2              52-54-00-12-35-02     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Answer:

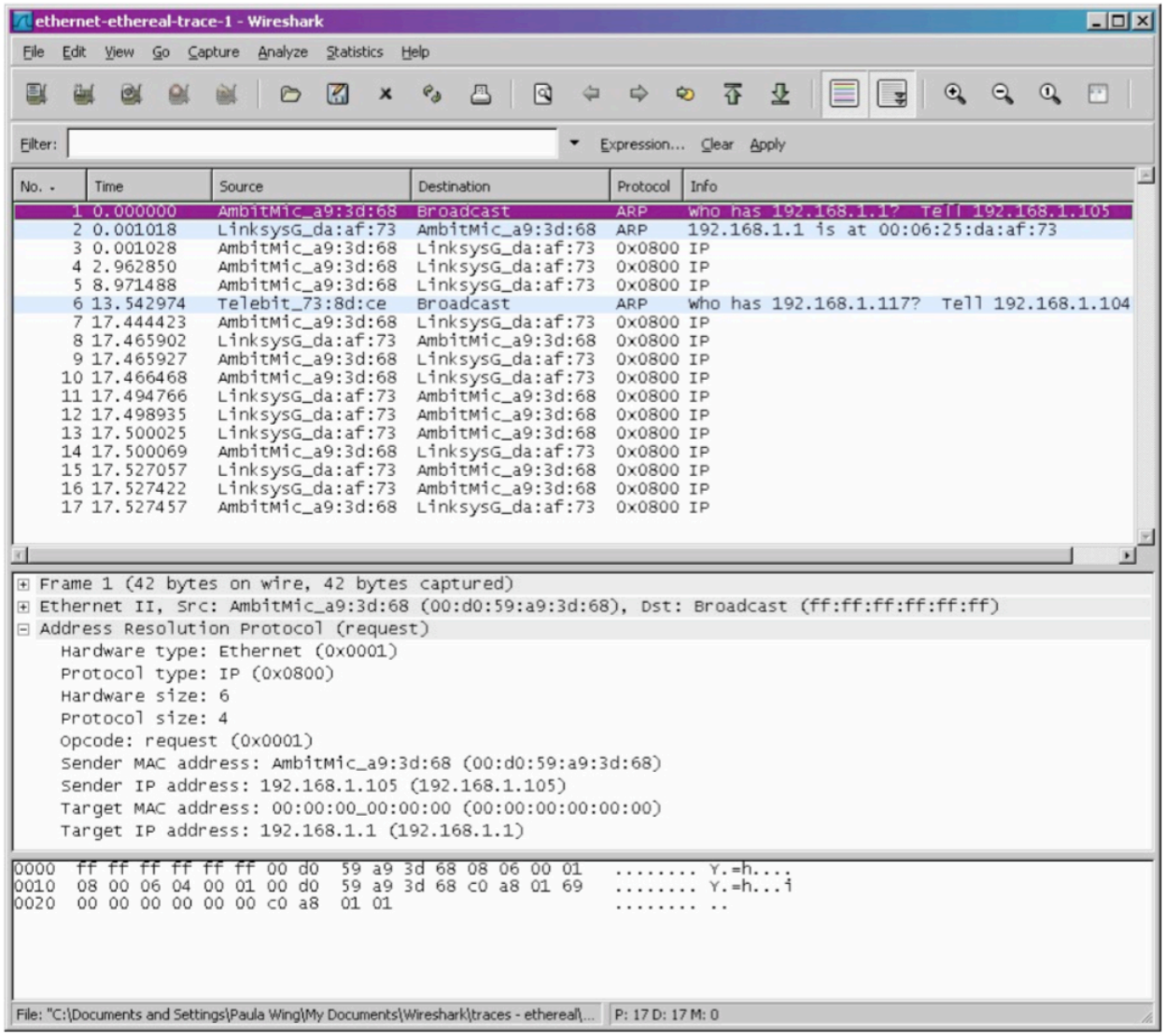
Contents of my computer's ARP cache:

Interface: 10.0.2.15 --- 0x2

Internet Address	Physical Address	Type
10.0.2.2	52-54-00-12-35-02	dynamic
10.0.2.255	ff - ff - ff - ff - ff - ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f -ff - fa	static
255.255.255.255	ff - ff - ff - ff - ff - ff	static

The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.

Q17-22:



17. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Answer:

The hex value for the source address is 00:d0:59:a9:3d:68. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.

18. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

Answer:

The hex value for the Ethernet Frame type field is 0x0806, for ARP.

19. Download the ARP specification from ftp://ftp.rfc-editor.org/innotes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
Answer:
The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
Answer:
The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request.

c) Does the ARP message contain the IP address of the sender?
Answer:
Yes, the ARP message containg the IP address 192.168.1.105 for the sender.

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
Answer:
The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

20. Now find the ARP reply that was sent in response to the ARP request.
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
Answer:
The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
Answer:
The hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply.

c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
Answer:
The answer to the earlier ARP request appears in the"Sender MAC address" field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.

21. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
Answer:
The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68 .

22. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indiated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
Answer:
There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address.