ECE 358 – Project 3

Encapsulation and Network Utilities

Objective:

After this project, students are expected to:

i. Understand the format of standard frames and packet headers.

ii. Use basic network utilities to monitor network traffic.

1. Overview

Refer to the textbook and the lecture notes for an introduction on the layered architecture (see Figure 1).

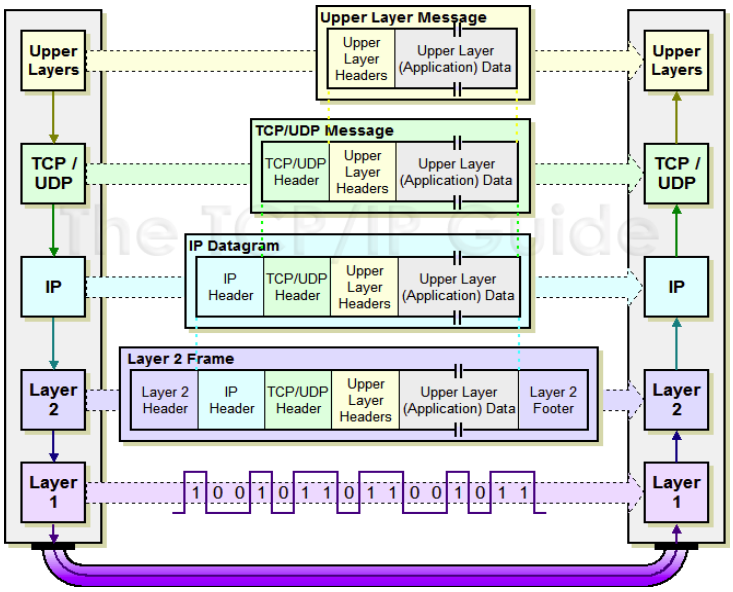

Figure 1

In this project, you will be asked to interpret all the encapsulated headers of captured Ethernet frames. You will also get an opportunity to use some network utilities to get an idea about the performances of the network. *If you have a Linux-based computer, you can run the utilities directly from your machine, otherwise, use one of the ECE Linux machines.*

2. Background Material

2.1 Ethernet Frame

Figure 2 shows the format of Ethernet frames sent and received by the MAC layer. The preamble bits are not shown. If a frame is received without bit errors, the "Data" portion is passed on to the upper layer (network layer).

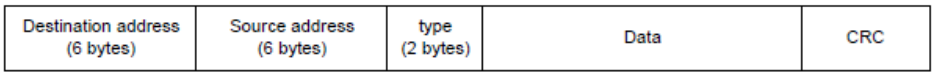

Figure 2: A sample of Ethernet frame

2.2 IP/TCP/UDP Header

The IP protocol is defined in RFC 791 (RFC: Request for Comment), and a summary of the IP header is given in Figure 3. The number on the top is the bit number and each row is four –byte long. Figures 4 and 5 show the format of the headers of TCP and UDP, respectively. They are defined in RFC 793 and RFC 768, respectively. All the RFCs can be found at http://www.ietf.org/rfc.html. The numbers on top again represent the bit number and each row is four-byte (32-bits) long. You will also need to refer to the ICMP protocol (RFC 792) and tell us what is the highest protocol (e.g., FTP, HTTP, etc.) .

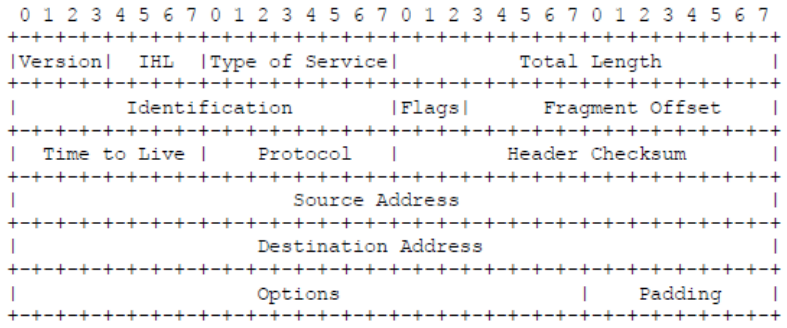

Figure 3: Example Internet Datagram Header

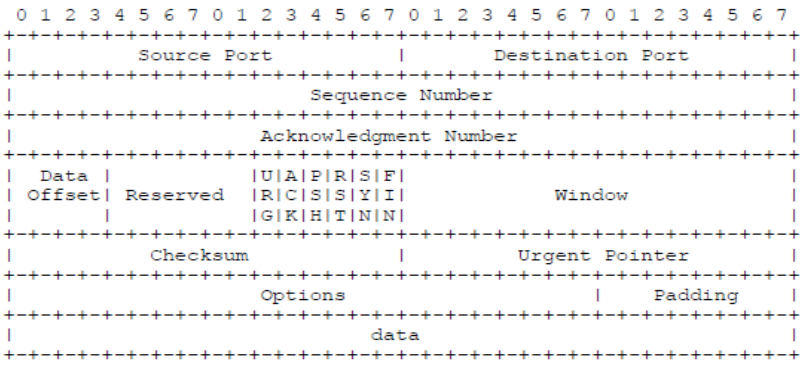

Figure 4: TCP Header Format

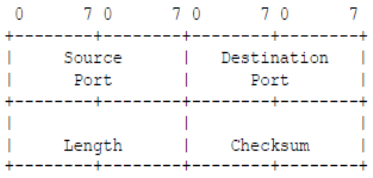

Figure 5: UDP Header Format

2.3 Protocol Header Analysis

The analysis of a sample MAC frame is being shown below.

Sample frame:

```
00 00 0c d9 fa 88 00 00 b4 a0 15 c1 08 00 45 00
00 28 04 04 40 00 80 06 42 a0 80 d3 a0 3c 80 0a
13 14 04 3a 00 15 54 f1 f2 09 d6 7d df 9d 50 10
40 5a b9 e8 00 00
```

Ethernet header:

`00 00 0c d9 fa 88:` Ethernet destination address is 00 00 0c d9 fa 88 (unicast).
`00 00 b4 a0 15 c1:` Ethernet source address: 00 00 b4 a0 15 c1 (unicast).
`08 00:` The payload type is IP (0x0800). (Note: 0x0806 is ARP.)

IP header:

45: This is an IP version 4 datagram,
45: The header length is 5x4 = 20 bytes. (There is no *options* field in the given IP header).

00

(0 0 0 0 0 0 0 0 in binary): This datagram has routine precedence (the lowest). The IP Precedence field is used by some routers to determine which datagram to drop, therefore datagrams with the lowest precedence will be dropped first.

(0 0 0 0 0 0 0 0 in binary): the 3 type of service (ToS) bits

0 0 0 *Normal delay*

0 0 0 *Normal throughput*

0 0 0 *Normal Reliability*

(0 0 0 0 0 0 0 0 in binary): The last two bits must be zero (for future use).

00 28: Total length of the IP datagram is 40 (0x0028) bytes.

04 04: The identification of this datagram is 0x0404 (for fragmentation purpose).

40 00: (0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0):

1 Don't Fragment flag set

0 More Fragment flag unset

The Fragment offset is 0.

This means that the datagram cannot be fragmented, and there are no fragments after this datagram. With a fragment offset equals to zero, we know that this is the only fragment of a datagram.

80: Time to live = 128 (0x80), meaning the datagram may exist for *at most* 128 more hops.

06: The Protocol on top is TCP (0x06) (Note: 0x01 is ICMP and 0x11 is UDP).

42 a0: This is the checksum of the datagram.

80 d3 a0 3c: Source IP address is 128.211.160.60.

80 0a 13 14: Destination IP address is 128.10.19.20.

TCP header:

04 3a: The Source port is 1082, which is an arbitrarily port number assigned by the operating system.

00 15: The Destination port is 21, which is the well-known port for FTP (File Transfer Protocol).

54 f1 f2 09: The Seq. no. is 1425142281.

d6 7d df 9d: The Ack no. is 3598573469.

50: Data offset is 20 (5 x 4) bytes. This is the length of the TCP header.

10 (0 0 0 1 0 0 0 0):

Flags: URG 0 ACK 1 PSH 0

RST 0 SYN 0 FIN 0

Only the ACK flag is set, meaning that the value carried in the acknowledgement field is valid. **(You should comment on all the flags that are set, i.e., equal to 1)**

`40 5a:` the receiver window size is 16474 (0x405a) bytes.

`b9 e8:` Checksum of the whole TCP segment.

`00 00:` Urgent pointer (Not used in this segment).

Data: none

Overall comment on the given frame: The given example frame contained a pure TCP ACK (no data). We observe a lot of those when we monitor the Internet. There may be data in a frame, so you just need to highlight the data portion without analyzing it. You should try to include as much information about the frame as possible. Do not try to analyze the TCP options (see Figure 4).

2.4 Network Utilities

In this project, you will use the following network utilities:

- `arp`
- `ifconfig`
- `nslookup`
- `netstat`
- `ping`
- `traceroute (tracert)`

Detailed information about each utility can be obtained from the Internet. Also, you can find information about the utilities by using the ***man*** command on Unix/Linux machines.

3. Questions:

To do questions 2 to 7, the student should try the commands on different machines/locations and keep the most interesting results. Note that in some environments, the output to the commands might be more difficult to interpret.

3.1 Protocol Header Analysis

Question 1: Obtain two frames from the folder "frames" under "Lab Manuals" in LEARN (please download the frames according to the last digit of your student ID, i.e., if last digit of ID = *i*, do frame *i* and frame *i+10*. Using the example given in section 2.3 as

a template, parse the frames in a human readable format and comment. For example, write an IP address in the dotted decimal notation and header length as a positive integer. Also, color (or, underline) the different parts of the frames to indicate their layers: 2, 3, 4, or app data and indicate the name of the highest layer protocol.

3.2 Network Utilities

In the manual, we tell you to use the network utilities using a command of the type /sbin/command. This only applies if you use one of the ECE Linux machines, otherwise use the command directly. You might get more interesting results by logging to an ECE Linux machine.

Question 2: (arp)

(a) Explain the functions of the utility.

(b) Use the command `/sbin/arp -a` to see the ARP table of the machine on which you are logged in. Include the output of the command in your report and explain it.

Question 3: (ifconfig)

(a) Explain the functions of the utility.

(b) Use the command `/sbin/ifconfig -a`. Include the output in your report and explain it.

Question 4: (netstat)

(a) Explain the functions of the utility.

(b) Use the command `netstat -in`. Change –in to –s to get some statistics. Include the output in your report and explain it.

(c) Use the command `netstat -r`. Include the output in your report and explain it.

Question 5: (nslookup)

(a) Explain, in your own words, what the utility does.

(b) Use the command to obtain the IP addresses of the following hosts and explain what you get.

1. `ecelinux.uwaterloo.ca` (do it twice)
2. `www.mit.edu`
3. `www.gmail.com`
4. `www.facebook.com`

Question 6: (ping)

(a) Explain the functions of the utility.

(b) Use `ping –c10 hostname` to estimate the average round-trip-time from the machine on which you are logged in to the following hosts. Include the output in your report and explain what you get.

1. `www.ualberta.ca`
2. `www.lemonde.fr`
3. `www.ucla.edu`

Check if each host above is up by using a web browser to connect to the hosts.

Question 7: (traceroute)

(a) Explain the functions of the utility.

(b) Use `/usr/sbin/traceroute hostname` to find out how many hops there are between the machine on which you are logged in and the following hosts. Include the outputs in your report and explain what you get.

1) `www.purdue.edu`
2) `www.youtube.com`
3) `www.nytimes.com`

What To Turn In:

1. Submit a print copy of your report with the following details:
   - Cover page: provided at the end of this document
   - Answers/explanations/comments for all the questions.
2. If you use color coding, print the pages in color. If you do not want to print it in color, use other techniques to identify the different blocks of bytes in MAC frames.

<Cover Page>

ECE358: Computer Networks

Fall 2013

Project 3: Encapsulation and Network Utilities

Date of submission:

Submitted by:

Student ID:

Student name <Last name, First name>

Waterloo Email address

Marks received: <Leave this blank>

Marked by: <Leave this blank>