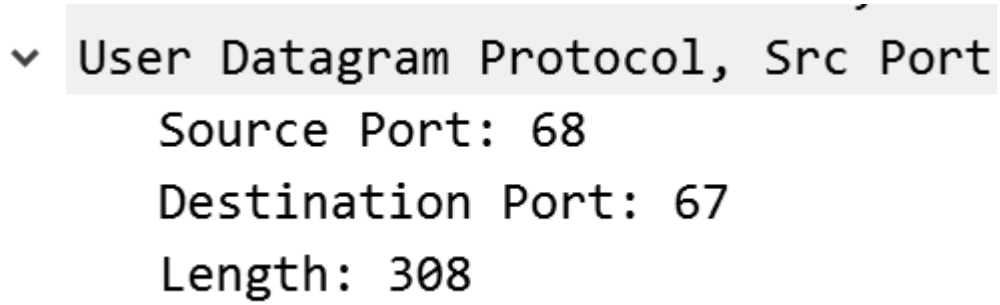
LAB 4B

Wireshark Lab: DHCP v8.0

Name: Hồ Đức Trí

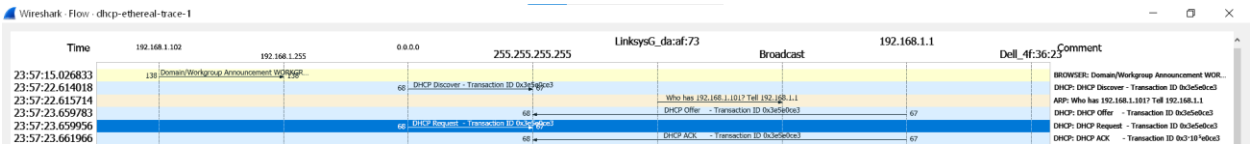
Student No: 1912288

1. Are DHCP messages sent over UDP or TCP?



The DHCP messages are sent via 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?



Discover packet: Src – 68, Dst – 67

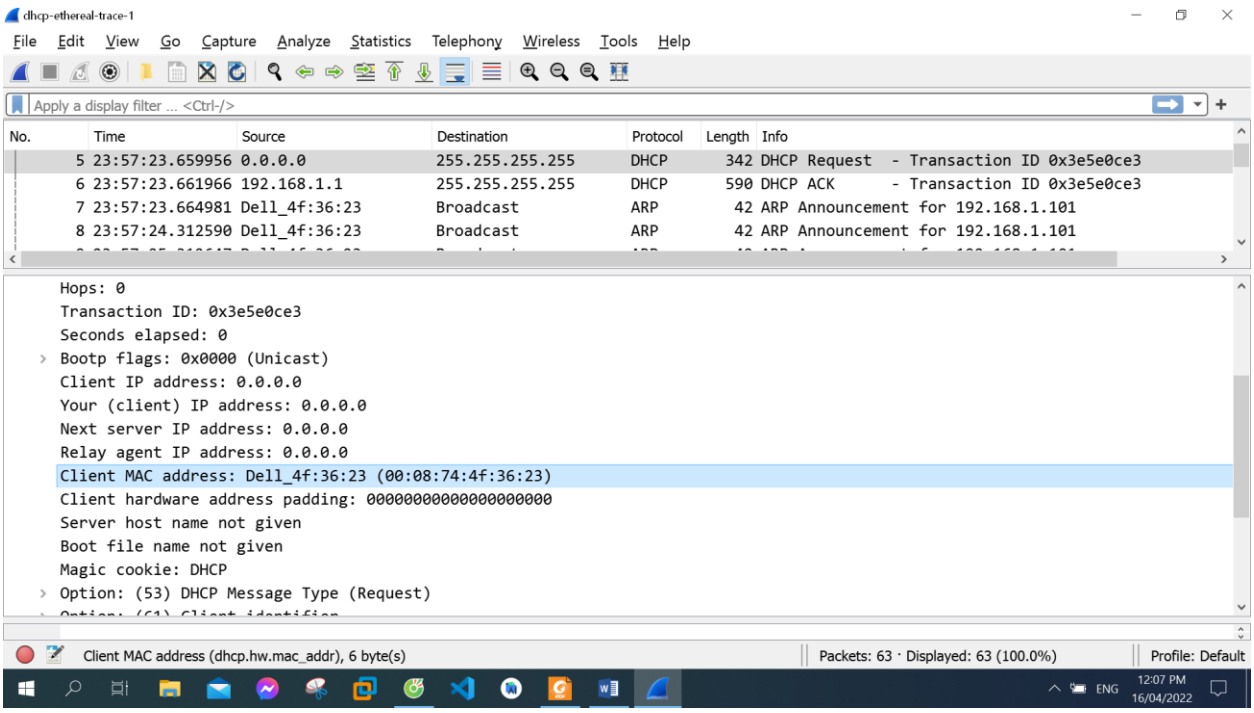
Offer packet: Dst – 67, Src – 68

Request packet: Src – 68, Dst – 67

ACK packet: Dst – 67, Src – 68

Yes, the port numbers the same as in the example given in this lab assignment

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



Source: DellComp_4f:36:23 (00:08:74:4f:36:23)

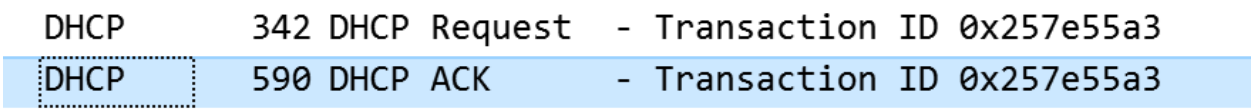
4. What values in the DHCP discover message differentiate this message from the DHCP request message?

The message type value for a discover message is a 1, but the message type value for a request packet is a 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?

```
DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
DHCP      590 DHCP Offer    - Transaction ID 0x3e5e0ce3
DHCP      342 DHCP Request  - Transaction ID 0x3e5e0ce3
DHCP      590 DHCP ACK      - Transaction ID 0x3e5e0ce3
```

The Transaction ID in the first four messages: 0x3e5e0ce3



The transaction ID in the second set of messages is 0x257e55a3

The transaction ID identifies if a message is part of a set of messages related to one transaction

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.

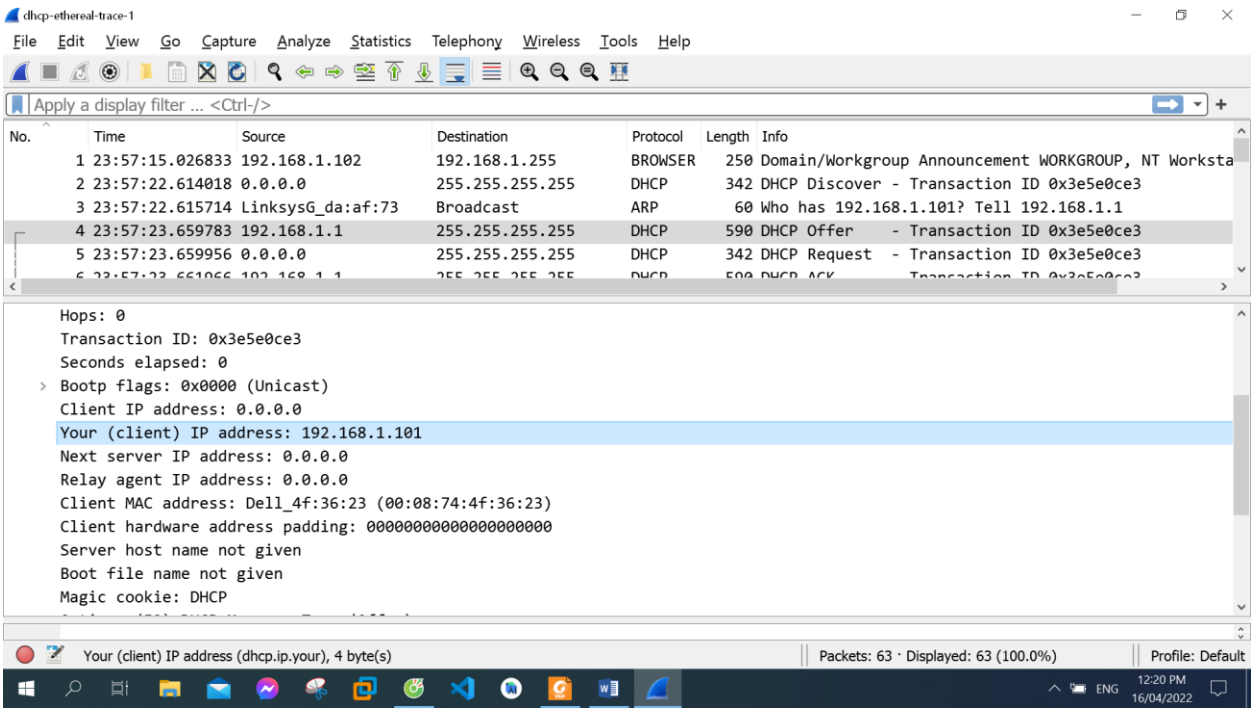
Discover source 0.0.0.0 Destination 255.255.255.255

Offer source 192.168.1.1 Destination 255.255.255.255

Request source 0.0.0.0 Destination 255.255.255.255

Ack DHCP 192.168.1.1 Destination 255.255.255.255

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



DHCP server address 192.168.1.101

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.

The DHCP server offers 192.168.1.101 as the ip address in the DHCP offer message.

Option: (t=53,l=1) DHCP Message Type = DHCP Offer

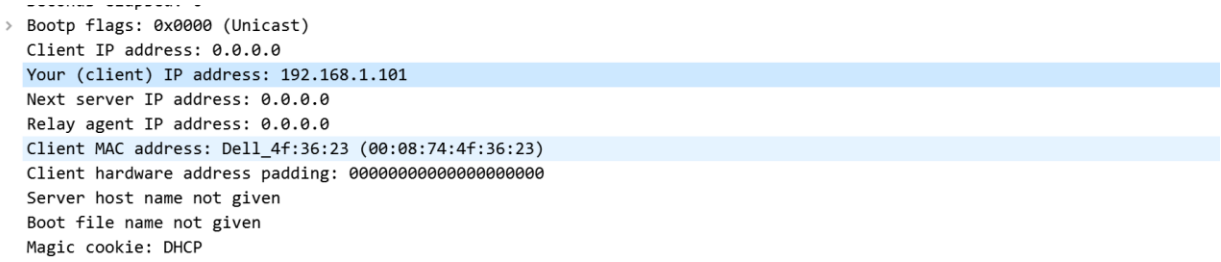
9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

The ip address being 0.0.0.0 indicates the absence of a relay agent. There is no relay agent in my experiment.

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

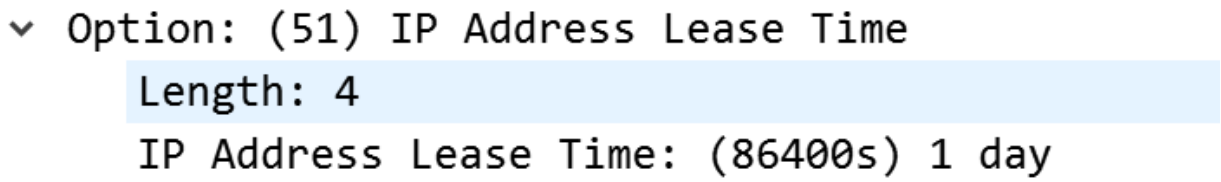
The IP address for the router identifies the default internet gateway. The subnet mask defines the subnet that is available.

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



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

The lease time is the amount of the time the user is allowed connection to the router.



IP Address Lease Time: 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 DHCP release message tells the dhcp server that you want to cancel the ip address offered. The DHCP server will not issue an ack of recipt of the client's DHCP request. If the release message is lost then the dhcp server retains the ip address until the lease time expires.

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.

Yes, there were arp packets sent and received to map the mac address with the ip address.

The ARP packets that show up are there in order to help sort out the MAC and IP addresses.