

CS344: Assignment #1

Due on Friday, August 20, 2021

Siddharth Charan 190101085

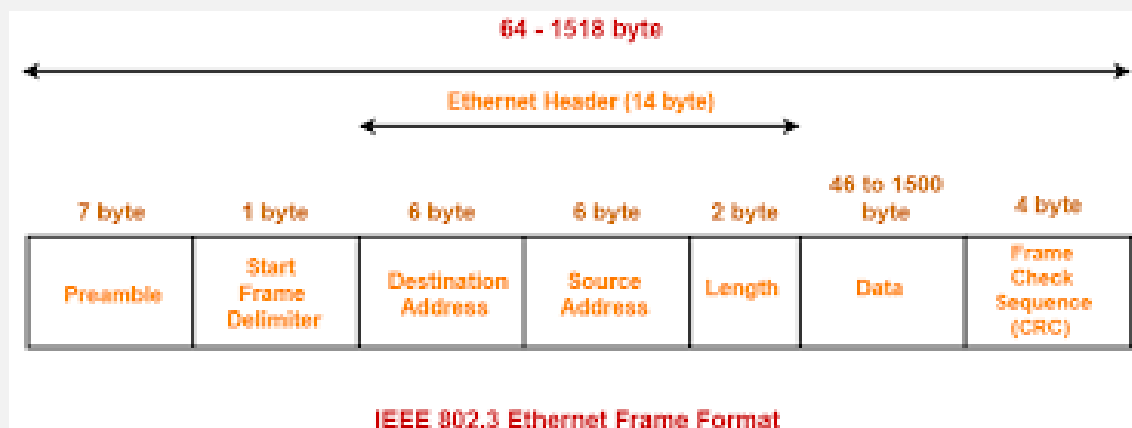
Question 1

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

1. Data Link Layer:

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

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.

```

✓ Ethernet II, Src: 3a:bd:dc:d7:66:ee (3a:bd:dc:d7:66:ee), Dst: HonHaiPr_87:fa:25 (90:32:4b:87:fa:25)
  ✓ Destination: HonHaiPr_87:fa:25 (90:32:4b:87:fa:25)
    Address: HonHaiPr_87:fa:25 (90:32:4b:87:fa:25)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ✓ Source: 3a:bd:dc:d7:66:ee (3a:bd:dc:d7:66:ee)
    Address: 3a:bd:dc:d7:66:ee (3a:bd:dc:d7:66:ee)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  
```

2. Network Layer

Network layer works for the transmission of data from one host to the other located in different networks. The following protocols were observed in the network layer:

Internet Protocol Version 4:

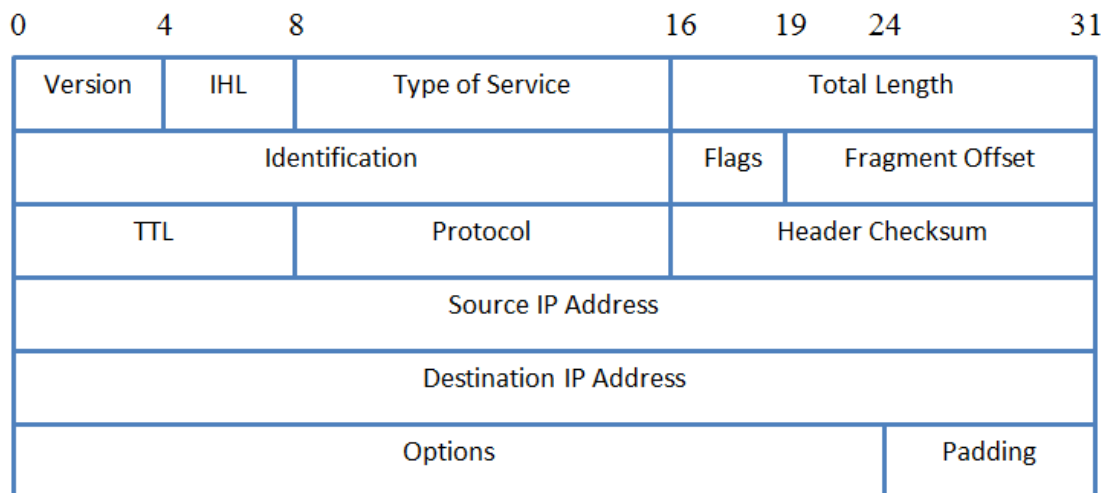


Fig: IPv4 Frame Format

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.

```

v Internet Protocol Version 4, Src: 13.234.210.38, Dst: 192.168.43.179
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1340
    Identification: 0xbb08 (47880)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 46
    Protocol: TCP (6)
    Header Checksum: 0xc047 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 13.234.210.38
    Destination Address: 192.168.43.179
  
```

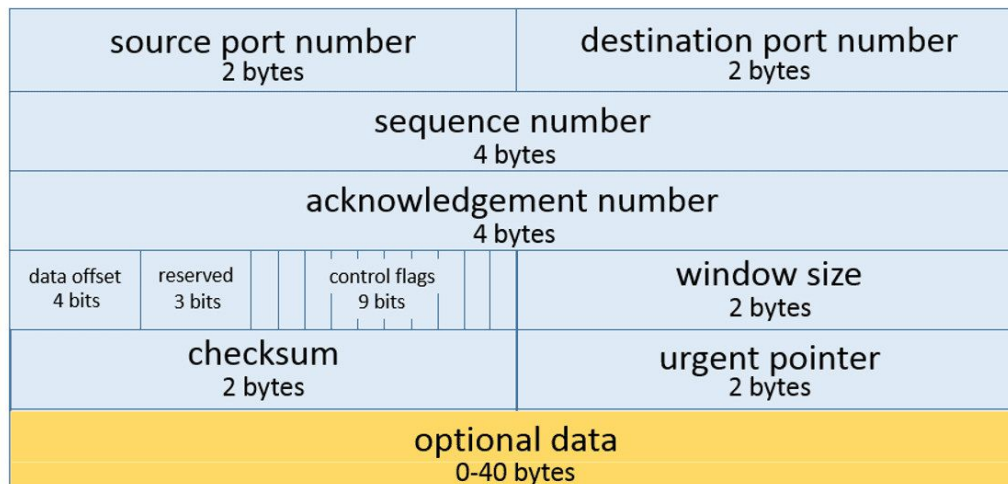
3. Transport layer:

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

Transmission Control Protocol(TCP):

Transmission Control Protocol (TCP) Header

20-60 bytes



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.

```

Transmission Control Protocol, Src Port: 443, Dst Port: 63584, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 63584
  [Stream index: 3]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 3340778925
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 3078976101
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window: 65535
  [Calculated window size: 65535]
  Checksum: 0x9c1d [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
  > [SEQ/ACK analysis]
  > [Timestamps]

```

4. Application layer:

Application layer is at the top of the stack. These applications produce the data, which has to be transferred over the network

Domain Name System (DNS) : This is a distributed database implemented in a hierarchy of DNS servers and an application-layer protocol that allows hosts to query the distributed database. It does translation from Host Name to IP

Header

Transaction ID: 0xd7da									
QR: 1	Opcode: 0	AA: 0	TC: 0	RD: 0	RA: 0	Z	AD: 0	CD: 0	Rcode: 0
Number of Questions: 1									
Number of Answer RRs: 0									
Number of Authority RRs: 13									
Number of Additional RRs: 16									

- Identification : Field is a 16-bit number that identifies the query. Flags in the flag field include query/reply flag, and authoritative flag.
- Destination : It indicates the address of the destination adapter.
- Authority : This section contains records of other authoritative servers
- QR, Query/Response : QR = 0 means a query, QR = 1 means a response.
- Rcode : Consists of 4 bits and the code returned to a query or response.
- Total Questions : Number of entries in the question list that were returned.

✓ **Domain Name System (query)**

Transaction ID: 0x56ab

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

[\[Response In: 812\]](#)

Question 2

Some of the important functionalities of GitHub are as follows:-

- Push to a Repository
- Pull a Repository
- Creating a Repository
- Creating Branch of the Repository
- Cloning a Repository

DNS protocol: It is used by the every functionality of GitHub. It is used to resolve the IP address for the github.com DNS uses UDP packets because these are fast and have low overhead and hence does not need any connection between the sever and the client.

TCP Protocol: It is used by all functionalities of GitHub. TCP always guarantees that data reaches its destination and it reaches there without duplication.It guarantees reliable data transfer by having handshaking protocol on connection establishment and connection termination.It is interoperable, i.e., it allows crossplatform communications among heterogeneous networks.It uses ow control, Error control and congestion control mechanisms.

TLS Protocol: It is also used by all the functionalities of this application.It is a connection-less protocol for use on packet-switched networks.It delivers packets using IP headers from the source to the destination.Existing in the network layer, IPv4 connection is hop to hop.

Ethernet II: Being the most widely used data link layer protocol, it is used by all the functionalities of the application, since it has a reliability, rate of data transfer coupled with flow control. It also allows proper error handling.

UDP: The User Datagram Protocol provides faster data transfer in comparison to TCP but it lacks components such as security and reliability. Thus GitHub uses UDP only for performing DNS queries.

OCSP : To check whether the server's certificate is revoked or not while using clone or pull in github.

Question 3

A. Cloning a Repository:

The client sends the data via TCP packets and TLS ensures that the exchanged data is encrypted.The packets may arrive out of order hence the data needs to be reassembled. No Handshaking is observed here.

B. Submit a File:

The client sends application data to the server when we create a repository in GitHub and the sever responds by sending ACK packets. No Handshaking is observed here.As shown in the above image, the packets (PDU,protocol data unit) need to be reassembled because they might arrive out of order (by using different routes, to ensure load balancing).

C. Handshaking

The following handshaking sequences were observed in the messages:-

1. TLS Handshaking

11 5.442552	192.168.43.179	13.234.210.38	TLSv1.2	235 Client Hello
12 5.552075	13.234.210.38	192.168.43.179	TLSv1.2	1354 Server Hello
13 5.557354	13.234.210.38	192.168.43.179	TLSv1.2	1316 Certificate, Server Key Exchange, Server Hello Done

Client sends a Client Hello and server responds with Server Hello and authentication key.

2. TCP connection establishment

To connect to the github, it requires TCP connection. For connection establishment TCP does 3 way handshake with the destination server as described. The client first sends packet with SYN ag set requesting the server to synchronize with provided sequence number. Then server sends packet with SYN and ACK ag set having the acknowledgement number one more than the sequence number sent by the client (as it represents the next packet number it is expecting) and having some random sequence number. Finally, client sends back packet with ACK and SYN ags set to the server having sequence number set to received ACK value and ACK number set to one more than the received sequence number.

Question 4

Property	9AM	4pm	9pm
Throughput			
RTTP packet Size			
Number of packets lost			
Number of UDP and TCP packets			
Responses per request sent			

Question 5

To achieve uniformity in experiment results, I performed wireshark traces multiple times during the day. All the experiences were performed using my mobile data. GitHub is a website having huge traffic at almost all times of the day. Hence, they use multiple servers to fasten up the data transfer which happens due to Load Balancing of data across servers since there is little network congestion increased reliability. Different servers are also helpful in ensuring reliability since there is no single point of failure. Even if some server experiences some issues, others can provide data to the client without any sort of interruptions.

Time	IP
Morning	13.234.210.38
Afternoon	13.234.168.60
Night	13.233.76.15