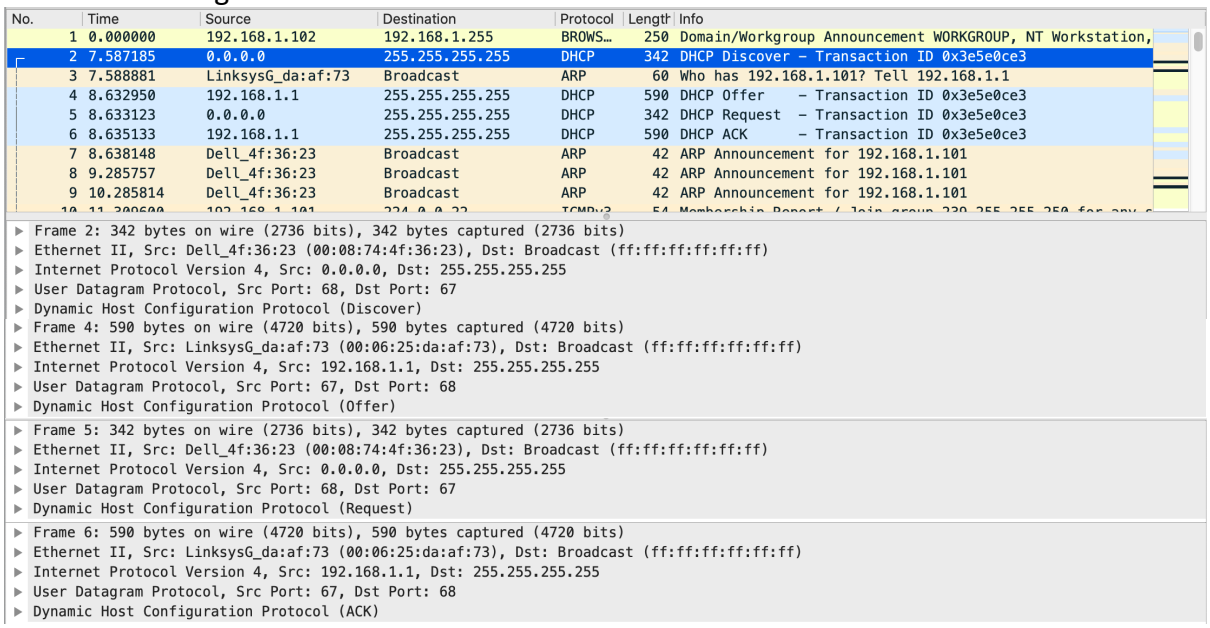
LAB 3 Report

Note: I'm unable to run Wireshark live on my MAC computer, thus, I choose to use data in the file *dhcp-ethereal-trace-1*.

Part 1: DHCP Answers

1. DHCP messages are sent over UDP

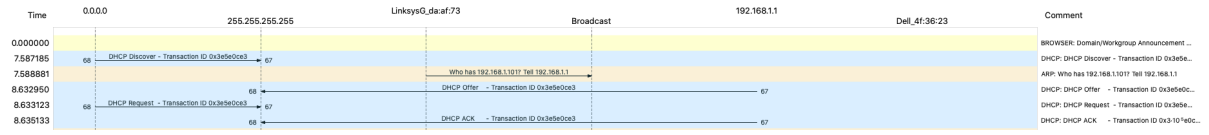


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	192.168.1.255	BROWS…	250	Domain/Workgroup Announcement WORKGROUP, NT Workstation,
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x3e5e0ce3
3	7.588881	LinksysG_da:af:73	Broadcast	ARP	60	Who has 192.168.1.101? 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	ARP Announcement for 192.168.1.101
8	9.285757	Dell_4f:36:23	Broadcast	ARP	42	ARP Announcement for 192.168.1.101
9	10.285814	Dell_4f:36:23	Broadcast	ARP	42	ARP Announcement for 192.168.1.101

```
▶ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), 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)
▶ 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
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▶ Dynamic Host Configuration Protocol (Offer)
▶ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), 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)
▶ Frame 6: 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
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▶ Dynamic Host Configuration Protocol (ACK)
```

2. DHCP uses client-server architecture

3. The DHCP flow graph:



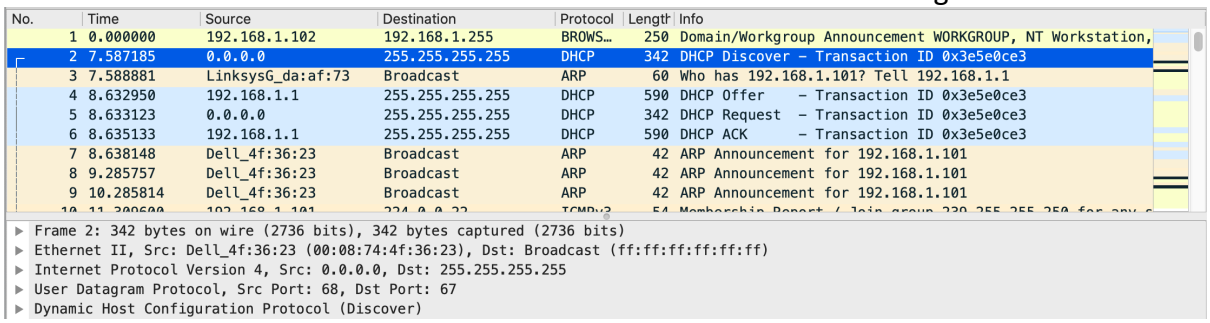
	Source port	Destination port
Discover packet	68	67
Offer packet	67	68
Request packet	68	67
ACK packet	67	68

4. The link-layer address of the host in hex format is 00:08:74:4f:36:23

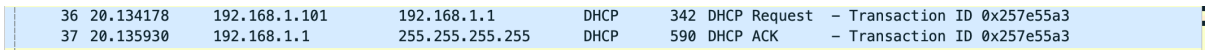
5. The message type value is a 1 for a discover message, but the message type value is 3 for a request message.

```
▶ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), 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: 0x3e5e0ce3
    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_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 (Discover)
      Length: 1
      DHCP: Discover (1)
▶ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▶ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), 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: 0x3e5e0ce3
    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_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)
      Length: 1
      DHCP: Request (3)
```

6. The value of the Transaction-ID in each of the first four DHCP messages is 0x3e5e0ce3



The value of the Transaction-ID in the second set (Request/ACK) of DHCP messages is 0x237e55a3.

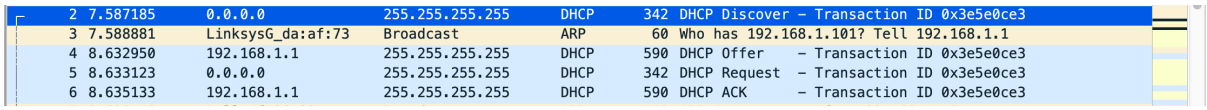


The transaction-ID is used to identify if a message is part of messages related to one transaction.

7.

	Source IP address	Destination IP address
Discover	0.0.0.0	255.255.255.255
Offer	192.168.1.1	255.255.255.255
Request	0.0.0.0	255.255.255.255

ACK	192.168.1.1	255.255.255.255



8. The IP address of my DHCP server is 192.168.1.1

9. The DHCP server offers 192.168.1.1 as the IP address in the DHCP offer message and the lease time is 1 day (86400s); The DHCP message with “DHCP Message Type = DHCP Offer” contains the offered DHCP address.

```
▼ Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
▼ Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
▼ Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 63.240.76.19
    Domain Name Server: 204.127.198.19
▼ Option: (15) Domain Name
    Length: 22
    Domain Name: ne2.client2.attbi.com
▼ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
▼ Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
▼ Option: (255) End
    Option End: 255
  Padding: 0000000000000000000000000000000000000000000000000…
```

10. DHCP server also provides network configuration information for the client.

11. In the given example, the IP address of relay agent is 0.0.0.0 indicates the absence of a relay agent. In my experiment, there is also no relay agent and the IP address of the agent is 0.0.0.0

12. The IP address for the router identifies the default Internet gateway for the client and the subnet mask defines which subnet is available.

13. The client accepts this IP address in the client’s response to the first server DHCP Offer message. The client’s requested IP address is in “Option: (50) Requested IP Address”.

```
▼ Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
▼ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
▼ Option: (50) Requested IP Address (192.168.1.101)
    Length: 4
    Requested IP Address: 192.168.1.101
```

14. The DHCP release message is used to tell the DHCP server to cancel the current IP address offered. The DHCP server does not issue an acknowledgment of receipt of the client’s DHCP request. If the client’s DHCP release message is lost, the DHCP server will wait and retains the IP address until the lease time expires.

15. Yes; Those ARP packets was used to map the MAC address with the IP address.

Part 2: ARP Answers

16. Each column contains the IP address, MAC address and protocol type respectively.

```
apple@appledeMacBook-Pro-54 ~ % arp -a
? (10.2.29.1) at cc:2d:e0:b5:7f:1d on en0 ifscope [ethernet]
? (10.2.29.252) at c4:2a:d0:e8:10:fe on en0 ifscope [ethernet]
? (10.2.29.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
```

17. The hexadecimal value for the source address is 00:d0:59:a9:3d:68; The hexadecimal value for the destination address is ff:ff:ff:ff:ff:ff

18. The hexadecimal value for the Ethernet Frame type field is 0x0806 for ARP.

19. a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    b) The hexadecimal value for opcode field within the ARP-payload of the request is 0x0001, for request.

    c) Yes;

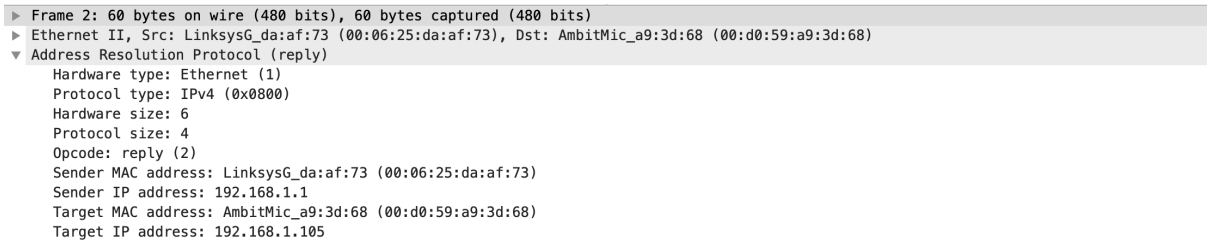
    d) In the “Target MAC address”

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▶ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

20. a) The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    b) The hexadecimal value for opcode field within the ARP-payload of the request is 0x0002, for reply.

    c) In the “Sender MAC address”



21. The hexadecimal value for the source address is 00:06:25:da:af:73 and the value for destination address is 00:d0:59:a9:3d:68 in the Ethernet frame containing the ARP reply message.

22. Because we are not located at the machine that used to send the request. The ARP request is broadcast, but the ARP reply is sent directly back to the sender's Ethernet address.