1 Lab Preparation

It is assumed that students already have Wireshark installed on their Linux VM. Wireshark does run on Windows, however the command line tools, such as `tshark` use a different syntax. Additionally, if you wish to capture using Wireshark you must install separate drivers to capture on a Windows host. The Linux and Windows GUI capabilities and layouts are largely similar. If you need to install Wireshark to your Linux VM, from the command line use the following command:

```
sudo apt-get install wireshark wireshark-common tshark
```

- Download the following trace files to your working directory:
  - `arp-bootup.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 sheet

2 Lab Assignment

1. Open the trace file: `arp-bootup.pcapng` in Wireshark.
   (a) What is the display filter for ARP?

2. Use the display filter for ARP, analyze the resulting ARP messages.
   (a) What is happening in packets 3, 4, and 5?

   (b) What unique feature of a gratuitous ARP message allows Wireshark (and you) to determine whether or not an ARP message is 'gratuitous' (Note: "Wireshark tells you under info" is not an acceptable answer as Wireshark fills out this column based on information it can parse from the packet.)

   (c) How did Wireshark know that these were ARP messages? What field-value pair within the packet tells Wireshark that the packets were ARP messages.

   (d) What are the display filters for the ARP's hardware type and protocol type? What are the values and types associated with these messages?

   (e) Using packet 23, what do the hardware size and protocol size fields represent? Be specific.

(f) What is the display filter for ARP requests? ARP replies?

(g) Research why packet 22, an ARP packet, would specifiy a target MAC address field that contains all zeros.

(h) Based on what you learned about packet 22 what is happening in packet 23?

(i) In the ARP messages 3, 4, 5, and 22, the destination MAC addresses were `ff:ff:ff:ff:ff:ff`, why? Explain in detail.

(j) Using only the ARP packets, list all known hosts on the network. Include all the relevant layer 2 and 3 addresses of the hosts. **Extra Credit:** Using any part of the trace, identify the type of network device of the host with an IP address of `24.6.168.1`.

(k) Would it be valid to assume that this network is a /24 based on the information gleaned from these ARP packets.

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

(a) Filter for all traffic with a layer 2 source address of `00:23:54:69:8f:58`. List the other types of protocol traffic seen from this device.

(b) How many packets are in the trace with a destination address of `00:23:54:69:8f:58`?

Review Questions

1. What is the purpose of ARP?

2. Why are ARP packets not forwarded via routers?

3. Research two additional hardware types and two additional protocol types supported by ARP? List with the hex values.

4. List three reasons ARP is vulnerable.

5. What is ARP poisoning?