

Fatemeh “Ellie” Solhjou Khah
Wireshark-DHCP v8.1

Lab 1

EE450

Abstract

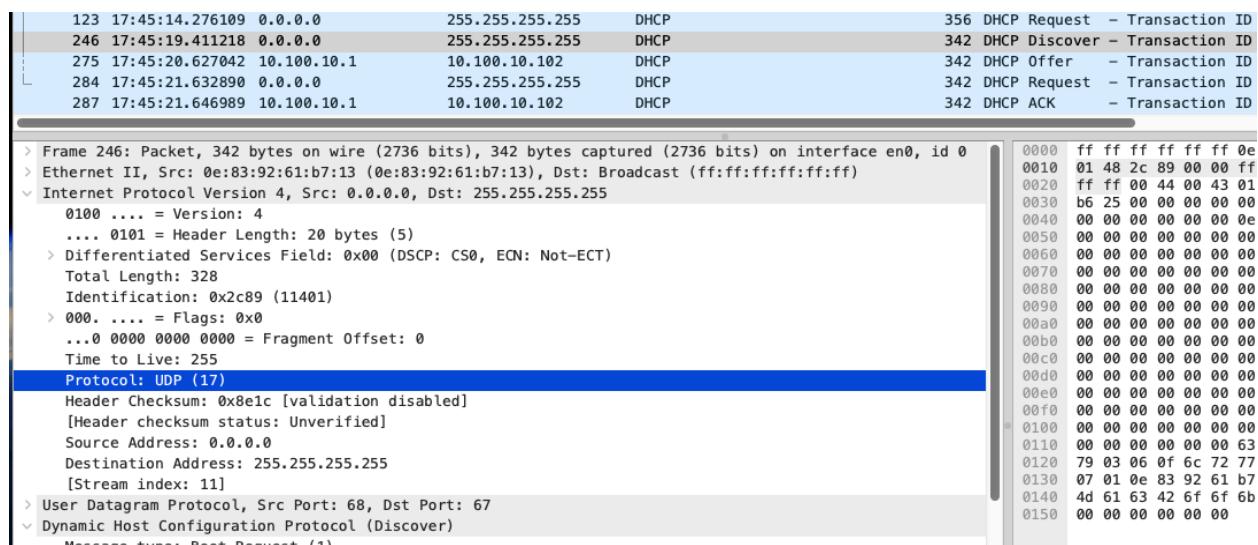
This lab examines the Dynamic Host Configuration Protocol (DHCP) using Wireshark to analyze how a client automatically obtains network configuration. By observing the Discover, Offer, Request, and ACK messages, the DHCP process was studied in detail. The analysis focused on key configuration parameters provided by the server, including the assigned IP address, subnet mask, default gateway (router), DNS server, lease time, and DHCP server identifier. This lab reinforced understanding of DHCP message structure and protocol encapsulation.

Let's explore the questions in the lab to better understand DHCP message structure and protocol encapsulation.

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

The DHCP Discover message is sent using UDP as the underlying transport protocol.

DHCP uses UDP because it is a connectionless protocol, which is appropriate at this stage since the client does not yet know the IP address of the DHCP server and cannot establish a TCP connection.



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

It is 0.0.0.0 as highlighted below. Because the client (my machine) is still in the discovery phase and has not been acknowledged yet to an IP address by a DHCP server.

123 17:45:14.276109 0.0.0.0	255.255.255.255	DHCP	356 DHCP Request - Transaction ID
246 17:45:19.411218 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
275 17:45:20.627042 10.100.10.1	10.100.10.102	DHCP	342 DHCP Offer - Transaction ID
284 17:45:21.632890 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID
287 17:45:21.646989 10.100.10.1	10.100.10.102	DHCP	342 DHCP ACK - Transaction ID

> Frame 246: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 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: 328
 Identification: 0x2c89 (11401)
 > 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 255
 Protocol: UDP (17)
 Header Checksum: 0x8e1c [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 0.0.0.0
 Destination Address: 255.255.255.255
 [Stream index: 11]
 User Datagram Protocol, Src Port: 68, Dst Port: 67
 Source Port: 68
 Destination Port: 67

0000 ff ff ff ff ff ff 0e
0010 01 48 2c 89 00 00 ff
0020 ff ff 00 44 00 43 01
0030 b6 25 00 00 00 00 00
0040 00 00 00 00 00 00 0e
0050 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63
0120 79 03 06 0f 6c 72 77
0130 07 01 0e 83 92 61 b7
0140 4d 61 63 42 6f 6f 6b
0150 00 00 00 00 00 00 00

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 is 255.255.255.255 which is for local broadcasting. Yet my device doesn't know anything other than its MAC address and this is why it is sending discovery messages to everyone on the LAN network to see if there is a server that can give the client an IP address.

123 17:45:14.276109 0.0.0.0	255.255.255.255	DHCP	356 DHCP Request - Transaction ID
246 17:45:19.411218 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
275 17:45:20.627042 10.100.10.1	10.100.10.102	DHCP	342 DHCP Offer - Transaction ID
284 17:45:21.632890 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID
287 17:45:21.646989 10.100.10.1	10.100.10.102	DHCP	342 DHCP ACK - Transaction ID

> Frame 246: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 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: 328
 Identification: 0x2c89 (11401)
 > 000. = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 255
 Protocol: UDP (17)
 Header Checksum: 0x8e1c [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 0.0.0.0
 Destination Address: 255.255.255.255
 [Stream index: 11]
 User Datagram Protocol, Src Port: 68, Dst Port: 67
 Source Port: 68
 Destination Port: 67

0000 ff ff ff ff ff ff 0e
0010 01 48 2c 89 00 00 ff
0020 ff ff 00 44 00 43 01
0030 b6 25 00 00 00 00 00
0040 00 00 00 00 00 00 0e
0050 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00
00a0 00 00 00 00 00 00 00
00b0 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00
00d0 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63
0120 79 03 06 0f 6c 72 77
0130 07 01 0e 83 92 61 b7
0140 4d 61 63 42 6f 6f 6b
0150 00 00 00 00 00 00 00

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

The value in the Transaction ID field of the Discover message is **0x3af8b625**. This identifier is used to uniquely match the Discover message with subsequent Offer, Request, and ACK messages within the same DHCP transaction.

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
52	17:45:11.819095	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - T
123	17:45:14.276109	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - T
246	17:45:19.411218	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - T
275	17:45:20.627042	10.100.10.1	10.100.10.102	DHCP	342	DHCP Offer - T
284	17:45:21.632890	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - T
287	17:45:21.646989	10.100.10.1	10.100.10.102	DHCP	342	DHCP ACK - T

> Frame 246: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13), 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: 0x3af8b625
 Seconds elapsed: 0

0000 ff ff f
0010 01 48 2
0020 ff ff 0
0030 b6 25 0
0040 00 00 0
0050 00 00 0
0060 00 00 0
0070 00 00 0
0080 00 00 0
0090 00 00 0
00a0 00 00 0
00b0 00 00 0
00c0 00 00 0
00d0 00 00 0

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?

DHCP Message Type, Parameter Request List, Maximum DHCP Message Size, Client Identifier, IP Address Lease Time, Host Name, End

No.	Time	Source	Destination	Protocol	Length	Info
123	17:45:14.276109	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request -
246	17:45:19.411218	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover -
275	17:45:20.627042	10.100.10.1	10.100.10.102	DHCP	342	DHCP Offer -
284	17:45:21.632890	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request -
287	17:45:21.646989	10.100.10.1	10.100.10.102	DHCP	342	DHCP ACK -

< Dynamic Host Configuration Protocol (Discover)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x3af8b625
 Seconds elapsed: 0

< Bootp flags: 0x0000 (Unicast)
 0... = Broadcast flag: Unicast
 .000 0000 0000 0000 = Reserved flags: 0x0000
 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: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
 Client hardware address padding: 000000000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 > Option: (53) DHCP Message Type (Discover)
 > Option: (55) Parameter Request List
 > Option: (57) Maximum DHCP Message Size
 > Option: (61) Client identifier
 > Option: (51) IP Address Lease Time
 > Option: (12) Host Name
 > Option: (255) End

0000 ff ff f
0010 01 48 2
0020 ff ff 0
0030 b6 25
0040 00 00
0050 00 00
0060 00 00
0070 00 00
0080 00 00
0090 00 00
00a0 00 00
00b0 00 00
00c0 00 00
00d0 00 00
00e0 00 00
00f0 00 00
0100 00 00
0110 00 00
0120 79 03
0130 07 01
0140 4d 61
0150 00 00

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?

The message type is noted as Boot Reply and has transaction id identical to the one in the discovery message

275	17:45:20.627042	10.100.10.1	10.100.10.102	DHCP	342	DHCP Offer
284	17:45:21.632890	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request
287	17:45:21.646989	10.100.10.1	10.100.10.102	DHCP	342	DHCP ACK

```

> Frame 275: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
> Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
> User Datagram Protocol, Src Port: 67, Dst Port: 68
< Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x3af8b625
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.100.10.102
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (10.100.10.1)
  > Option: (51) IP Address Lease Time
  < Option: (1) Subnet Mask (255.255.252.0)
  
```

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

It is 10.100.10.1 which is sharing the same net id with the offered but not yet assigned IP to the client. The offer comes from a real configured IP address, since the DHCP server already has an assigned address.

275	17:45:20.627042	10.100.10.1	10.100.10.102	DHCP	342	DHCP Offer
284	17:45:21.632890	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request
287	17:45:21.646989	10.100.10.1	10.100.10.102	DHCP	342	DHCP ACK

```

> Frame 275: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
< Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0. ECN: Not-ECT)
  
```

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.]

It is 10.100.10.102 . It is the IP address being offered to the client. The client does not yet officially own this IP address. The server is sending the Offer as a unicast instead of a broadcast since in the discovery message, the bootp flags field was set to zero indicating the client is capable of receiving unicast responses.

```

275 17:45:20.627042 10.100.10.1      10.100.10.102    DHCP          342 DHCP Offer
284 17:45:21.632890 0.0.0.0        255.255.255.255  DHCP          342 DHCP Request
287 17:45:21.646989 10.100.10.1      10.100.10.102    DHCP          342 DHCP ACK

> Frame 275: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

```

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?

Per the image below, the server offers to provide:

1. DHCP Server Identifier - 10.100.10.1
2. IP Address Lease Time
3. Subnet Mask - 255.255.252.0
4. Router - 10.100.10.1
5. Domain Name Server (DNS)

```

275 17:45:20.627042 10.100.10.1      10.100.10.102    DHCP          342 DHCP Offer
284 17:45:21.632890 0.0.0.0        255.255.255.255  DHCP          342 DHCP Request
287 17:45:21.646989 10.100.10.1      10.100.10.102    DHCP          342 DHCP ACK

Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x3af8b625
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    0... .... .... = Broadcast flag: Unicast
    .000 0000 0000 0000 = Reserved flags: 0x0000
  Client IP address: 0.0.0.0
  Your (client) IP address: 10.100.10.102
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Client hardware address padding: 00000000000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (10.100.10.1)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.252.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (255) End

```

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?**

IP datagram contains a UDP segment which is expanded in below snippet

UDP Source Port (Client)= 68

UDP Destination Port (Server) = 67

```
✓ 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: 328
    Identification: 0xf4ab (62635)
  ✓ 000. .... = Flags: 0x0
    0.... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0xc5f9 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 255.255.255.255
      [Stream index: 39]
  ✓ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
```

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

It is 0.0.0.0 because the IP address for the client has not been acknowledged/leased by the DHCP server. It gets assigned to the client after it is ACK by the DHCP server.

284 17:45:21.632890 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1	10.100.10.102	DHCP	342 DHCP ACK - Transaction ID 0x3af8b625
> Frame 284: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0			
> Ethernet II, Src: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)			
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255			
0100 = Version: 4			

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

It is 255.255.255.255 a local broadcast IP address. The reason is that the client lets the other DHCP servers offering IP addresses know that it rejected their offer.

284 17:45:21.632890 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1	10.100.10.102	DHCP	342 DHCP ACK - Transaction ID 0x3af8b625
> Frame 284: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0			
> Ethernet II, Src: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13), Dst: Broadcast (ff:ff:ff:ff:ff:ff)			
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255			
0100 = Version: 4			

13. 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?

0x3af8b625 - yes

246 17:45:19.411218 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x3af8b625
275 17:45:20.627042 10.100.10.1	10.100.10.102	DHCP	342 DHCP Offer - Transaction ID 0x3af8b625
284 17:45:21.632890 0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1	10.100.10.102	DHCP	342 DHCP ACK - Transaction ID 0x3af8b625
User Datagram Protocol, Src Port: 68, Dst Port: 67			
Dynamic Host Configuration Protocol (Request)			
Message type: Boot Request (1)			
Hardware type: Ethernet (0x01)			
Hardware address length: 6			
Hops: 0			
Transaction ID: 0x3af8b625			
Seconds elapsed: 2			
> Bootp flags: 0x0000 (Unicast)			
0000 ff ff ff ff ff ff 0e 83 92 61 b7 13 08			
0010 01 48 2c 8a 00 00 ff 11 8e 1b 00 00 00			
0020 ff ff 00 44 00 43 01 34 f2 9a 01 01 01			
0030 b6 25 00 02 00 00 00 00 00 00 00 00 00 00			
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00			
0050 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			
0070 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			
0090 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			

14. 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?

There is no difference between the Parameter Request List in the DHCP Discover message and the DHCP Request message. The client requests the same set of configuration parameters in both messages.

```

    ▼ Option: (53) DHCP Message Type (Request)
        Length: 1
        DHCP: Request (3)
    ▼ Option: (55) Parameter Request List
        Length: 12
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (121) Classless Static Route
        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: (108) IPv6-Only Preferred
        Parameter Request List Item: (114) DHCP Captive-Portal
        Parameter Request List Item: (119) Domain Search
        Parameter Request List Item: (252) Private/Proxy autodiscovery
        Parameter Request List Item: (95) LDAP [TODO:RFC3679]
        Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
        Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    ▼ Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    ▼ Option: (55) Parameter Request List
        Length: 12
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (121) Classless Static Route
        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: (108) IPv6-Only Preferred
        Parameter Request List Item: (114) DHCP Captive-Portal
        Parameter Request List Item: (119) Domain Search
        Parameter Request List Item: (252) Private/Proxy autodiscovery
        Parameter Request List Item: (95) LDAP [TODO:RFC3679]
        Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
        Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type

```

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

15. 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 10.100.10.1, which is the DHCP server's IP address. This address is special because it is equal to the DHCP server identifier that assigns the client's IP address and typically represents the router on the local network - the relay agent IP address value is 0.0.0.0 which means the client is talking to the DHCP server

directly - they are on LAN . and the DHCP Server Identifier value is identical to the router's IP address value which means the router and DHCP Server are same device.

```

246 17:45:19.411218 0.0.0.0      255.255.255.255    DHCP          342 DHCP Discover - Transaction ID 0x3af8b625
275 17:45:20.627042 10.100.10.1   10.100.10.102    DHCP          342 DHCP Offer - Transaction ID 0x3af8b625
284 17:45:21.632890 0.0.0.0      255.255.255.255    DHCP          342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1   10.100.10.102    DHCP          342 DHCP ACK - Transaction ID 0x3af8b625

> Frame 287: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
      Total Length: 328
      Identification: 0x6524 (25892)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)
      Header Checksum: 0xab52 [validation disabled]
        [Header checksum status: Unverified]
      Source Address: 10.100.10.1
      Destination Address: 10.100.10.102
      Stream index: 331

0000  0e 83 92 61 b7 13 00 18 0a 86 ab fc
0010  01 48 65 24 40 00 40 11 ab 52 0a 64
0020  0a 66 00 43 00 44 01 34 fb 01 02 01
0030  b6 25 00 02 00 00 00 00 00 00 00 04
0040  00 00 00 00 00 00 00 0e 83 92 61 b7 13
0050  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
0070  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
0090  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
00b0  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
00d0  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
00f0  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
0110  00 00 00 00 00 00 63 82 53 63 35 01
0120  64 0a 01 33 04 00 01 51 80 01 04 ff
0130  04 0a 64 0a 01 06 08 08 08 08 08 08

Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xe898e760
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.100.10.102
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
Client hardware address padding: 000000000000000000000000
Server host name not given
  Boot file name not given
  Option: (1) Subnet mask (255.255.252.0)
  Option: (2) Router
  Option: (3) Router
    Length: 4
    Router: 10.100.10.1

```

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

The destination IP address is 10.100.10.102, which is the newly assigned IP address of the client; the DHCP server sends the ACK as a unicast to this address, indicating that the client has just been assigned this IP and that the DHCP process has completed successfully.

```

246 17:45:19.411218 0.0.0.0      255.255.255.255    DHCP          342 DHCP Discover - Transaction ID 0x3af8b625
275 17:45:20.627042 10.100.10.1   10.100.10.102    DHCP          342 DHCP Offer  - Transaction ID 0x3af8b625
284 17:45:21.632890 0.0.0.0      255.255.255.255    DHCP          342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1   10.100.10.102    DHCP          342 DHCP ACK   - Transaction ID 0x3af8b625

> Frame 287: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCH: CS0, ECN: Not-ECT)
      Total Length: 328
      Identification: 0x6524 (25892)
    > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)
      Header Checksum: 0xab52 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 10.100.10.1
      Destination Address: 10.100.10.102
      !Stream index: 331

```

Hex dump of the DHCP ACK message:

```

0000 0e 83 92 61 b7 13 00 18 0a 86 ab fc
0010 01 48 65 24 40 00 40 11 ab 52 0a 6
0020 0a 66 00 43 00 44 01 34 fb 01 02 0
0030 b6 25 00 02 00 00 00 00 00 00 02 64
0040 00 00 00 00 00 00 00 0e 83 92 61 b7 13
0050 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
0070 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
0090 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
00b0 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
00d0 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
00f0 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
0110 00 00 00 00 00 00 63 82 53 63 35 01
0120 64 0a 01 33 04 00 01 51 80 01 04 f1
0130 04 0a 64 0a 01 06 08 08 08 08 08 08
0140 04 0a 64 0a 01 06 08 08 08 08 08 08
0150 04 0a 64 0a 01 06 08 08 08 08 08 08

```

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?

Your (Client) IP address.

```

284 17:45:21.632890 0.0.0.0      255.255.255.255    DHCP          342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1   10.100.10.102    DHCP          342 DHCP ACK   - Transaction ID 0x3af8b625

> Frame 287: Packet, 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: CiscoMeraki_86:ab:fc (00:18:0a:86:ab:fc), Dst: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
  Internet Protocol Version 4, Src: 10.100.10.1, Dst: 10.100.10.102
  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
    Transaction ID: 0x3af8b625
    Seconds elapsed: 2
    > Boot flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.100.10.102
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
    Client hardware address padding: 000000000000000000000000
    Server host name not given

```

Hex dump of the DHCP ACK message:

```

0000 0e 83 92 61 b7 13 00 18 0a 86 ab f
0010 01 48 65 24 40 00 40 11 ab 52 0a 6
0020 0a 66 00 43 00 44 01 34 fb 01 02 0
0030 b6 25 00 02 00 00 00 00 00 00 02 6
0040 00 00 00 00 00 00 00 00 0e 83 92 61 b7 1
0050 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
0070 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
0090 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
00b0 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
00d0 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
00f0 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
0110 00 00 00 00 00 00 63 82 53 63 35 0
0120 64 0a 01 33 04 00 01 51 80 01 04 f
0130 04 0a 64 0a 01 06 08 08 08 08 08 0
0140 00 00 00 00 00 00 00 00 00 00 00 00
0150 00 00 00 00 00 00 00 00 00 00 00 00

```

18. For how long a time (the so-called “lease time”) has the DHCP server assigned this IP address to the client?

1 Day

```

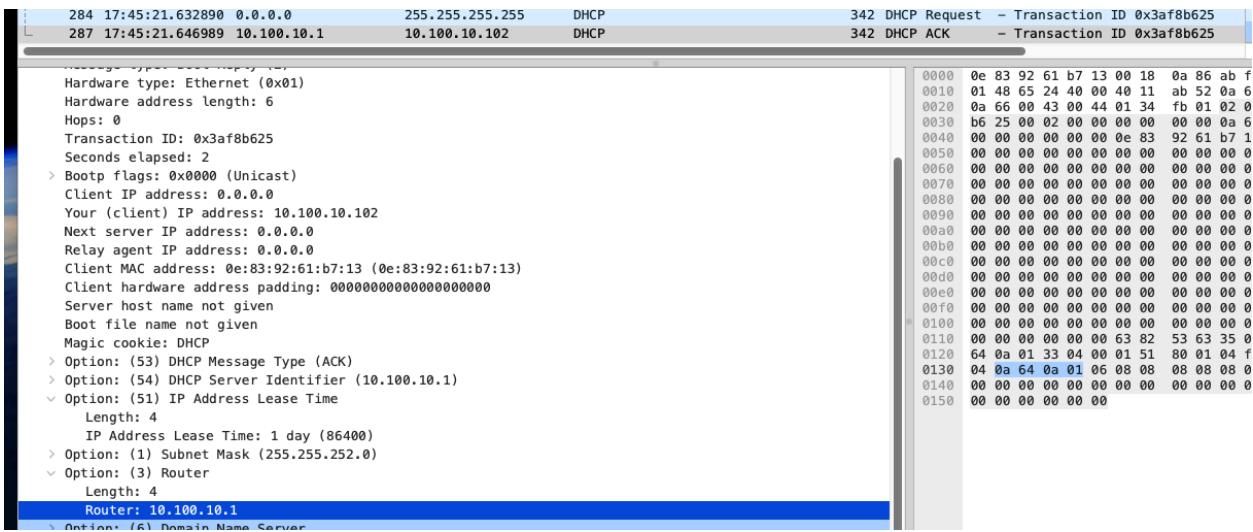
284 17:45:21.632890 0.0.0.0      255.255.255.255    DHCP          342 DHCP Request - Transaction ID 0x3af8b625
287 17:45:21.646989 10.100.10.1   10.100.10.102    DHCP          342 DHCP ACK   - Transaction ID 0x3af8b625

  Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3af8b625
    Seconds elapsed: 2
    > Boot flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.100.10.102
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 0e:83:92:61:b7:13 (0e:83:92:61:b7:13)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    > Option: (53) DHCP Message Type (ACK)
    > Option: (54) DHCP Server Identifier (10.100.10.1)
    Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: 1 day (86400)

```

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?

Router: 10.100.10.1



Conclusion

This lab provided a detailed examination of the Dynamic Host Configuration Protocol (DHCP) through packet analysis using Wireshark. By observing the complete four-step DHCP process - Discover, Offer, Request, and ACK - the interaction between the client and server was analyzed across multiple protocol layers, including IP and UDP. The lab reinforced the understanding that DHCP operates over UDP, uses broadcast communication when the client has no assigned IP address, and relies on a transaction ID to correctly associate messages within the same exchange.

Through inspection of the DHCP options fields, key configuration parameters provided by the server were identified, including the assigned IP address, subnet mask, default gateway (router), DNS server, lease time, and DHCP server identifier. The analysis also emphasized the importance of the broadcast flag behavior and the relay agent IP address field in determining whether the DHCP server is on the same local network as the client. In this trace, the value was 0.0.0.0, confirming that no relay agent was involved and that the client and DHCP server were on the same LAN.

Additionally, the distinction between the DHCP Server Identifier (Option 54) and the Router option (Option 3) was examined to determine whether the DHCP server and the default gateway were the same device. Since both options contained the same IP address, it was concluded that the router and DHCP server were operating on the same device in this network configuration.

Wireshark proved to be an effective and powerful tool for protocol analysis. Its layered packet visualization made it possible to observe encapsulation across Ethernet, IP, UDP, and DHCP, and its detailed decoding of protocol fields simplified interpretation of complex packet structures. The ability to filter traffic and inspect individual fields allowed precise correlation of messages within the DHCP exchange. However, the tool requires careful attention to detail and a strong understanding of protocol layering to avoid misinterpretation.

Overall, this lab strengthened understanding of DHCP message structure, protocol encapsulation, automatic IP configuration, and practical methods for analyzing network topology using DHCP packet fields.