CHAPTER 5

Lab Assignments for Chapter 5

We have created two lab assignments for this chapter, Lab5-1 and Lab5-2. We have also included two lab-report sheets, which means that each lab should be reported in a separate sheet.

The first assignment, Lab5-1, is about the Ethernet protocol. The second, Lab5-2, is about an auxiliary protocol, ARP, which is part of the network layer, but it is used as a liaison between the network and the data-link layer.

Lab5-1: Ethernet

In this lab, we examine the contents of an Ethernet frame sent by the data-link layer. We find the value of different fields such as destination and source link-layer addresses, the value of the protocol field, which shows which payload is being carried by the frame, and so on.

Assignment

- Start your web browser and clear the browser's cache memory, but do not access any website yet.
- Open the Wireshark and start capturing.
- Go to your browser and retrieve any file from a website. Wireshark starts capturing packets.
- After enough packets have been captured, stop capturing and save the captured file.

Part I: Frame

In the packet list pane, select any packet that is initiated from your computer. In the packet detail pane, expand the Frame (packet at the data-link layer).

Questions

Note that the Ethernet filters the preamble and FSD fields; they are not passed to Wireshark. Also most Ethernet interfaces either do not supply the CRC to Wireshark or are not configured by their driver to do so. You may notice that the Wireshark can capture padded bytes in request messages, but not in the reply messages. Using the captured information, answer the following question in your lab-report sheet.

1. What is the frame size?
2. What is the payload size (data and padding)?
3. From the answer to question 2, can you say that there is padding in the payload?
4. Try to find a frame that is exactly 60 bytes (without counting the CRC bytes). Using the total payload length, find the number of padded bytes.

Part II: Ethernet Header

In the list packet pane, select a packet. In the packet detail pane, select the Ethernet.

Questions

Using the captured information, answer the following question in your lab-report sheet.

1. From the hexdump, determine
   a. destination link-layer address.
   b. source link-layer address.
   c. upper layer protocol.
2. Using the packet detail pane, verify your answers to the first question.
3. Is the destination link-layer address unicast or multicast?
4. Does the source link-layer address define your network? Explain.
5. Is there a relationship between the destination link-layer address and the destination IP address?

Documents to Turn in

1. A copy of Lab5-1 report sheet that contain answered questions.
2. A printout of the supporting captured information.

Lab5-2: ARP

As we discussed in the textbook, ARP is an auxiliary protocol that maps the IP address of connection to the host or router to the link-layer address of that connection. In this lab, we trace and examine ARP packets

Assignment

- Start your web browser and clear the browser's cache memory, but do not access any website yet.
- Open the Wireshark and start capturing.
- Go to your browser and retrieve any file from a website. Wireshark starts capturing packets.
- In the filter field of the Wireshark window type **arp** (lower case) and click **Apply**. Stop capturing and save the captured file.

Part I: ARP request message

From the packet list pane, select the first ARP request packet. From the packet detail pane, select the Address Resolution Protocol.

Questions

Using the hexdump and consulting Figure 5.48 in the textbook, answer the following question in your lab-report sheet.

1. From the hexdump, determine
   a. the hardware type.
   b. the protocol type.
   c. the hardware length.
   d. the protocol length.
   e. the value of the *operation* field. What is the meaning of this field?
   f. the source hardware address.
   g. the source IP address (in dotted decimal notation)?
   h. the destination hardware address.
   i. the destination IP address (in dotted decimal notation)?
2. Using the packet detail pane, verify your answers to the first question.
3. What is the type of the destination hardware address (unicast, multicast, broadcast)? Which hardware interface does the destination address define?
4. Checking the packet byte pane, you will notice that the ARP request is followed by zero-bytes. How many 0s are there? Explain the reason for the existence of these 0s.

Part II: ARP reply message

From the packet list pane, select the first ARP reply packet. From the packet detail pane, select the Address Resolution Protocol; the packet's hexdump will be highlighted in the packet byte pane.

Questions

Using the hexdump and consulting Figure 4.8 in the textbook, answer the following question in your lab-report sheet.

1. Using the hexdump, determine
   a. the hardware type.
   b. the protocol type.
   c. the hardware length.
   d. the protocol length.
   e. the operation code.
   f. the source hardware address.
   g. the source IP address (in dotted decimal notation)?
   h. the destination hardware address.
   i. the destination IP address (in dotted decimal notation)?
2. Using the packet detail pane, verify your answers to the first question.
3. What Type of address is the destination hardware address? What network interface does the address define?

Documents to Turn in

1. A copy of Lab5-2 report sheet that contain answered questions.
2. A printout of the supporting captured information.