Lab 8

Wireshark DHCP

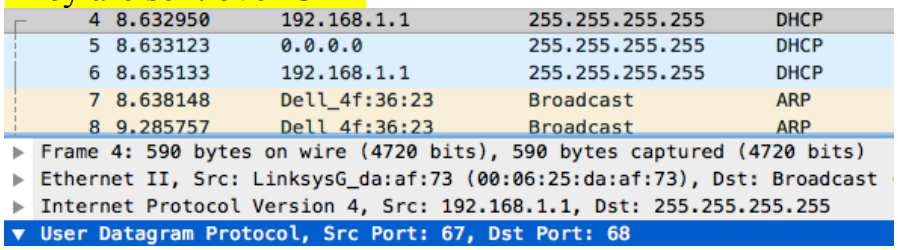
Nicole Merritt

Questions

I am doing this assignment on a public network and therefore cannot make my own captures. I have used the trace file.

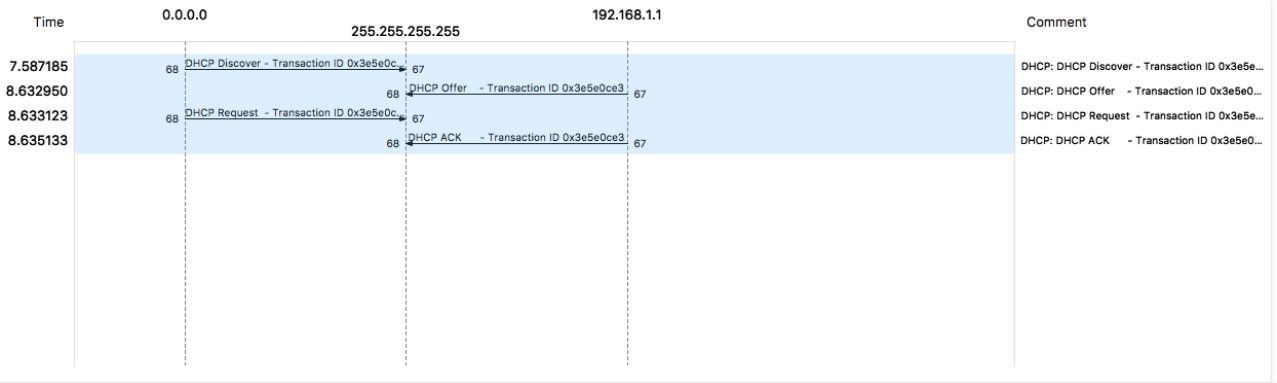
1. Are DHCP messages sent over UDP or TCP?

They are sent over UDP

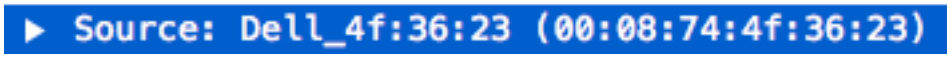


2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

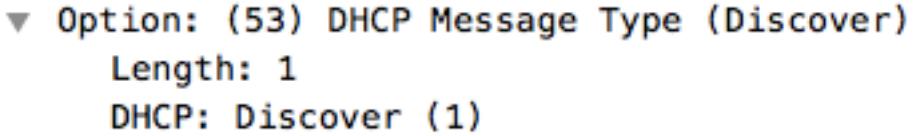
Yes the ports are the same, this is because DHCP uses the UDP port 67/68



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

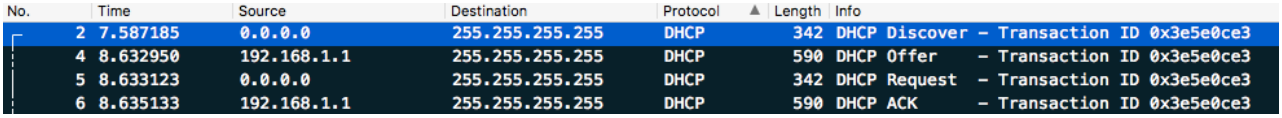


4. What values in the DHCP discover message differentiate this message from the DHCP request message?

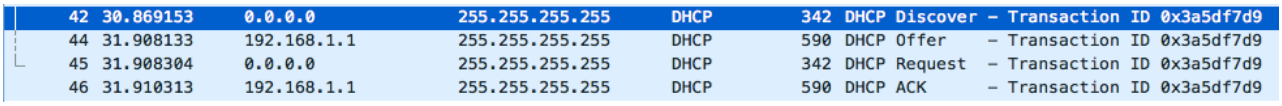


```
▼ Option: (53) DHCP Message Type (Request)
     Length: 1
     DHCP: Request (3)
```

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?



No.	Time	Source	Destination	Protocol	Length	Info
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3



42	30.869153	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3a5df7d9
44	31.908133	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3a5df7d9
45	31.908304	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3a5df7d9
46	31.910313	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3a5df7d9

The purpose of the transaction-ID field is to show what messages go together. It is a client only thing

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.

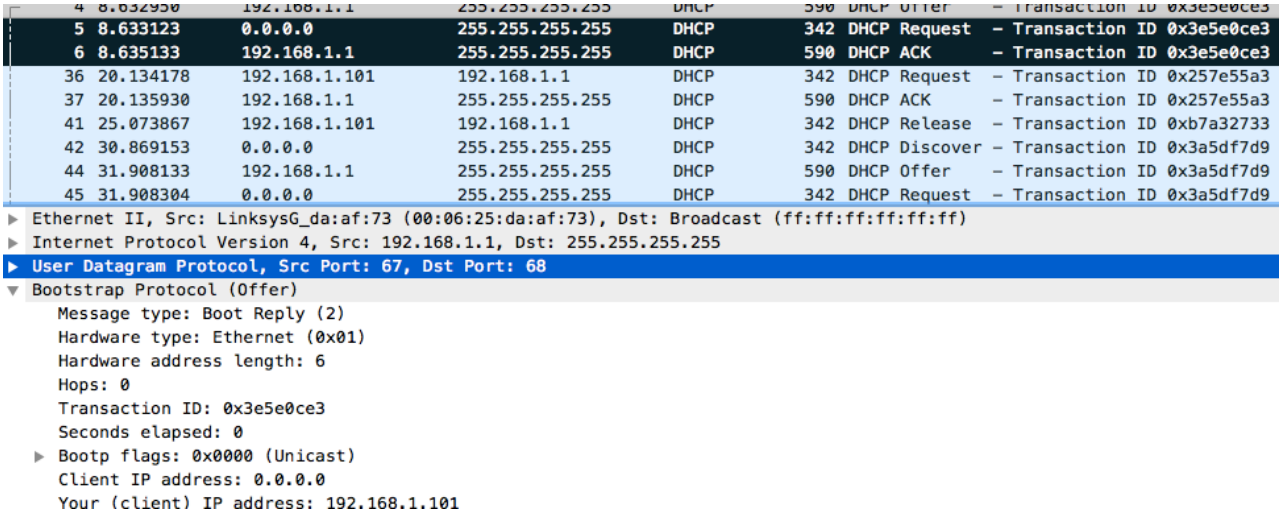
Number	Source IP	Destination IP
1- Discover	0.0.0.0	255.255.255.255
2 - Offer	192.168.1.1	255.255.255.255
3- Request	0.0.0.0	255.255.255.255
4 - ACK	192.168.1.1	255.255.255.255

0.0.0.0 is the value used in IP datagrams

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

192.168.1.1

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.



Offering me 192.168.1.101

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?

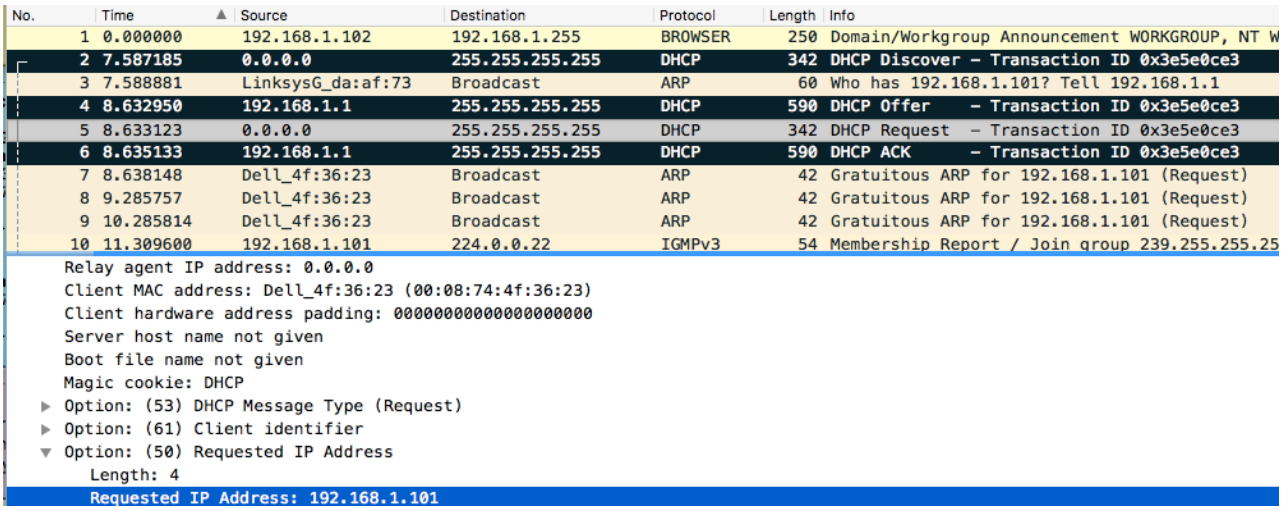
The IP address in the trace is 0.0.0.0. so there is no relay agent. This is because you use a relay agent when the device and server are located on different subnets.

10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.

```
Boot file name not given
Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Offer)
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
```

Subnet mask: tells the client which subnet mask should be used
Router: tells the client what the default gateway should be.

11. In the DHCP trace file noted in footnote 2, the DHC 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?



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.255	BROWSER	250	Domain/Workgroup Announcement WORKGROUP, NT W
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
3	7.588881	LinksysG_da:af:73	Broadcast	ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3
7	8.638148	Dell_4f:36:23	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.101 (Request)
8	9.285757	Dell_4f:36:23	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.101 (Request)
9	10.285814	Dell_4f:36:23	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.101 (Request)
10	11.309600	192.168.1.101	224.0.0.22	IGMPv3	54	Membership Report / Join group 239.255.255.25

```
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
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
    Length: 4
    Requested IP Address: 192.168.1.101
```

The client requests the offered IP address. It is shown in the DHCP request.

12. Explain the purpose of the lease time. How long is the lease time in your experiment?

The lease time is the length to keep the IP address once you ACK it. At every half-life point of the lease the client checks back to make sure that you are still

there. The point of the lease time is to make sure that people don't keep and IP address forever, otherwise there wont be any more IP address to give out.
Our lease time here is 1 day

```
IP Address Lease Time: (86400s) 1 day
```

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?

The release message lets the client know that the IP address is now available and ready to use.
If the DHCP release message is lost the client would release the IP address.

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.255	BROWSER	250	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
3	7.588881	LinksysG_da:af:73	Broadcast	ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x3e5e0ce3
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x3e5e0ce3
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x3e5e0ce3

Yes – ARP packets work together with the DHCP to help keep things organized. It asks who has what IP address. Fills in all the ARP (MAC ID) tables as we change things.