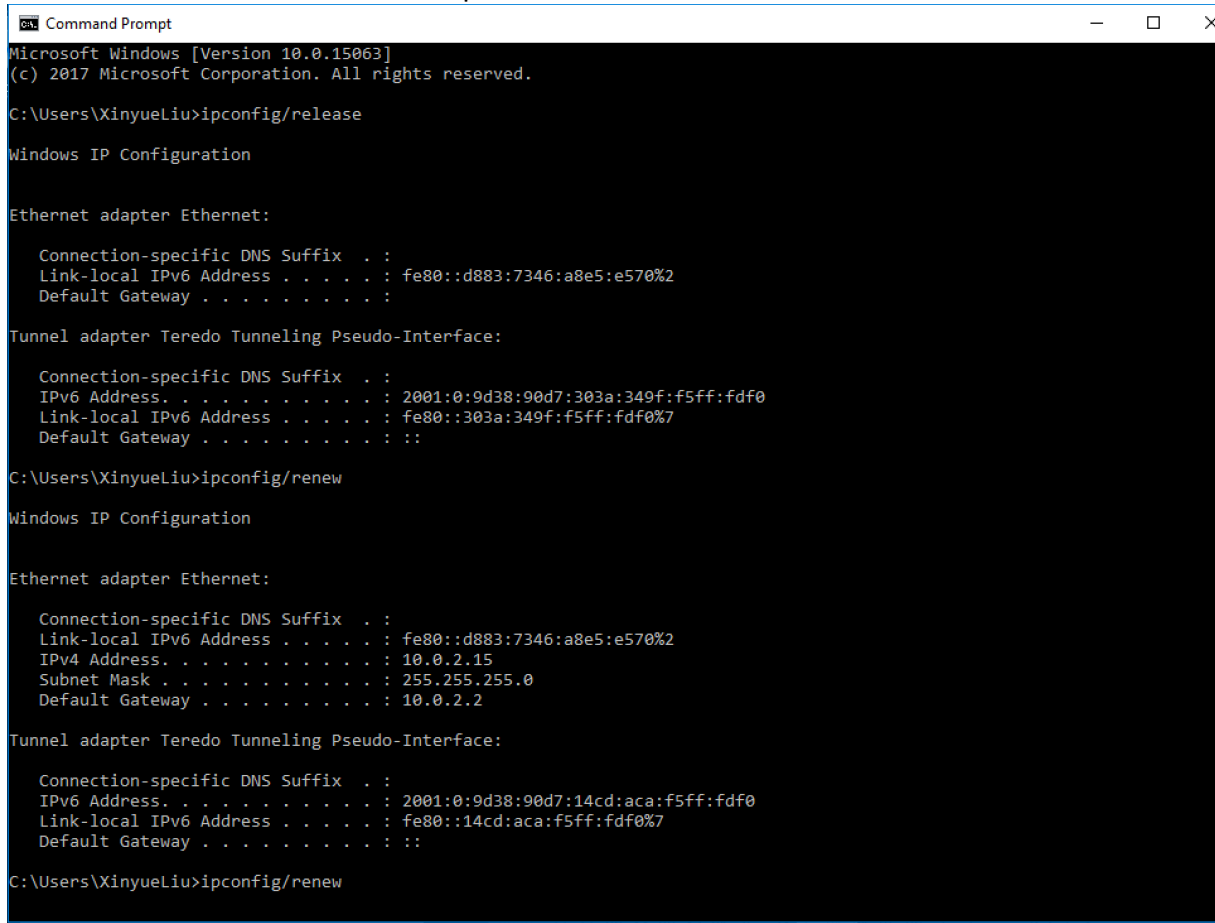


EE450 – Lab2 Report
XINYUE LIU
1332044343

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:fd0
    Link-local IPv6 Address . . . . . : fe80::303a:349f:f5ff:fd0%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:fd0
    Link-local IPv6 Address . . . . . : fe80::14cd:aca:f5ff:fd0%7
    Default Gateway . . . . . : ::

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

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

Answer: UDP

Snapshot:

The image is a screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes. The top pane, titled 'bootp', shows a list of captured packets. The middle pane shows the details of the selected packet (No. 40), including the Internet Protocol Version 4 header and the User Datagram Protocol (UDP) header. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet list shows a series of DHCP messages: Discover, Offer, Request, ACK, Release, Discover, Offer, Request, and ACK. The details pane for the selected packet (No. 40) shows the UDP header with source port 68 and destination port 67. The raw packet data shows the DHCP message structure.

No.	Time	Source	Destination	Protocol	Length	Info
39	15.236241	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xc6
40	15.236604	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0xc6
41	15.238169	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xc6
42	15.238488	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0xc6
327	36.961288	10.0.2.15	10.0.2.2	DHCP	357	DHCP Request - Transaction ID 0x5c
328	36.961625	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0x5c
416	67.431536	10.0.2.15	10.0.2.2	DHCP	342	DHCP Release - Transaction ID 0xd0
441	74.635238	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0x88
442	74.635569	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0x88
443	74.636804	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0x88
444	74.637049	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0x88

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: 329
- Identification: 0x3f8f (16271)
- > Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source: 0.0.0.0
- Destination: 255.255.255.255
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

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

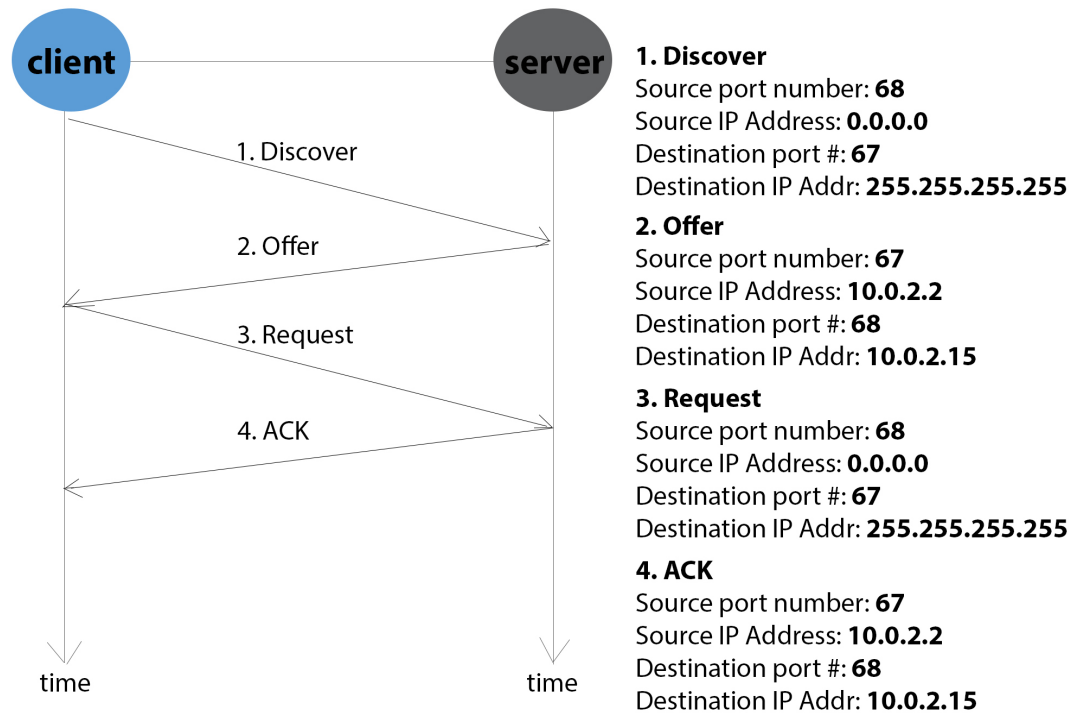
Offset	Hex	ASCII
0000	ff ff ff ff ff 08 00 27 1c d7 49 08 00 45 00 '..I..E.
0010	01 49 3f 8f 00 00 80 11 00 00 00 00 00 ff ff	.I?.....
0020	ff ff 00 44 00 43 01 35 34 de 01 01 06 00 c6 af	...D.C.5 4.....
0030	bb 33 00 00 00 00 00 00 00 00 00 00 00 00 00	.3.....

Bootstrap Protocol: Protocol | Packets: 702 · Displayed: 11 (1.6%) · Dropped: 0 (0.0%) | Profile: Default

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.



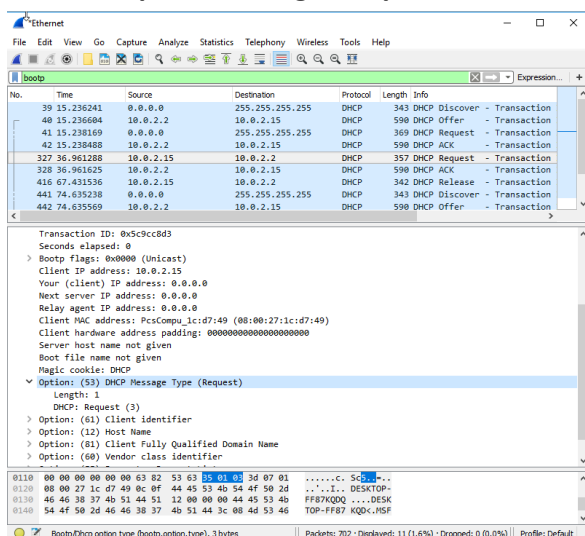
4. What is the link-layer (e.g., Ethernet) address of your host in hex format?

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

[illegible]

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.

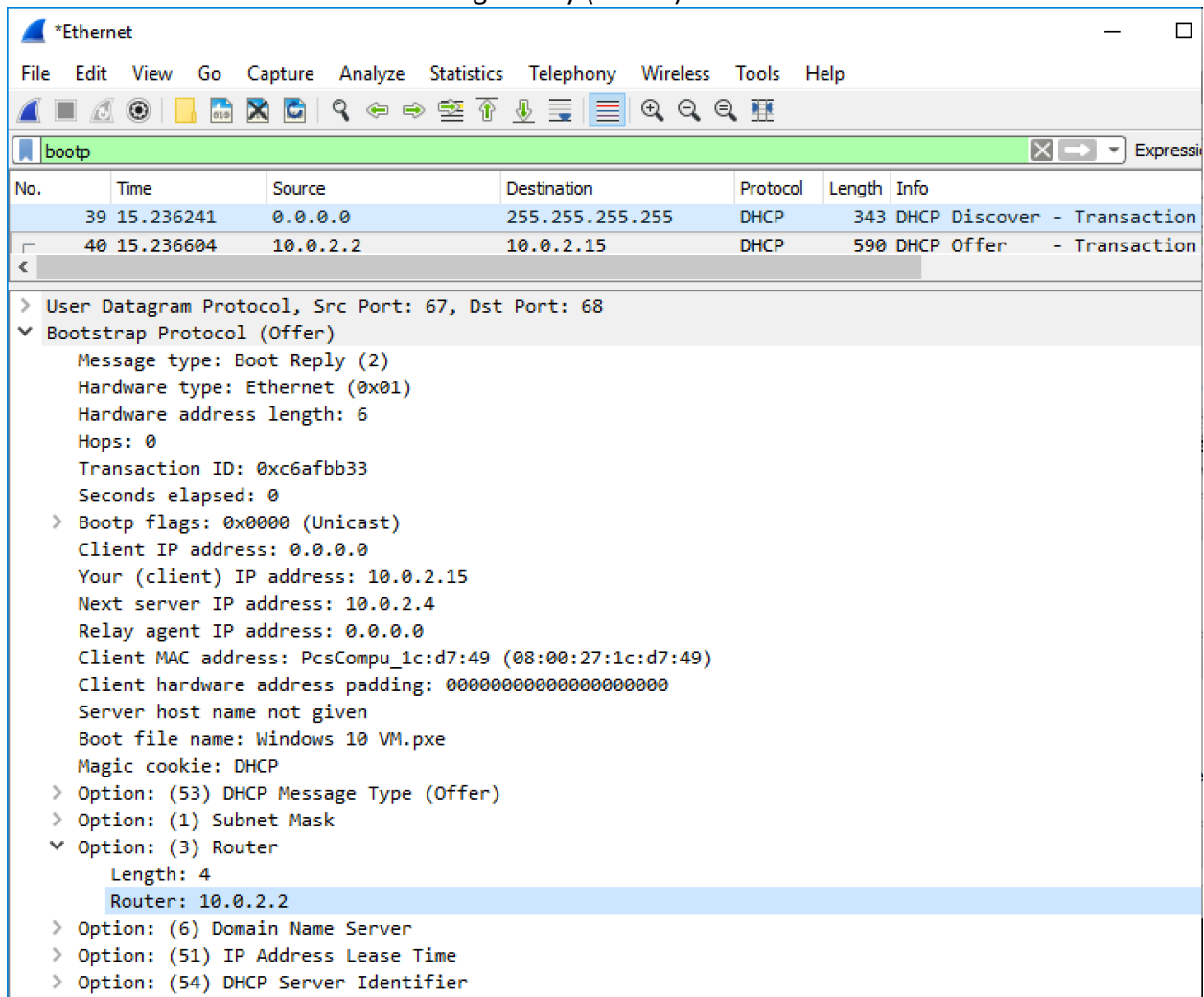
[illegible]

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.

[illegible]

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).



The image shows a Wireshark packet capture window titled "*Ethernet". The packet list on the left shows two DHCP packets. The second packet, at time 15.236604, is a DHCP Offer from source 10.0.2.2 to destination 10.0.2.15. The packet details pane on the right shows the structure of this DHCP Offer message.

No.	Time	Source	Destination	Protocol	Length	Info
39	15.236241	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction
40	15.236604	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction

Packet 40 details:

- User Datagram Protocol, Src Port: 67, Dst Port: 68
- Bootstrap Protocol (Offer)
 - Message type: Boot Reply (2)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xc6afbb33
 - Seconds elapsed: 0
 - Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0
 - Your (client) IP address: 10.0.2.15
 - Next server IP address: 10.0.2.4
 - Relay agent IP address: 0.0.0.0
 - Client MAC address: PcsCompu_1c:d7:49 (08:00:27:1c:d7:49)
 - Client hardware address padding: 00000000000000000000
 - Server host name not given
 - Boot file name: Windows 10 VM.pxe
 - Magic cookie: DHCP
 - Option: (53) DHCP Message Type (Offer)
 - Option: (1) Subnet Mask
 - Option: (3) Router
 - Length: 4
 - Router: 10.0.2.2
 - Option: (6) Domain Name Server
 - Option: (51) IP Address Lease Time
 - Option: (54) DHCP Server Identifier

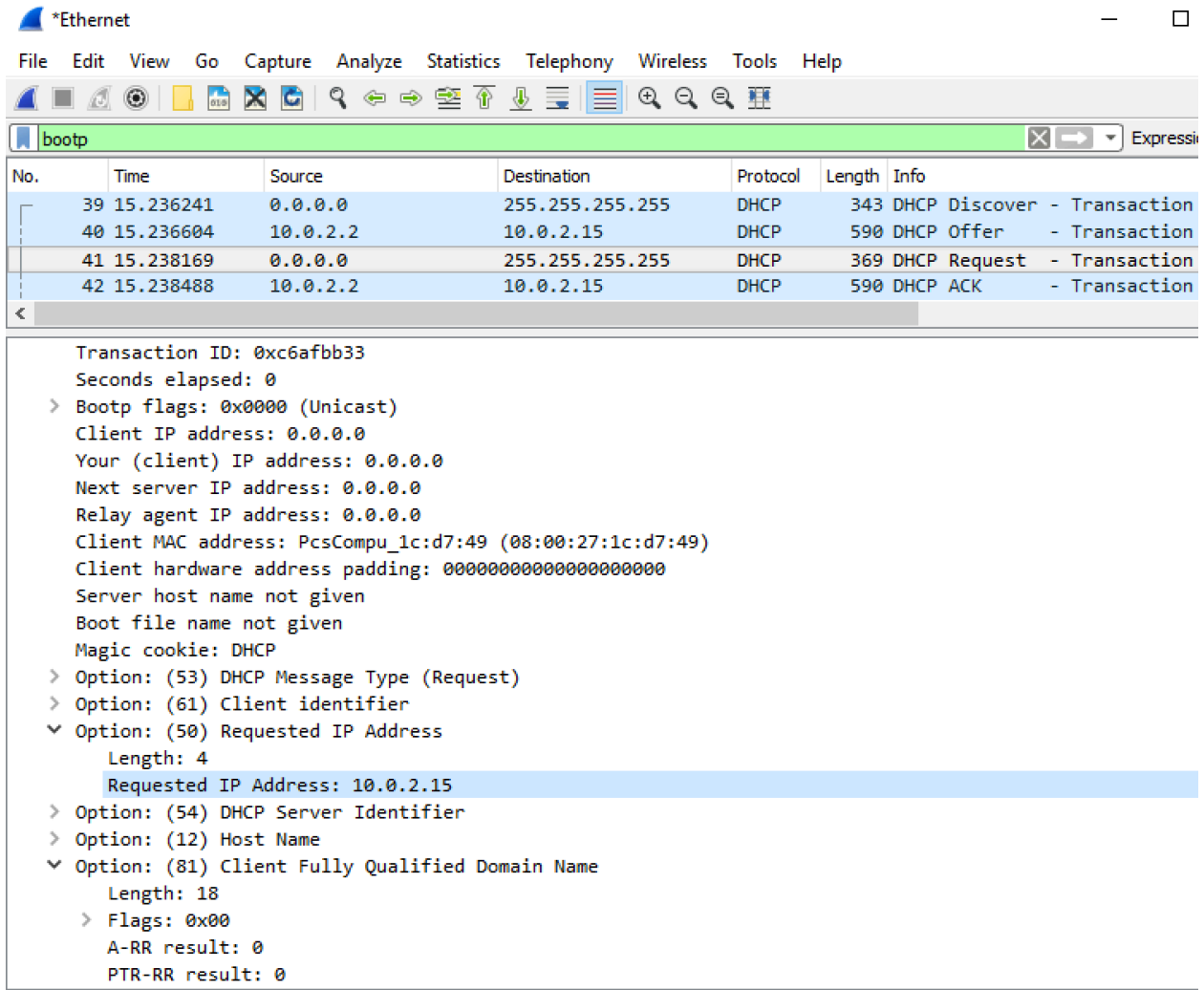
Answer:

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?



*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
39	15.236241	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction
40	15.236604	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction
41	15.238169	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction
42	15.238488	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction

Transaction ID: 0xc6afbb33
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_1c:d7:49 (08:00:27:1c:d7:49)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
✓ Option: (50) Requested IP Address
 Length: 4
 Requested IP Address: 10.0.2.15
> Option: (54) DHCP Server Identifier
> Option: (12) Host Name
✓ Option: (81) Client Fully Qualified Domain Name
 Length: 18
 > Flags: 0x00
 A-RR result: 0
 PTR-RR result: 0

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.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expressi

No.	Time	Source	Destination	Protocol	Length	Info
40	15.236604	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction
41	15.238169	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction
42	15.238488	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction
43	15.245690	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M
44	15.246905	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M
45	15.254205	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M
46	15.254550	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Join gr
47	15.254983	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M
48	15.255252	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Join gr
49	15.269316	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M
50	15.269599	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Leave g
51	15.279312	PcsCompu_1c:d7:49	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0
52	15.279698	RealtekU_12:35:02	PcsCompu_1c:d7:49	ARP	60	10.0.2.2 is at 52:54:00:12:
53	15.311521	10.0.2.15	128.125.253.194	DNS	84	Standard query 0x710e A win:
54	15.316443	128.125.253.194	10.0.2.15	DNS	549	Standard query response 0x7:
55	15.325944	fe80::d883:7346:a8e...	ff02::1:3	LLMNR	95	Standard query 0x1948 ANY DI
56	15.326578	10.0.2.15	224.0.0.252	LLMNR	75	Standard query 0x1948 ANY DI
57	15.327363	fe80::d883:7346:a8e...	ff02::16	ICMPv6	90	Multicast Listener Report M

<

> Frame 51: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 > Ethernet II, Src: PcsCompu_1c:d7:49 (08:00:27:1c:d7:49), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (request)

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:

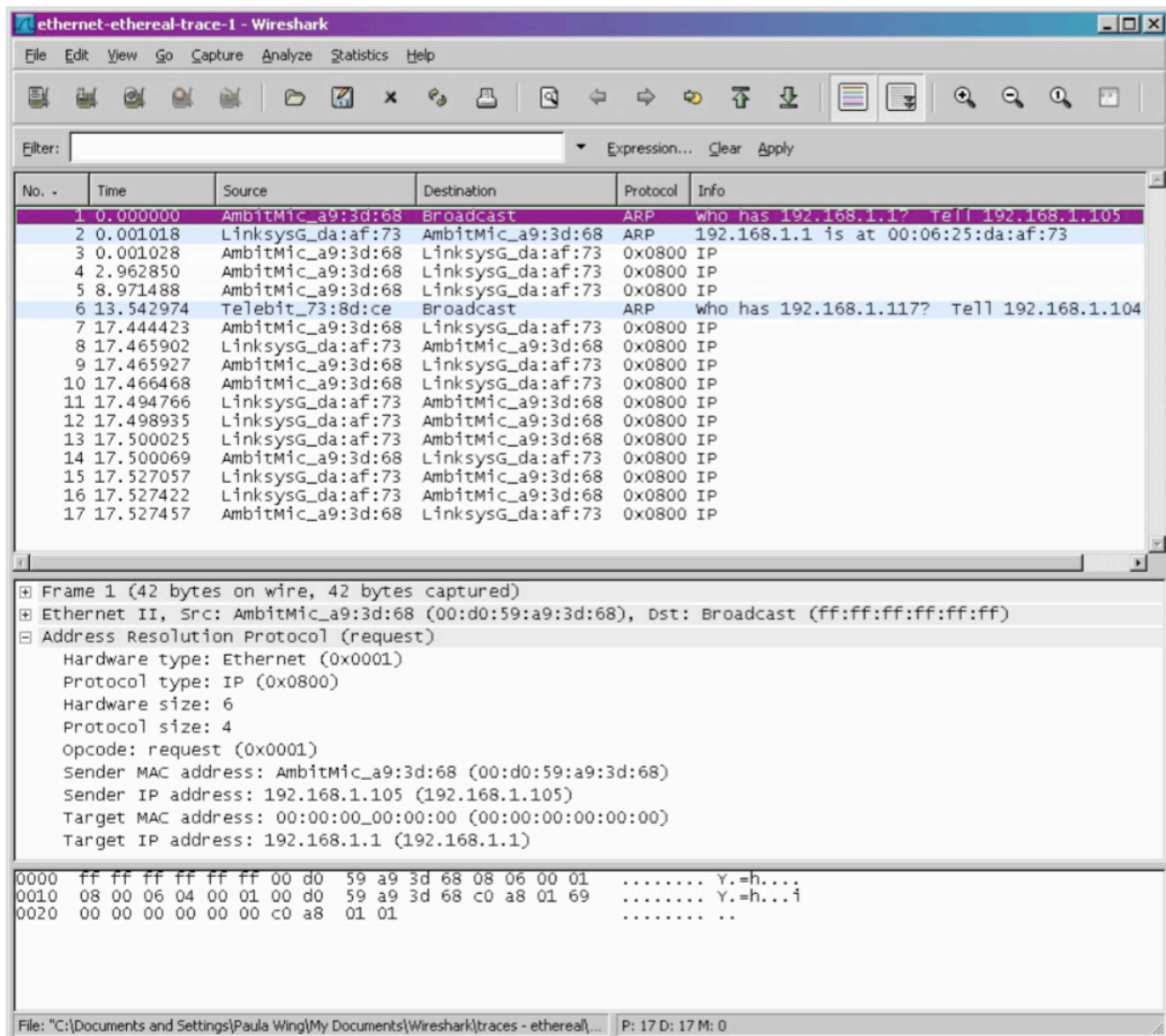
Contents of my computer's ARP cache:

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 indicated 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.