CSC358 Assignment 5 Wireshark

March 14, 2016

1 Capturing and analyzing Ethernet frames

Let's begin by capturing a set of Ethernet frames to study. Do the following:

- First make sure your browser's cache is empty.
- Start WireShark capturing.
- Access this URL in your browser: `http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html`.
- Stop WireShark capturing.

Find the corresponding stream in the captured file, and answer the following questions:

1. In the packet that contains the http GET message, what is the source mac address? Is this your computer's mac address?
2. What is the destination mac address of the above packet, is this the mac address of gaia.cs.umass.edu? If not, then which device has this mac address?
3. What is the hexadecimal frame type field in the ethernet header of this packet? What is the correspond upper layer protocol?
4. Do you notice that WireShark can display the manufacturer of the sender (source) and receiver (destination) of this packet? How this can be done? What is the manufacture of the mac address CC:20:E8:11:22:33?
5. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Explain how do you obtain this result.

2 The Address Resolution Protocol

Open the `ethernet-ethereal-trace-1` trace file (you may need to change the file name extension) in `http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip`. Answer the following questions:

6. Focus on the first packet in the trace file. What is the frame type in ethernet header? What is the destination mac address?
7. Is the destination of the above packet a real computer? If not, who will receive the above packet?
8. Which type of arp packet is the above one? What operation does this packet try accomplishing? Find the corresponding packet of the above arp packet. Which type of arp packet is this one? What information it provides?

9. In the first packet, what is the target mac address in the arp header? Is it the same as the destination mac address in ethernet header? If not, will this be a problem? (you may need refer to wikipedia for this question)

10. Notice that the 6th packet in the trace file is also an arp packet, explain why we didn't see a corresponding arp packet to this one. (you don't need to provide screenshot for this question)