CS3506 Lab 1 - Wireshark UDP/DHCP.

In this lab, we'll explore several aspects of the User Datagram Protocol and the Dynamic Host Configuration Protocol:

- UDP traffic generated by DNS queries
- The format and content of a UDP packet;
- Traffic generated by DHCP messages;
- The format and contents of a DHCP packet.

Please boot into Kubuntu Linux, and use the following credentials to login:

User:	shark
Password:	shark1ng

You have to run Wireshark as the root user, so at the command line type "**sudo wireshark**" (without the quotation marks). When prompted for a password please enter the password above.
You may first also need to run "**xhost +**" to ensure that the X Window System allows Wireshark access to the display.

UDP

We will produce some UDP traffic. Start the packet capture. Run "**nslookup www.ucc.ie**". When nslookup finishes, stop the capture. DNS queries use UDP.
Filter the packets displayed in the Wireshark window by entering "**udp.port == 53**" (lowercase, no quotes, and don't forget to press return after entering!) into the display filter specification window towards the top of the Wireshark window. What you should see is some UDP messages sent from your computer to your DNS server.

• Now answer questions 1.1-1.6

DHCP

In this lab, we will examine the packets transmitted during a DHCP handshake. Since the lab PCs are using the network to mount network drives (and your home directories), we will be using a trace file previously captured by wireshark. Make sure you have downloaded **dhcp tracefile (dhcp.pcap)** from **CS3506 course website**. The DHCP messages in the trace are the result of the following commands (you can repeat them on your personal computer, but not on the lab PCs):

	Linux	Windows
1. Release IP address	**sudo dhclient -r**	**ipconfig /release**
2. Begin packet capture	*Begin packet capture*	*Begin packet capture*
3. Obtain an IP address	**sudo dhclient**	**ipconfig /renew**
4. Renew IP address	**sudo dhclient**	**ipconfig /renew**
5. Release IP address	**sudo dhclient -r**	**ipconfig /release**
6. Obtain an IP address	**sudo dhclient**	**ipconfig /renew**
7. Stop packet capture	*Stop packet capture*	*Stop packet capture*

To see only the DHCP packets, 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. To see DHCP packets in the current version of wireshark, you need to enter "**bootp**" and not "**dhcp**" in the filter.)
Step 3 caused four DHCP packets to be generated, a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

• Now answer questions 2.1-2.9

Submission - LAB 1: UDP-DHCP

Please submit during this lab session or else at next week's lab session.

***Student name:*__________________________ *Student ID:*______________________**

1. UDP

1.1. Select one UDP packet. From the packet content field, name and determine the length (in bytes) of each of the UDP header fields.

1.2. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

1.3. Input to the network interface is zeroes and ones. How does it know where the next frame starts? Based on the headers you see (Ethernet, IP, UDP), what is the maximum frame size?

1.4. Based on information in the UDP header alone, what is the highest possible source port number? Explain your answer.

1.5. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

1.6. Consider a system using Ethernet/IP/UDP, with a maximum Ethernet Frame size of 500 bytes + the three last digits of your student number. What is the maximum number of bytes of UDP payload supported?

2. DHCP

2.1. Draw a time sequence diagram illustrating the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicate the source and destination port numbers.

2.2. What is the link-layer (i.e., Ethernet) address of the host sending the DHCP Discover message?

2.3. What is the purpose of having a DHCP discover and a DHCP request message? Why are they both needed?

2.4. What is the purpose of the Transaction-ID field?

2.5. 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), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

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

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

2.8. Explain the purpose of the lease time.

2.9. 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?