

Terminal :

```
C:\ Command Prompt
Link-local IPv6 Address . . . . . : fe80::a05f:8ec9:7a03:27d5%4
Default Gateway . . . . . :

C:\Users\ratho>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a05f:8ec9:7a03:27d5%4
    IPv4 Address. . . . . : 192.168.1.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\ratho>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 10 while it has its media disconnected.

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a05f:8ec9:7a03:27d5%4
    IPv4 Address. . . . . : 192.168.1.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\ratho>ipconfig/release
```

1. Are DHCP messages sent over UDP or TCP?

Answer : DHCP messages are sent over UDP.

The screenshot shows a Wireshark capture of a DHCP exchange on a Wi-Fi interface. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601ddea2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601ddea2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601ddea2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601ddea2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

The details pane for packet 63 shows the following structure:

- Frame 63: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{33AB546E-B38C-4C5F-9431-33834A3996BC}, id 0
- Ethernet II, Src: Microsoft_f1:73:19 (98:5f:d3:f1:73:19), 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
 - Source Port: 68
 - Destination Port: 67
 - Length: 336
 - Checksum: 0x8955 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 15]
- Dynamic Host Configuration Protocol (Request)

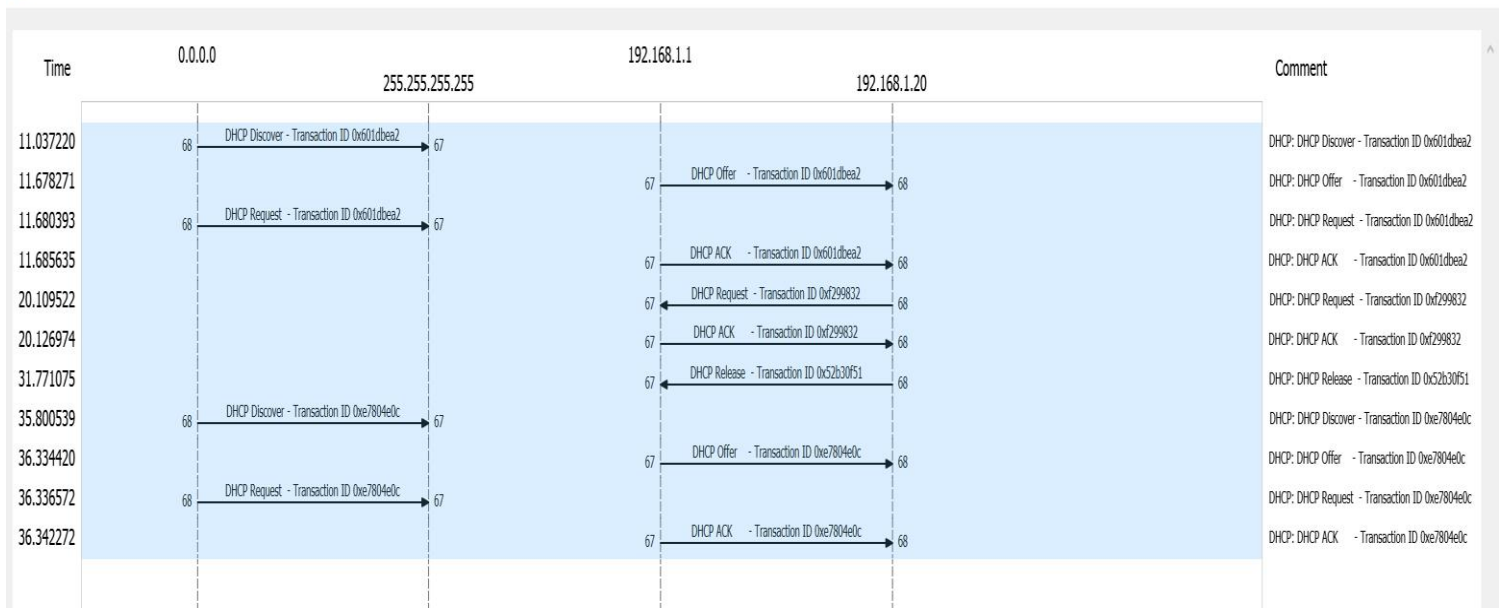
The packet bytes pane shows the raw data in hexadecimal and ASCII format.

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?

Answer:

Yes, the ports are the same as in the example given in this assignment.

1. Src – 68 , Dst – 67
2. Dst – 67 , Src – 68
3. Src – 68 , Dst – 68
4. Dst – 67 , Src – 68.



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

Answer :

The Link-Layer Address is : (Source: Microsof_f1:73:19) **98:5f:d3:f1:73:19**

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbee2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbee2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbee2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbee2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

> Frame 63: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{33AB546E-B38C-4C5F-9431-33834A3996BC}, id 0

▼ Ethernet II, Src: Microsof_f1:73:19 (98:5f:d3:f1:73:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Microsof_f1:73:19 (98:5f:d3:f1:73:19)

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

> Dynamic Host Configuration Protocol (Request)

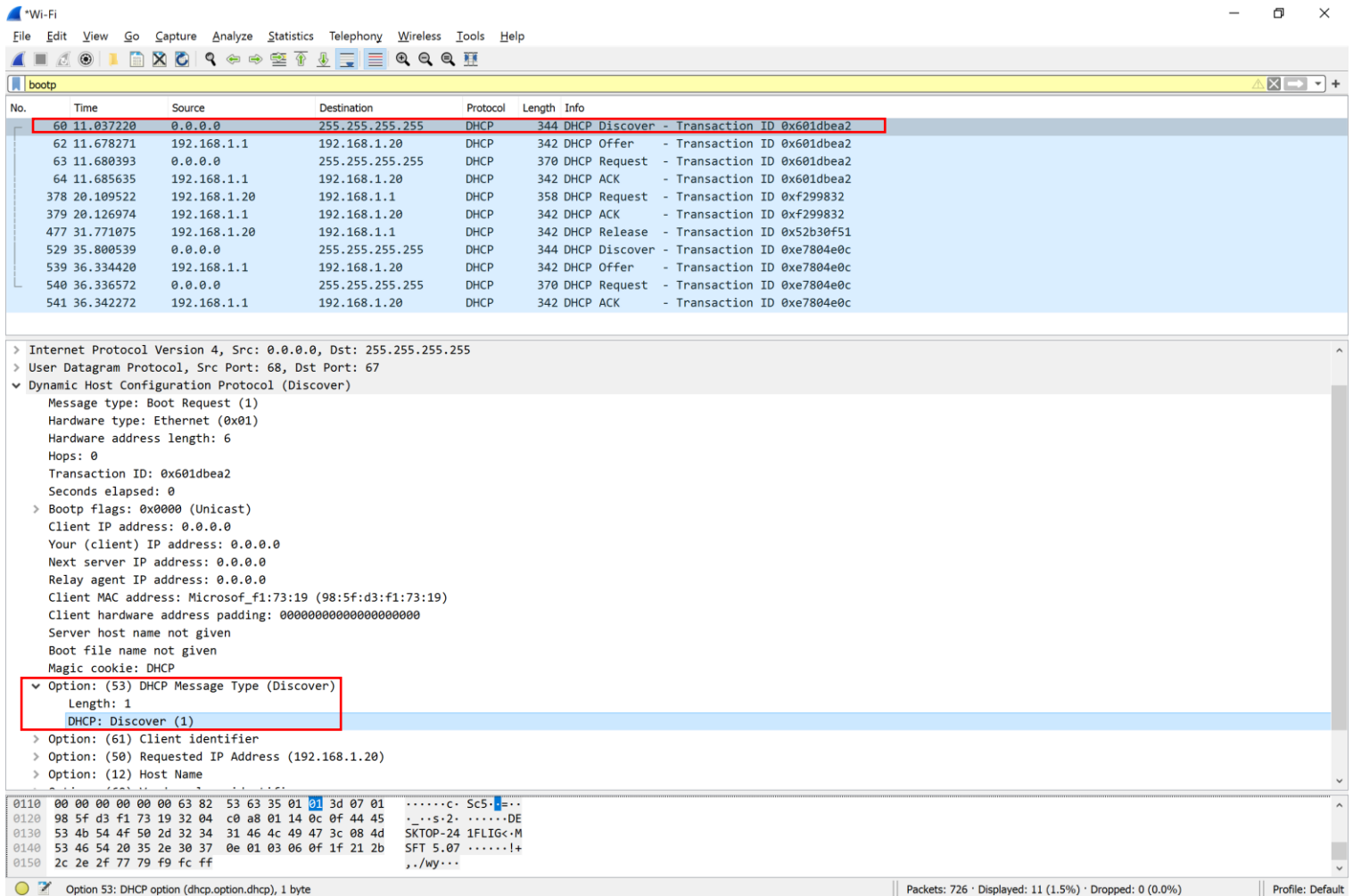
4. What values in the DHCP discover message differentiate this message from the DHCP request message?

Answer :

Message type values helps differentiate between the types of messages.

DHCP request – message type value is 3

DHCP discover – message type value is 1.



Wireshark packet capture showing a DHCP Discover message. The packet list shows a DHCP Discover message from 0.0.0.0 to 255.255.255.255. The packet details show the DHCP Discover message type (1) and the DHCP Discover option (1). The packet bytes show the DHCP Discover message structure.

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbee2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbee2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbee2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbee2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

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: 0x601dbee2
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: Microsof_f1:73:19 (98:5f:d3:f1:73:19)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
> Option: (61) Client identifier
> Option: (50) Requested IP Address (192.168.1.20)
> Option: (12) Host Name

0110 00 00 00 00 00 63 82 53 63 35 01 01 3d 07 01c- Sc5-
0120 98 5f d3 f1 73 19 32 04 c0 a8 01 14 0c 0f 44 45 ...s.2.DE
0130 53 4b 54 4f 50 2d 32 34 31 46 4c 49 47 3c 08 4d SKTOP-24 1FLIG-M
0140 53 46 54 20 35 2e 30 37 0e 01 03 06 0f 1f 21 2b SFT 5.07!+
0150 2c 2e 2f 77 79 f9 fc ff ,./wy...

Option 53: DHCP option (dhcp.option.dhcp), 1 byte

Packets: 726 · Displayed: 11 (1.5%) · Dropped: 0 (0.0%) Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbea2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbea2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbea2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbea2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

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 (Request)

Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x601dbea2
 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: Microsof_f1:73:19 (98:5f:d3:f1:73:19)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)
 Length: 1
 DHCP: Request (3)

Option: (61) Client identifier
 Length: 7
 Hardware type: Ethernet (0x01)

Option 53: DHCP option (dhcp.option.dhcp), 1 byte

Packets: 726 · Displayed: 11 (1.5%) · Dropped: 0 (0.0%)

Profile: Default

5. 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?

Answer :

Transaction-ID – First Four set :

1. Discover = 0x601dbea2
2. Offer = 0x601dbea2
3. Request = 0x601dbea2
4. ACK = 0x601dbea2

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbea2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbea2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbea2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbea2

Transaction-ID - second set :

1. Request = 0xf299832
2. ACK = 0xf299832

378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832

The purpose of the Transaction-ID field is so that host can differentiate between different request made by user. (Differentiate between the group of message)

6. 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.

Answer :

Discover :

Source : 0.0.0.0

Destination : 255.255.255.255.

Offer :

Source : 192.168.1.1

Destination : 192.168.1.20.

Request :

Source : 0.0.0.0

Destination : 255.255.255.255.

Ack :

Source : 192.168.1.1

Destination : 192.168.1.20

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbea2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbea2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbea2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbea2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

> Frame 63: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{33AB546E-B38C-4C5F-9431-33834A3996BC}, id 0

> Ethernet II, Src: Microsof_f1:73:19 (98:5f:d3:f1:73:19), 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 (Request)

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

Answer :

The value of IP address of DHCP Server is : 192.168.1.1.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbee2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbee2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbee2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbee2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

> Frame 62: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{33AB546E-B38C-4C5F-9431-33834A3996BC}, id 0

> Ethernet II, Src: Netgear ab:c2:0e (cc:40:d0:ab:c2:0e), Dst: Microsof f1:73:19 (98:5f:d3:f1:73:19)

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.20

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 328
 - Identification: 0x0000 (0)
- > Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: UDP (17)
 - Header checksum: 0xf63f [validation disabled]
 - [Header checksum status: Unverified]
- Source: 192.168.1.1
- Destination: 192.168.1.20

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

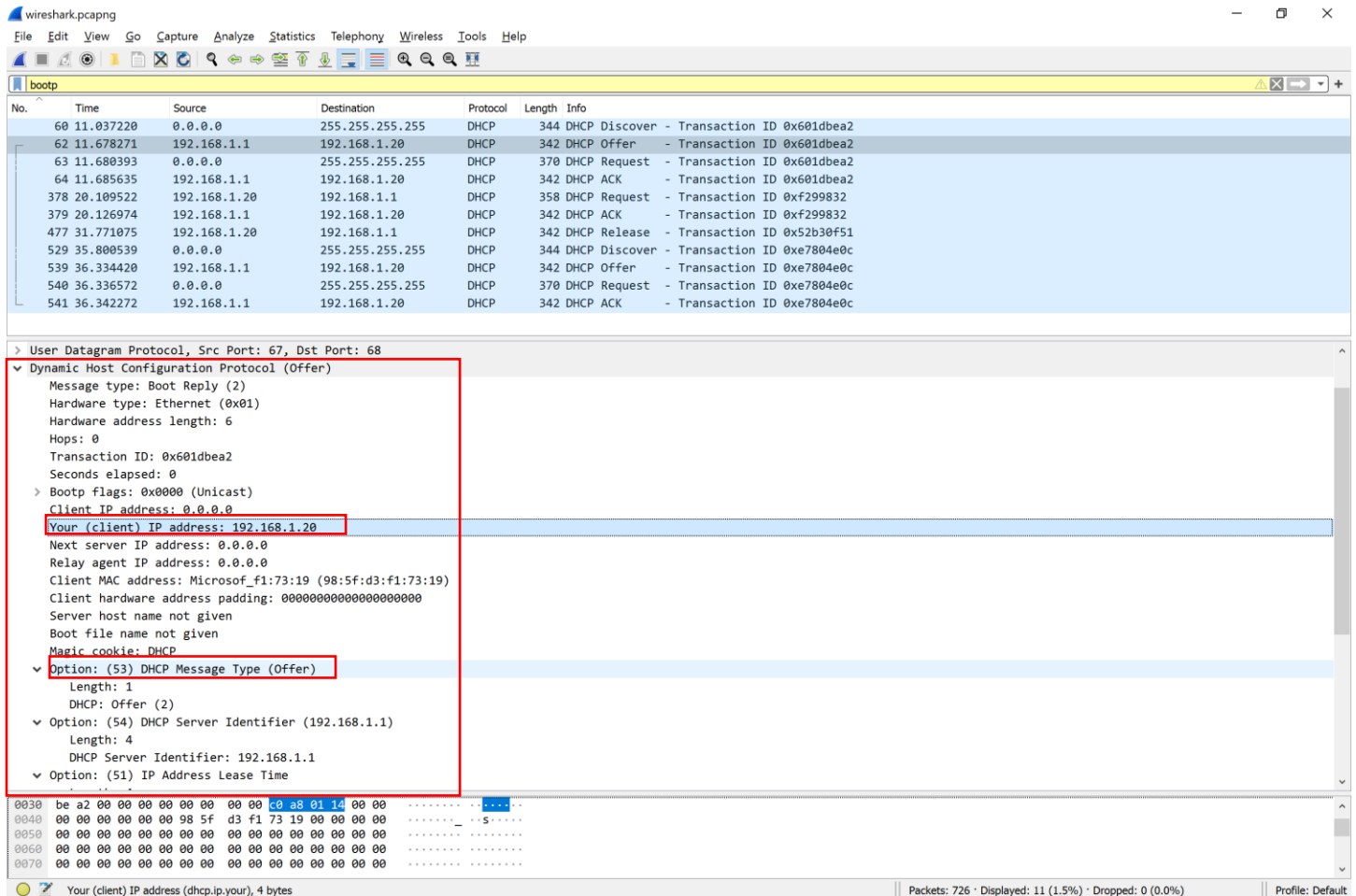
> Dynamic Host Configuration Protocol (Offer)

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.

Answer :

DHCP server offered host the IP address: 192.168.1.20.

DHCP Offer message type contained the DHCP address.



Wireshark packet capture showing DHCP messages. The packet list shows a DHCP Offer message at 62 seconds. The packet details pane shows the DHCP Offer message structure, with the 'Your (client) IP address' field highlighted in red, showing 192.168.1.20. The packet bytes pane shows the raw data of the DHCP Offer message.

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbee2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbee2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbee2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbee2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c
541	36.342272	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xe7804e0c

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: 0x601dbee2
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.20
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Microsoft_f1:73:19 (98:5f:d3:f1:73:19)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)
Length: 1
DHCP: Offer (2)

Option: (54) DHCP Server Identifier (192.168.1.1)
Length: 4
DHCP Server Identifier: 192.168.1.1

Option: (51) IP Address Lease Time

0030 be a2 00 00 00 00 00 00 c0 a8 01 14 00 00S.....
0040 00 00 00 00 00 00 98 5f d3 f1 73 19 00 00 00-S.....
0050 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
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Your (client) IP address (dhcp.ip.your), 4 bytes

Packets: 726 · Displayed: 11 (1.5%) · Dropped: 0 (0.0%) Profile: Default

9. 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 : The Ip address in the trace is 0.0.0.0 indicating no DHCP relay.
so there is no relay.

Wireshark packet capture showing DHCP transactions. The filter is set to 'bootp'. The packet list shows a DHCP Discover (Frame 60) from 0.0.0.0 to 255.255.255.255. The packet details pane shows the DHCP Discover message with fields like Message type, Hardware type, Transaction ID, and various options. The 'Relay agent IP address' field is highlighted with a red box and shows 0.0.0.0.

Frame 60: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{33AB546E-B38C-4C5F-9431-33834A3996B8}, id 0

Ethernet II, Src: Microsof_f1:73:19 (98:5f:d3:f1:73:19), 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: 0x601dbee2

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: Microsof_f1:73:19 (98:5f:d3:f1:73:19)

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

Option: (50) Requested IP Address (192.168.1.20)

Option: (12) Host Name

Option: (60) Vendor class identifier

Option: (55) Parameter Request List

Option: (255) End

Relay agent IP address (dhcp.ip.relay), 4 bytes

Packets: 726 · Displayed: 11 (1.5%)

Profile: Default

17:17 12-08-2020

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 server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Answer :

Yes, The Client Accept the offer message.

It is seen in option number 50.

The screenshot shows a Wireshark packet capture of a DHCP transaction. The packet list at the top shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
60	11.037220	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x601dbee2
62	11.678271	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0x601dbee2
63	11.680393	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x601dbee2
64	11.685635	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0x601dbee2
378	20.109522	192.168.1.20	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0xf299832
379	20.126974	192.168.1.1	192.168.1.20	DHCP	342	DHCP ACK - Transaction ID 0xf299832
477	31.771075	192.168.1.20	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x52b30f51
529	35.800539	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe7804e0c
539	36.334420	192.168.1.1	192.168.1.20	DHCP	342	DHCP Offer - Transaction ID 0xe7804e0c
540	36.336572	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe7804e0c

The packet details for the DHCP Request (63) are shown below:

- 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: 0x601dbee2
 - 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: Microsof_f1:73:19 (98:5f:d3:f1:73:19)
 - 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 (192.168.1.20)
 - Length: 4
 - Requested IP Address: 192.168.1.20
 - Option: (54) DHCP Server Identifier (192.168.1.1)
 - Option: (12) Host Name
 - Option: (81) Client Fully Qualified Domain Name
 - Option: (60) Vendor class identifier
 - Option: (55) Parameter Request List
 - Option: (255) End

The status bar at the bottom shows: Option 50: Requested IP Address (dhcp.option.requested_ip_address), 4 bytes. Packets: 726 · Displayed: 11 (1.5%). Profile: Default.

Answer : Lease time is the duration of time in which the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the given IP address given any other client. Once the lease time expires the IP address can be reused by the DHCP server.

IP Address Lease Time: (86400s) 1 day

[illegible]

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?

Answer : DHCP release message is to cancel the lease so that IP address can be reused by the DHCP server.

DHCP server does not acknowledge the receipt of the clients DHCP request.

If the client's DHCP release message is lost, the DHCP server will have to wait until the lease period is over.

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.

Answer : **Yes**, There are ARP packets in the DHCP packet exchange period.

ARP is used to gather all the IP address and make sure the IP address is not used by others.

wireshark.pcapng

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Wireless

Tools

Help

</