COMPUTER NETWORKS – LAB 2

PART 1: IP Protocol

Steps

1. Start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen

2. If you are using a Windows platform, start up pingplotter (search for it on Google) and enter the name of a target destination in the "Address to Trace Window." Enter 3 in the "# of times to Trace" field, so you don't gather too much data. Select the menu item Edit->Advanced Options->Packet Options and enter a value of 56 in the Packet Size field and then press OK. Then press the Trace button

3. Send a set of datagrams with a longer length, by selecting Edit->Advanced Options->Packet Options and enter a value of 2000 in the Packet Size field and then press OK. Then press the Resume button.

4. Finally, send a set of datagrams with a longer length, by selecting Edit->Advanced Options->Packet Options and enter a value of 3500 in the Packet Size field and then press OK. Then press the Resume button.

5. Stop Wireshark tracing.

Questions (answer by typing the text below the questions and insert the screenshots if needed):

1. What is the IP address of your computer?

2. Within the IP packet header, what is the value in the upper layer protocol field?

3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

7. Describe the pattern you see in the values in the Identification field of the IP datagram

8. What is the value in the Identification field and the TTL field?

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotterto be 2000. Has that message been fragmented across more than one IP datagram?

11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

13. What fields change in the IP header between the first and second fragment?

14. How many fragments were created from the original datagram?

15. What fields change in the IP header among the fragments?

PART 2: DHCP Protocol

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 (answer by typing the text below the questions and insert the screenshots if needed):

1. Are DHCP messages sent over UDP or TCP?

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

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

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?

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.

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

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.

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?

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

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?

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

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?

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.