

# DHCP

Yogesh P  
201EE138

dhcp-wireshark-trace1-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
5	3.696138	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
9	5.285935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
12	6.962432	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
13	6.962436	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
16	7.965588	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x56f415ed
17	7.977178	192.168.86.1	192.168.86.65	DHCP	342	DHCP ACK - Transaction ID 0x56f415ed

Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0

Ethernet II, Src: Apple\_98:d9:27 (78:4f:43:98:d9:27), 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: 0x56f415ed

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: Apple\_98:d9:27 (78:4f:43:98:d9:27)

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: (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

Padding: 00000000000000000000

0000	ff ff ff ff ff ff 78 4f	43 98 d9 27 00 00 45 00	.....xO C.....E
0010	01 48 bb 0c 00 00 ff 11	ff 08 00 00 00 00 ff ff	..H.....
0020	ff ff 00 44 00 43 01 34	95 bf 01 01 06 00 56 f4	....D.C.4.....V
0030	15 ed 00 00 00 00 00 00	00 00 00 00 00 00 00 00	....D.C.4.....V
0040	00 00 00 00 00 78 4f	43 98 d9 27 00 00 00 00	.....xO C.....E
0050	00 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 00	.....
0070	00 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 00	.....
0090	00 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 00	.....
00b0	00 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 00	.....
00d0	00 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 00	.....
00f0	00 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 00	.....
0110	00 00 00 00 00 63 82	53 63 35 01 01 37 0a 01	.....c Sc5-7...
0120	79 03 06 0f 77 fc 5f 2c	2e 39 02 05 dc 3d 07 01	y...w...,.9...=...
0130	78 4f 43 98 d9 27 33 04	00 76 a7 00 0c 0d 4d 61	xOC-'3- v...-Ma
0140	63 42 6f 6f 6b 2d 50 72	6f 2d 36 ff 00 00 00 00	cBook-Pr o-6.....
0150	00 00 00 00 00 00 00 00		.....

Dynamic Host Configuration Protocol: Protocol

Packets: 1018 · Displayed: 6 (0.6%)

Profile: Default

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

A: This DHCP Discover message is sent out using UDP as the underlying transport protocol.

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

A: The source IP address is 0.0.0.0. The speciality is the IP address 0.0.0.0 allows the computer and servers to temporarily communicate on the network before they receive a valid IP address from a DHCP server.

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

A: The destination IP address used is 255.255.255.255. It represents the broadcast address, or place to route messages to be sent to every device within a network.

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

A: The value in the transaction ID field is 0x2b036af7.

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?

A: Parameter request list, Client identifier, Host name, Maximum DHCP message size, DHCP message type are the five pieces of information that the client is requesting

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?

A:In the message type field, it is mentioned as a Boot reply. Whereas in the Discover message, the type was boot request.

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

A:The source IP address used is 172.20.10.1. IP address is in a reserved range. Address ranges below are reserved by IANA for private intranets, and not routable to the Internet.

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.]

A:The destination IP address used is 172.20.10.2. It is a private IP address, and is only used in internal network environments. And it is just one number more than the source IP address.

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?

A:DHCPMessage type, DHCP Server Identifier, Subnet Mask, Router, Domain Name Server are five pieces of information that the DHCP server is providing to the DHCP client.

dhc

No.	Time	Source	Destination	Protocol	Length	Info
5	3.696138	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
9	5.285935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
12	6.962432	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
13	6.962436	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
16	7.965588	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x56f415ed
17	7.977178	192.168.86.1	192.168.86.65	DHCP	342	DHCP ACK - Transaction ID 0x56f415ed

▶ Frame 17: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0

▶ Ethernet II, Src: Google\_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple\_98:d9:27 (78:4f:43:98:d9:27)

▶ Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.65

▶ 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: 0x56f415ed  
Seconds elapsed: 4

▶ Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 192.168.86.65  
Next server IP address: 192.168.86.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: Apple\_98:d9:27 (78:4f:43:98:d9:27)  
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  
▶ 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: (6) Domain Name Server  
▶ Option: (255) End

000078 4f 43 98 d9 27 3c 28 6d 89 0e c8 08 00 45 c0 xOC...<( m...E-  
001001 48 e3 6a 00 00 40 11 67 e7 c0 a8 56 01 c0 a8 -H j...@. g...V-  
002056 41 00 43 00 44 01 34 78 fe 02 01 06 00 56 f4 VA C D 4 x...-V-  
003015 ed 00 04 00 00 00 00 00 00 c0 a8 56 41 c0 a8 VA...-VA-  
004056 01 00 00 00 00 78 4f 43 98 d9 27 00 00 00 00 V...x0 C...'...  
005000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
006000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
007000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
008000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
009000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00b000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00c000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
010000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
011000 00 00 00 00 00 63 82 53 63 35 01 05 36 04 c0 .....c. Sc5..6-  
0120a8 56 01 33 04 00 01 51 80 3a 04 00 00 a8 c0 3b -V.3...Q .:....;  
013004 00 01 27 50 01 04 ff ff ff 00 1c 04 c0 a8 56 ...'P...-...V  
0140ff 03 04 c0 a8 56 01 0f 03 6c 61 6e 06 04 c0 a8 ...-V...-lan...  
015056 01 ff 00 00 00 V.....

Dynamic Host Configuration Protocol: Protocol

Packets: 1018 · Displayed: 6 (0.6%)

Profile: Default

dhcp-wireshark-trace1-1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
5	3.696138	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
9	5.285935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x56f415ed
12	6.962432	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
13	6.962436	192.168.86.1	192.168.86.65	DHCP	342	DHCP Offer - Transaction ID 0x56f415ed
16	7.965588	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x56f415ed
17	7.977178	192.168.86.1	192.168.86.65	DHCP	342	DHCP ACK - Transaction ID 0x56f415ed

Frame 16: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
Ethernet II, Src: Apple\_98:d9:27 (78:4f:43:98:d9:27), 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)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x56f415ed

Seconds elapsed: 4

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: Apple\_98:d9:27 (78:4f:43:98:d9:27)

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: (55) Parameter Request List

Option: (57) Maximum DHCP Message Size

Option: (61) Client identifier

Option: (50) Requested IP Address (192.168.86.65)

Option: (54) DHCP Server Identifier (192.168.86.1)

Option: (12) Host Name

Option: (255) End

Padding: 00000000

0000 ff ff ff ff ff ff 78 4f 43 98 d9 27 08 00 45 00

0010 01 48 bb 0e 00 00 ff 11 ff 96 00 00 00 00 ff ff

0020 ff ff 00 44 00 43 01 34 d8 99 01 01 06 00 56 f4

0030 15 ed 00 04 00 00 00 00 00 00 00 00 00 00 00 00

0040 00 00 00 00 00 00 78 4f 43 98 d9 27 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

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 03 37 0a 01

0120 79 03 06 0f 77 fc 5f 2c 2e 39 02 05 dc 3d 07 01

0130 78 4f 43 98 d9 27 32 04 c0 a8 56 41 36 04 c0 a8

0140 56 01 0c 0d 4d 61 63 42 6f 6f 6b 2d 50 72 6f 2d

0150 36 ff 00 00 00 00

Dynamic Host Configuration Protocol: Protocol

Packets: 1018 · Displayed: 6 (0.6%)

Profile: Default

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?

A: The UDP source port number is 68 and the UDP destination port number is 67.

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

A: The source IP address is 0.0.0.0. As already mentioned it allows the computer and servers to temporarily communicate on the network before they receive a valid IP address from a DHCP server.

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

A: The destination IP address is 255.255.255.255., The destination IP address 255.255.255.255 is a special address known as the "limited broadcast address" in IPv4 networking. When a packet is sent to this address, it is broadcasted to all devices on the same network segment.

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?

A: The transaction ID is 0x2b036af7. Yes, it matches the transaction IDs of the earlier Discover and Offer messages.

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?

A: There is no difference between the entries in the ‘parameter request list’ in both the cases.



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

A: The source IP address 172.20.10.1 in the ACK message is a private IP address commonly used within local networks. It represents the device sending the acknowledgment and is not directly routable over the internet.

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

A: The destination IP address 172.20.10.2 in the ACK message is a standard IP address within the local network subnet. It identifies the specific device receiving the acknowledgment, facilitating direct communication within the network.

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?

A: The name of the field in the DHCP ACK message that contains the assigned client IP the address is 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?

A:As indicated in one of the option fields, the lease time is 1 day(86400s)

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?

A:The IP address of the first-hop router on the default path from the client to the rest of the Internet 172.20.10.2