Stripping IP Packets

Due at midnight on Sunday, October 18, 2020

Object

You will be collecting a trace of packets using Wireshark or Tcpdump. You need to parse the trace to disclose packet's information in the trace. This homework will help you to understand IP header clearly and extend your experience on networking tools and utilities.

Packet Trace

Using either Wireshark or Tcpdump you will be collecting packets into a file. Generate as various traffic as possible so that your trace would include different types of packets. I require your trace to have following property.

1. **At least 500 packets**
2. **IPv4**
3. **TCP, UDP, ICMP**
4. **Ten different applications running over TCP and 3 different applications running over UDP**
5. **At least 10 fragmented packets (using special applications or commands)**
6. **TCP options**

Format of Trace (PCAP formatted)

The first 24 bytes is for the file information. You may safely ignore this file header. Each packet is encapsulated a number of packet headers. The outmost one is 16-byte `pcap_pkthdr`. The format of this header is shown in Figure 1. The `struct timeval sec` refers to the timestamp that packet was recorded into the trace in second. The `struct timeval usec` refers to the timestamp that packet was recorded into the trace in micro-second. The `caplen` refers to the length of the packet presented in the trace. The `len` refers to the actual length of the packet. Headers in the next are the Ethernet header and IP header. The formats of these headers are available in elsewhere.

References http://www.tcpdump.org.

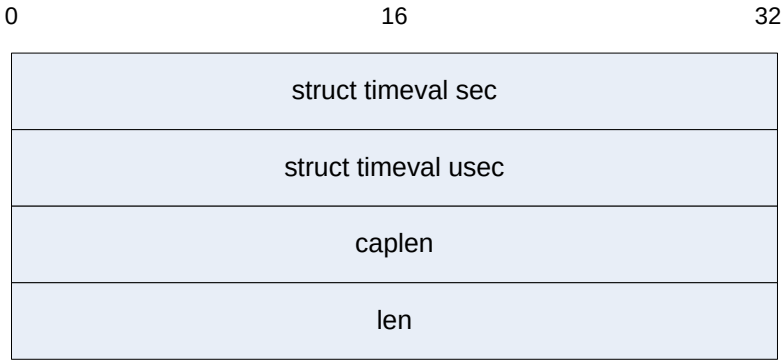

Figure 1: The format of pcap_pkthdr

Parsing Information

You need to parse the following information in the trace.

7. **Local time that was recorded in the format of hh:mm:ss.xxxxxx where xxxxxx refers to the micro second.**
8. **The captured length, actual length and the length in the IP header.**
9. **Source MAC address → Destination MAC address. The format of the MAC address should be XX:XX:XX:XX:XX:XX.**
10. **Source IP address → Destination IP address. The IP address must be in the dotted decimal format.**
11. **A protocol presented in the IP payload.**
12. **Identification and Flags in the IP header.**
13. **Identification in decimal and Flags in either DF or MF.**
14. **TTL**

Word of Caution) Please pay attention to the Endian. Depending upon the endian type the way you parse the information should be different. Verify your result against Wireshark.

Instruction

You are asked to use only C/C++ programming to implement this homework. I recommend using the Linux system over Microsoft Windows.

For verification purpose compare your result with outputs of Wireshark.

Extra credits] You may install this `pcap` package or you may have had this package in your Linux box. I recommend you to use such open source libraries if possible.

Deliverables

Complete the report in MS Word and upload onto "iCampus". In the report you must include all of following. Name your file as yourSchoolID_hw2.[docx|hwp]. Do not zip your file nor submit your trace.

- Source code
- Screenshots of your output for three sample packets
- Verification
- Discussion of your unique experience would be extra credits