Name : Jay Modi
Username: jmmodi

Assignment No : 3
Wiretap

In this project we were expected to analyze the packets being transmitted or received over LAN. Analysis of packets are also done by programs like tcpdump and Wireshark. We were expected to make project similar to it. We were asked to download the software Wireshark and we were provided with two pcap files(Packet Capture). pcap files are the files generated by Wireshark software. These are nothing but the capture files which capture the packets on the LAN and give analysis of these packets. We were expected to make files similar to it and print the analysis to console.

The input to this programme is nothing but an pcap file and output is statistics of that file. For, the compilation purpose we used an -lpcap library. This library had some predefined functions to open and functions to use pcap files. Like, pcap_open_offline() - this function is used to open a pcap file. As, we were expected to print analysis of packets which only belong to Ethernet, so to check that we used a function pcap_datalink().

Most important function in this programme is nothing but the pcap_loop(). This is called every time for each packet. So each and every iteration had to done is this loop. This function has a parameter which is the name of the function, which is to be called every time a new packet is looped in , and that function is called a callback function.

The output of the program was expected to have :

Summary : Summary of all packets in nutshell. Like, Total number of packets, Max size of the packet , min size of packet, average size of packets, etc.

Link Layer : Under this, we were expected print information of packets, like source MAC address and destination MAC address. Like, for every address how many packets do we have.

Network Layer : Under this we were expected to print total number of packets per protocol like for IP, ARP. Also, total number of packets for every source IP address and for every Destination addrsess. Unique ARP participants with their associated MAC and IP addresses.

Transport Layer : Under this, we were expected to print total number of packets under each protocol like TCP, UDP and ICMP. Unique Source and destination ports associated with each protocol. Some additional topics were also expected from us print like TCP flags and TCP Options.

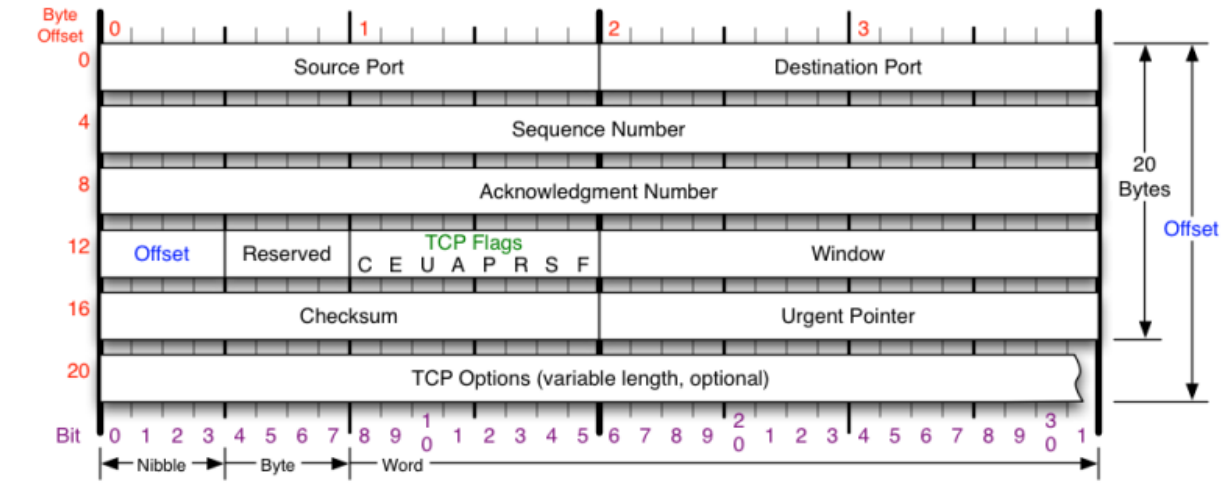
Some key points of code :

1. To save total number of packets per address or ports, same logic of storing in ***map*** is used. As no data structure is better than map to store unique and objects with key value pairs.

Name : Jay Modi
Username: jmmodi

2. Different structures used in this code are : tcphdr , udphdr, arphdr, iphdr and important libraries used in this project are : ether.h, ip.h, ip6.h, bpf.h,pcap.h etc.

3. Important header used in this project :



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

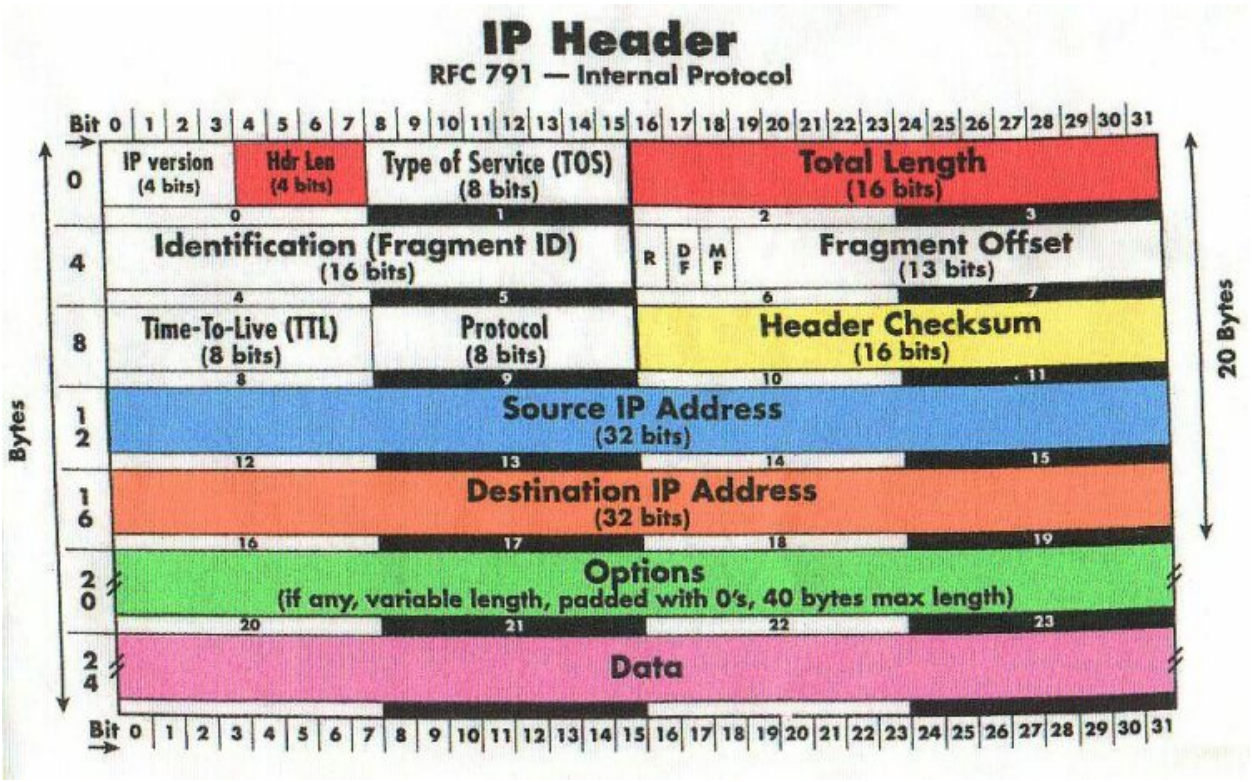
Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Name : Jay Modi
Username: jmmodi



Citations :-

1. http://www.firewall.cx/networking-topics/protocols/tcp/136-tcp-flag-options.html
2. http://beej.us/guide/bgnet/output/html/multipage/index.html
3. http://stackoverflow.com/questions/16519846/parse-ip-and-tcp-header-especially-common-tcp-header-optionsof-packets-capture
4. http://www.cplusplus.com/
5. http://www.firewall.cx/networking-topics/protocols/tcp/138-tcp-options.html
6. http://www.tcpipguide.com/free/t_IPDatagramOptionsandOptionFormat.htm
7. http://www.freesoft.org/CIE/Course/Section4/8.htm
8. http://www.firewall.cx/networking-topics/protocols/tcp/138-tcp-options.html
9. http://books.google.com/books?id=6H9AxyFd0v0C&pg=PT1092&lpg=PT1092&dq=TCPOPT_MAXSEG&source=bl&ots=b6gL8taNmM&sig=9YSMjteOd4niW5kNQTOcO2slum0&hl=en&sa=X&ei=8KZRVOGtPJT-yQSSooDwCw&ved=0CEcQ6AEwBw#v=onepage&q=TCPOPT_MAXSEG&f=false