COMP247 Data Communications Laboratory

**Practical 2B IP**

Your Name:

Your Student ID:

**Documentation Task 1**.

1. Examine one of the ICMP messages. For its IP part match the fields to those listed in the IP lecture. Some fields have different labels. List the correspondence between these.

| Field | Size (bits) | Wireshark Terminology |
| --- | --- | --- |
| Version Number | 4 | Same |
| Header Length | 4 |  |
| Type of Service | 8 |  |
| Total Length | 16 |  |
| Idenfifiers | 16 |  |
| Flags | 3 |  |
| Packet Offset | 13 |  |
| Hop Limit | 8 |  |
| Protocol | 8 |  |
| CRC | 16 |  |
| Source Address | 32 |  |
| Destination Address | 32 |  |
| Options | 32 |  |

1. List the details from the ICMP messages of your ping attempt:

IP source address:

IP destination address:

TTL field:

Protocol field:

Type field of the ping (echo) request:

Type field of the ping (echo) response:

1. What differences are there between the equivalent messages in the four pairs of ping request and reply pairs?
2. From the information in the time columns of the Wireshark display calculate the time that elapses between the sending of each Echo request and the receipt of the corresponding Echo reply. Compare the maximum, average, and minimum of the delays with those provided by the PING command.
3. What is the delivered ‘data’ (see the field labelled ‘data’) in the ICMP messages? *Hint: you will see the data in hexadecimal and ASCII form in the bottom panel.*

**Documentation Task 2**.

1. List the IP addresses from the tracert output and the ICMP messages in the Wireshark capture. Do they match?
2. Do all the ICMP Echo (ping) request messages have the same destination IP address? What is it?
3. Is the type field in the ICMP section of all the ICMP time-to-live exceeded messages the same? What is it?
4. Is the delivered data in the ICMP messages for tracert the same as for the ping messages in task 1?
5. Find the difference between the ICMP Echo (ping) request messages in your capture. What is it and what purpose does it serve? (hint, it’s in the IP section)
6. The time-to-live exceeded message in the ICMP reply appears to be encapsulating the immediately previously sent ICMP echo (ping) request message. Is the encapsulated message **exactly** the same? If not, where does it differ and why do you think this is so?
7. Is there anything else worth noting about these messages, especially when compared to the similar messages generated for Ping?
8. ICMP is encapsulated within IP – does this make it a transport layer protocol? Explain your answer.

**Documentation Task 3**.

Examine the capture and answer the following questions

1. How many different computers were pinged?
2. List the IP addresses of the source computer, the computers pinged and the intervening nodes?
3. List the names of the computers pinged? *Hint: you will find these in DNS messages, so make sure you have cleared any filtering you might have set for ICMP messages.*
4. For each system pinged, did the ping request need to be fragmented and if so into how many pieces? Explain how you determined whether or not the datagram has been fragmented.
5. For each of the three sets of ping request messages, how many bytes are there (total, not fragmented) in the payload of the IP datagram? Explain how you determined the number of payload bytes.
6. How do you think a receiver of these fragments knows what order to put them together in? Specifically, what field is most important for this?
7. Examine the fields in the IP datagrams generated by these pings. What can you tell us about the values in them? We are especially interested in any patterns you can see in how the ways the fields in the fields change or how they stay constant