Name and Solution: McKenzie Eshleman

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?
   There are 2073 packets in this trace

- Select the first packet in the trace file.

2. How did Wireshark know that this packet contained encapsulated IP?
   Wireshark knows that this packet has an encapsulated IP based off of the Ethernet

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

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

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

5. What is the display filter for the IP header length?
   The display filter for the IP header is ip.hdr_len == 20

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

   The header length of this packet is 20 bytes, this is calculated by wireshark by ip header length + Tcp Header length+ application

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?

   The total size of the IP datagram is 1500 bytes, the total size of the ethernet frame is 1460 bytes. The two sizes are different because of the data portion of the packet

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?

This packet is fragmented, it is possible for this packet to be fragmented at a later time if less then 1500 bytes because there tends to be a buffer when transporting.

9. What is the TTL value? What is the display filter for the TTL field?
   The TTL value is 52, the display filter is ip.ttl == 52

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?

    The transport layer protocol used is TCP, containing 6 bytes

    Filer ip.proto == 6

11. What are the source and destination IP and MAC addresses for this packet?
    IP SRC: 216.235.91.31 IP Dest: 192.168.0.104

    MAC SRC: 00:13:46:cc:a3:ea MAC Dest: 00:18:de:d0:27:d7

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

    The identification value for this packet is 0x9e9f
    the display filter is ip.id ==0x9e9f

- 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?

    display filter ip, there are still 2073 packets in the frame

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

    ip.hdr_len != 20, there were no headers of a different length, this is to be expected because the typical IPv4 header length is 20

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

    216.235.91.31
    192.168.0.104
    192.168.0.109

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

    216.235.91.145
    224.0.0.252
    192.168.0.109
    192.168.0.104

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?

    The ARP packets did not have a source and a destination, this address is address resolution protocol

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

    id.src == 192.168.0.104, all these packets are TCP going from port 49639 to 80

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

Types: -DNS (domain name system)
- NBNS (NetBIOS Name Service)
- TCP (Transmission Control Protocol)
- SNMS (Simple Network Management Protocol)
- LLMNR (Link-local multicast Name Resolution)
- HTTP (Hypertext Transfer Protocol)
- ARP (Address Resolution Protocol)

Review Questions

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

The purpose of layer three is combining the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. The defines packet structures that encapsulate the data to be delivered.

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

-Identication is populated with an ID number unique for the combination of source & destination addresses and Protocol field
-Flags reserved bit of the Flags field (3 bits) will be 0 (unset) and the second bit, Don't Fragment (DF), will also be unset. Unlike the original packet, all but the last fragment will have the third bit of the field, More Fragments (MF), set to 1
-Fragement Offset is used to indicate the starting position of the data in the fragment in relation to the start of the data in the original packet.

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

No. If all the switches are layer-2 switches, the frames are switched without any changes. Only with routers, including layer-3 switches where the packets need to cross to other VLANs, will the frames be stripped and rewritten for the new network or VLAN

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

the source and destination IP addresses don't change. In practice, NAT may be used, and, depending on the NAT used, either the source, destination, or both IP addresses may be changed.