Maxwell Sullivan: Computer Science
This blog was created to submit assignments for CSC251

Wireshark Lab 9: DHCP

April 7, 2013
Lab Video:

http://www.youtube.com/watch?v=P7ulCo2PnDU&feature=youtu.be (http://www.youtube.com/watch?v=P7ulCo2PnDU&feature=youtu.be)

Steps:

1. Begin by opening the Windows Command Prompt application. As shown in Figure 1, enter "ipconfig /release".

2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.

3. Now go back to the Windows Command Prompt and enter "ipconfig /renew". This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108

4. Wait until the "ipconfig /renew" has terminated. Then enter the same command "ipconfig /renew" again.

5. When the second "ipconfig /renew" terminates, enter the command "ipconfig/release" to release the previously-allocated IP address to your computer.

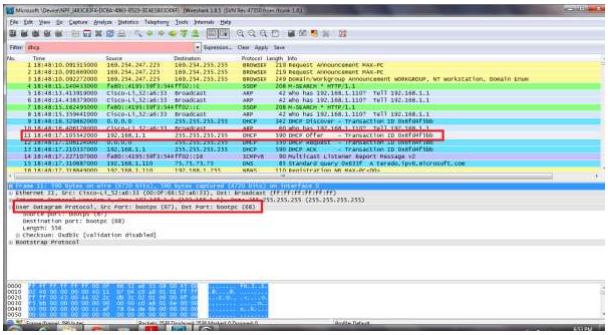
6. Finally, enter "ipconfig /renew" to again be allocated an IP address for your computer.

7. Stop Wireshark packet capture.

Questions:

1. Are DHCP messages sent over UDP or TCP?

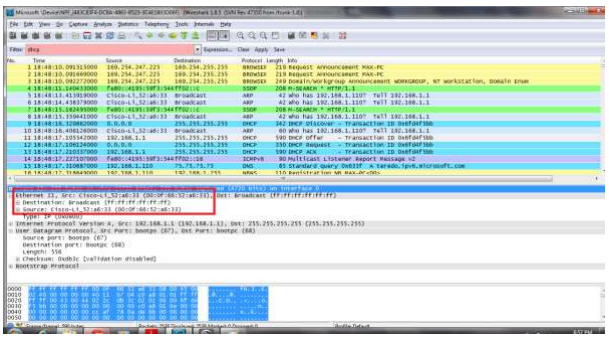
The DHCP messages are sent via UDP.



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-1.png)

3. What is the link-layer (e.g., Ethernet) address of your host?

The ethernet address of my host is 00:0f:66:52:a6:33



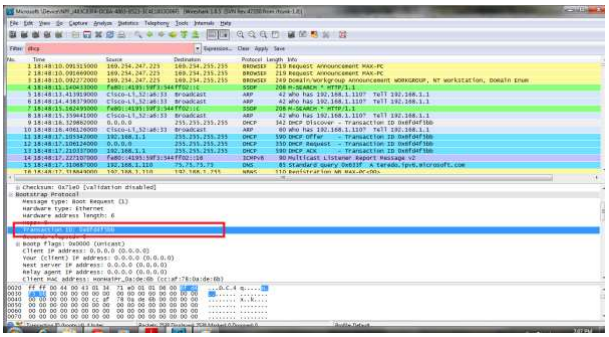
(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-3.png)

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

DHCP Message Type
Request includes a server identifier field

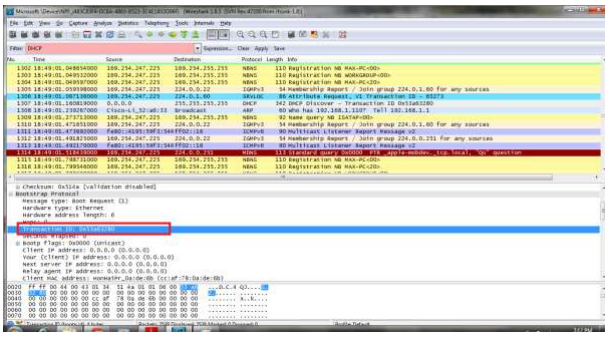
5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

1st set of messages: 0x6fd4f5bb



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-5.png)

2nd Set of messages: 0x53a63280



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-5b.png)

Purpose: The transaction ID is different so that the host can differentiate between different requests made by the user.

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.

Discover: 0.0.0.0/255.255.255.255

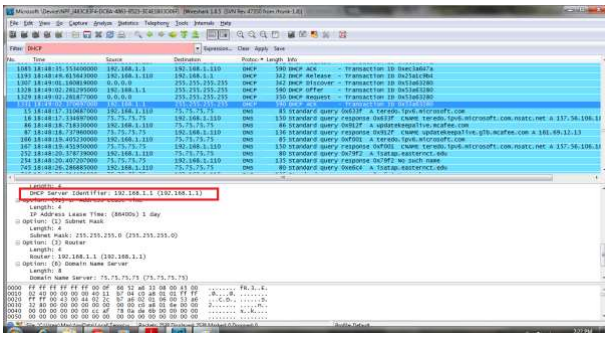
Offer: 192.168.1.1/255.255.255.255

Request: 0.0.0.0/255.255.255.255

ACK:192.168.1.1/255.255.255.255

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

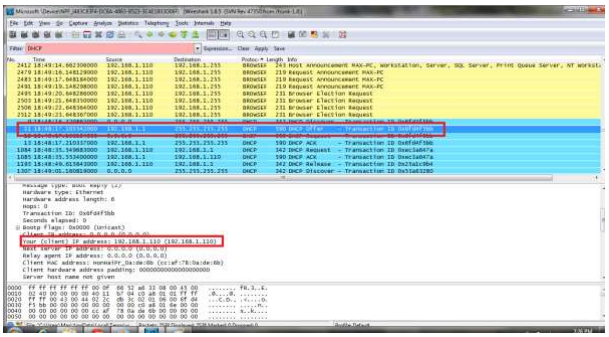
192.168.1.1



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-7.png)

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

My client is offered 192.168.1.10 by the DHCP server. The offer message contains the DHCP address offered by the server



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-8.png)

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?

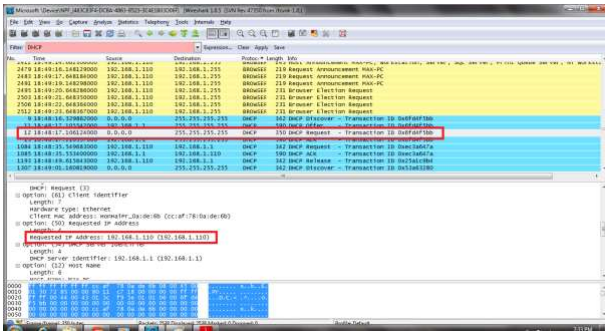
In the example given, the value that indicates there is no relay agent is 0.0.0.0, in the case of my capture, I also have a value for the relay agent of 0.0.0.0 indicating that I too did not have a relay agent.

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

The subnet mask line tells the client which subnet mask to use.
The router line indicates where the client should send messages by default.

11. In the DHCP trace file noted in footnote 2, the DHCP 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?

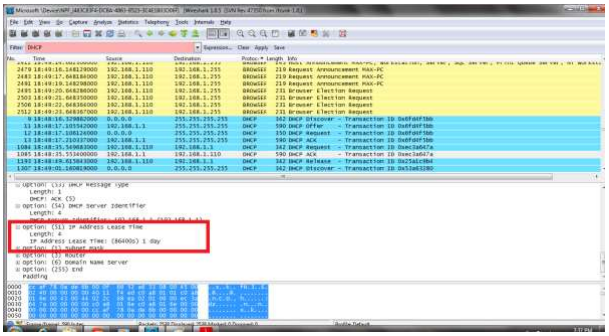
The client accepts the IP address given in the offer message within the request message. After being offered the IP address 192.168.1.110 in the offer message, my client sent back a message further requesting that specific IP address.



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-11.png)

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

The purpose of lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one.
The lease time in my experiment is 86400 seconds or 1 day



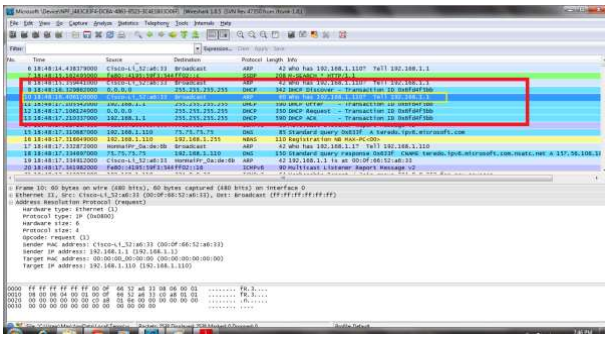
(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-12.png)

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?

The purpose of the release message is to release the IP address back to the server.
There is no verification that the release message has been received by the server.
If the message is lost, the client releases the IP address, but the server will not reassign that address until the clients lease on the address expires.

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.

Yes, they appear to be broadcasts sent out by the network to build up the known IP addresses by the clients network.



(https://maxwellsullivan.wordpress.com/wp-content/uploads/2013/04/9-15.png)

From → Wireshark Labs

Leave a Comment