Name and Solution: _____

1 Lab Preparation

- Download the following trace files to your working directory:
  - `app-iradio.pcapng`
- Use the Layer 2/3 Reference Sheet - Header Format (Ehternet, IPv4, ARP & ICMP Echo), located on the course website, for use in analyzing the Wireshark packets throughout this lab

Submission

Submit all of your work in **neatly hand-written** format. Ensure you show all your work and steps you took to solve the problem, as needed.

What to turn in:
- The completed answer sheets

2 Lab Assignment

- Open the trace file: `app-iradio.pcapng` in Wireshark.

1. How many packets are in this trace?

- Select the first packet in the trace file.

2. How did Wireshark know that this packet contained encapsulated IP?

- Select and expand the IP header in the Packet Details Pane.

3. What is the display filter for the IP version field?

4. What is the IP version? How many bits are in this field?

5. What is the display filter for the IP header length?

6. What is the header length of this packet? How was this calculated by Wireshark? *Explain the math using the values from this packet*

7. What is the total size of the IP datagram? The ethernet frame? Why are the two different sizes? What is the size of the encapsulated data portion of the IP datagram?

8. Is this packet fragmented? Is it possible for this packet to be fragmented at a later time if it transits a segment with an MTU less then 1500 bytes? Why?

9. What is the TTL value? What is the display filter for the TTL field?

10. What Transport Layer Protocol is encapsulated within this IP datagram? How many bytes is this field? What is the IPv4 protocol value, in hex that tells us what the encapsulated Layer 4 protocol is? What is the display filter for this field?

11. What are the source and destination IP and MAC addresses for this packet?

12. What is the identification value for this packet? What is the display filter for this field?

- Answer the following questions using display filters. *Always list your display filter as part of your answer.*

13. Filter for IP datagrams only. How many packets are still in the frame? What are the non IP packets? What filter did you use to find this?

14. Filter for IP datagrams with a header length not equal to 20 bytes. Explain why these results were to be expected.

- Answer the following questions using "tshark". *Always list your "tshark" commands as part of your answer.*

15. List all of the unique source IP addresses in this trace.

16. List all of the unique destination IP addresses in this trace.

17. **Extra credit:** Explain any addresses that were not seen as both a source and a destination. What type of address is this? What is it used for?

18. Output the IP identification values from all packets with a source address `192.168.0.104` to a file. What can you glean from the output? What is the range of values?

19. List all of the unique protocol type values and the corresponding protocol name that are encapsulated within IP.

Review Questions

1. What is the purpose of layer 3? What are the functions of IP?

2. What IPv4 header fields are used with IP fragmentation? Explain the purpose of each field.

3. Does the source MAC address change when a switch forwards a packet? When a router forwards a packet?

4. Does the source IP address change when a switch forwards a packet? When a router forwards a packet?