CS-342 Computer Networks Lab Assignment-2

Rishav Mondal-190101072

August 31, 2021

I ran the Wireshark traces on my home Wi-Fi network at three different times of the day - morning, evening and night (and also on different dates), and whose corresponding traces I have provided in the google drive link. I had to run the traces on Outlook web application on google chrome as I faced authentication issues on the desktop application which logged me out every time I opened it. After running Outlook on google chrome with all other tabs closed so as to reduce interference, I used display filter functionality on Wireshark to segregate the packets generated due to the running of Outlook only.

1 Question 1

I identified the following protocols used in different layers by performing the traces:

1.1 Data Link Layer

The following protocols were observed in the data link layer:

1. **Ethernet II**: Ethernet is a widely used LAN technology. The frame of the ethernet packet starts with a **preamble** which enables the receiver to synchronise and know that a data frame is about to be sent. There is also the **SFD** (Start Frame Delimiter) which indicates the start of the frame. The preamble takes up 8 bytes. The **Destination Address** part gives the station MAC address where the packet is to intended to be sent. The first bit indicates whether it is an individual address or a group address. The **source address** consists of six bytes, and it is used to identify the sending station. **Type** field is the one which differentiates between the type of ethernet connection. **User Data block** contains the data to be sent and it may be up to 1500 bytes long. **FCS** contains Cyclic Redundancy Check (CRC) for error detection and analysis.

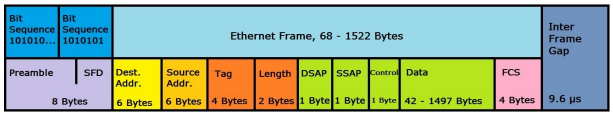

Figure 1: Ethernet frame structure

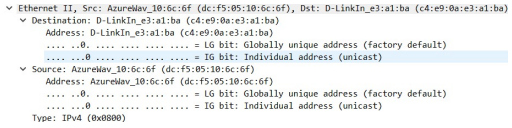

Figure 2: Ethernet II

The **Src** and **Dst** field contain the source and destination endpoint MAC addresses whose values are dc:f5:05:10:6c:6f and c4:e9:0a:e3:a1:ba respectively. Both source and destination contain a **LG** bit which distinguishes vendor assigned (0) and administratively assigned MAC addresses (1) and **IG** bit which specifies whether the MAC address is unicast (0) or multicast (1). In this case both LG and IG bits are 0 for source and destination each indicating both are Globally unique addresses and unicast. **Type** indicates the upper layer protocol to be used which is IPv4 in our case.

1.2 Network Layer

The following protocols were observed in the network layer:

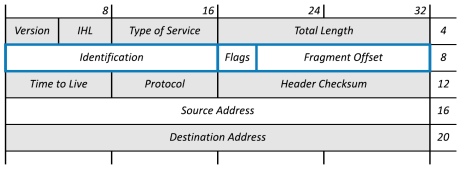

Figure 3: IPv4 header

Internet Protocol Version 4: IP is responsible for transferring data packets from the source to the host. The packet header contains many fields. **Version** indicates the version of the IP used, in this case, it is version-4. The **header length** specifies the length of IP header. **Total length** field determines the entire packet size in bytes, including header and data. The **identification** field is primarily used for uniquely identifying the group of fragments of a single IP datagram. **Fragment offset** specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.

We can observe from the given data that the version of IP protocol used is 4 i.e. IPv4. The header length is 20 bytes and the total length of packet is 1400 bytes. The DF bit is set which indicates that packet should not be fragmented. Time to live(TTL) is 128 which means that packet can make at most 128 hops. The next level protocol to be used is TCP and source and destination addresses are 192.168.0.5 and 40.100.140.226 respectively.

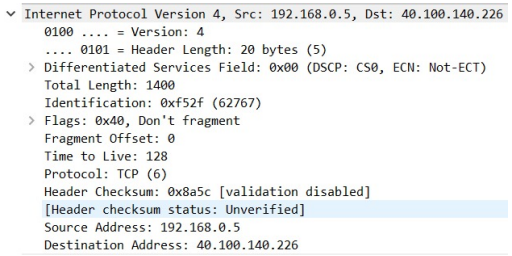

Figure 4: IPv4

1.3 Transport Layer

The following protocols were observed in the Transport Layer:

1. **Transmission Control Protocol(TCP)**: TCP is used for organizing data in a way that ensures the secure transmission between the server and client. Source Port and Destination Port indicates the port of the sending and receiving application. Sequence Number contains the sequence number of the first data byte. Acknowledgement Number field (32 bits) contains the sequence number of the data byte that receiver expects to receive next from the sender. Header Length specifies the length of the TCP header. There is a total of 6 types of Flags of 1 bit each. Some of them are ACK, PSH and SYN. Checksum is used to verify the integrity of data in the TCP payload. Window Size contains the size of the receiving window of the sender. It advertises how much data (in bytes) the sender can receive without acknowledgement. Urgent Pointer indicates how much data in the current segment counting from the first data byte is urgent. Options are used for different purposes like timestamp, window size extension, parameter negotiation, padding.

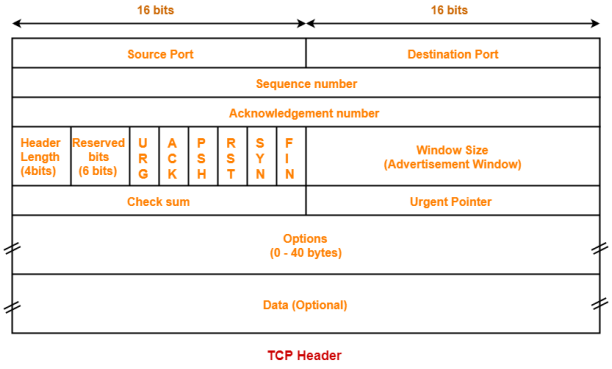

Figure 5: TCP header structure

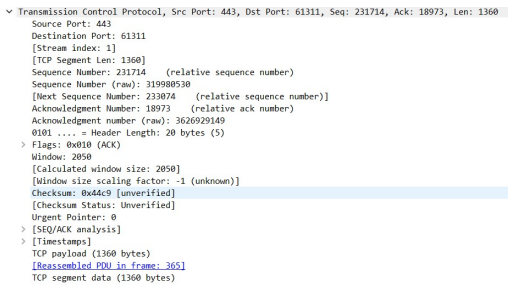

Figure 6: TCP

The Source(Src) port and Destination(Dst) port in this case is 443 and 61311 respectively. Sequence number is 231714 and acknowledgement number is 18973. Only the ACK flag is set which means that the machine sending the packet is acknowledging data that is received from another end. The Header length is 20 bytes. Urgent Pointer is 0 which means that no further bytes are urgent.

2. **User Datagram Protocol(UDP)**: This is a protocol used in communications for establishing low-latency and loss-tolerating connections between applications on the internet. Source Port is a 2 byte field that identifies the port of the sending application. Destination Port is a 2 byte field which identifies the port of the sending application. Length (2 bytes) specifies the combined length of UDP Header and Encapsulated data. Checksum (2 bytes) is used for error control and calculated on UDP Header, encapsulated data and IP pseudo-header.

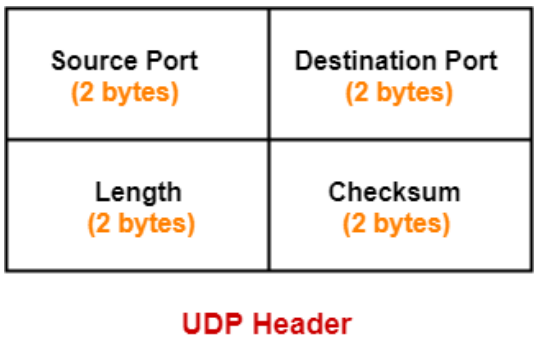

Figure 7: UDP header structure

The fields which can be observed from the following information are the source port and the destination port which are 56103 and 53 respectively. The length of the packet is 44 and the checksum status is unverified. Stream index is an internal Wireshark mapping to [IP address A, TCP port A, IP address B, TCP port B].

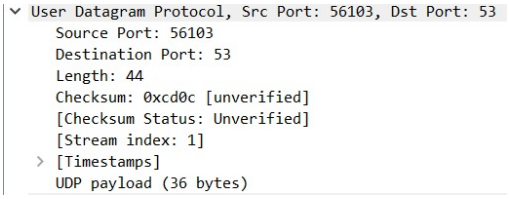

Figure 8: UDP