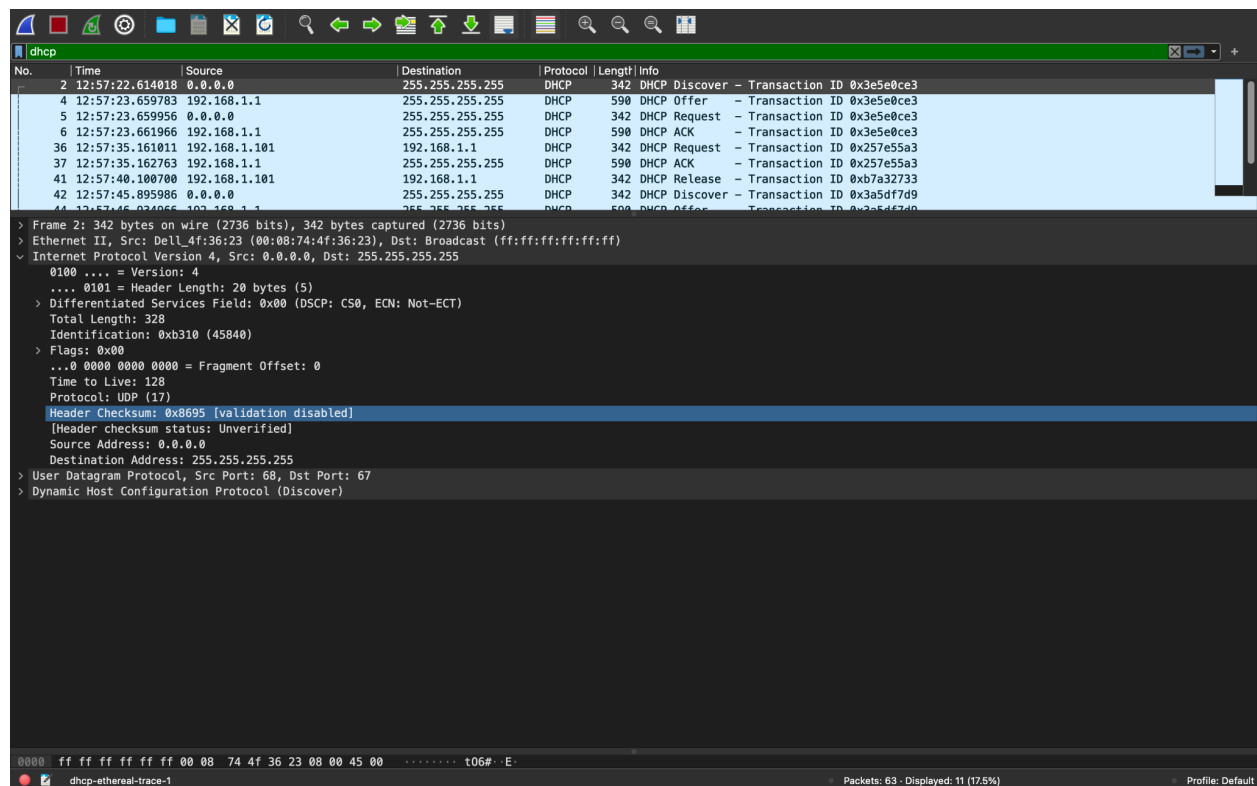


Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)

```
Bhavin@Ozas-MacBook-Pro ~ % sudo ipconfig set en0 none
Password:
Bhavin@Ozas-MacBook-Pro ~ % ipconfig set en0 dhcp
ipconfig_set en0 dhcp failed: permission denied
Bhavin@Ozas-MacBook-Pro ~ % sudo ipconfig set en0 dhcp
Bhavin@Ozas-MacBook-Pro ~ %
```



1). UDP

Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)

Wireshark packet capture showing DHCP transactions. The packet list displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
2	12:57:22.614018	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	12:57:23.659783	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	12:57:23.659956	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	12:57:23.661966	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	12:57:35.161011	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	12:57:35.162763	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	12:57:40.100700	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	12:57:45.895986	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	12:57:45.921056	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9

Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)

Ethernet II, Src: LinksysG da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.1.1, 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: 576

Identification: 0x0100 (264)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 150

Protocol: UDP (17)

Header Checksum: 0x5ffc [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.1

Destination Address: 255.255.255.255

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

> Dynamic Host Configuration Protocol (Offer)

0000 ff ff ff ff ff ff 00 06 25 da af 73 08 00 45 00 %s-E

dhcp-ethereal-trace-1

Packets: 63 - Displayed: 11 (17.5%)

Profile: Default

Wireshark packet capture showing DHCP transactions. The packet list displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
2	12:57:22.614018	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	12:57:23.659783	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	12:57:23.659956	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	12:57:23.661966	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
36	12:57:35.161011	192.168.1.101	192.168.1.1	DHCP	342	DHCP Request - Transaction ID 0x257e55a3
37	12:57:35.162763	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x257e55a3
41	12:57:40.100700	192.168.1.101	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0xb7a32733
42	12:57:45.895986	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	12:57:45.921056	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9

Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)

Ethernet II, Src: Dell_4f:36:23 (00:08:74:f3:36:23), 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: 328

Identification: 0xb311 (45841)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x8694 [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)

0000 ff ff ff ff ff ff 00 08 74 4f 36 23 08 00 45 00 t06#-E

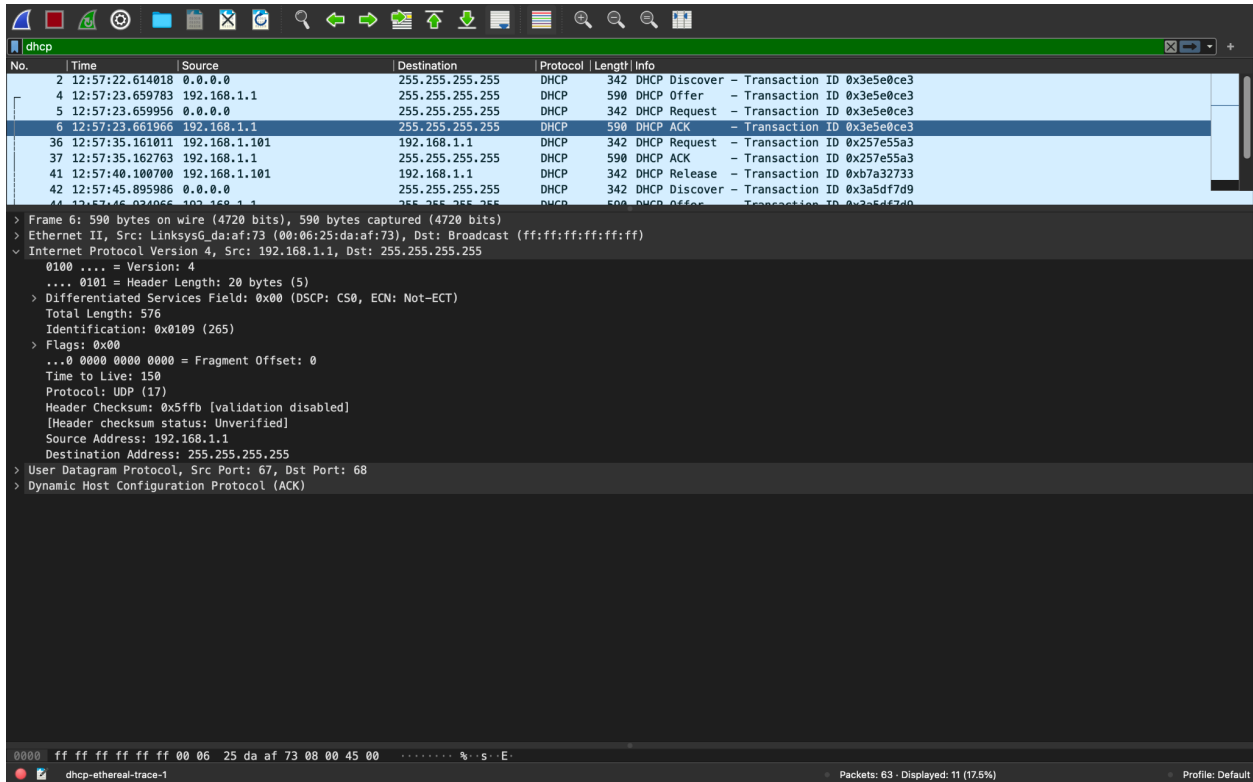
dhcp-ethereal-trace-1

Packets: 63 - Displayed: 11 (17.5%)

Profile: Default

Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)



2).

Discover Packet: Source port → 68, Destination Port → 67

Offer Packet: Source port → 67, Destination Port → 68

Request Packet: Source port → 68, Destination Port → 67

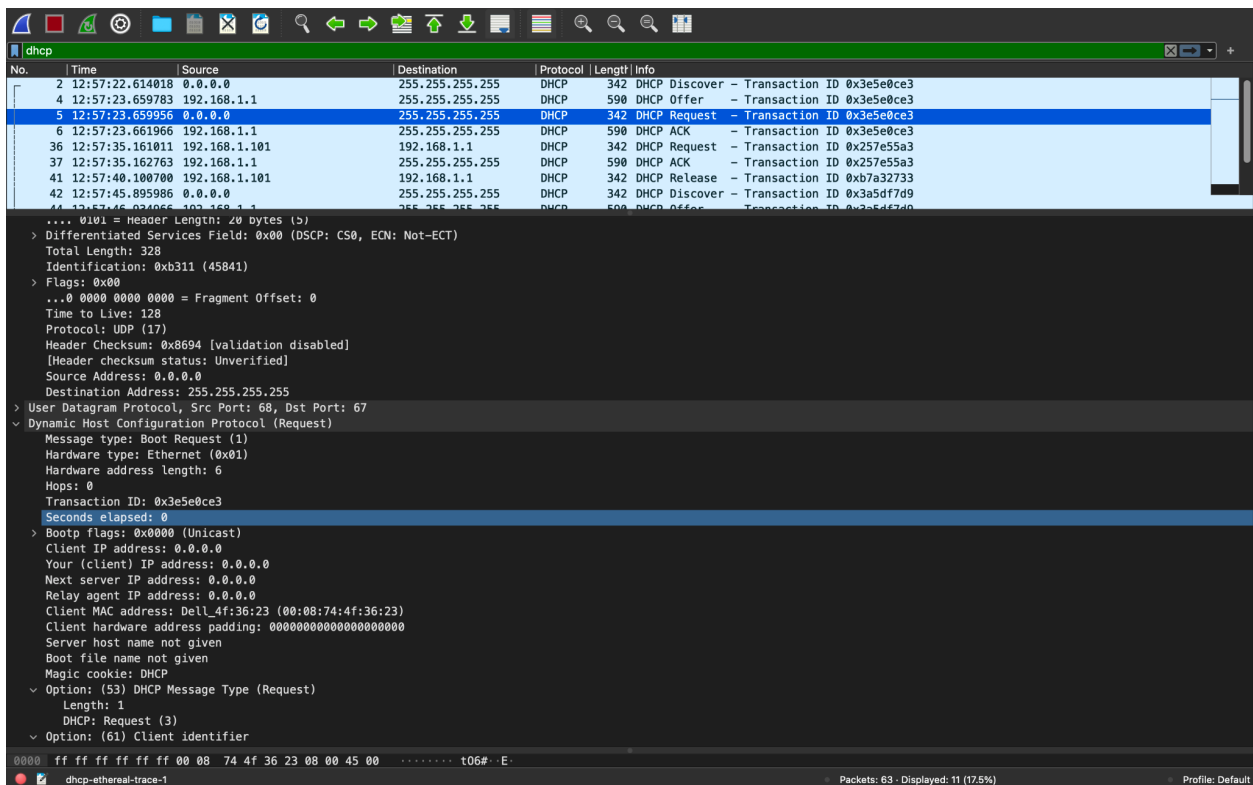
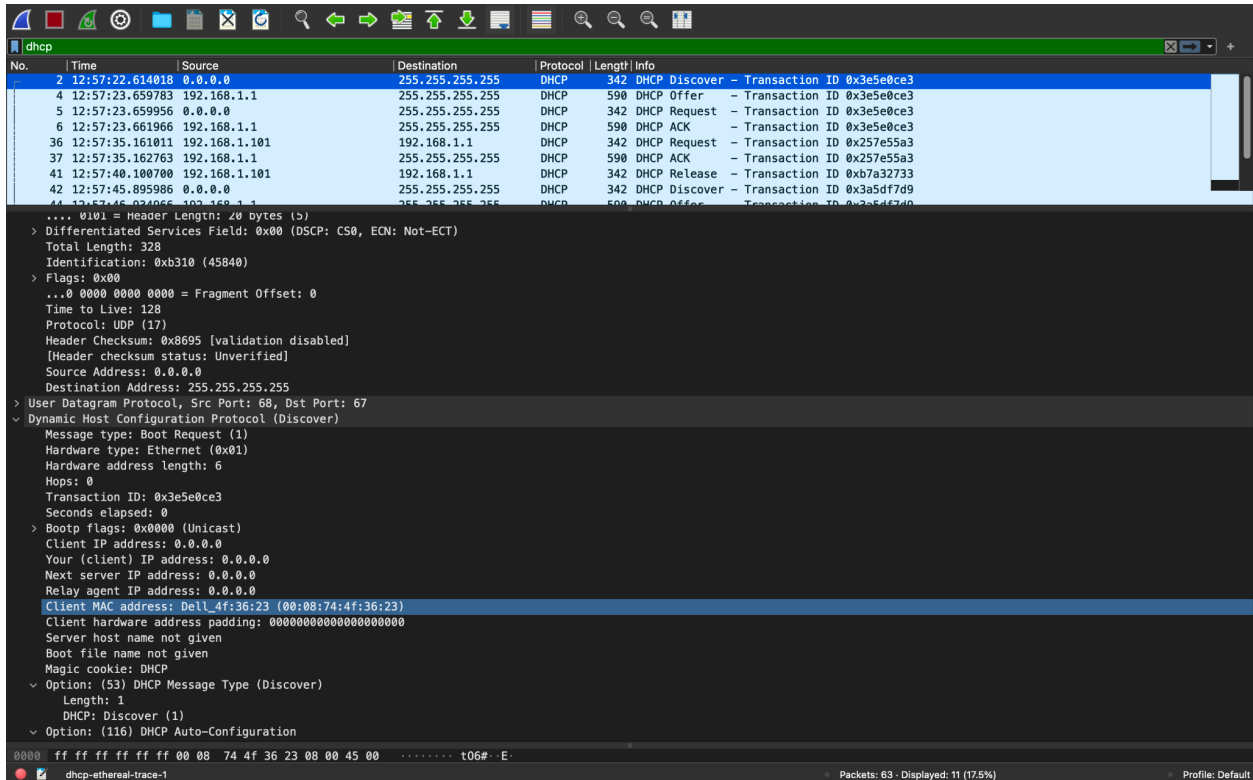
ACK Packet: Source port → 67, Destination Port → 68

Yes, port numbers are the same as in example in lab assignments.

3). 00:06:05:da:af:73

Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)



4). The value of Option 53 - DHCP message type differentiate DHCP Discover from DHCP Request.

Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)

5). Transaction ID for first set of DHCP messages: 0x3e5e0ce3

Transaction ID for second set of DHCP messages: 0x257e55a3

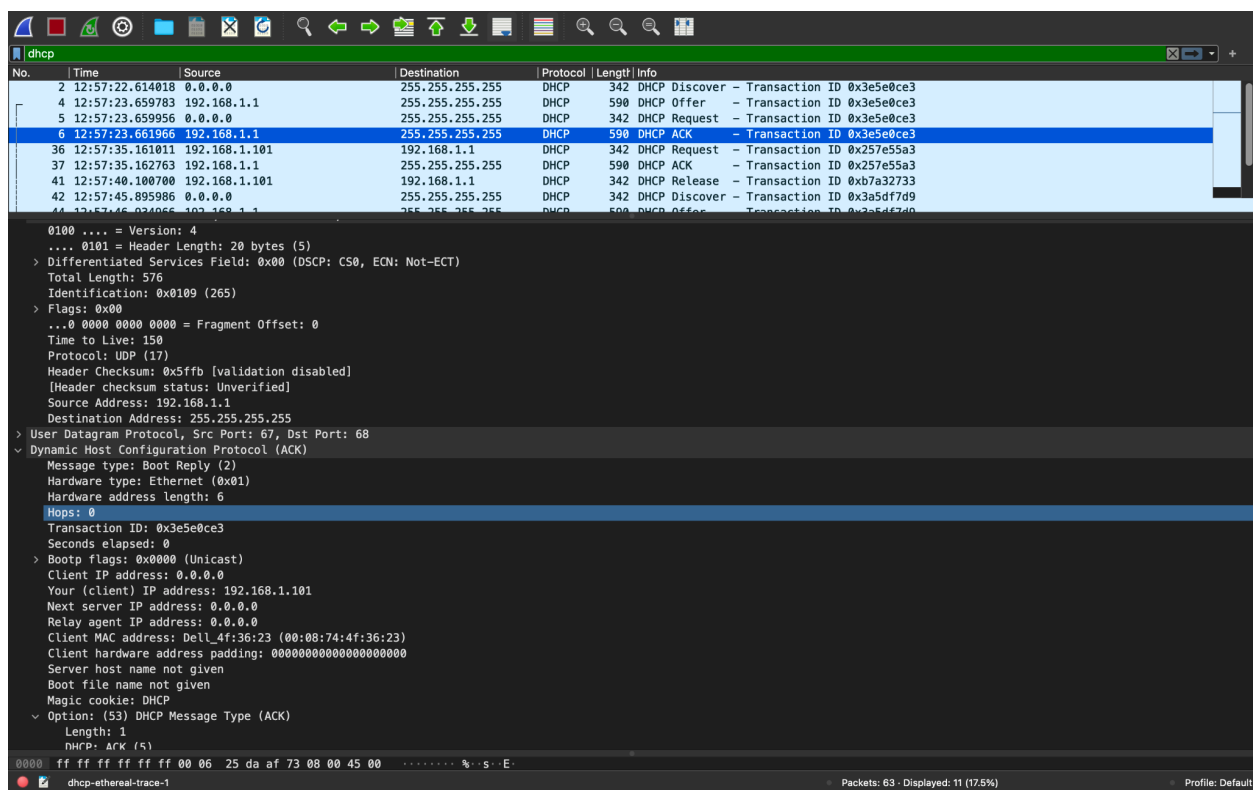
The Transaction-ID field is used for differentiating between different DHCP requests.

6). The client uses 0.0.0.0 as its source address, and 255.255.255.255 as its destination address. The server uses its actual address as source address and 255.255.255.255 as its destination address.

7). The IP address for the DHCP server is 192.168.1.1

8). The IP address offered by the DHCP Offer message is 192.168.1.101

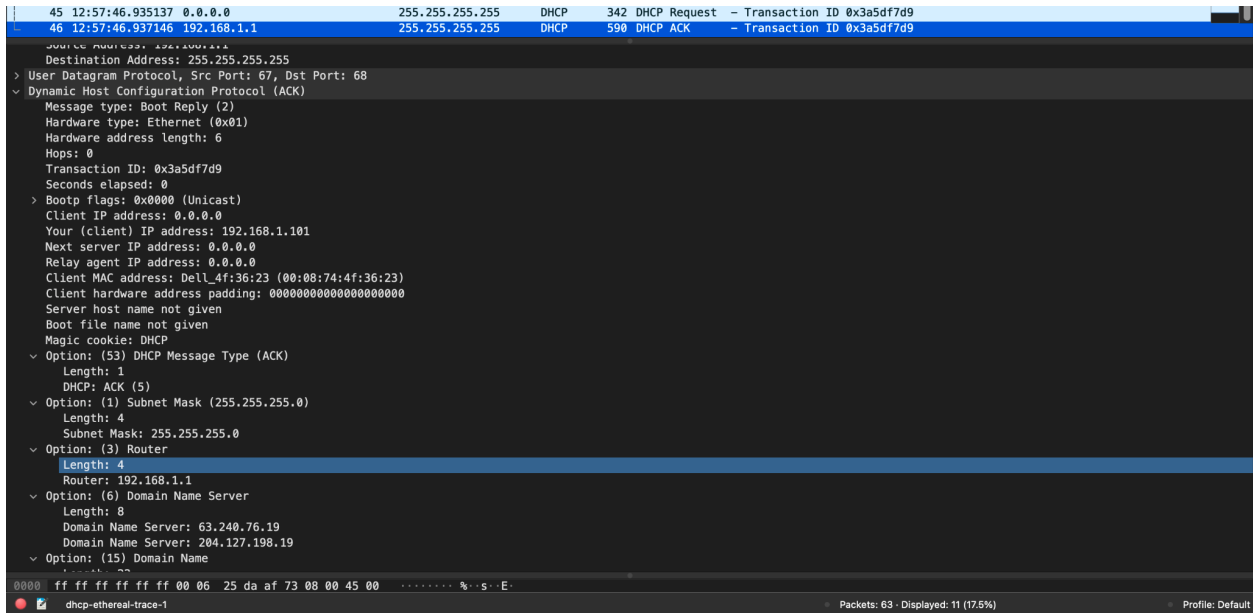
The DHCP Message of Offer Type had the above IP address.



9). The value of the Relay agent IP address is 0.0.0.0 in the DHCP ACK packet. This indicates that there are no relay agents used.

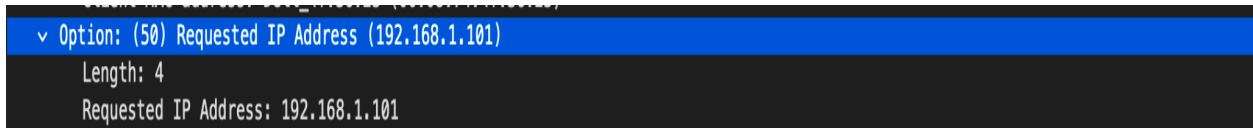
Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)

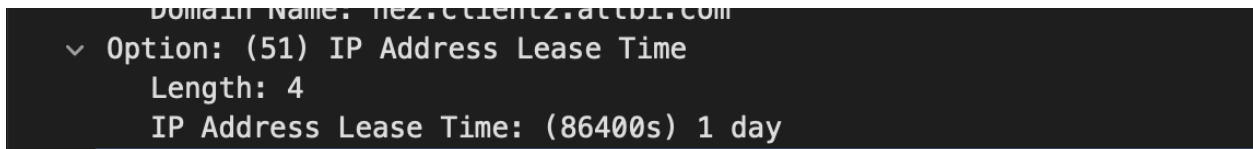


10). The router field in the DHCP Offer indicates the default gateway to the client.
The subnet field in the DHCP Offer indicates the subnet mask to be used by the client.

11). The host is requesting the offered IP address in the DHCP Request message.



12). The amount of time an DHCP server takes to assign an IP to a host.



13). The DHCP Release message is sent by the client to DHCP Server to cancel its lease on the given IP address.

The server does not send back any acknowledgement for the same message.

In case the DHCP Release message is lost, the server will wait till the lease period, and then assign that address to the different client.

14). Yes.

A DHCP server makes an ARP request with the IP address, to check if it is already assigned to another client. If not, it assigns the IP address to the client.