## CT2108 Lab – Network Utilities and ARP / DNS / ICMP Packet Analysis

The purpose of this lab session is to learn about and experiment with some useful network utilities that are available on most PCs and Laptops. Start Wireshark running on your PC or laptop then open a command prompt on your computer and issue the following commands. Take some time to understand what each command is doing and what information is being displayed. Note that due to firewall restriction within the University and HEAnet some of these commands, particularly traceroute, may not work fully or give complete results. However, they should work fine on your home internet connection:

```
C:\> arp –a              C:\arp –d *

C:\> ipconfig /all       C:\ipconfig /displaydns      C:\> ipconfig /flushdns

C:\> netstat –an         C:\> netstat –r

C:\> nslookup www.rte.ie

C:\> ping www.rte.ie   C:\> ping –f –l 1600 www.rte.ie

C:\> tracert -d www.rte.ie  (this probably won't work in the lab network)
```

Stop the Wireshark packet capture and answer the following questions:

1. What are the hexadecimal values for the source and destination MAC addresses in the Ethernet frame containing the ARP request messages?
2. What is the hex value for the two-byte Ethernet Frame type field in the ARP request message? What upper layer protocol does this correspond to?
3. What is the IP address of your host and what is the IP address of the destination host for the ping command? Why is it that an ICMP packet does not have source and destination port numbers?
4. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
5. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
6. Locate the DNS query and response messages. Are they sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port of DNS response message?
7. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
8. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
9. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
10. Why doesn't the ping –f –l 1600 command work properly? What is the maximum buffer size that will work with the ping command on your device?