

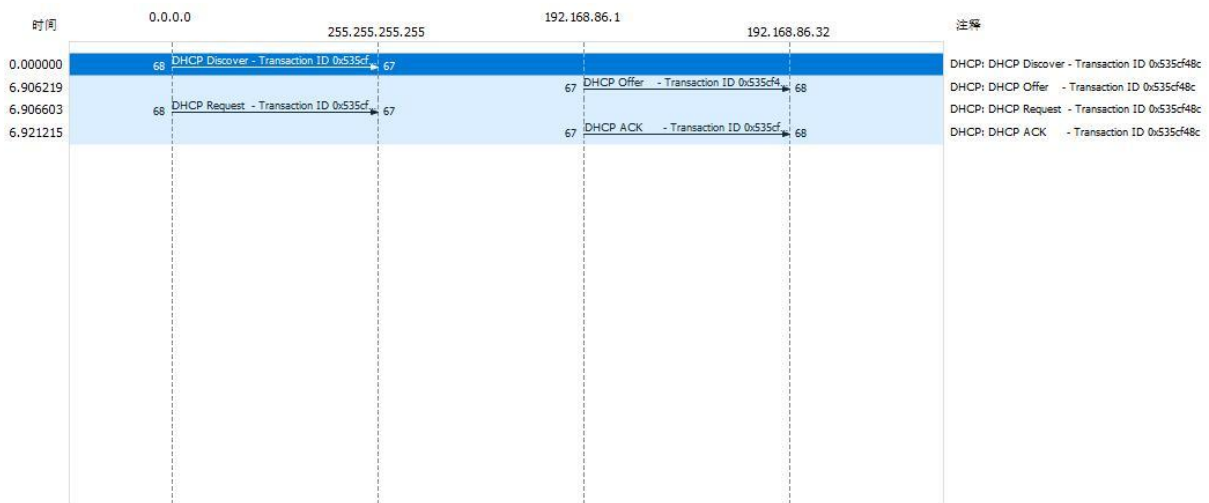
Sheng Wang  
**Wireshark-DHCP Lab 1**  
EE450

## 1. Are DHCP messages sent over UDP or TCP?

Wireshark packet capture showing DHCP messages over UDP. The packet list shows a DHCP Discover message (Transaction ID 0x535cf48c) from 0.0.0.0 to 255.255.255.255. The packet details pane shows the Ethernet II, Internet Protocol Version 4, User Datagram Protocol (Source Port: 68, Destination Port: 67), and Dynamic Host Configuration Protocol (Discover) layers. The packet bytes pane shows the raw data.

DHCP messages sent over UDP

## 2. Draw a timing diagram 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. Are the port numbers the same as in the example given in this lab assignment?



- Discover:  
Source port: 68  
Dest port: 67

- Source ip: 0.0.0.0  
Dest ip: Broadcast (255.255.255.255)  
Source MAC: a8:7e:ea:34:c2:09  
Dst MAC: Broadcast (ff:ff:ff:ff:ff:ff)
2. Offer:  
Source port: 67  
Dest port: 68  
Source ip: 192.168.86.1  
Dest ip: 192.168.86.32  
Source MAC: b0:6a:41:c7:5f:d8  
Dst MAC: a8:7e:ea:34:c2:09
3. Request:  
Source port: 68  
Dest port: 67  
Source ip: 0.0.0.0  
Dest ip: Broadcast (255.255.255.255)  
Source MAC: a8:7e:ea:34:c2:09  
Dst MAC: Broadcast (ff:ff:ff:ff:ff:ff)
4. ACK:  
Source port: 67  
Dest port: 68  
Source ip: 192.168.86.1  
Dest ip: 192.168.86.32  
Source MAC: b0:6a:41:c7:5f:d8  
Dst MAC: a8:7e:ea:34:c2:09

Yes, They have the same port numbers.

3. What is the link-layer (e.g., Ethernet) address of your host?

Encapsulation type: Ethernet (1)  
 Arrival Time: Sep 23, 2023 14:07:26.774594000 Pacific Daylight Time  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1695503246.774594000 seconds  
 [Time delta from previous captured frame: 0.895557000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 14.964049000 seconds]  
 Frame Number: 161  
 Frame Length: 342 bytes (2736 bits)  
 Capture Length: 342 bytes (2736 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: eth:ethertype:ip:udp:dhcp]  
 [Coloring Rule Name: UDP]  
 [Coloring Rule String: udp]  
 Ethernet II, Src: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
 Source: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
 User Datagram Protocol, Src Port: 68, Dst Port: 67

a8:7e:ea:34:c2:09

- What values in the DHCP discover message differentiate this message from the DHCP request message?

Message type: Root Request (1)  
 Hardware type: Ethernet (eth)  
 Hardware address length: 6  
 Hops: 0  
 Transaction ID: 0x535cf48c  
 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: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
 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 (54) Client Identifier  
 Option (50) Requested IP Address (192.168.86.32)  
 Option (50) DHCP Server Identifier (192.168.86.1)  
 Option (12) Host Name  
 Option (81) Client Fully Qualified Domain Name  
 Option (60) Vendor class Identifier  
 Option (55) Parameter Request List  
 Option (255) End

DHCP Message Type and DHCP Server Identifier

- What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the

Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

The screenshot shows a Wireshark packet capture of DHCP messages. The packet list at the top displays a sequence of DHCP messages, all with Transaction ID 0x535cf48c. The packet details pane for packet 1458 (DHCP Discover) is expanded, showing fields like Message type, Hardware type, and Transaction ID (0x535cf48c). The packet bytes pane shows the raw data of the DHCP Discover message.

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x535cf48c
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x87f382bc
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0x87f382bc
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x87f382bc
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x87f382bc
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x87f382bc
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc

Packet 1458 details:

- Dynamic Host Configuration Protocol (Discover)
- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x535cf48c
- 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: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)
- 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

first Discover: 0x535cf48c

first Offer: 0x535cf48c

first Request: 0x535cf48c

first ACK: 0x535cf48c

Wireshark packet capture showing DHCP transactions. The packet list shows a sequence of DHCP messages. Packet 1458 is highlighted, showing a DHCP Discover message with Transaction ID 0xdc1c073a. The packet details pane shows the structure of the Dynamic Host Configuration Protocol (Request) message, including fields like Message type, Hardware type, and Transaction ID. The packet bytes pane shows the raw data of the message.

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xdc1c073a
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xdc1c073a
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xdc1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Packet 1458 details:

- [Timestamps]
- UDP payload (310 bytes)
- Dynamic Host Configuration Protocol (Request)
  - Message type: Boot Request (1)
  - Hardware type: Ethernet (0x01)
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0xdc1c073a
  - Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
  - Client IP address: 192.168.86.32
  - 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: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)
  - 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

Second Request: 0xdc1c073a

Second ACK: 0xdc1c073a

The purpose of the transaction ID is used to distinguish the different requests from clients.

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

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650f53ae
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xdc1c073a
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xdc1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Discover: Src: 0.0.0.0, Dst: 255.255.255.255  
Offer: Src: 192.168.86.1, Dst: 192.168.86.32  
Request: Src: 0.0.0.0, Dst: 255.255.255.255  
ACK: Src: 192.168.86.1, Dst: 192.168.86.32

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

Wi-Fi

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

bootp

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.629604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650ff53ae
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xd1c073a
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xd1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Hardware address length: 6  
Hops: 0  
Transaction ID: 0x535cf48c  
Seconds elapsed: 0  
Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 192.168.86.32  
Next server IP address: 192.168.86.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Option: (53) DHCP Message Type (Offer)  
Option: (54) DHCP Server Identifier (192.168.86.1)  
Option: (51) IP Address Lease Time  
Option: (58) Renewal Time Value  
Option: (59) Rebinding Time Value  
Option: (1) Subnet Mask (255.255.255.0)  
Option: (28) Broadcast Address (192.168.86.255)

DHCP/BOOTP option type (dhcp.option.type), 3 byte(s)

分组: 2771 · 已显示: 16 (0.6%) · 已丢弃: 0 (0.0%) 配置: Default

192.168.86.1

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.



The screenshot shows a Wireshark packet capture of a DHCP transaction. The packet list at the top shows a DHCP Offer (No. 212) from 192.168.86.1 to 192.168.86.32. The packet details pane shows the DHCP Offer message with the 'Your (client) IP address' field set to 192.168.86.32. The packet bytes pane shows the raw data of the DHCP Offer message.

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650f53ae
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xd1c073a
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xd1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x535cf48c  
Seconds elapsed: 0  
> Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
**Your (client) IP address: 192.168.86.32**  
Next server IP address: 192.168.86.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
> Option: (53) DHCP Message Type (Offer)  
Option: (54) DHCP Server Identifier (192.168.86.1)  
Length: 4  
DHCP Server Identifier: 192.168.86.1  
> Option: (51) IP Address Lease Time

192.168.86.32

Offer DHCP message contain the offered DHCP address

- 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?

The screenshot shows a Wireshark packet capture of a DHCP transaction. The packet list at the top shows a DHCP Offer (No. 212) and a DHCP Discover (No. 1458). The packet details for the DHCP Offer (No. 212) are expanded, showing the 'Relay agent IP address' as 0.0.0.0. The packet bytes pane at the bottom shows the raw data of the DHCP message, including the magic cookie and various options.

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650f53ae
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xd1c073a
1466	47.875588	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xd1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Packet Details for DHCP Offer (No. 212):

- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x535cf48c
- Seconds elapsed: 0
- Bootp flags: 0x0000 (Unicast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 192.168.86.32
- Next server IP address: 192.168.86.1
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)
- Client hardware address padding: 0000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Offer)
- Option: (54) DHCP Server Identifier (192.168.86.1)
- Option: (51) IP Address Lease Time
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (1) Subnet Mask (255.255.255.0)

Packet Bytes for DHCP Offer (No. 212):

```

0000 a8 7e ea 34 c2 09 b0 6a 41 c7 5f d8 08 00 45 c0 ~4...j
0010 01 48 91 2b 00 00 40 11 ba 47 c0 a8 56 01 c0 a8 H+...@
0020 56 20 00 43 00 44 01 34 e1 8e 02 01 06 00 53 5c V...C.D.4
0030 f4 8c 00 00 00 00 00 00 00 00 c0 a8 56 20 c0 a8 V...P...
0040 56 01 00 00 00 00 a8 7e ea 34 c2 09 00 00 00 00 V...~
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 .....
00b0 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 .....
00d0 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 .....
00f0 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 .....
0110 00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 c0 .....C...
0120 a8 56 01 33 04 00 01 51 80 3a 04 00 00 a8 c0 3b V:3...Q
0130 04 00 01 27 50 01 04 ff ff ff 00 1c 04 c0 a8 56 .....P...
0140 ff 03 04 c0 a8 56 01 0f 03 6c 61 6e 06 04 c0 a8 V...V...
0150 56 01 ff 00 00 00 .....

```

The "Relay agent IP address" indicates the absence of a relay agent. There is no relay agent in my lab, due to the value of this is "Relay agent IP address: 0.0.0.0"

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

The screenshot shows a Wireshark packet capture of a DHCP transaction. The packet list at the top shows a DHCP Offer (No. 212) and a DHCP ACK (No. 1997). The packet details for the DHCP Offer (No. 212) are expanded, showing options for Subnet Mask (255.255.255.0) and Router (192.168.86.1). The packet bytes pane shows the raw data for the DHCP Offer.

No.	Time	Source	Destination	Protocol	Length	Info
161	14.964049	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
196	18.679604	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
212	21.870268	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
213	21.870652	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
214	21.885264	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
559	23.338485	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
562	23.371969	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
1458	47.310260	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650f53ae
1465	47.862481	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xd1c073a
1466	47.875508	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xd1c073a
1770	60.419617	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
1858	65.454939	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
1959	75.627529	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
1995	78.884936	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
1996	78.885380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
1997	78.901193	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Client MAC address: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
 Client hardware address padding: 0000000000000000  
 Server host name not given  
 Boot file name not given  
 Magic cookie: DHCP  
 > Option: (53) DHCP Message Type (Offer)  
 > Option: (54) DHCP Server Identifier (192.168.86.1)  
 > Option: (51) IP Address Lease Time  
 > Option: (58) Renewal Time Value  
 > Option: (59) Rebinding Time Value  
 > Option: (1) Subnet Mask (255.255.255.0)  
 Length: 4  
 Subnet Mask: 255.255.255.0  
 > Option: (28) Broadcast Address (192.168.86.255)  
 > Option: (3) Router  
 Length: 4  
 Router: 192.168.86.1  
 > Option: (15) Domain Name  
 > Option: (6) Domain Name Server  
 > Option: (255) End  
 Padding: 000000

The subnet mask tells the client which part is the internet part, which part is the host part. The router line tells the clients what is the ip address of the default router.

11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first serve OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

The screenshot shows a Wireshark capture of DHCP traffic. The packet list on the left shows a sequence of DHCP messages: Discover, Offer, Request, ACK, Request, ACK, Release, Discover, Offer, Request, and ACK. The packet details pane for the selected DHCP Request (No. 5) shows the following options: (53) DHCP Message Type (Request), (61) Client identifier, (50) Requested IP Address (192.168.1.101), (54) DHCP Server Identifier (192.168.1.1), (12) Host Name, (60) Vendor class identifier, (55) Parameter Request List, and (255) End. The packet bytes pane on the right shows the raw data of the DHCP message.

No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	20.134178	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	20.135930	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	25.073867	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

Next server IP address: 0.0.0.0  
 Relay agent IP address: 0.0.0.0  
 Client MAC address: Dell\_4f:36:23 (00:08:74:4f:36:23)  
 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 (192.168.1.101)  
 > Option: (54) DHCP Server Identifier (192.168.1.1)  
 > Option: (12) Host Name  
 > Option: (60) Vendor class identifier  
 > Option: (55) Parameter Request List  
 > Option: (255) End  
 Padding: 000000000000

The client accepts this ip address, due to it sending a request message for this ip address.

## 12. Explain the purpose of the lease time. How long is the lease time in your experiment?

The screenshot shows a Wireshark capture of DHCP traffic. The packet list on the left shows a sequence of DHCP messages: Discover, Offer, Request, ACK, Request, ACK, Release, Discover, Offer, Request, and ACK. The packet details pane for the selected DHCP Offer (No. 8) shows the following options: (53) DHCP Message Type (ACK), (54) DHCP Server Identifier (192.168.86.1), (51) IP Address Lease Time (Length: 4, IP Address Lease Time: (86400s) 1 day), (58) Renewal Time Value, (59) Rebinding Time Value, (1) Subnet Mask (255.255.255.0), (28) Broadcast Address (192.168.86.255), (3) Router, (15) Domain Name, and (81) Client Fully Qualified Domain Name. The packet bytes pane on the right shows the raw data of the DHCP message.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
2	3.715555	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x535cf48c
3	6.906219	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0x535cf48c
4	6.906603	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x535cf48c
5	6.921215	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x535cf48c
6	8.374436	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0x87f382bc
7	8.407920	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0x87f382bc
8	32.346211	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x650f53ae
9	32.898432	192.168.86.32	192.168.86.1	DHCP	352	DHCP Request - Transaction ID 0xd1c073a
10	32.911539	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xd1c073a
11	45.455568	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbfeb8b17
12	50.490890	192.168.86.32	192.168.86.1	DHCP	342	DHCP Release - Transaction ID 0xd622bc39
13	60.663480	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa48449e1
14	63.920887	192.168.86.1	192.168.86.32	DHCP	342	DHCP Offer - Transaction ID 0xa48449e1
15	63.921331	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa48449e1
16	63.937144	192.168.86.1	192.168.86.32	DHCP	360	DHCP ACK - Transaction ID 0xa48449e1

Client IP address: 0.0.0.0  
 Your (client) IP address: 192.168.86.32  
 Next server IP address: 192.168.86.1  
 Relay agent IP address: 0.0.0.0  
 Client MAC address: IntelCor\_34:c2:09 (a8:7e:ea:34:c2:09)  
 Client hardware address padding: 00000000000000000000  
 Server host name not given  
 Boot file name not given  
 Magic cookie: DHCP  
 > Option: (53) DHCP Message Type (ACK)  
 > Option: (54) DHCP Server Identifier (192.168.86.1)  
 > Option: (51) IP Address Lease Time  
 Length: 4  
 IP Address Lease Time: (86400s) 1 day  
 > Option: (58) Renewal Time Value  
 > Option: (59) Rebinding Time Value  
 > Option: (1) Subnet Mask (255.255.255.0)  
 > Option: (28) Broadcast Address (192.168.86.255)  
 > Option: (3) Router  
 > Option: (15) Domain Name  
 > Option: (81) Client Fully Qualified Domain Name

The purpose of the lease time is to provide the expiration date for the offered ip address.

The number of the ip address is limited. Thus, the ip address will be returned when you do not need to use your ip address.

The lease time of my ip address is 1 day.

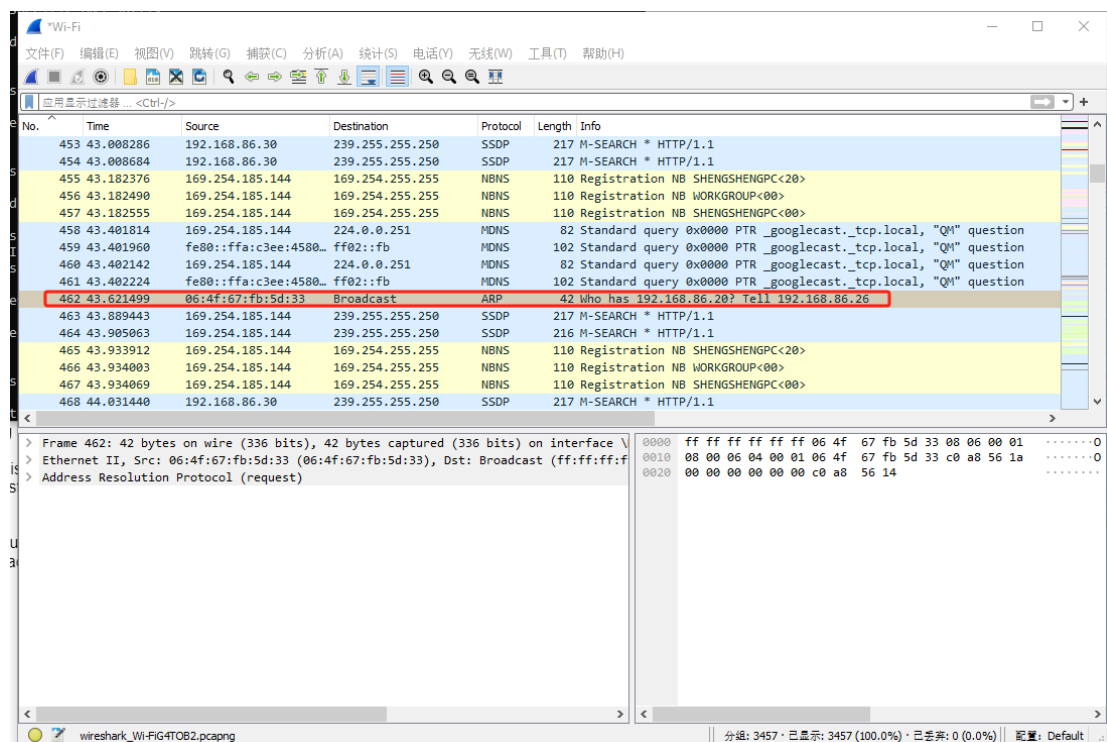
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

The purpose of the DHCP release message is telling the DHCP server that the client is releasing its current ip address. Then the DHCP server can distribute this ip address later.

There is no ACK for DHCP release request, but there is ACK for DHCP ip request. I am not sure what you are asking here.

If a DHCP release message is lost, the DHCP server will not distribute this ip address to others, it will think someone still uses this ip address until it reaches its lease time.

14. 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.



Yes, there is one ARP packet in my Lab

The purpose of those ARP packets is to ask the MAC address of the specified ip address.