Assignment No. A7.

Title: Analyze packet formats

Problem Statement:

Write a program in C/C++ to analyze packet formats captured through wireshark for wired network

1. Ethernet
2. IP
3. TCP
4. UDP

Objectives: Understand ethernet, IP, TCP, UDP packet formats.

Theory:

1) Ethernet

Preamble	Destination address	Source address	Type	data	TCS

The preamble consists of 7 bytes all of the form 10101010 and is used by receiver to allow it to establish synchronization

The MAC addresses used in 8023 are always 48 bits long

The length/ othertype field indicates number of bytes of data in the frames payload and can be 0 to 1500 bytes.

The frame check sequence (FCS) is a 4-octet CRC that allows detection of corrupted data

2020/11/09 11:44

IP:

<table>
<tr><td>Version</td><td>Length</td><td>Type Of Service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Tags</td><td>Fragment offset</td></tr>
<tr><td>Time to live</td><td colspan="2">Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Version: A 4-bits field that identifies the IP version being used -
Eg: IPV4.

Length: A 4-bit field containing length of IP header in 32-bit increments.

IP Precedence:
A 3-bit field used to identify level of service a packet receives in network.

Total length:
Specifies the length of the IP, packet which is $2^{16}-1$.

Time to live: (TTL)
It is initially set to a number and is decremented by every router to it passes and is discarded if its value is 0.

3) TCP:

→

3) TCP:

Source port	Destination port
Sequence number	
Acknowledgement number	
Data offset | Reserved | Code	Windows
Checksum	Urgent Pointer
Options	Padding
Data	

Each TCP header has 10 required fields totaling 20 bytes (160 bits)
Source and destination port numbers are communication end points for sending/receiving
The data offset stores the total size of a TCP header in multiples of 4 bytes

4) UDP

0 16 31

Source port UDP length	Destination port UDP checksum
data.	

Because UDP is significantly more limited in capability than TCP its hardness are much smaller
UDP inserts header files into its message stream as follows:

- source and destination UDP ports are communication endpoints
- The length field in UDP represents total size of datagram which ranges from 8 bytes to above 6500 bytes.

Conclusion:

Thus the packets received are analysed using a C++ program.