CPE 400/600: Computer Communication Networks

HW 3 (Total 26.6 points)

1. DHCP experiment

In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands.

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). Enter "*ipconfig /release*". The executable for *ipconfig* is in C:\windows\system32. This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.

2. Start up the Wireshark packet sniffer 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.

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.

If you are using linux, use the following commands. Note that, the commands may vary depending on linux distributions.

sudo dhclient -v -r (release, -v for verbose)
sudo dhclient -v (renew, -v for verbose)

Now let's take a look at the resulting Wireshark window. To see only the DHCP packets, you may need to enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68.)

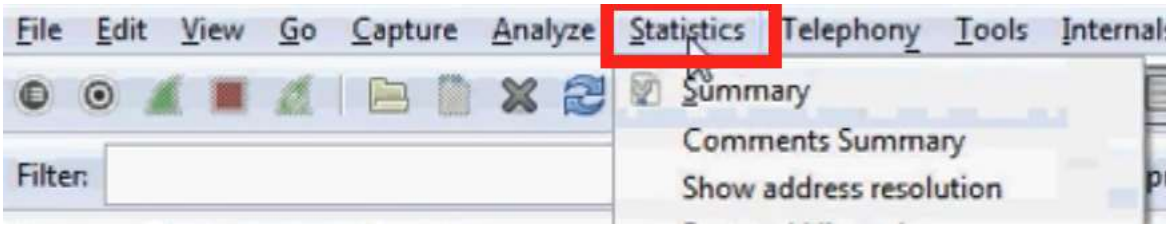
[Important Note for experiments: When answering the Wireshark questions, you must take screen shots of the appropriate messages and indicate where in the message you've found the information that answers the questions.]

Answer the following questions:

Make sure you set the filter for "bootp" as described above previously

a) Generate a Flow Graph illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server as captured by Wireshark.

To generate the Flow Diagram, in Wireshark, after completing above steps 1-7, click on "Statistics" tab:



Click on Flow Graph

Change the filter on the next screen to “Displayed packets” to only see DHCP related content

Capture the screenshot(s) showing the sequence and details for each of the 4-step process for DHCP that you will see on the Flow Graph.

b) **For each of the 4 DHCP packets** (you may either work off of the graph data, or return to the main display and expand the messages and look into the details), indicate the source and destination port numbers.

Best, if you organize your answer by listing Discover/Offer/Request/ACK DHCP, and capture screenshots and comments under each of them.

c) **For each of the 4 DHCP packets** indicate the source and destination IP addresses that are carried in the encapsulating IP datagram (include screenshots).

Best, if you organize your answer by listing Discover/Offer/Request/ACK DHCP, and capture screenshots and comments under each of them.

d) What are the values of the Transaction-ID **in each** packet of the first four lines (Discover/Offer/Request/ACK) DHCP messages?

e) What is the purpose of the Transaction-ID field?

f) What values in the DHCP discover message differentiate this message from the DHCP request message?

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

h) 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?