

Lab 05_DHCP

DHCP DISCOVER

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

This DHCP Discover message is sent via UDP

The screenshot shows a Wireshark capture of a DHCP Discover message. The packet list at the top shows four packets: a DHCP Discover message (No. 1, 21:07:02.299, Source: 0.0.0.0, Destination: 255.255.255.255, Protocol: DHCP, Length: 344), a DHCP Offer message (No. 2, 21:07:02.303, Source: 192.168.1.3, Destination: 172.31.98.151, Protocol: DHCP, Length: 342), a DHCP Request message (No. 3, 21:07:02.304, Source: 0.0.0.0, Destination: 255.255.255.255, Protocol: DHCP, Length: 370), and a DHCP ACK message (No. 4, 21:07:02.320, Source: 192.168.1.3, Destination: 172.31.98.151, Protocol: DHCP, Length: 362). The packet details pane shows the selected packet (No. 1) with the following structure:

- Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A73}...
- Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), 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: 330
 - Identification: 0xebad (60333)
 - > 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 128
 - Protocol: UDP (17)
 - Header Checksum: 0x0000 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 0.0.0.0
 - Destination Address: 255.255.255.255
- User Datagram Protocol, Src Port: 68, Dst Port: 67
 - Source Port: 68
 - Destination Port: 67
 - Length: 310
 - Checksum: 0xb9b5 [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 0]
 - > [Timestamps]
 - UDP payload (302 bytes)
 - Dynamic Host Configuration Protocol (Discover)

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

source IP address: 0.0.0.0

This address is known as the "unspecified address" and is special because This isn't really a valid IP address.

This is because the host does not yet have an IP address assigned to it, and is broadcasting its request for an IP address to all DHCP servers on the network.

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

destination IP address: 255.255.255.255

This is the broadcasting IP address, which means the message is sent to all devices on the network. The host uses this broadcast address to ensure that all DHCP servers on the network can receive the discover message and respond with an offer.

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

transaction ID: 0xb13d321f

dgcp_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

[Stream index: 0]
> [Timestamps]
UDP payload (302 bytes)

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xb13d321f
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_e8:f2:10 (94:e2:3c:e8:f2:10)
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 (172.31.98.151)
> Option: (12) Host Name
> Option: (60) Vendor class identifier
> Option: (55) Parameter Request List
> Option: (255) End

0000 ff ff ff ff ff ff 9
0010 01 4a eb ad 00 00 8
0020 ff ff 00 44 00 43 0
0030 32 1f 00 00 00 00 0
0040 00 00 00 00 00 00 9
0050 00 00 00 00 00 00 0
0060 00 00 00 00 00 00 0
0070 00 00 00 00 00 00 0
0080 00 00 00 00 00 00 0
0090 00 00 00 00 00 00 0
00a0 00 00 00 00 00 00 0
00b0 00 00 00 00 00 00 0
00c0 00 00 00 00 00 00 0
00d0 00 00 00 00 00 00 0
00e0 00 00 00 00 00 00 0
00f0 00 00 00 00 00 00 0
0100 00 00 00 00 00 00 0
0110 00 00 00 00 00 00 6
0120 94 e2 3c e8 f2 10 3
0130 53 4b 54 4f 50 2d 5
0140 53 46 54 20 35 2e 3
0150 2c 2e 2f 77 79 f9 f

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?

five pieces of information (beyond an IP address):

- DHCP Message Type (Discover)
- Client identifier
- Host Name
- Vendor class identifier
- Parameter Request List

dgcp_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

[Stream index: 0]
 > [Timestamps]
 UDP payload (302 bytes)
 Dynamic Host Configuration Protocol (Discover)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xb13d321f
 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_e8:f2:10 (94:e2:3c:e8:f2:10)
 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 (172.31.98.151)
 > Option: (12) Host Name
 > Option: (60) Vendor class identifier
 > Option: (55) Parameter Request List
 > Option: (255) End

0000 ff ff ff ff ff ff 94
 0010 01 4a eb ad 00 00 80
 0020 ff ff 00 44 00 43 01
 0030 32 1f 00 00 00 00 00
 0040 00 00 00 00 00 00 94
 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 94 e2 3c e8 f2 10 32
 0130 53 4b 54 4f 50 2d 54
 0140 53 46 54 20 35 2e 30
 0150 2c 2e 2f 77 79 f9 fc

DHCP OFFER

- 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?

Because it has the same transaction ID with the DHCP Discover message.

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

Offset	Length	Value
0000	94	e2 3c e8 f2 10 6c f
0010	01	48 00 00 00 00 40 f
0020	62	97 00 43 00 44 01 :
0030	32	1f 00 00 00 00 00 e
0040	62	01 c0 a8 01 03 94 e
0050	00	00 00 00 00 00 00 e
0060	00	00 00 00 00 00 00 e
0070	00	00 00 00 00 00 00 e
0080	00	00 00 00 00 00 00 e
0090	00	00 00 00 00 00 00 e
00a0	00	00 00 00 00 00 00 e
00b0	00	00 00 00 00 00 00 e
00c0	00	00 00 00 00 00 00 e
00d0	00	00 00 00 00 00 00 e
00e0	00	00 00 00 00 00 00 e
00f0	00	00 00 00 00 00 00 e
0100	00	00 00 00 00 00 00 e
0110	00	00 00 00 00 00 63 e
0120	1f	62 01 33 04 00 00 e
0130	04	00 00 93 a8 1c 04 e
0140	08	08 08 08 08 08 08 e
0150	04	ff ff fe 00 ff

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

source IP address: 192.168.1.3

This is the IP address of the DHCP, where the server is running.

The specific IP address will vary depending on the DHCP server's configuration and the network setup.

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.]

destination IP address: 172.31.98.151

This is the previous IP address of the client. The destination IP address used in the IP datagram containing the DHCP Offer message is the IP address of the client that sent the DHCP Discover message.

The DHCP server sends the Offer message as a unicast packet directly to the requesting client's IP address. This ensures that only the intended client receives the offer and prevents other clients on the network from processing the message.

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?

five pieces of information:

- DHCP Server identifier (172.31.98.1)
- IP Address Lease Time
- Broadcast Address (172.31.99.255)
- Router
- Subnet Mask (255.255.254.0)

dhcp_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 2
Transaction ID: 0xb13d321f
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 172.31.98.151
Next server IP address: 172.31.98.1
Relay agent IP address: 192.168.1.3
Client MAC address: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10)
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 (172.31.98.1)
> Option: (51) IP Address Lease Time
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
> Option: (28) Broadcast Address (172.31.99.255)
> Option: (254) Private
> Option: (6) Domain Name Server
> Option: (3) Router
> Option: (1) Subnet Mask (255.255.254.0)
> Option: (255) End

0000 94 e2 3c e8 f2 10 6c f
0010 01 48 00 00 00 00 40 1
0020 62 97 00 43 00 44 01 3
0030 32 1f 00 00 00 00 00 0
0040 62 01 c0 a8 01 03 94 e
0050 00 00 00 00 00 00 00 0
0060 00 00 00 00 00 00 00 0
0070 00 00 00 00 00 00 00 0
0080 00 00 00 00 00 00 00 0
0090 00 00 00 00 00 00 00 0
00a0 00 00 00 00 00 00 00 0
00b0 00 00 00 00 00 00 00 0
00c0 00 00 00 00 00 00 00 0
00d0 00 00 00 00 00 00 00 0
00e0 00 00 00 00 00 00 00 0
00f0 00 00 00 00 00 00 00 0
0100 00 00 00 00 00 00 00 0
0110 00 00 00 00 00 00 63 8
0120 1f 62 01 33 04 00 00 a
0130 04 00 00 93 a8 1c 04 a
0140 08 08 08 08 08 08 08 0
0150 04 ff ff fe 00 ff

DHCP REQUEST

dhcp_1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

> Frame 3: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{185BC2D4-588F-4111-8BE5-6B56836A}

> Ethernet II, Src: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10), 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: 0xfa0e [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

> [Timestamps]

UDP payload (328 bytes)

▼ Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xb13d321f

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_e8:f2:10 (94:e2:3c:e8:f2:10)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Dynamic Host Configuration Protocol (dhcp), 328 bytes

Packets: 529 · Displayed: 4

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?

UDP source port: 68
UDP destination port: 67

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

source IP address: 0.0.0.0
This address is known as the "unspecified address" and is special because This isn't really a valid IP address.
This is because the host does not yet have an IP address assigned to it, and is broadcasting its request for an IP address to all DHCP servers on the network.

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

destination IP address: 255.255.255.255
This is the broadcasting IP address, which means the message is sent to all devices on the network. The host uses this broadcast address to ensure that all DHCP servers on the network can receive the discover message and respond with an offer.

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?

transaction ID: 0xb13d321f

Yes.

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?

The differences between the entries in the ‘parameter request list’ option in this Request message and list option in the earlier Discover message are added 2 options:

- DHCP Server Identifier (172.31.98.151)
- Client Fully Qualified Domain Name

The image shows a Wireshark packet capture of a DHCP Request message. The packet list pane at the top shows four packets: a DHCP Discover (344 bytes), a DHCP Offer (342 bytes), a DHCP Request (370 bytes), and a DHCP ACK (362 bytes). The DHCP Request packet is selected, and its details pane is expanded. The 'Dynamic Host Configuration Protocol (Request)' section is expanded, showing the following fields: Message type: Boot Request (1), Hardware type: Ethernet (0x01), Hardware address length: 6, Hops: 0, Transaction ID: 0xb13d321f, 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_e8:f2:10 (94:e2:3c:e8:f2:10), Client hardware address padding: 00000000000000000000, Server host name not given, Boot file name not given, Magic cookie: DHCP. The 'Option' section is expanded, showing the following options: Option: (53) DHCP Message Type (Request), Option: (61) Client identifier, Option: (50) Requested IP Address (172.31.98.151), Option: (54) DHCP Server Identifier (172.31.98.1), Option: (12) Host Name, Option: (81) Client Fully Qualified Domain Name, Option: (60) Vendor class identifier, Option: (55) Parameter Request List, and Option: (255) End. The packet bytes pane on the right shows the raw data of the packet, with the DHCP Request packet starting at offset 0x0000 and ending at 0x0170.

DHCP ACK

The image shows a Wireshark capture of a DHCP ACK message. The packet list at the top shows four packets: a DHCP Discover, a DHCP Offer, a DHCP Request, and a DHCP ACK. The DHCP ACK is the fourth packet, sent from 192.168.1.3 to 172.31.98.151. The packet details pane shows the structure of the DHCP ACK message, including the Transaction ID, Client IP address, and various options. The options include IP Address Lease Time (12 hours) and Router (172.31.98.1). The packet bytes pane shows the raw data of the DHCP ACK message.

No.	Time	Source	Destination	Protocol	Length	Info
1	21:07:02.299	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb13d321f
2	21:07:02.303	192.168.1.3	172.31.98.151	DHCP	342	DHCP Offer - Transaction ID 0xb13d321f
3	21:07:02.304	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb13d321f
4	21:07:02.320	192.168.1.3	172.31.98.151	DHCP	362	DHCP ACK - Transaction ID 0xb13d321f

Dynamic Host Configuration Protocol (ACK)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 2
Transaction ID: 0xb13d321f
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 172.31.98.151
Next server IP address: 172.31.98.1
Relay agent IP address: 192.168.1.3
Client MAC address: IntelCor_e8:f2:10 (94:e2:3c:e8:f2:10)
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 (172.31.98.1)
Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (43200s) 12 hours
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (28) Broadcast Address (172.31.99.255)
Option: (81) Client Fully Qualified Domain Name
Option: (254) Private
Option: (6) Domain Name Server
Option: (3) Router
Length: 4
Router: 172.31.98.1

Packets: 529 · Displayed: 4 (0.8%)

15. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

source IP address: 192.168.1.3

This is the IP address of the DHCP, where the server is running.

The specific IP address will vary depending on the DHCP server's configuration and the network setup.

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

destination IP address: 172.31.98.151

This is the previous IP address of the client. The destination IP address used in the IP datagram containing the DHCP Offer message is the IP address of the client that sent the DHCP Discover message.

The DHCP server sends the Offer message as a unicast packet directly to the requesting client's IP address. This ensures that only the intended client receives the offer and prevents other clients on the network from processing the message.

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?

The field in the DHCP ACK message that contains the assigned client IP address is called "Your (client) IP address".

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

IP Address Lease Time: (43200s) 12 hours

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?

IP Address Router: 172.31.98.1