21CY681– Internet Protocol lab

ASSIGNMENT -5

Name: B.Shebu

Register Number : CYS22005

Title: Analyzing DHCP using protocol analyser .

Date of Assignment provided: 31/11/2022

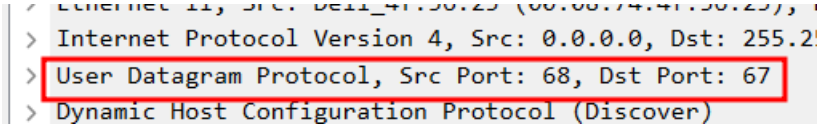
Aim: To analyse DHCP using protocol analyzer

PROCEDURE -

2. Open the captured traffic file and given pcap file “dhcp” in Wireshark to answer the following questions.

a) Are DHCP messages sent over UDP or TCP?

All the dhcp packets are sent via UDP

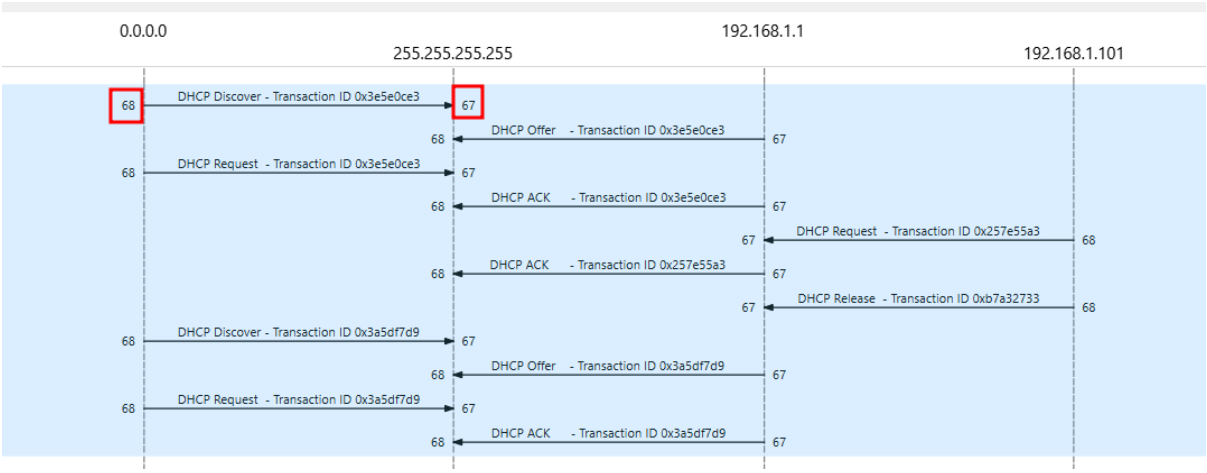


b) Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers.

From the below screenshot we can find out that the

- For the DISCOVER and OFFER requests sent by the server the source port is 68 and destination port is 68.

- For the REQ and ACK requests sent by the client , the source port is 68 and the destination port is 67.



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

Link layer address means the data link layer which means the MAC address of the host. So the MAC address of the client/host is 00:08:74:4f:36:23.

```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
v Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  v Source: Dell_4f:36:23 (00:08:74:4f:36:23)
      Address: Dell_4f:36:23 (00:08:74:4f:36:23)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

d) What values in the DHCP discover message differentiate this message from the DHCP request message?

The only difference between the DHCP Discover and Request are “DHCP Server Identifier and DHCP message type”

Wireshark · Packet 5 · dhcp

```
    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 (192.168.1.101)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
```

Wireshark · Packet 2 · dhcp

```
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (116) DHCP Auto-Configuration
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.101)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
```

e) 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?

The transaction ID in the first four packets is “0x3e5e0ce3”.

The transaction ID in the second set of DHCP messages is “0x3a5d7d9” .

```
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x3e5e0ce3
- Transaction ID 0x257e55a3
- Transaction ID 0x257e55a3
- Transaction ID 0xb7a32733
- Transaction ID 0x3a5df7d9
- Transaction ID 0x3a5df7d9
- Transaction ID 0x3a5df7d9
- Transaction ID 0x3a5df7d9
```

The transaction ID is used by the server to identify/ to take note of which message was sent by which computer

f) 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.

If IP address is not set until the end of the four message exchange , then 0.0.0.0 is used as the IP in the DHCP exchange.

For Discover and Request , the source IP is 0.0.0.0 and dst IP is 255.255.255.255

For Offer and ACK , the source IP is 172.17.18.2 and dst IP is 172.17.136.155

Source	Src.port	Destination	dpt port	Protocol	Lengtl	Info
0.0.0.0	68	255.255.255.255	67	DHCP	344	DHCP Discover -
172.17.18.2	67	172.17.136.155	68	DHCP	361	DHCP Offer -
0.0.0.0	68	255.255.255.255	67	DHCP	370	DHCP Request -
172.17.18.2	67	172.17.136.155	68	DHCP	361	DHCP Offer -

g) What is the IP address of your DHCP server?

The IP address of the DHCP server is 192.168.1.1

```
8 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Discover - Transaction ID 0x3e5e0ce3
3 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP Offer    - Transaction ID 0x3e5e0ce3
```

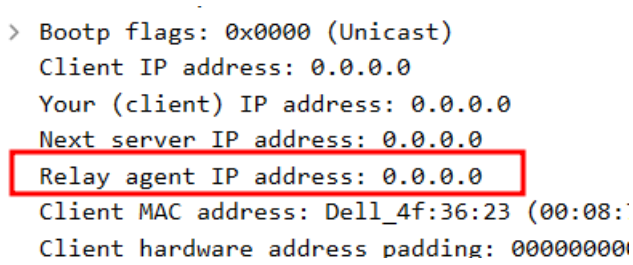
h) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The DHCP offered address is 192.168.1.101

```
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.101
  Next server IP address: 0.0.0.0
```

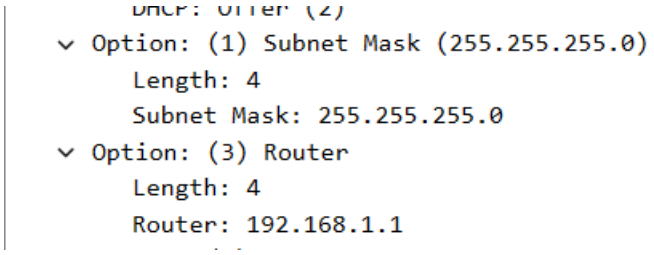
i) In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

There is no Relay agent in our experiment so the value for it is 0.0.0.0



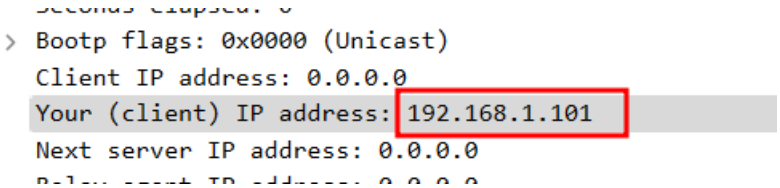
j) Explain the purpose of the router and subnet mask lines in the DHCP offer message.

When the DHCP server is not present in our network and if it is present in some other LAN then the DHCP DISCOVER message is sent to the router in its network. That router forwards the request packet to the network and it reaches the DHCP server in the other LAN network.



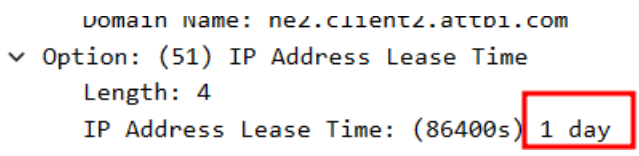
k) In the DHCP trace file, the DHCP server offers a specific IP address to the client. In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

The server accepted the offered IP address. The client IP requested address is mentioned in the packet as shown below.



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

The lease time of the IP for an computer is 1 day.



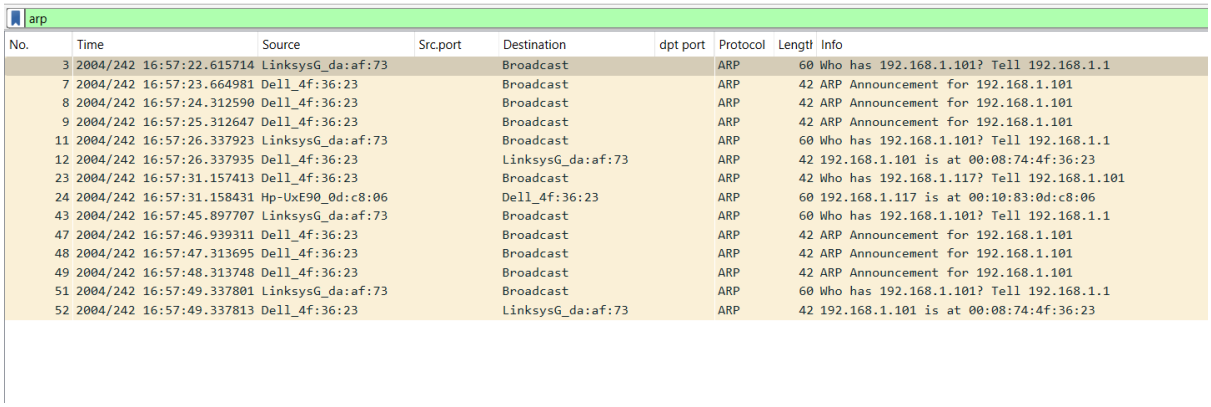
m) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

The purpose of release message is to release the IP address assigned to the computer. The DHCP server doesn't send an ACK receipt of client's DHCP request.

If the client's DHCP message is lost then the server might not know whether the client issued an release request or not . So the IP assigned to the computer previously still remains the same.

n) Clear the DHCP 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

Yes , we can see many ARP packets that were transferred in the experiment since the server verifies whether the IP which is to be allocated to the requested computer is used already by any other other computer.



arp

No.	Time	Source	Src.port	Destination	dpt port	Protocol	Length	Info
3	2004/242 16:57:22.615714	LinksysG_da:af:73		Broadcast		ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
7	2004/242 16:57:23.664981	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
8	2004/242 16:57:24.312590	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
9	2004/242 16:57:25.312647	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
11	2004/242 16:57:26.337923	LinksysG_da:af:73		Broadcast		ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
12	2004/242 16:57:26.337935	Dell_4f:36:23		LinksysG_da:af:73		ARP	42	192.168.1.101 is at 00:08:74:4f:36:23
23	2004/242 16:57:31.157413	Dell_4f:36:23		Broadcast		ARP	42	Who has 192.168.1.117? Tell 192.168.1.101
24	2004/242 16:57:31.158431	Hp-UxE90_0d:c8:06		Dell_4f:36:23		ARP	60	192.168.1.117 is at 00:10:83:0d:c8:06
43	2004/242 16:57:45.897707	LinksysG_da:af:73		Broadcast		ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
47	2004/242 16:57:46.939311	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
48	2004/242 16:57:47.313695	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
49	2004/242 16:57:48.313748	Dell_4f:36:23		Broadcast		ARP	42	ARP Announcement for 192.168.1.101
51	2004/242 16:57:49.337801	LinksysG_da:af:73		Broadcast		ARP	60	Who has 192.168.1.101? Tell 192.168.1.1
52	2004/242 16:57:49.337813	Dell_4f:36:23		LinksysG_da:af:73		ARP	42	192.168.1.101 is at 00:08:74:4f:36:23

RESULT –

Thus the experiment to analyse DHCP using protocol analyser has been done succesfully