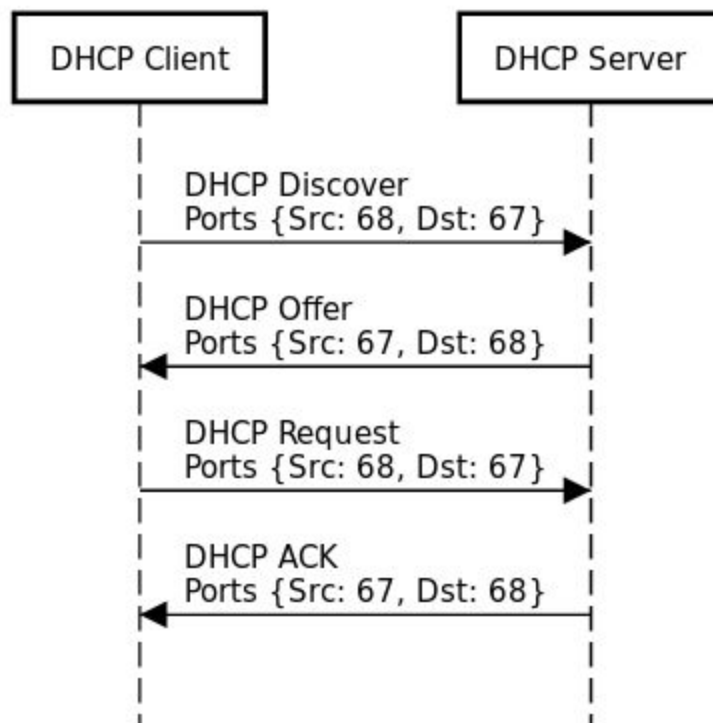Zachary Kaplan
CS356
DHCP Lab
4/13/17

Frame 98: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on
interface 0
Ethernet II, Src: HonHaiPr_59:00:19 (34:68:95:59:00:19), Dst: Cisco_77:e4:00
(00:25:46:77:e4:00)
Internet Protocol Version 4, Src: 10.200.205.210, Dst: 192.0.2.1
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Release)

1. DHCP runs over UDP.

DHCP Timing Diagram

2. Yes, the port numbers of my packets match that in the example (port 67 and 68).

Frame 112: 342 bytes on wire (2736 bits), 342 bytes captured (2736
bits) on interface 0
Ethernet II, Src: HonHaiPr_59:00:19 (34:68:95:59:00:19), 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
Bootstrap Protocol (Discover)

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x74f07121
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: HonHaiPr_59:00:19 (34:68:95:59:00:19)
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: (50) Requested IP Address
Option: (12) Host Name
Option: (55) Parameter Request List
Option: (255) End
Padding: 000000000000000000000000000000000000000000000000
```

3. The link-layer address of my device is 34:68:95:59:00:19.
4. The value for Option 53 is 3 in the Discover packet, while it is 1 in the Request packet.

```
112 6.536348515 0.0.0.0          255.255.255.255   DHCP   342 DHCP Discover - Transaction ID 0x74f07121
114 6.542536702 192.0.2.1        10.200.206.179    DHCP   450 DHCP Offer    - Transaction ID 0x74f07121
115 6.542678477 0.0.0.0          255.255.255.255   DHCP   342 DHCP Request  - Transaction ID 0x74f07121
116 6.545852517 192.0.2.1        10.200.206.179    DHCP   450 DHCP ACK      - Transaction ID 0x74f07121
156 7.544223948 0.0.0.0          255.255.255.255   DHCP   342 DHCP Request  - Transaction ID 0xf026bb73
163 7.598869888 192.0.2.1        10.200.206.179    DHCP   450 DHCP ACK      - Transaction ID 0xf026bb73
```

5. The Transaction ID for the first four packets is always 0x74f07121, while for the next two packets is always 0xf026bb73 (see above rightmost column). Clearly, the transaction differentiates between separate transaction, as the first four packets are the initial address renewal, and the final two packets are part of the redundant renewal.

```
Frame 112: 342 bytes on wire (2736 bits), 342 bytes captured (2736
bits) on interface 0
Ethernet II, Src: HonHaiPr_59:00:19 (34:68:95:59:00:19), 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
Bootstrap Protocol (Discover)
```

```
Frame 114: 450 bytes on wire (3600 bits), 450 bytes captured (3600
bits) on interface 0
Ethernet II, Src: Cisco_64:57:60 (b0:00:b4:64:57:60), Dst:
HonHaiPr_59:00:19 (34:68:95:59:00:19)
Internet Protocol Version 4, Src: 192.0.2.1, Dst: 10.200.206.179
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (Offer)

Frame 115: 342 bytes on wire (2736 bits), 342 bytes captured (2736
bits) on interface 0
Ethernet II, Src: HonHaiPr_59:00:19 (34:68:95:59:00:19), 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
Bootstrap Protocol (Request)

Frame 116: 450 bytes on wire (3600 bits), 450 bytes captured (3600
bits) on interface 0
Ethernet II, Src: Cisco_64:57:60 (b0:00:b4:64:57:60), Dst:
HonHaiPr_59:00:19 (34:68:95:59:00:19)
Internet Protocol Version 4, Src: 192.0.2.1, Dst: 10.200.206.179
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (ACK)
```

6. It can be seen that both packets that originate from the client use 0.0.0.0 as the client's source address, and 255.255.255.255 as the destination address (the server). Both responses from the server use 192.0.2.1 as the source address of the server (the server's real IP address), and use 10.200.206.179 for the destination address (the client). This client address seems to be the address the server ends up assigning to the client.

7. My DHCP server's address is 192.0.2.1.

```
Frame 114: 450 bytes on wire (3600 bits), 450 bytes captured (3600
bits) on interface 0
Ethernet II, Src: Cisco_64:57:60 (b0:00:b4:64:57:60), Dst:
HonHaiPr_59:00:19 (34:68:95:59:00:19)
Internet Protocol Version 4, Src: 192.0.2.1, Dst: 10.200.206.179
User Datagram Protocol, Src Port: 67, Dst Port: 68
Bootstrap Protocol (Offer)
        Message type: Boot Reply (2)
        Hardware type: Ethernet (0x01)
        Hardware address length: 6
```

Zachary Kaplan
CS356
DHCP Lab
4/13/17

```
Hops: 0
Transaction ID: 0x74f07121
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 10.200.206.179
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: HonHaiPr_59:00:19 (34:68:95:59:00:19)
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: (1) Subnet Mask
Option: (58) Renewal Time Value
Option: (59) Rebinding Time Value
Option: (51) IP Address Lease Time
Option: (54) DHCP Server Identifier
Option: (3) Router
Option: (15) Domain Name
Option: (6) Domain Name Server
Option: (119) Domain Search
Option: (44) NetBIOS over TCP/IP Name Server
Option: (255) End
Padding: 0000
```

8. The offered address to my device was 10.200.206.179. This was found in the DHCP Offer packet.
9. In both the example screenshot, and in my own packets, the Hops field was set to 0, indicating that no relay agents were involved in these DHCP transactions.
10. These lines indicate the gateway router for the client and which subnet the client should use respectively.

```
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
Bootstrap Protocol (Offer)
        Message type: Boot Reply (2)
        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: 192.168.1.101
        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 (Offer)
        Option: (1) Subnet Mask
        Option: (3) Router
        Option: (6) Domain Name Server
        Option: (15) Domain Name
        Option: (51) IP Address Lease Time
        Option: (54) DHCP Server Identifier
        Option: (255) End
        Padding: 0000000000000000000000000000000000000000000000...

    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
    Bootstrap 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)
              Option: (61) Client identifier
              Option: (50) Requested IP Address
              Length: 4
              Requested IP Address: 192.168.1.101
              Option: (54) DHCP Server Identifier
              Option: (12) Host Name
              Option: (60) Vendor class identifier
              Option: (55) Parameter Request List
              Option: (255) End
              Padding: 000000000000
```

11. The client did accept the offered IP address, as the Request message contained the option `Request IP Address` specifying the offered IP address, 192.168.1.101.

```
              ...
              Option: (51) IP Address Lease Time
              Length: 4
              IP Address Lease Time: (3600s) 1 hour
              ...
```

12. The purpose of an IP Address Lead Time is to ensure that if a device was allocated an address and does not release it, the address can still be readmitted to the address pool after a timeout (the lease time). Stops addresses from being lost forever. My lease time was 1 hour.

13. The release message signifies to the server that the released address can be readmitted to the available address pool. If an address was not released (or the release message was lost), the address would simply be readmitted after the lease time is up.

14. Yes, there were several ARP messages captured during these DHCP transaction. These messages allow the DHCP server to ensure that the IP address it is issuing to the requesting client is not already in use.