Data Communications Laboratory
IP Headers

Your Name: Jai Carey

Your Student ID: 45188416

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	**Version**
Header Length	4	**Header Length**
Type of Service	8	**Differentiated Services Field**
Total Length	16	**Same**
Identifiers	16	**Identification**
Flags	3	**Flags (Reserved Bit, Don't Fragment, More Fragment)**
Packet Offset	13	**Flags (Fragment Offset)**
Hop Limit	8	**Time To Live (TTL)**
Protocol	8	**Protocol**
CRC	16	**Header Checksum**
Source Address	32	**Source Address**
Destination Address	32	**Destination Address**
Options	32	**N/A (No options)**

2.

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

This is a ping command to www.facebook.com

IP source address: **192.168.1.245**

IP destination address: **157.240.8.35**

TTL field: **128**

Protocol field: **ICMP (1)**

Type field of the ping (echo) request: **8 (Echo (ping) request)**

Type field of the ping (echo) response: **0 (Echo (ping) reply)**

3. What differences are there between the equivalent messages in the four pairs of ping request and reply pairs?

Differences:

- **Source and Destination Addresses are flipped**
- **TTL is different (Request is 128, Reply is 58)**
- **Time is slightly different between pairs (less than an ms)**

4. 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.

Time differences:

- **Ping 1: 0.005902 sec**
- **Ping 2: 0.005453 sec**
- **Ping 3: 0.005428 sec**
- **Ping 4: 0.005899 sec**

Maximum: 5.902 ms

Minimum: 5.428 ms

Average: 5.6705 ms

5. 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.*

Both the request and reply ping contain the same data message.

HEX: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69

ASCII: abcdefghijklmn opqrstuvwabcdefg hi

Documentation Task 2.

1. List the IP addresses from the tracert output and the ICMP messages in the Wireshark capture. Do they match?

Trace Route Ips (CMD Prompt):

- **192.168.1.1**
- **10.20.20.215**
- **203.29.134.125**
- **209.85.149.84**
- **72.14.239.249**
- **142.250.224.191**
- **142.250.66.228**

Wireshark ICMP Source Addresses:

- **192.168.1.1 (x3)**
- **10.20.20.215 (x3)**
- **203.29.134.125 (x3)**
- **209.85.149.84(x3)**
- **72.14.239.249 (x3)**
- **142.250.224.191 (x3)**
- **142.250.66.228 (x3)**

These match exactly

2. Do all the ICMP Echo (ping) request messages have the same destination IP address? What is it?

Yes, all of the ICMP Echo (ping) request messages have the same destination IP.

Destination: 142.250.66.228

3. Is the type field in the ICMP section of all the ICMP time-to-live exceeded messages the same? What is it?

Yes, all of the ICMP TTL exceeded messages have the same type field.

Type: 11 (Time-to-live exceeded)

4. Is the delivered data in the ICMP messages for tracert the same as for the ping messages in task 1?

No, the trace route data length is now 64 bytes (as opposed to 32 bytes for the ping)

The trace route data includes all values that are 0.

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)

The key difference between the ICMP Echo (ping) request messages is the TTL set on the message. The TTL starts at 1 and pings the desired destination 3 times. If there is no response to any of the pings, the TTL is incremented and the final destination is pinged again 3 times.

The purpose of this is to identify each of the hops destinations used on the message to the desired destination. This also helps us identify how many total hops are required to reach the desired destination.

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?

The encapsulated message is NOT exactly the same. The request pings will increment the TTL value to move to the next location. The response will only respond with a TTL of 1 every time.

I speculate that this is occurs as the message is that is passed to the next destination (hop) includes the previous message, and before the message is attempted to be broadcasted to the next hop destination, there is a check to see if TTL is 1. If it is, it knows that we cannot go further as we have consumed all of the TTL of this message and sends a response back to the original source which includes the new message this furthest destination received. This means that when we reach the end of TTL, that address will ALWAYS have a TTL of 1 and it will be included in the message.

7. Is there anything else worth noting about these messages, especially when compared to the similar messages generated for Ping?

A key thing to note is that the source address of the trace route replies is vastly different to an ICMP ping as the source changes depending on our current TTL of the tracert request.

This allows us to identify the different addresses our request is passing through to reach our final destination.

8. ICMP is encapsulated within IP – does this make it a transport layer protocol? Explain your answer.

ICMP is not a transport layer as it in not used for sending and receiving data, with the core exceptions being ping and trace route.

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