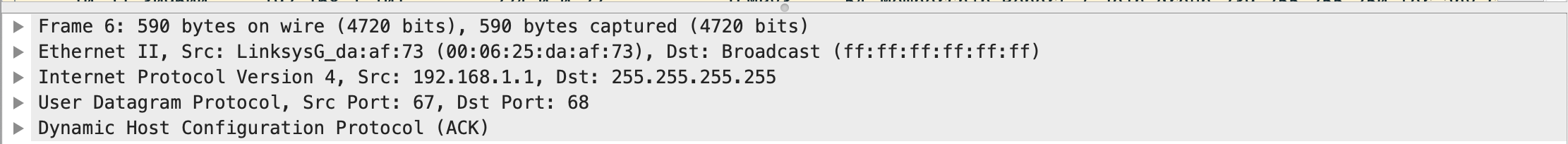
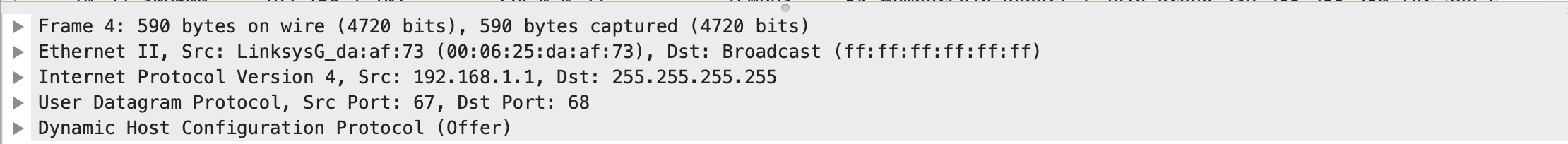
**LAB 3 Report**

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

A screenshot of a cell phone

Description automatically generated

1. DHCP uses client-server architecture
2. The DHCP flow graph:

A screenshot of a cell phone

Description automatically generated

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

1. The link-layer address of the host in hex format is 00:08:74:4f:36:23
2. The message type value is a 1 for a discover message, but the message type value is 3 for a request message.

A screenshot of a social media post

Description automatically generatedA screenshot of a social media post

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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

A screenshot of a cell phone

Description automatically generated

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



|  |  |  |
| --- | --- | --- |
|  | 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 |

A screenshot of a cell phone

Description automatically generated

1. The IP address of my DHCP server is 192.168.1.1
2. 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.

A screenshot of a cell phone

Description automatically generated

1. DHCP server also provides network configuration information for the client.
2. 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
3. The IP address for the router identifies the default Internet gateway for the client and the subnet mask defines which subnet is available.
4. 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”.

A close up of a logo

Description automatically generated

1. 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.
2. Yes; Those ARP packets was used to map the MAC address with the IP address.

**Part 2: ARP Answers**

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

A screenshot of a cell phone

Description automatically generated

1. 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
2. The hexadecimal value for the Ethernet Frame type field is 0x0806 for ARP.
3. 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”

A screenshot of a cell phone

Description automatically generated

1. 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”

A screenshot of a cell phone

Description automatically generated

1. 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.
2. 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.