ECE 361 Lab #1: Wireshark Exercises

Introduction

Wireshark is a free, open source network packet analyzer used for troubleshooting, analysis, software and protocol development and education. The software is available for download at https://www.wireshark.org/. In this lab you will use Wireshark to analyze packet captures and work through a series of exercises in order to develop a better understanding of how networks operate.

Pre-lab

As a first step you'll need to get familiar with the *Wireshark* software. Review the slides from the *Wireshark* lecture and also see https://www.wireshark.org/docs/ for a complete user guide and instructional videos.

In order to analyze the packet captures in this lab you must have a firm understanding of addressing in networks (both Ethernet and IP) and port numbers.

Ethernet Addressing

Ethernet is a protocol corresponding to the data link layer of a network. It is tasked with the delivery of frames between machines on the same local area network (LAN). Ethernet addresses are 6 bytes long (48 bits). The first bit distinguishes between single and group addresses while the second indicates whether the address is local or global. There are, therefore, 2^{48} unique global addresses. The convention is to specify the address as 6 pairs of hexadecimal digits. The first 3 bytes specify the vendor of the network interface card (NIC).

An example of an Ethernet address is: *18:03:73:D4:9A:93* which indicates the vendor as Dell (*18:03:73*). **Refer to Section 6.6.1 from the text to learn more about Ethernet addressing.**

IP Addressing

The Internet Protocol (IP) corresponds to the network layer in the OSI reference model providing a connectionless, best-effort delivery service to the transport layer. To identify a node on the Internet an IP address is assigned to each. IPv4 addresses have a fixed length of 32 bits. The structure was originally defined to have a two-level hierarchy with network ID and host ID implying that routers in the Internet can forward packets based on the network ID only.

The IP address structure is divided into five address classes as below (figure from Section 8.2.2):

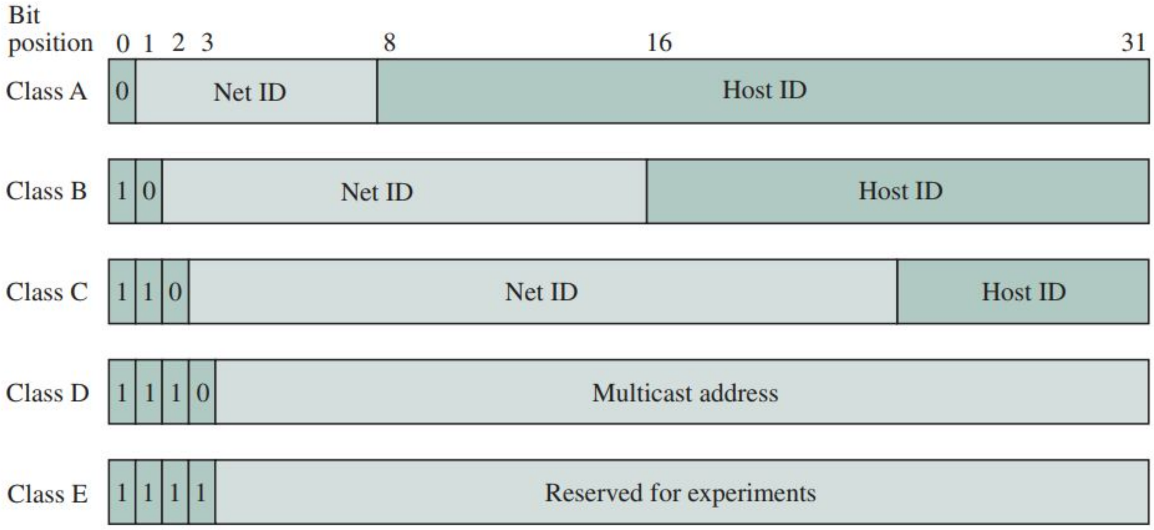

FIGURE 8.5 The five classes of IP addresses

IP addresses are usually written in dotted-decimal notation so that they can be communicated conveniently. An IP address of *10000000 10000111 01000100 00000101* is written as *128.135.68.5.* **Refer to Section 8.2.2 from the text to learn more about the Internet Protocol addressing.**

SMTP (E-mail), DNS and HTTP are examples of application-layer protocols using the communication services provided by the TCP and UDP transport layer protocols. Both TCP and UDP utilize port numbers to identify the source and destination processes in each host. **Refer to Sections 8.4 and 8.5.2 (TCP Segment) from the text to learn more about UDP and TCP.**

Exercises

Open Wireshark on an EECG machine (*Applications -> Internet -> Wireshark)* and perform the following exercises.

Part 1: Web Browsing Traffic Inspection

In this first part you will examine a packet capture for a web browsing operation. Open the capture file *'http.cap'* (clear any display filters) and use WireShark to answer the following questions:

1. What is the IP address of the host?

2. What is the IP address of the router?

3. What protocol is used to resolve the website domain name?

4. What is the IP address of the HTTP server?

5. Which transport layer protocol is used by DNS?

6. Which well-known port is used when contacting the DNS server?

7. Which ephemeral port does the host initiating the DNS query use?

8. What is the Ethernet address of the host?

9. What is the Ethernet address of the router?

10. How long does the 3-way handshake take to complete?

11. Which website is the host machine trying to access?

12. What version of HTTP is the browser running?

13. In the filter box enter the following query: **udp.dstport==53** and click apply. What does the query mean and what are the results?

14. Go to *Statistics -> Protocol Hierarchy* and answer:

   A. What percentage of frames are Ethernet frames?
   B. Which transport layer protocols were present and which one made up more of the traffic?

15. Now plot the UDP and TCP traffic as follows:

- Go to *Statistics -> IO Graph* (Adjust Interval as appropriate)
- Click **+** and add Display filter: *tcp* (Rest of the information can be default)

- Click **+** and add Display filter: *udp* (Rest of the information can be default)
- Click **+** and add Display filter: *http* and Y Axis: *Bits* (Rest of the information can be default)

Answer the following questions:

A. What is the highest number of TCP packets/sec observed? Around what time (second)?
B. What is the highest number of UDP packets/sec observed? Around what time (second)?
C. What is the highest number of HTTP bits/sec observed? Around what time (second)?

Part 2: Mystery Traffic Inspection

In this second part you will work through a series of questions to deduce what is going on in the provided capture. Open the capture file *'mystery.pcap'* (clear any display filters) to answer the following questions:

1. What is the protocol in packet #50 and what is it used for?
2. What is the protocol in packet #55 and what is it used for?
3. Examine the details of packet #55 and study the "payload type". What is likely in this payload?
4. How much time elapses from packet #55 to packet #1329? How much Bytes has been used during this period? Hint: Use IO Graph to answers these questions
5. What is going on in this capture?

Once you have completed the exercise try your own live captures! You can also analyze various traffic using sample captures posted on Wireshark:
https://wiki.wireshark.org/SampleCaptures

Demonstration

Once you have completed the exercises, **signal the Lab TA that you are ready to perform the demo**. Each student in the group may be asked a question about Wireshark or asked to perform a specific operation on the captures in order to demonstrate understanding of the lab.

Submission Instructions

You must submit the answers to the questions in the Exercises section in a text file. The file must be named **exercises_lab1.txt**. This file must also contain the names and student numbers of the group members (at the beginning of the file) prefixed by #. Please do not prefix other lines by # as this would confuse the automated scripts.

```
#first1 last1, studentnum1
#first2 last2, studentnum2
```

Note: Only one student in the group needs to submit.

You can submit the file using the following command:

```
submitece361s <lab_number> <filename>
```

Example: `submitece361s 1 exercises_lab1.txt`

You can verify if you have submitted successfully by using the following command:

```
submitece361s -l 1
```

For more information regarding the command, please refer to it’s man page:

```
submitece361s
```

The submitted files will be used to verify your answers and check for plagiarism.

Marking

This lab is worth a total of **3 marks** with the following break down:

- Exercises: 2 marks (marked as group)
- Demonstration: 1 mark (marked individually)

All marks will be assigned by the end of the lab session.