Name and Section: _____

1 Lab Preparation

- Download the following trace files to your working directory:
  - `icmp1.pcapng`
  - `icmp2.pcapng`

Submission

Submit all of your work in **neatly hand-written** or **typed** format.

What to turn in:
- The completed lab packet

2 Lab Assignment

- Open the trace file: `icmp1.pcapng` in Wireshark.

1. What is the display filter for ICMP? Apply the filter.

2. What is the exact filter for an ICMP Echo Request message? Echo Response message? (*i.e field.name == x*)

3. How did Wireshark ascertain that the data encapsulated within the IPv4 packet was was an ICMP message?

4. With respect to ICMP, explain what is happening in this trace? What command line tool that you have used would create this type of traffic?

5. What is the layer 2 address of the device that initiated the network traffic?

6. What are the ICMP ID values for each of the Echo Request messages? Why are there two values displayed in wireshark? ("LE" and "BE")

7. What are the ICMP ID values for the Echo Response messages?

8. What are the ICMP Sequence Number values for the Echo Request messages? List in hex format using the big endian value

9. What are the ICMP Sequence Number values for the Echo Response messages? List in hex format using the little endian value

10. What can you deduce based on the answers to questions '7-9'?

- Open the trace file: `icmp2.pcapng` in Wireshark.

11. What is the display filter for an ICMPv4 Time Exceeded - TTL Exceeded in Transit Message?

12. Using the display filter for TTL Exceeded in Transit, you should have only TTL exceeded messages remaining. Why do the resulting packets have two ICMP messages encapsulated within them?

- In Wireshark, make the following modifications to your column layout preferences
- Hide the columns; 'time', 'length', and 'info'
- Add custom columns for the ICMP type, ICMP code, and the useful version of the ICMP Sequence number.

13. What are the display filters for the new columns? Does the GUI kinda look similar to your tshark output?Which method was easier and/or quicker for you to identify what was happening with the traffic?

- Hide the columns you just added, add a column to display the IPv4 id value

14. What is the display filter you used? What does this column provide that is helpful for identifying what is going on with the traffic?

3 Review Questions

15. What is the purpose of ICMP?

16. What was the `'ping'` tool originally designed for? What else is `'ping'` commonly used for?

17. What type of device might generate an ICMP Type 3, Code 13 message?

18. You have captured only ICMP packets on your network. How can you determine what triggered the ICMP Type 11 packets you see in the traffic?

19. What should an IPv4 router do when a packet arrives with a TTL value of 1?