Assignment - 7

Date:

Title: Packet analysis

Problem Statement:
Write a program in C/C++ to analyze the following packet formats captured through wireshark for wired internet:
- ethernet
- IP
- TCP
- UDP

Objectives:
Analysis of ethernet, TCP, UDP, IP packet structures.

Outcomes:
Demonstrate various fields in header structure of TCP / IP / UDP and ethernet packets.

Requirements:
Wireshark, eclipse IDE

Theory:
Ethernet Frame Format: Basic frame format is defined in ISEE 802.3. Preamble: this is pattern of alternate 0s and 1s to indicate shifting of frame and allow sender

Date :

and to establish synchronization.

SFD : This 1 byte is always set to '01010111' indicating upcoming bit starting of frame.

Destination address : MAC address of destination.

Source address : MAC address of source

Length : Length of entire ethernet.

Definition : Place where actual data is inserted as a protocol. Max length is 1500 bits.

CRC : This contains 32 bit hash code of data which is generated over destination addr, source addr, length of data field.

UDP : It is the simplest transport layer comm^n protocol available of TCP/IP protocol suite. It involves min. amount of comm^n mechanism.

Date :

Source port: This 16 bit info is used to identify source port of the packet.

Destination ~~port~~: This 16 bit port is used to identify application level service on dest^n machine.

Length: Length of UDP packet

Checksum: Stores checksum value generated by sender before sending

UDP is simple and suitable for query based comm^n.

TCP:

- It identifies source point of applicant process on sending.
- It identifies dest^n port of application process on recieving device.
- Sequence no. of data types of segment in a source.
- This no. contains the next sequence no. of type expected.
- Used for flow control b/w 2 stations.
- Points to urgent datatype if urg flag is set.

Date :

Internet Protocol:

1. Version: version of IP used
2. IHL: length of IP header
3. DSCP: differential services code point, types of services
4. ECN: carrier information used about congestion seen in route
5. Total length: length of active IP.
6. Identification: to identify original IP packet they belong to.
7. Flags: as required by network resources
8. Source address: 32 bit address of sender.

Capture packets using wireshark:

- Open wireshark
- Export packet in CSV format
- Analyze and extract nesessary info in program.

Conclusion:

Thus we have successfuly analyzed data packet transfer from one machine to another on different protocols using fuctionalities of libcap in C++.