

## Lab #5: DHCP

### DHCP Experiment

1. The DHCP messages are sent over UDP.

No.	Time	Source	Destination	Protocol	Length	Info
4	21:32:28.136617	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x41e8f500
7	21:32:28.632040	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x41e8f500
64	21:32:35.876264	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x863007e0
67	21:32:36.619103	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x863007e0
105	21:32:45.114762	192.168.0.127	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0xc2832d01
136	21:32:46.979776	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf6e99016
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

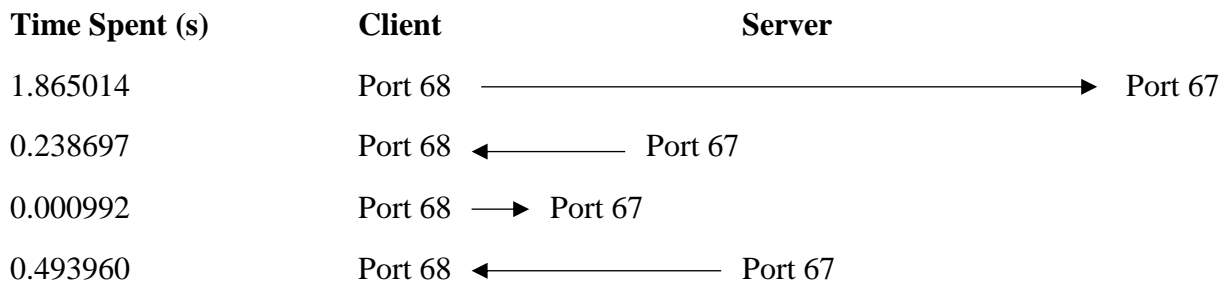
```

> Frame 4: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: ZyxelCom_97:36:c7 (10:7b:ef:97:36:c7)
> Internet Protocol Version 4, Src: 192.168.0.127, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
> Bootstrap Protocol (Request)

```

2.

### Timing Diagram:



The port number are the same as in the example given in this lab.

3. Link-Layer address of my host is 5c:51:4f:1c:96:a2

```

> Frame 4: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: ZyxelCom_97:36:c7 (10:7b:ef:97:36:c7)
> Internet Protocol Version 4, Src: 192.168.0.127, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
> Bootstrap Protocol (Request)

```

4. The only value that differentiates in the DHCP discover message from the DHCP request message is Option: (53) DHCP Message Type from Request to Discover, along with the deletion of Option: (54) DHCP Server Identifier and Option: (81) Client Fully Qualifies Domain Name.

### DHCP Discover Message:

136	21:32:46.970776	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347 DHCP Offer
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361 DHCP Request
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371 DHCP ACK

```

> Frame 136: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), 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 (68), Dst Port: 67 (67)
v Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf6e99016
  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_1c:96:a2 (5c:51:4f:1c:96:a2)
  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: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
  Padding: 000000

```

### DHCP Request Message:

136	21:32:46.970776	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347 DHCP Offer
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361 DHCP Request
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371 DHCP ACK

```

> Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), 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 (68), Dst Port: 67 (67)
v Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf6e99016
  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_1c:96:a2 (5c:51:4f:1c:96:a2)
  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
  > Option: (54) DHCP Server Identifier
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End

```

5. The value of the Transaction-ID in each of the four (Discover/Offer/Request/ACK) DHCP messages is 0xf6e99016

Unsure what second set (Request/ACK) set of DHCP messages is considered within my trace, but there are those first two sets whose Transaction-IDs are 0x41e8f500 and 0x863007e0.

No.	Time	Source	Destination	Protocol	Length	Info
4	21:32:28.136617	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x41e8f500
7	21:32:28.632040	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x41e8f500
64	21:32:35.876264	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x863007e0
67	21:32:36.619103	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x863007e0
105	21:32:45.114762	192.168.0.127	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0xc2832d01
136	21:32:46.979776	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf6e99016
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

The purpose of the Transaction-ID field is to identify each client transaction for the DHCP server.

6. If the IP address is not set until the end of the four-message exchange, the values of 255.255.255.255 and 0.0.0.0 are used in the IP datagrams in the four-message exchange.

No.	Time	Source	Destination	Protocol	Length	Info
136	21:32:46.979776	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf6e99016
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

7. The IP Address of my DHCP server is 192.168.0.1

No.	Time	Source	Destination	Protocol	Length	Info
4	21:32:28.136617	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x41e8f500

8. The IP address 192.168.0.127 is the DHCP server is offering to my host in the DHCP Offer message, which is also the DHCP message that contains the offered DHCP address.

No.	Time	Source	Destination	Protocol	Length	Info
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

<p>Frame 138: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0</p> <p>Ethernet II, Src: ZyxelCom_97:36:c7 (10:7b:ef:97:36:c7), Dst: IntelCor_Ic:96:a2 (5c:51:4f:1c:96:a2)</p> <p>Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.127</p> <p>User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)</p> <p>Bootstrap Protocol (Offer)</p> <p>Message type: Boot Reply (2)</p> <p>Hardware type: Ethernet (0x01)</p> <p>Hardware address length: 6</p> <p>Hops: 0</p> <p>Transaction ID: 0xf6e99016</p> <p>Seconds elapsed: 0</p> <p>Bootp flags: 0x0000 (Unicast)</p> <p>Client IP address: 0.0.0.0</p> <p>Your (client) IP address: <b>192.168.0.127</b></p> <p>Next server IP address: 192.168.0.1</p> <p>Relay agent IP address: 0.0.0.0</p> <p>Client MAC address: IntelCor_Ic:96:a2 (5c:51:4f:1c:96:a2)</p> <p>Client hardware address padding: 0000000000000000</p> <p>Server host name not given</p> <p>Boot file name not given</p> <p>Magic cookie: DHCP</p> <p>Option: (53) DHCP Message Type (Offer)</p> <p>Option: (54) DHCP Server Identifier</p> <p>Option: (51) IP Address Lease Time</p> <p>Option: (58) Renewal Time Value</p> <p>Option: (59) Rebinding Time Value</p> <p>Option: (1) Subnet Mask</p> <p>Option: (28) Broadcast Address</p> <p>Option: (15) Domain Name</p> <p>Option: (6) Domain Name Server</p> <p>Option: (3) Router</p> <p>Option: (255) End</p>						
---	--	--	--	--	--	--

9. The value of 0.0.0.0 indicates the absence of a relay agent. There is no relay agent in my experiment.

```
> Frame 4: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2), Dst: ZyxeCom_97:36:c7 (10:7b:ef:97:36:c7)
> Internet Protocol Version 4, Src: 192.168.0.127, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
✓ Bootstrap Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x41e8f500
  Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 192.168.0.127
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
```

10. The purpose of the router and subnet mask lines in the DHCP offer message is that the router line tells the client what the default gateway should be and the subnet mask line tells the client what subnet mask should be used.

No.	Time	Source	Destination	Protocol	Length	Info
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

```
> Ethernet II, Src: ZyxeCom_97:36:c7 (10:7b:ef:97:36:c7), Dst: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.127
> User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
✓ Bootstrap Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xf6e99016
  Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.0.127
  Next server IP address: 192.168.0.1
  Relay agent IP address: 0.0.0.0
  Client MAC address: IntelCor_1c:96:a2 (5c:51:4f:1c:96:a2)
  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
> Option: (51) IP Address Lease Time
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
✓ Option: (1) Subnet Mask
  Length: 4
  Subnet Mask: 255.255.255.0
> Option: (28) Broadcast Address
> Option: (15) Domain Name
> Option: (6) Domain Name Server
✓ Option: (3) Router
  Length: 4
  Router: 192.168.0.1
> Option: (255) End
```



11. The client does not accept this IP address in the client's response to the first server OFFER message. Where the source IP address is displayed within the header is where the client's requested address is at in the client's RESPONSE.

No.	Time	Source	Destination	Protocol	Length	Info
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016

12. The purpose of the lease time is to set a predetermined amount of time a device/client can have an offered IP address from the server.

The lease time in my experiment is 1 day (86400s).

No.	Time	Source	Destination	Protocol	Length	Info
4	21:32:28.136617	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x41e8f500
7	21:32:28.632040	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x41e8f500
64	21:32:35.876264	192.168.0.127	192.168.0.1	DHCP	349	DHCP Request - Transaction ID 0x863007e0
67	21:32:36.619103	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0x863007e0
105	21:32:45.114762	192.168.0.127	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0xc2832d01
136	21:32:46.979776	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf6e99016
138	21:32:47.218473	192.168.0.1	192.168.0.127	DHCP	347	DHCP Offer - Transaction ID 0xf6e99016
139	21:32:47.219465	0.0.0.0	255.255.255.255	DHCP	361	DHCP Request - Transaction ID 0xf6e99016
144	21:32:47.713425	192.168.0.1	192.168.0.127	DHCP	371	DHCP ACK - Transaction ID 0xf6e99016

> Frame 7: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface 0

> Ethernet II, Src: ZyxelCom\_97:36:c7 (10:7b:ef:97:36:c7), Dst: IntelCor\_1c:96:a2 (5c:51:4f:1c:96:a2)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.127

> User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)

> Bootstrap Protocol (ACK)

Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x41e8f500  
Seconds elapsed: 0  
Bootp flags: 0x0000 (Unicast)  
Client IP address: 192.168.0.127  
Your (client) IP address: 192.168.0.127  
Next server IP address: 192.168.0.1  
Relay agent IP address: 0.0.0.0  
Client MAC address: IntelCor\_1c:96:a2 (5c:51:4f:1c:96:a2)  
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  
Option: (51) IP Address Lease Time  
Length: 4  
IP Address Lease Time: (86400s) 1 day

13. The purpose of the DHCP release message is to end early the assigned IP address offered by the server to client. The DHCP server does not issue an acknowledgement of receipt of the client's DHCP request. If the client's DHCP release message is lost, then the server would just have to wait till the lease time of that client's IP address is up/has expired in order to have that certain IP address ready for another client's use again.
14. Yes, there were some ARP packets sent/received during the DHCP packet-exchange period. The purpose of those ARP packets is to make sure that the potential offered IP address for the client is not use by another client already.