**CS3506 Lab 1 - Wireshark UDP/DHCP.**

In this lab, we will 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.

It is assumed that you are running Wireshark using Ubuntu Linux.

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 your password for the admin user

You may first also need to run “**xhost +**” to ensure that the X Window System allows Wireshark access to the display.

**UDP**

We will first produce some UDP traffic. Start the packet capture in Wireshark and then run “**nslookup www.ucc.ie**”. When nslookup finishes, stop the capture on Wireshark.

nslookup is a program that generates a DNS query, and this is sent using UDP by default.

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 area towards the top of the Wireshark window. What you should see is a set of UDP messages sent between your computer and the configured name server. DNS servers use port 53 by default so that is why we use it in the filter.

*Now answer the relevant questions of the assignment*

**DHCP**

Next we will examine the packets transmitted during a DHCP handshake. We will be using a trace file previously captured by Wireshark called **dhcp.pcap** and available via the Canvas page. The DHCP messages in the trace are the result of the following command sequence – you may wish to see if you can run this on your own computer and live capture the DHCP packets.

| **DHCP action** | **Linux command** |
| --- | --- |
| *1. Release IP address* | sudo dhclient -r |
| *2. Begin packet capture* | *Begin packet capture* |
| *3. Obtain an IP address* | sudo dhclient |
| *4. Renew IP address* | sudo dhclient |
| *5. Release IP address* | sudo dhclient -r |
| *6. Obtain an IP address* | sudo dhclient |
| *7. Stop packet capture* | *Stop packet capture* |

To see only the DHCP packets, enter into the Wireshark filter field “**bootp**”. (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68.)

Note that Action 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 the relevant questions of the assignment*