# CPE 400: Homework 3

Due on April 14, 2024

*Igor Remizov Section 1001*

**Christopher Howe**

# Experiement prodedure

The goal of this experiment is to gain an understanding of how DHCP transactions occur. First, the machine's IP is released. Next wireshark is started to monitor what packets are part of the DHCP transaction. Then, a DHCP transaction is started to renew the lease twice. Then the lease is released and renewed one last time before finally stopping the wireshark capture. This all is accomplished using the Linux commands described below. Figure 1 shows all the packets captured in this experiment.

```
#!/bin/bash
sudo dhclient -v -r // release command, -v flag means verbose
sudo dhclient -v // renew command, -v flag means verbose
```

| | | | | | | |
|---|---|---|---|---|---|---|
| 285 | 28.270487806 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xe0d7743e |
| 286 | 28.378819366 | 192.168.86.1 | 192.168.86.66 | DHCP | 342 | DHCP Offer - Transaction ID 0xe0d7743e |
| 287 | 28.378960884 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0xe0d7743e |
| 288 | 28.394942202 | 192.168.86.1 | 192.168.86.66 | DHCP | 347 | DHCP ACK - Transaction ID 0xe0d7743e |
| 406 | 36.342458061 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x7760a7a |
| 407 | 36.456720871 | 192.168.86.1 | 192.168.86.66 | DHCP | 347 | DHCP ACK - Transaction ID 0x7760a7a |
| 468 | 43.237012600 | 192.168.86.66 | 192.168.86.1 | DHCP | 342 | DHCP Release - Transaction ID 0xf32ee06 |
| 499 | 46.642366641 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0x602bc865 |
| 528 | 49.730332288 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0x602bc865 |
| 529 | 49.733944894 | 192.168.86.1 | 192.168.86.66 | DHCP | 342 | DHCP Offer - Transaction ID 0x602bc865 |
| 530 | 49.734156523 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction ID 0x602bc865 |
| 531 | 49.741112342 | 192.168.86.1 | 192.168.86.66 | DHCP | 342 | DHCP Offer - Transaction ID 0x602bc865 |
| 532 | 49.751314623 | 192.168.86.1 | 192.168.86.66 | DHCP | 347 | DHCP ACK - Transaction ID 0x602bc865 |

Figure 1: DHCP Packets captured during this experiment

# Questions

## Question A - Generate a flow graph for the first transaction

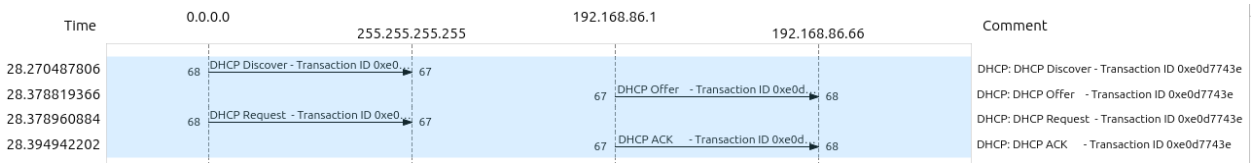


Figure 2: Flow Graph for the initial DHCP transaction performed

## Questions B and C - DHCP Transaction Source and Destination IP and Ports

The following chart describes which ports and IP addresses were used for the first DHCP transaction described in this experiment. The values found are shown in the screenshots shown below (figures 3 - 6)

Table 1: DHCP Packet Information

| DHCP Packet Name | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|
| Discover | 0.0.0.0 | 68 | 255.255.255.255 | 67 |
| Offer | 192.168.86.1 | 67 | 192.168.86.66 | 68 |
| Request | 0.0.0.0 | 68 | 255.255.255.255 | 67 |
| Acknowledge | 192.168.86.1 | 67 | 192.168.86.66 | 68 |

```
▸ Frame 285: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78), 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: 0xe0d7743e
    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: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Discover)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
```

Figure 3: Discover packet for the first DHCP Transaction, the source port is 68 and destination port is 67

```
▸ Frame 286: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0
▸ Ethernet II, Src: Google_a8:2a:96 (58:cb:52:a8:2a:96), Dst: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
▸ Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.66
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe0d7743e
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.86.66
    Next server IP address: 192.168.86.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▸ Option: (54) DHCP Server Identifier (192.168.86.1)
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (28) Broadcast Address (192.168.86.255)
  ▸ Option: (3) Router
  ▸ Option: (15) Domain Name
  ▸ Option: (6) Domain Name Server
  ▸ Option: (255) End
    Padding: 000000
```

Figure 4: Offer packet for the first DHCP Transaction, the source port is 67 and destination port is 68

```
▸ Frame 287: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78), 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: 0xe0d7743e
    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: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
    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: (54) DHCP Server Identifier (192.168.86.1)
  ▸ Option: (50) Requested IP Address (192.168.86.66)
  ▸ Option: (12) Host Name
  ▸ Option: (55) Parameter Request List
  ▸ Option: (255) End
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
```

Figure 5: Request packet for the first DHCP Transaction, the source port is 68 and destination port is 67

```
▸ Frame 288: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface wlo1, id 0
▸ Ethernet II, Src: Google_a8:2a:96 (58:cb:52:a8:2a:96), Dst: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
▸ Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.66
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe0d7743e
    Seconds elapsed: 0
  ▸ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.86.66
    Next server IP address: 192.168.86.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_a0:c3:78 (f8:ac:65:a0:c3:78)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (ACK)
  ▸ Option: (54) DHCP Server Identifier (192.168.86.1)
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (58) Renewal Time Value
  ▸ Option: (59) Rebinding Time Value
  ▸ Option: (1) Subnet Mask (255.255.255.0)
  ▸ Option: (28) Broadcast Address (192.168.86.255)
  ▸ Option: (3) Router
  ▸ Option: (15) Domain Name
  ▸ Option: (12) Host Name
  ▸ Option: (6) Domain Name Server
  ▸ Option: (255) End
```

Figure 6: ACK packet for the first DHCP Transaction, the source port is 67 and destination port is 68

## Question D and E - Transaction ID

The transaction ID for all 4 of the packets involved in this DHCP Transaction is "0xe0d7743e". This can be seen in all the packet screenshots in figures 3 - 6 in the transaction ID field. The transaction ID is a random string chosen by the client so that the DHCP server and client can differentiate different transactions. It also assists in debugging DHCP transactions since developers can tell which packets are responding to which transactions. The DHCP server can use this value to differentiate different requests, especially when multiple transactions are occurring at the same time.

## Question F - Differences between Request packet and Discover Packet

Many values differ between a request packet and a discover packet. They have different message types (option 53). The request packet additionally includes the DHCP Server Identifier field (option 54 with value 192.168.86.1) The requestion packet also additionally includes the requested DHCP address (option 50 with value 192.168.86.66) All of the IP/UDP information is the same between these two packets. These differences can be seen in figures 3 and 5

## Question G - Lease Times

The purpose of DHCP lease times is to make sure that the DHCP server can reclaim unused IPs. For example, if one device disconnects from the network and never comes back, then the DHCP server does not renew its lease allowing it to assign the IP to another device. This reduces the need to keep track of a large number of IPs. It also creates a more secure network by making sure that devices that are no longer authorized to access the network do not have an IP to access it.

In this experiment, the lease time is 86400 seconds or 1 day. This can be seen in figure 7.

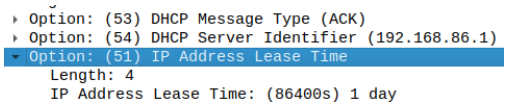


Figure 7: Acknowledgement packet specification of the lease time

## Question H - DHCP Releases

The purpose of the DHCP release message is to inform a DHCP server that a DHCP client no longer needs the address assigned to it. This can be done for a variety of reasons. For example, if a DHCP client is shutting down or moving to another network, it should release the IP it is currently using so that the DHCP server can assign it to another device without having to wait for the lease to expire. Additionally, releasing an IP can be done to troubleshoot network issues. Sometimes releasing and renewing an IP can resolve connection issues.

The DHCP server did not issue an acknowledgment of receipt of the DHCP release request. This is because the release request does not require the server to do anything. This is because if the client's DHCP release message is lost, nothing significant will happen. The DHCP server would still have a lease for the IP, but since the client would not request to renew that lease, the lease would eventually expire. This leads to the same outcome as if the release message reached the server. The only difference is that the lease would be held for its full duration instead of being returned to the pool of available IPs. The release packet from this experiment is shown in figure 8.

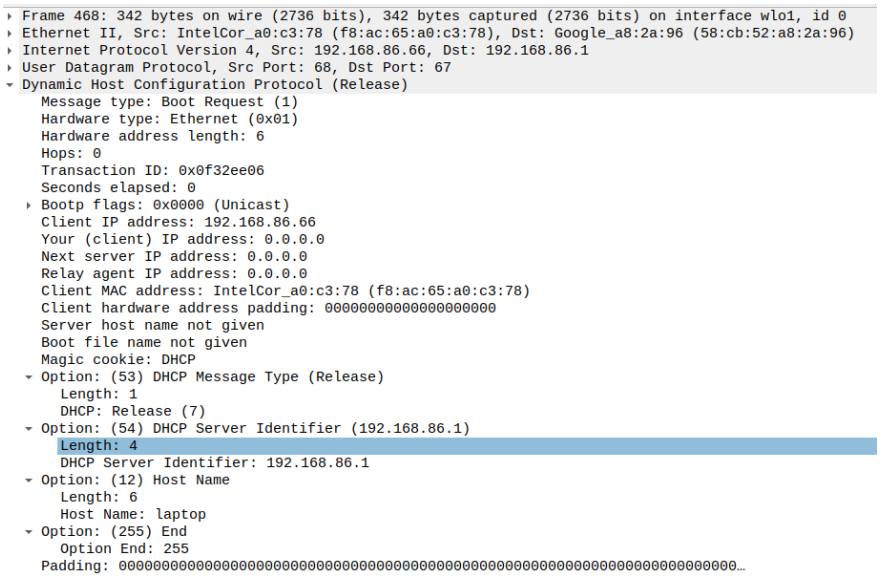


Figure 8: Release Packet From the experiment