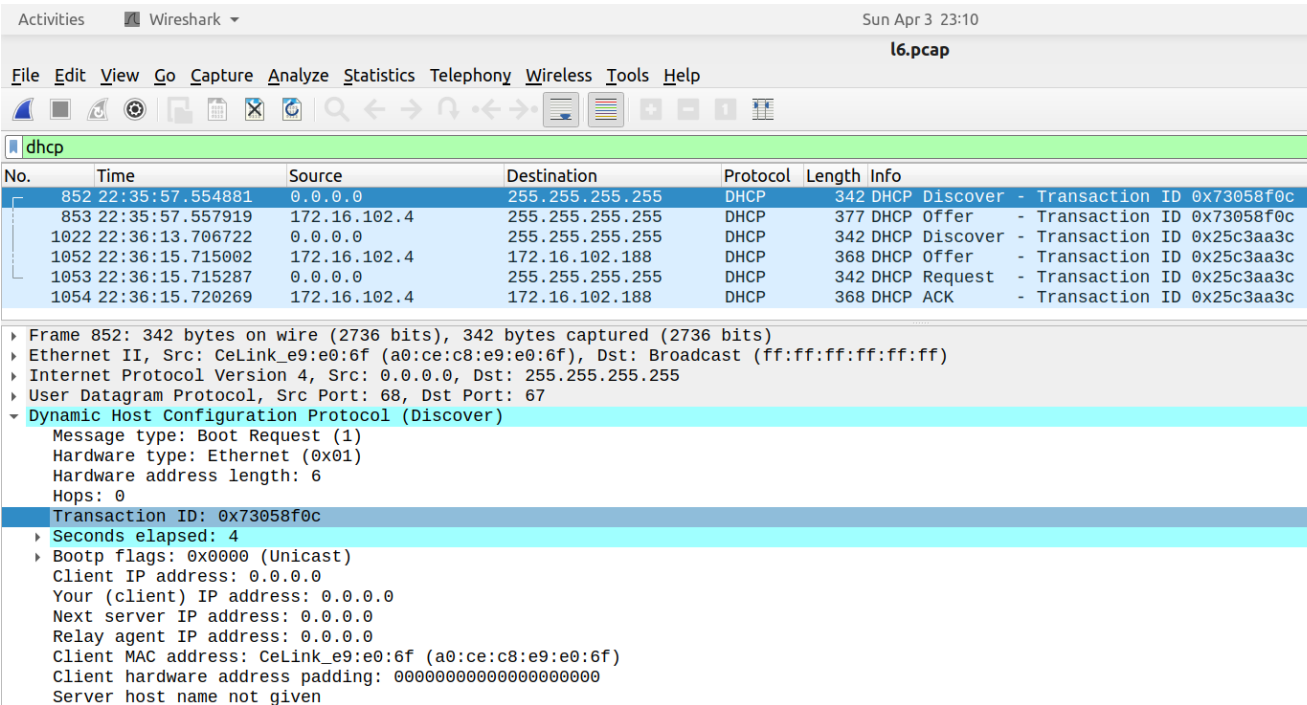


ASSIGNMENT 6

BY - PRIYANKA SACHAN (1901CS43)

1. Answer the following questions based on your examination of the DHCP fields for both the DHCP Request and DHCP Ack.

a. How long is the Transaction ID field? Say whether it is likely that concurrent DHCP operations done by different computers will happen to pick the same Transaction ID.



No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

▶ Frame 852: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
 ▶ Ethernet II, Src: CeLink_e9:e0:6f (a0:ce:c8:e9:e0:6f), 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: 0x73058f0c
 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: CeLink_e9:e0:6f (a0:ce:c8:e9:e0:6f)
 Client hardware address padding: 00000000000000000000
 Server host name not given

Transaction ID size = 32 bits

Thus, the probability that concurrent DHCP operations done by different computers will happen to pick the same Transaction ID in $(2^{32}-1) = 4.3$ Billion addresses is very unlikely.

b. What is the name of the field that carries the IP address that is being assigned to the client? You will find this field filled in on the DHCP Ack, as that message is completing the assignment.

Activities Wireshark Sun Apr 3 23:20 l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

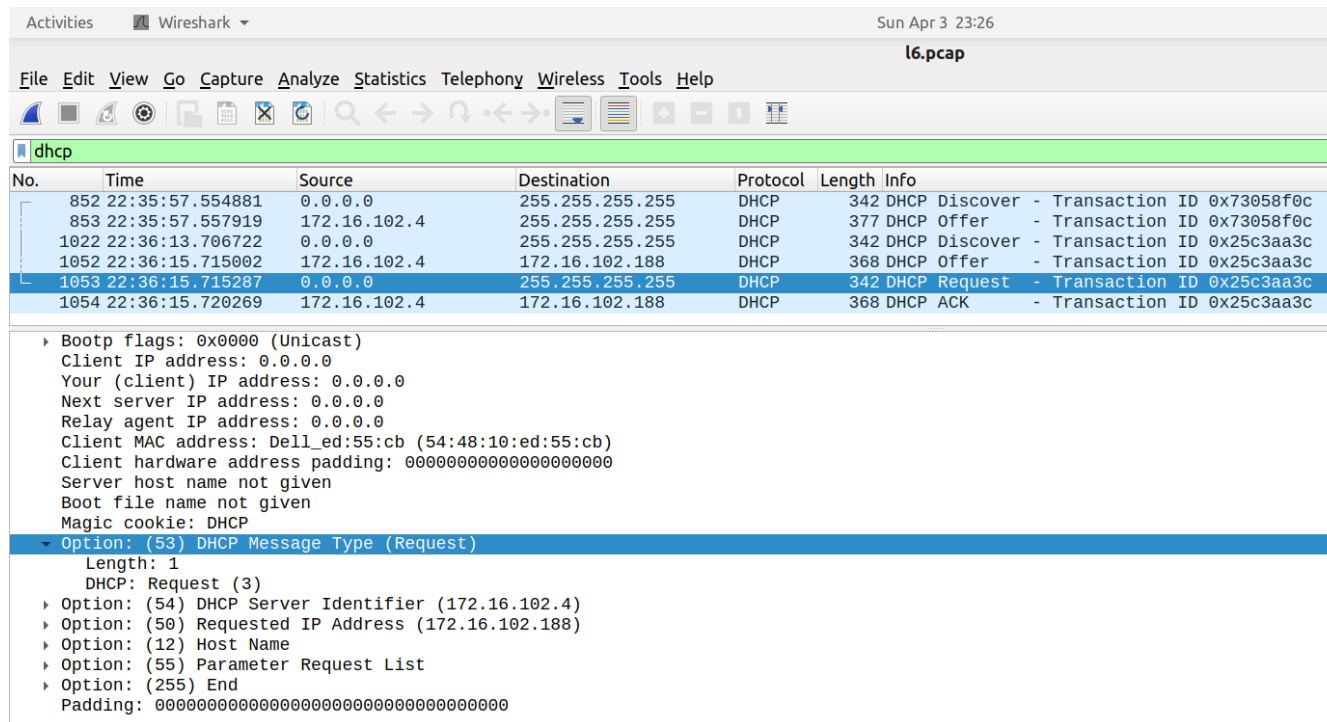
dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

Frame 1054: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)
Ethernet II, Src: Cisco_64:7a:e3 (54:86:bc:64:7a:e3), Dst: Dell_ed:55:cb (54:48:10:ed:55:cb)
Internet Protocol Version 4, Src: 172.16.102.4, Dst: 172.16.102.188
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: 0x25c3aa3c
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 172.16.102.188
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_ed:55:cb (54:48:10:ed:55:cb)
Client hardware address padding: 00000000000000000000
Server host name not given

Your (client) IP address (or dhcp.ip.your) carries the IP address that is being assigned to the client.

c. The first DHCP option is DHCP Message Type. What option value stands for this type? DHCP Requests will typically have a Client Identifier option. Look at the value of this option. How does it identify the client? Take a guess.



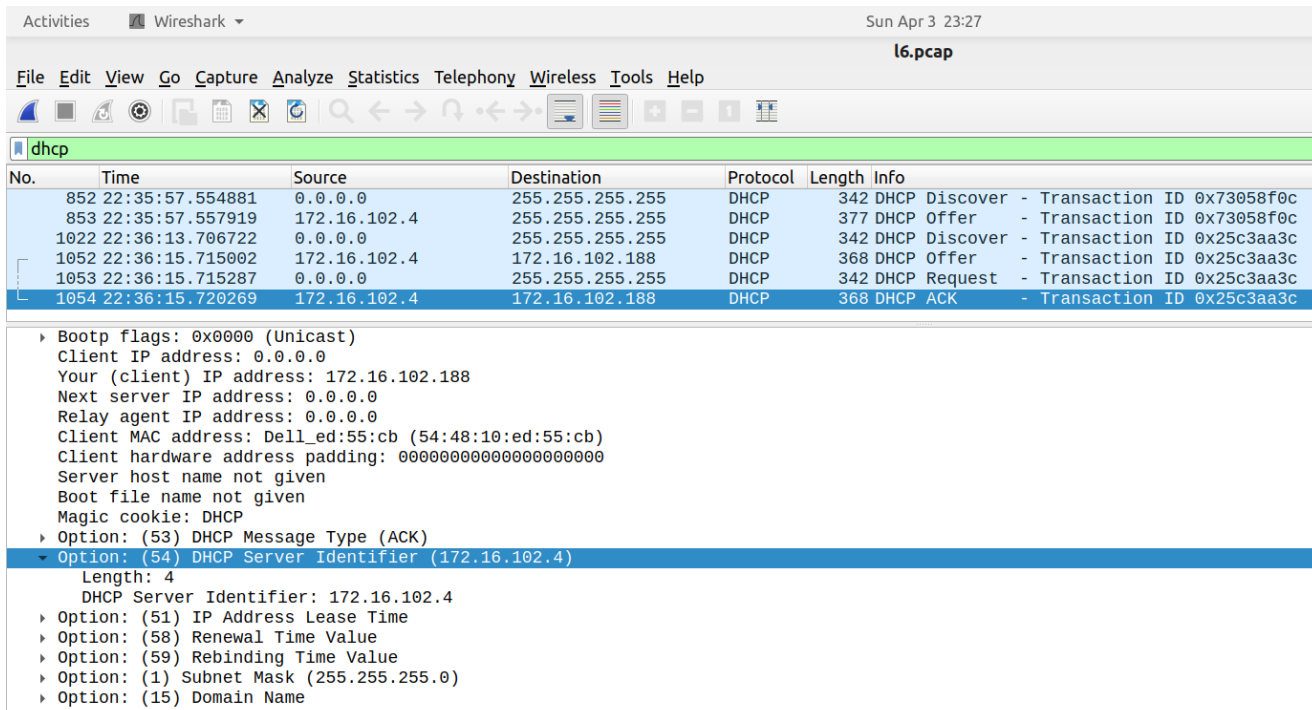
No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

▶ 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: Dell_ed:55:cb (54:48:10:ed:55:cb)
Client hardware address padding: 000000000000000000000000
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: (54) DHCP Server Identifier (172.16.102.4)
▶ Option: (50) Requested IP Address (172.16.102.188)
▶ Option: (12) Host Name
▶ Option: (55) Parameter Request List
▶ Option: (255) End
Padding: 00000000000000000000000000000000

The option value of 53 stands for DHCP Message Type.

It is typical for the Client Identifier to carry the Ethernet address of the client, but possible to use some other kind of identifier (e.g., hostname, serial number).

d. DHCP Acks typically have a Server Identifier option. Look at the value of this option. How does it identify the server? Take a guess.



Activities Wireshark Sun Apr 3 23:27

l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 172.16.102.188
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_ed:55:cb (54:48:10:ed:55:cb)
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 (172.16.102.4)
Length: 4
DHCP Server Identifier: 172.16.102.4

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: (15) Domain Name

The option value of 54 stands for DHCP Server Identifier.

In this, a server Identifier carries the IP address of the DHCP server but it is possible to use some other kind of identifier.

e. What option value stands for the Requested IP Address option? And for the IP Address Lease Time option?

Activities Wireshark Sun Apr 3 23:28

l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

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: Dell_ed:55:cb (54:48:10:ed:55:cb)
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) DHCP Server Identifier (172.16.102.4)
Option: (50) Requested IP Address (172.16.102.188)
Length: 4

Activities Wireshark Sun Apr 3 23:29

l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

Your (client) IP address: 172.16.102.188
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_ed:55:cb (54:48:10:ed:55:cb)
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 (172.16.102.4)
Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (432000s) 5 days
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value

The option value of 50 stands for Requested IP Address and the value of 51 stands for IP Address Lease Time.

f. How does the recipient of a DHCP message know that it has reached the last option?

Activities Wireshark Sun Apr 3 23:30

l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_ed:55:cb (54:48:10:ed:55:cb)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

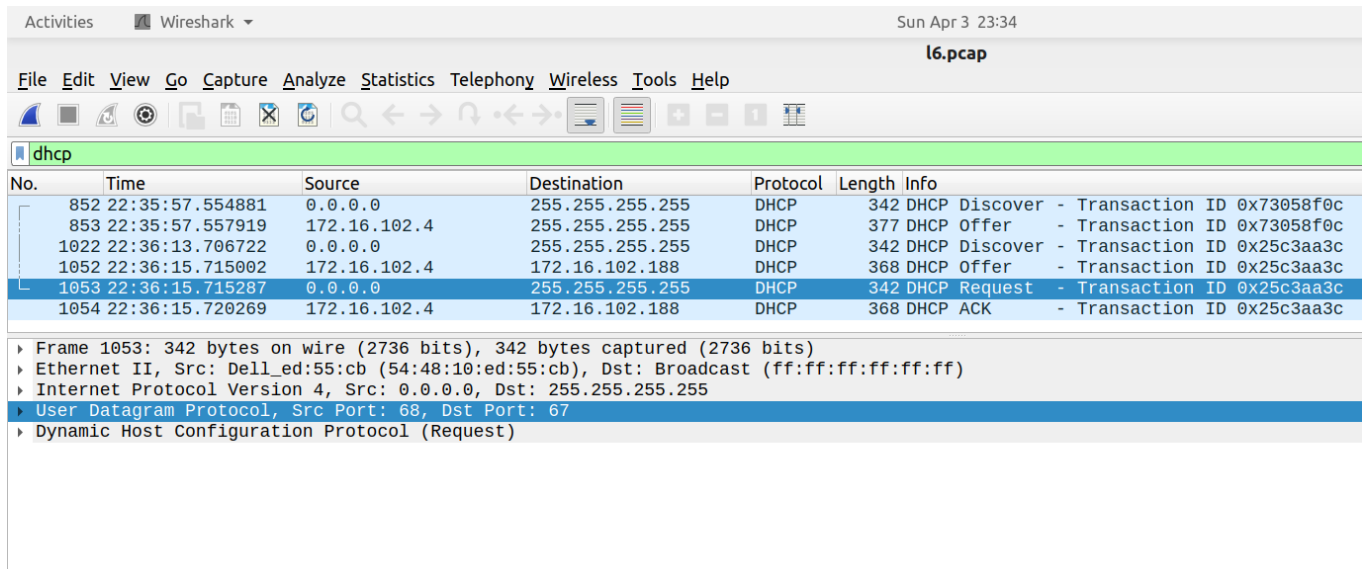
- Option: (53) DHCP Message Type (ACK)
- Option: (54) DHCP Server Identifier (172.16.102.4)
- Option: (51) IP Address Lease Time
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (1) Subnet Mask (255.255.255.0)
- Option: (15) Domain Name
- Option: (6) Domain Name Server
- Option: (3) Router
- Option: (0) Padding
- Option: (255) End

Option End: 255

By a DHCP option called End with value 255.

2. Answer the following questions by selecting a DHCP Request packet and looking at its UDP details in the middle Wireshark panel.

a. What port number does the DHCP client use, and what port number does the DHCP server use?



No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

▶ Frame 1053: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_ed:55:cb (54:48:10:ed:55:cb), 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)

Source Port: 68

Destination Port: 67

Activities Wireshark Sun Apr 3 23:36

l6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

▶ Frame 1053: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
 ▶ Ethernet II, Src: Dell_ed:55:cb (54:48:10:ed:55:cb), 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: 0x10 (DSCP: Unknown, ECN: Not-ECT)
 Total Length: 328
 Identification: 0x0000 (0)
 ▶ Flags: 0x00
 Fragment Offset: 0
 Time to Live: 128
 Protocol: UDP (17)
 Header Checksum: 0x3996 [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
 ▶ Dynamic Host Configuration Protocol (Request)

b. What source IP address is put on the Request message? It is a special value meaning “this host on this network” used for initialization.

Source Address: 0.0.0.0

c. What destination IP address is put on the Request message? It is also a reserved value designed to reach the DHCP server wherever it is on the local network.

Destination Address: 255.255.255.255

d. What source Ethernet address is put on the Request message, and what destination Ethernet address is put on the Request message? One of these addresses is a reserved address.

No.	Time	Source	Destination	Protocol	Length	Info
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x73058f0c
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377	DHCP Offer - Transaction ID 0x73058f0c
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x25c3aa3c
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368	DHCP Offer - Transaction ID 0x25c3aa3c
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x25c3aa3c
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368	DHCP ACK - Transaction ID 0x25c3aa3c

Frame 1053: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

Ethernet II, Src: Dell_ed:55:cb (54:48:10:ed:55:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Dell_ed:55:cb (54:48:10:ed:55:cb)
 - 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)

Source: Dell_ed:55:cb (54:48:10:ed:55:cb)

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

e. How does a computer work out whether a DHCP message it receives is intended as a reply to its DHCP Request message, and not a reply to another computer? Hint: If you are not sure then go over the fields you inspected previously.

dhcph					
No.	Time	Source	Destination	Protocol	Length
852	22:35:57.554881	0.0.0.0	255.255.255.255	DHCP	342
853	22:35:57.557919	172.16.102.4	255.255.255.255	DHCP	377
1022	22:36:13.706722	0.0.0.0	255.255.255.255	DHCP	342
1052	22:36:15.715002	172.16.102.4	172.16.102.188	DHCP	368
1053	22:36:15.715287	0.0.0.0	255.255.255.255	DHCP	342
1054	22:36:15.720269	172.16.102.4	172.16.102.188	DHCP	368

Frame 1053: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

Ethernet II, Src: Dell_ed:55:cb (54:48:10:ed:55:cb), 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: 0x25c3aa3c

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: Dell_ed:55:cb (54:48:10:ed:55:cb)

Client hardware address padding: 00000000000000000000

Frame 1054: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits)

Ethernet II, Src: Cisco_64:7a:e3 (54:86:bc:64:7a:e3), Dst: Dell_ed:55:cb (54:48:10:ed:55:cb)

Internet Protocol Version 4, Src: 172.16.102.4, Dst: 172.16.102.188

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: 0x25c3aa3c

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 172.16.102.188

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: Dell_ed:55:cb (54:48:10:ed:55:cb)

Client hardware address padding: 00000000000000000000

The DHCP messages in a single exchange carry the same Transaction ID. Thus a computer looks for a DHCP reply such as an Ack with a Transaction ID that matches the value it placed on the earlier DHCP message such as a Request.