CT2108 Lab Solutions - ARP / DNS / ICMP Packet Analysis

As explained in the live class, values of Mac / IP addresses will be different on your device.

1: Source MAC address: whatever is on your computer (e.g. 54:e0:32:9e:02:01)

destination MAC address: Broadcast to all (ff:ff:ff:ff:ff:ff)

2: The frame type is ARP (0x0806)

3a: Host: Something like 192.168.7.122 (private). Destination: 104.16.42.72 (public)

3b: ICMP packets merely exist to send messages and control signals between IP addresses, so there is no need for a source or destination port.

4: IMCP type is 8 (ping request) It also has a checksum, ID, sequence number and 32 bytes of data, the default for a ping command. Checksum: 2 bytes, Sequence number: 2 2-byte parts, ID: 2 2-byte fields.

5: IMCP type is 0 (ping reply). It has the same properties as a request ping, and the same data. Checksum: 2 bytes, Sequence number: 2 2-byte parts, ID: 2 2-byte fields.

6: UDP protocol is used. The DNS query destination port: 53 and the DNS response source port: 53

7: Query is sent to 192.168.20.10. There are two DNS servers, one with the IP above, and the other with IP 192.168.20.11.

8: The type is 0x0100 Standard query. It should have some answers.

9: The query should receive at least one answer that should look something like this:
10.20.168.192.in-addr-arpa: type PTR, class IN, ns1.it.nuigalway.ie

10: The ping command does not work because -f forbids fragmenting and the 1600-byte buffer is too large. The size limit for the ICMP payload is usually 1472 bytes on Ethernet networks which have an MTU of 1500 bytes. The maximum payload is then 1472 because the ICMP Header is 8 bytes and the IP Header is 20 bytes leaving 1472 for the ICMP Payload.