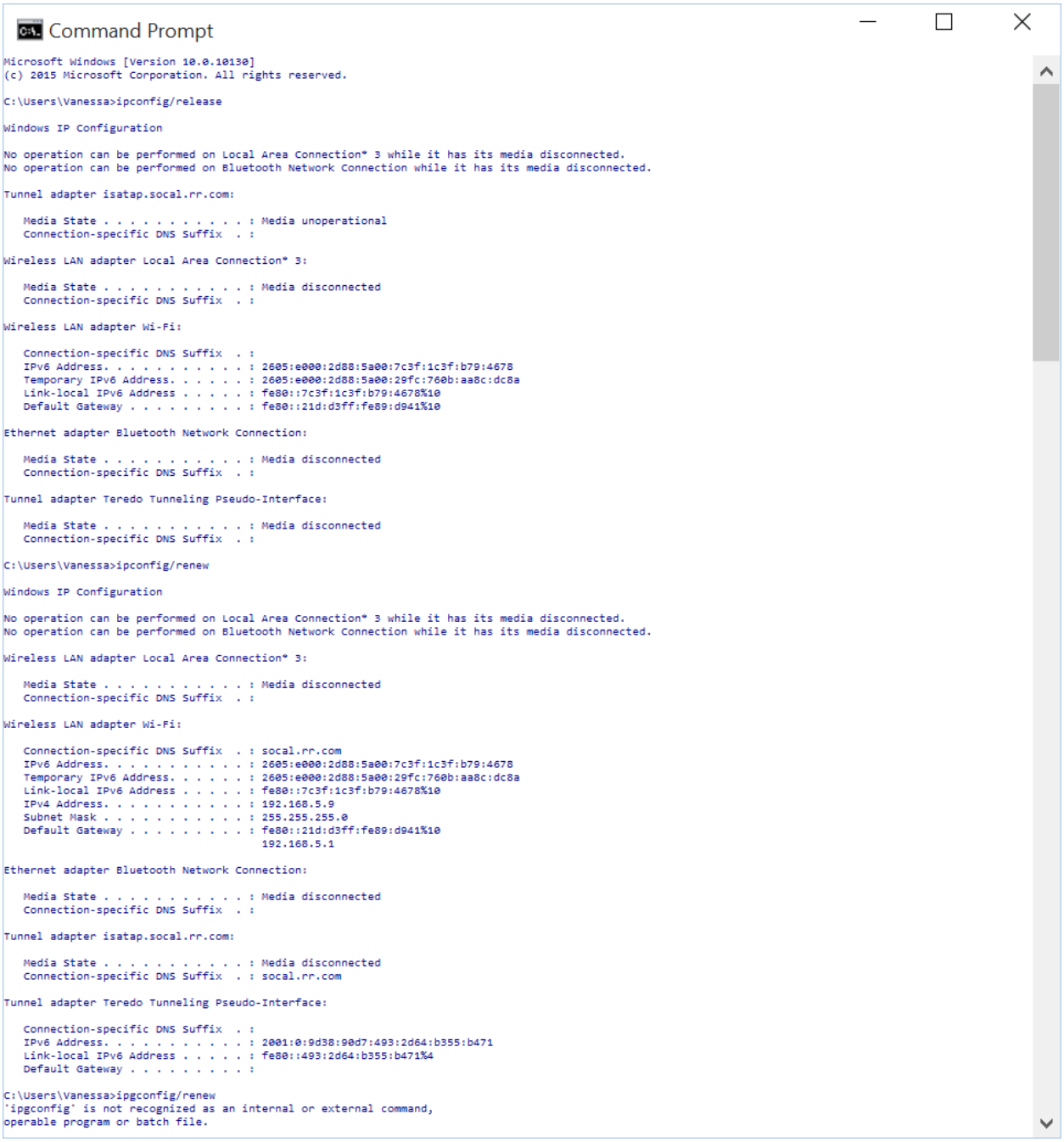
Vanessa Ulloa

Daniel Kushner

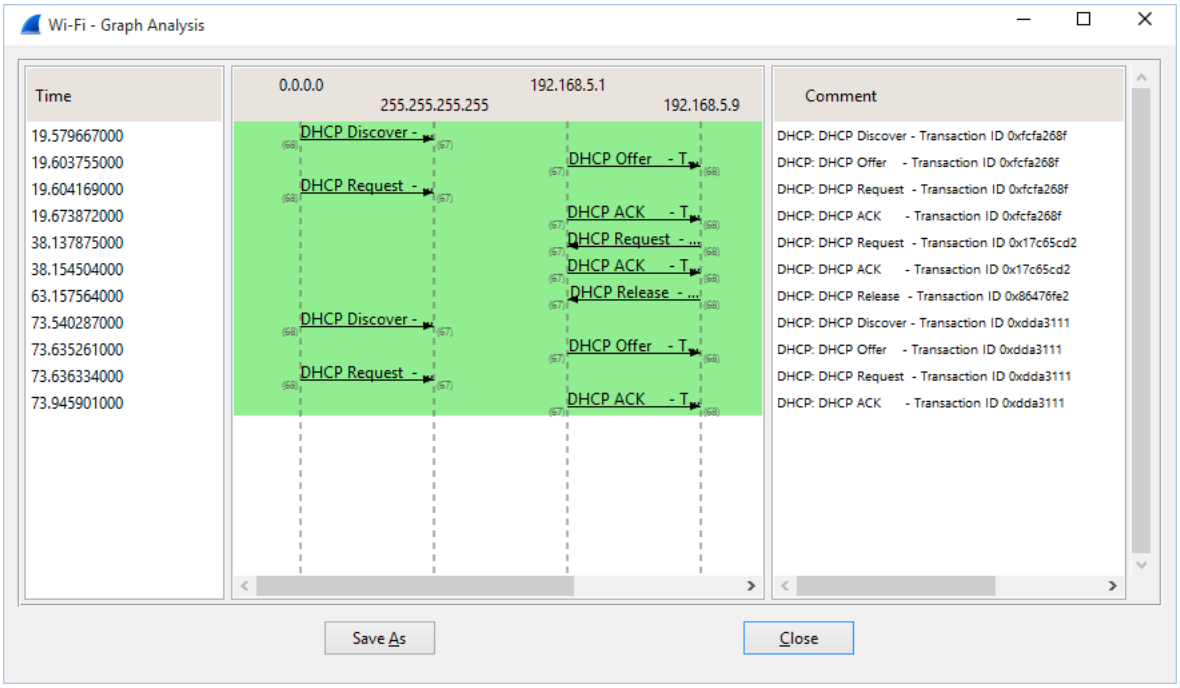
CST 311

09 June 2015

Lab 6



1. Are DHCP messages sent over UDP or TCP?
    a. UDP
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?




    a. Not quite, 255.255.255.255 is the same however 192.168.2.1 is 192.168.5.9
3. What is the link-layer (e.g., Ethernet) address of your host?

```
⊞ Frame 141: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
⊟ Ethernet II, Src: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
⊞ Bootstrap Protocol (Discover)
```

    a. 50:1a:c5:ec:d6:73

4. What values in the DHCP discover message differentiate this message from the DHCP request message?
    a. The discover message has Option: (53) DHCP Message Type (Discover)
    b. The request message has Option: (53) DHCP Message Type (Request)
5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 141 | 19.5796670 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xfcfa268f |
| 142 | 19.6037550 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP Offer - Transaction ID 0xfcfa268f |
| 143 | 19.6041690 | 0.0.0.0 | 255.255.255.255 | DHCP | 359 | DHCP Request - Transaction ID 0xfcfa268f |
| 144 | 19.6738720 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP ACK - Transaction ID 0xfcfa268f |
| 933 | 38.1378750 | 192.168.5.9 | 192.168.5.1 | DHCP | 347 | DHCP Request - Transaction ID 0x17c65cd2 |
| 934 | 38.1545040 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP ACK - Transaction ID 0x17c65cd2 |
| 1166 | 63.1575640 | 192.168.5.9 | 192.168.5.1 | DHCP | 342 | DHCP Release - Transaction ID 0x86476fe2 |
| 1549 | 73.5402870 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xdda3111 |
| 1589 | 73.6352610 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP Offer - Transaction ID 0xdda3111 |
| 1590 | 73.6363340 | 0.0.0.0 | 255.255.255.255 | DHCP | 359 | DHCP Request - Transaction ID 0xdda3111 |
| 1607 | 73.9459010 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP ACK - Transaction ID 0xdda3111 |

a. 0xfcfa268f
b. 0x17c65cd2
c. It keeps the “sets” of requests separate from one another

6. A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 141 | 19.579667000 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xfcfa268f |
| 142 | 19.603755000 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP Offer - Transaction ID 0xfcfa268f |
| 143 | 19.604169000 | 0.0.0.0 | 255.255.255.255 | DHCP | 359 | DHCP Request - Transaction ID 0xfcfa268f |
| 144 | 19.673872000 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP ACK - Transaction ID 0xfcfa268f |

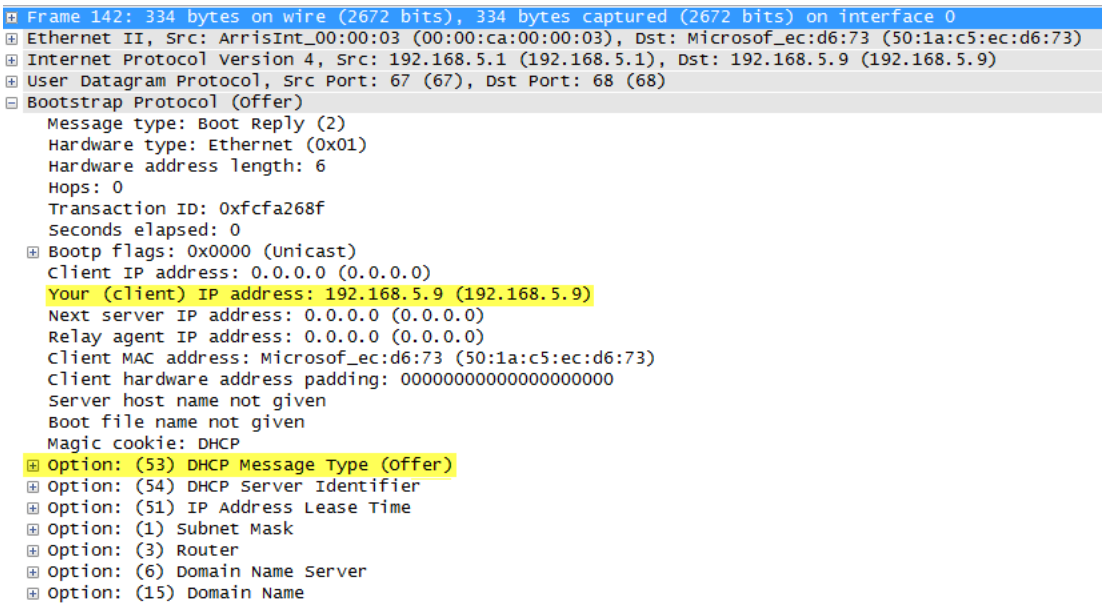
a. The client and server both use 255.255.255.255, the client uses 0.0.0.0 as a source and the server uses 255.255.255.255

7. What is the IP address of your DHCP server?

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 141 | 19.579667000 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction ID 0xfcfa268f |
| 142 | 19.603755000 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP Offer - Transaction ID 0xfcfa268f |
| 143 | 19.604169000 | 0.0.0.0 | 255.255.255.255 | DHCP | 359 | DHCP Request - Transaction ID 0xfcfa268f |
| 144 | 19.673872000 | 192.168.5.1 | 192.168.5.9 | DHCP | 334 | DHCP ACK - Transaction ID 0xfcfa268f |

a. 192.168.5.1

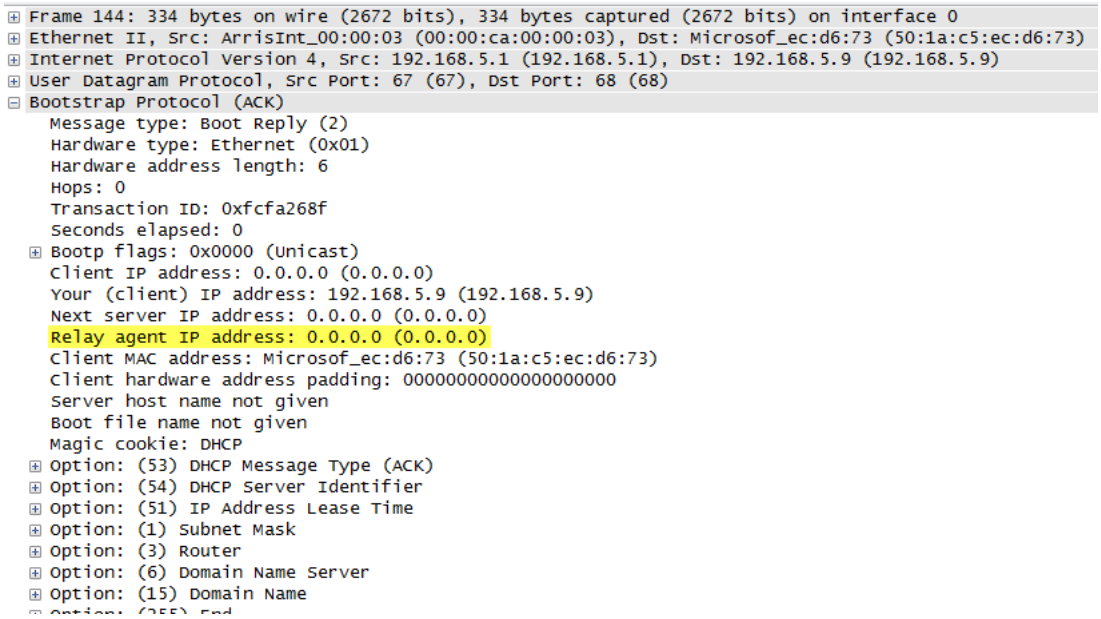
8. What is the IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message containers the coffered DHCP address.




a. 192.158.243.92

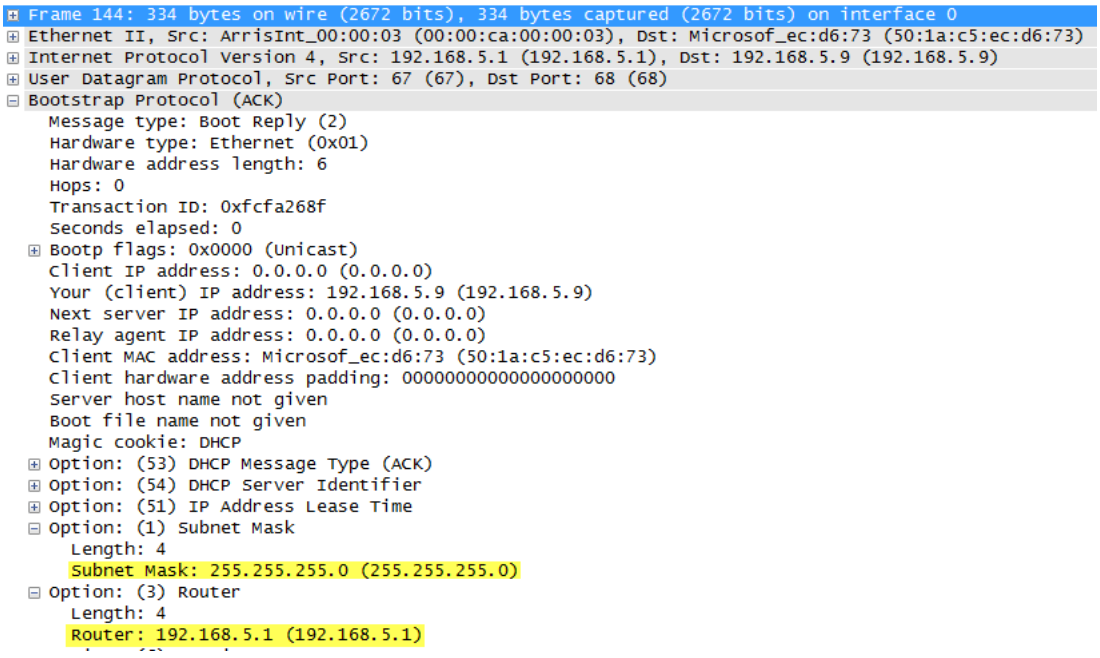
b. Message containers Option: (53) DHCP Message Type (Offer)

9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?



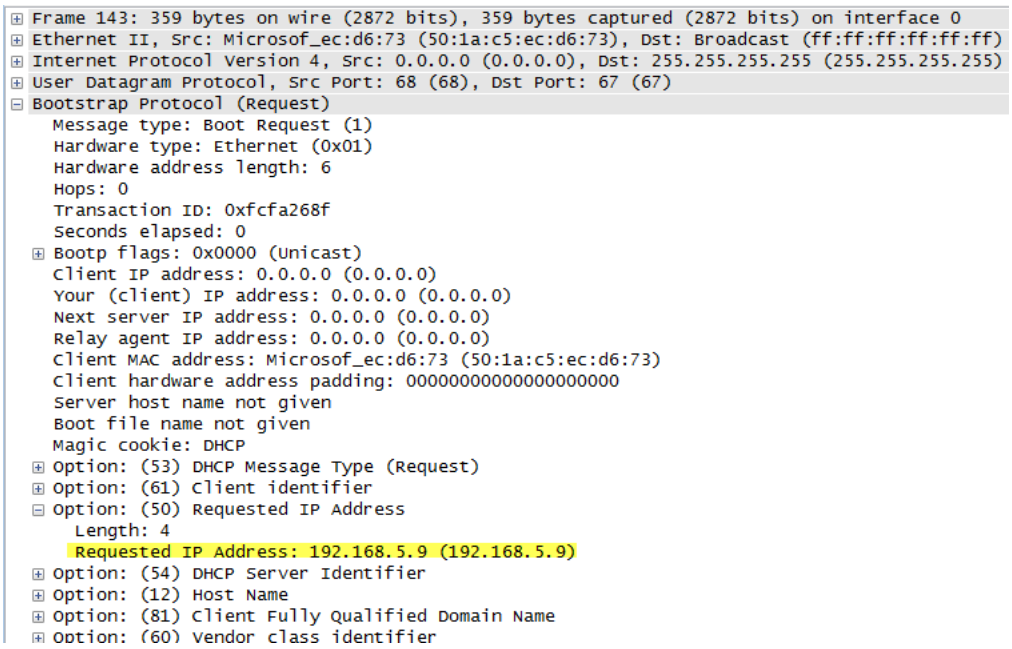

a. There is no IP address identified for the Relay agent IP address in the ACK message.

10. Explain the purpose of the router and the subnet mask lines in the DHCP offer message




a. The Router line tells the client what the default is
b. The Subnet Mask line tells the client what the mask should be

11. In the DHCP trace file noted in footnote 2, the HDCP server offers a specific IP address to the client (see also question 8. Above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?




a. The host requested IP address 192.168.5.9

12. Explain the purpose of the lease time. How long is the lease time in your experiment?

    a. The least time is how long the client is assigned the IP address, the IP address will not be assigned to another client during this time or until it is released.

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?
    a. The release message is basically a cancellation notice on the IP address assigned to the client by the server. If it is lost then the IP address will be automatically released when the lease time is up.
14. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.
    a. Yes, these are sent to make sure the IP address is not already assigned to another client.