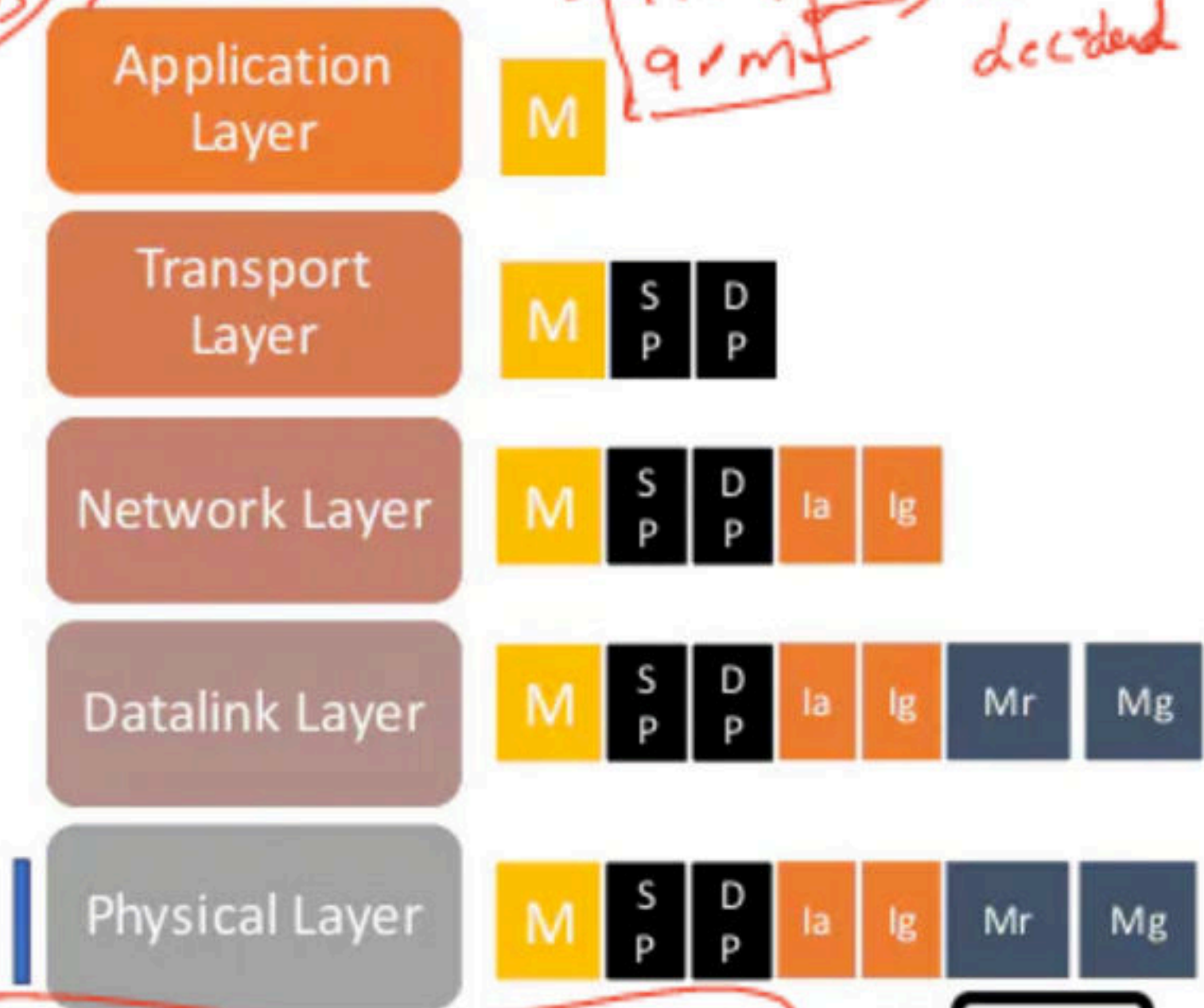# TCP Header - Part II and Retransmission in TCP
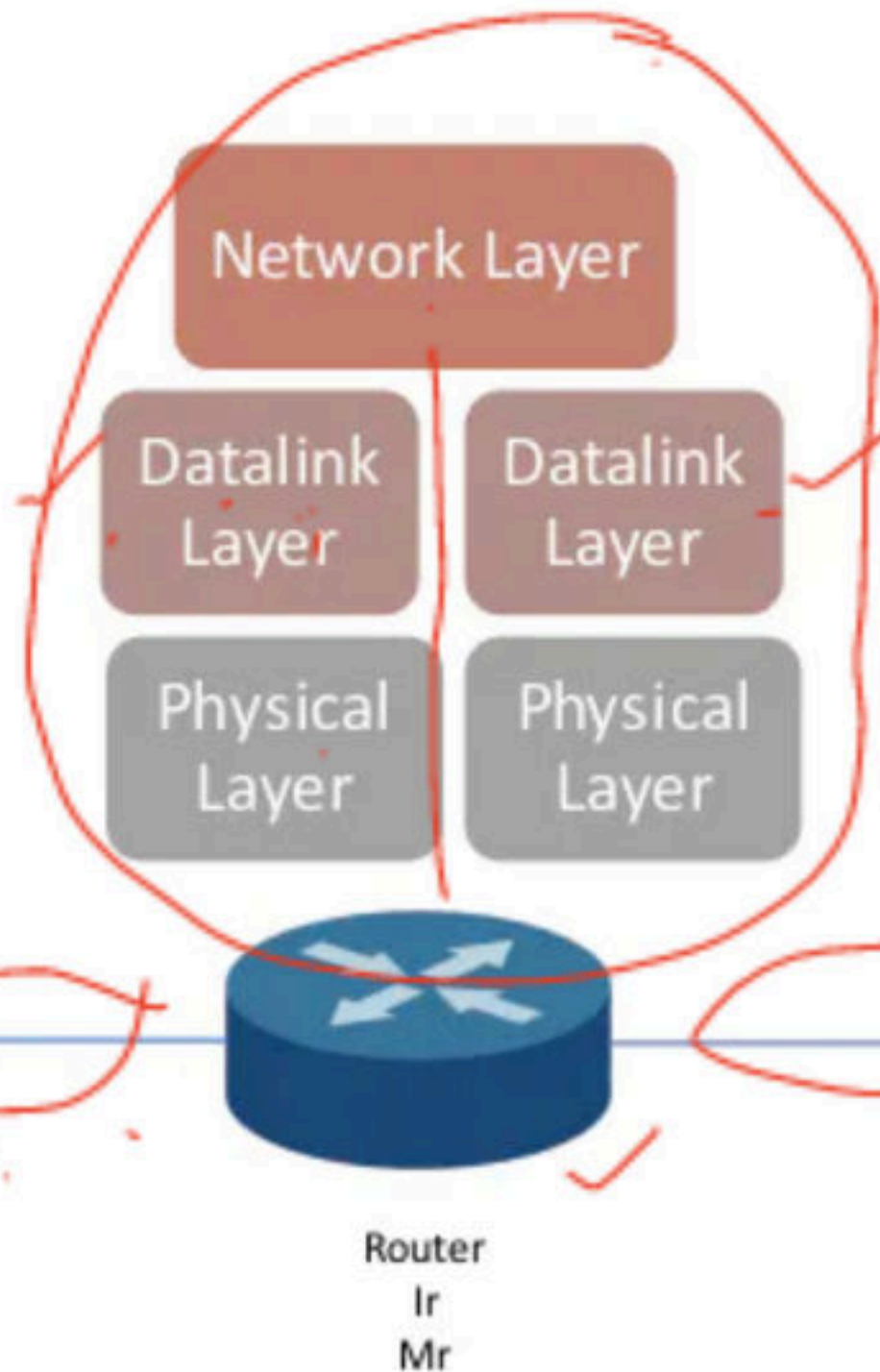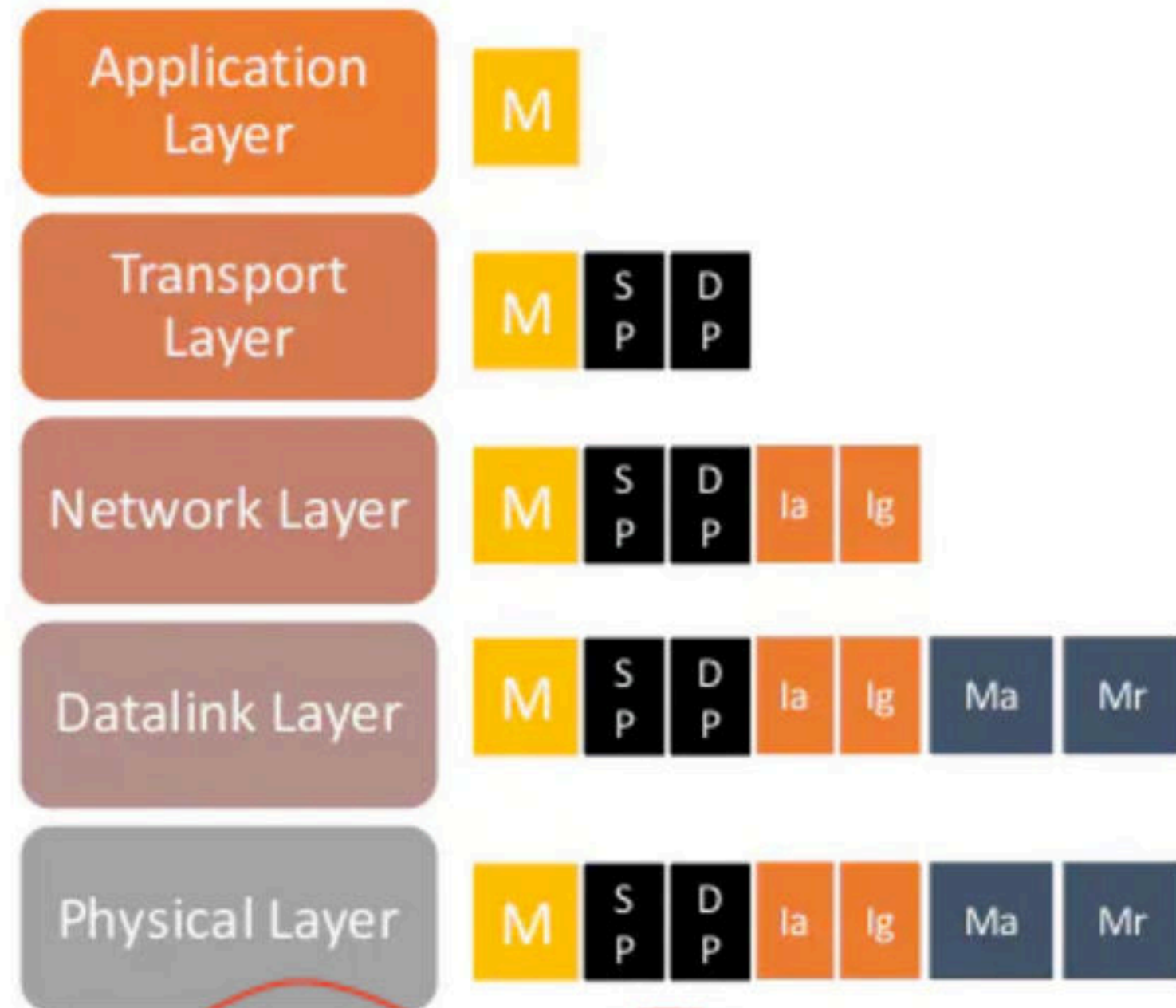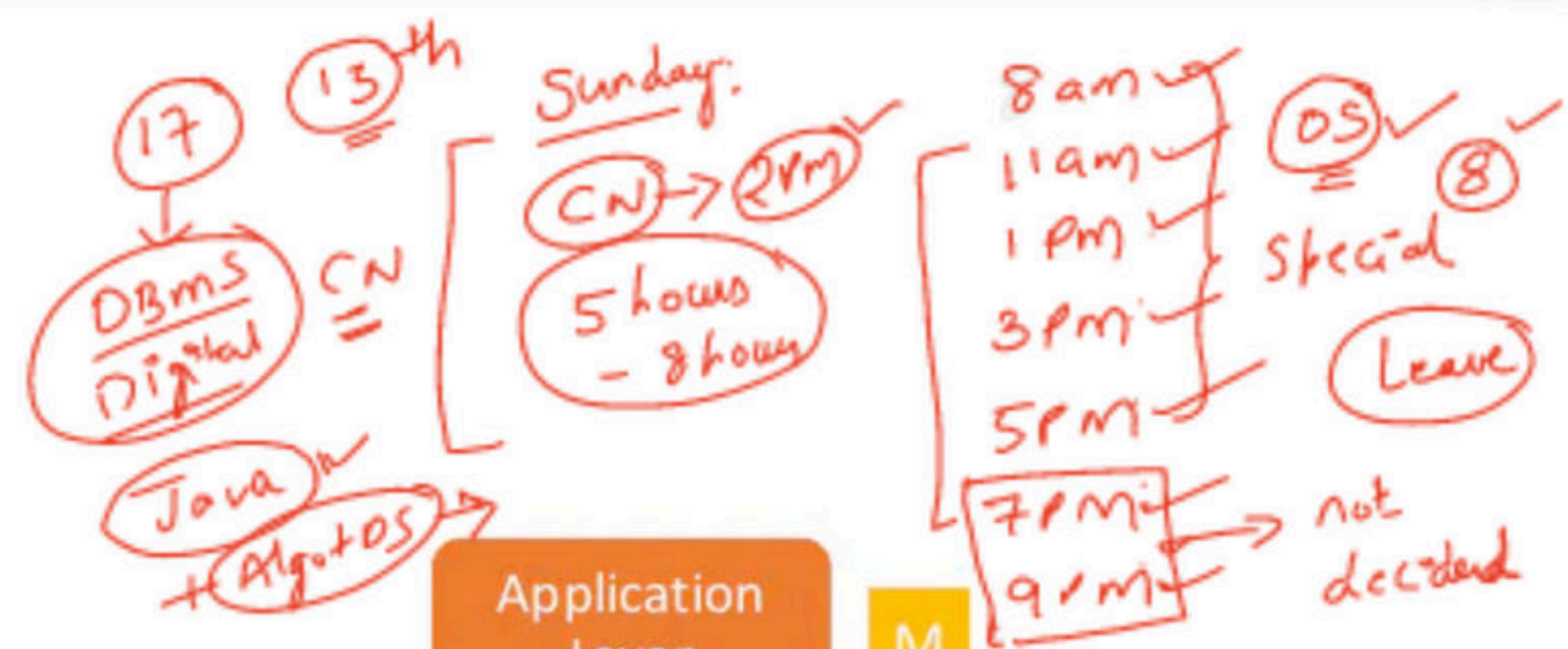
Complete Course on Computer Networks - Part II

Application Layer — M

Transport Layer — M | S P | D P

Network Layer — M | S P | D P | Ia | Ig

Datalink Layer — M | S P | D P | Ia | Ig | Ma | Mr

Physical Layer — M | S P | D P | Ia | Ig | Ma | Mr

Source
Ia
Ma

Router
Ir
Mr

Network Layer

Datalink Layer | Datalink Layer

Physical Layer | Physical Layer

Application Layer — M

Transport Layer — M | S P | D P

Network Layer — M | S P | D P | Ia | Ig

Datalink Layer — M | S P | D P | Ia | Ig | Mr | Mg

Physical Layer — M | S P | D P | Ia | Ig | Mr | Mg

Destination
Ig
Mg

source   ethernet.   Tb'an   Data
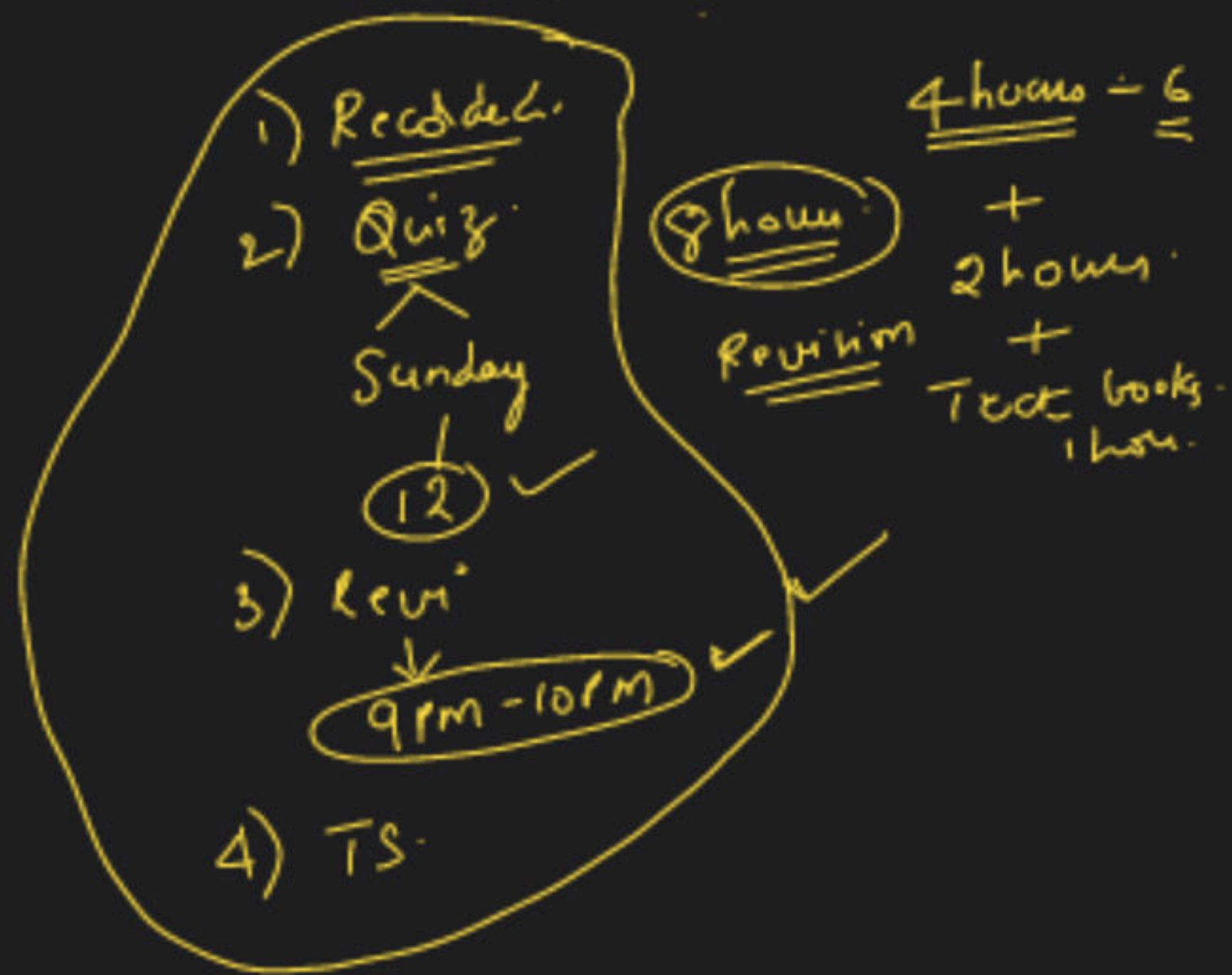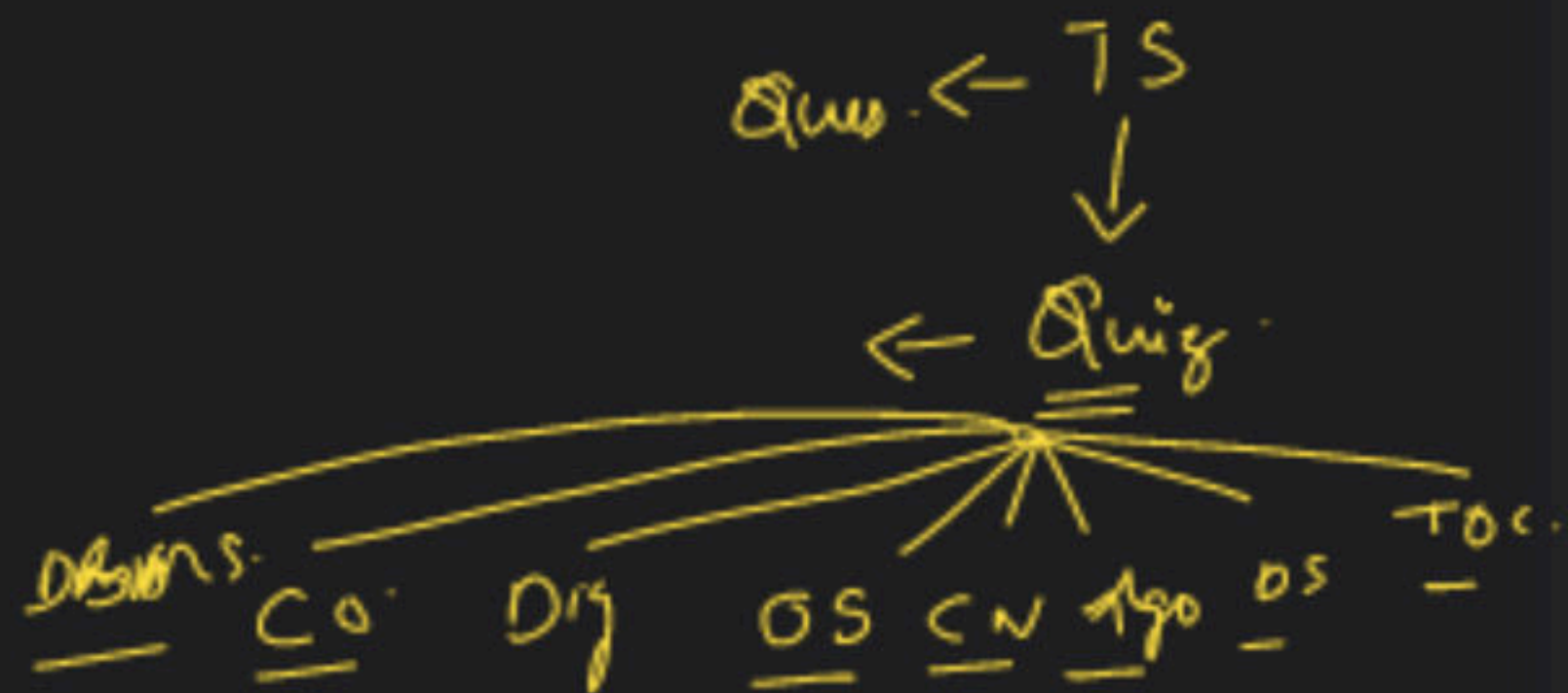
17   13th   Sunday.   8am   OS
DBmS   CN   CN → 2Pm   11am
Digital   1PM
    5 hours   3PM   Special
Java   − 8 hours   5PM   Leave
+ Algo+OS   7PM → not
        9PM   decided   8

Ques. ← TS

← Quiz

Ques. ——— CO   Dig   OS   CN Algo OS ——— TOC

1) Recorded.

2) Quiz
      ╱╲
    Sunday
       │
     (12) ✓

3) Revi
       ↓
   (9PM - 10PM) ✓   ✓

4) TS.

4 hours = 6

(8 hours)   +

Revision   2 hours
            +
          Text books.
            1 hour.

IP
MAC

IP
MAC.

NIC → Rom → H/W

N/w
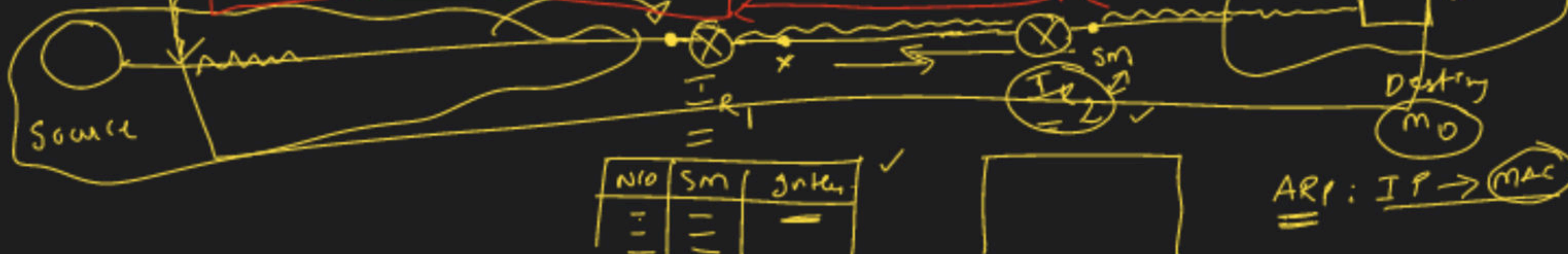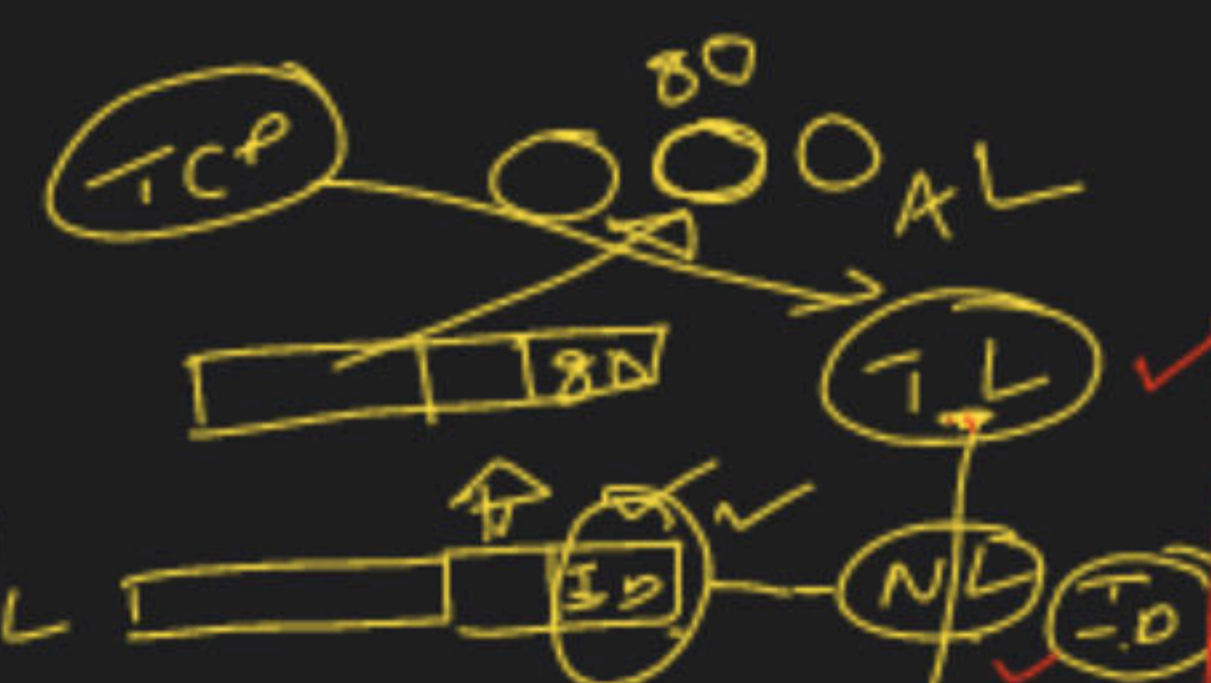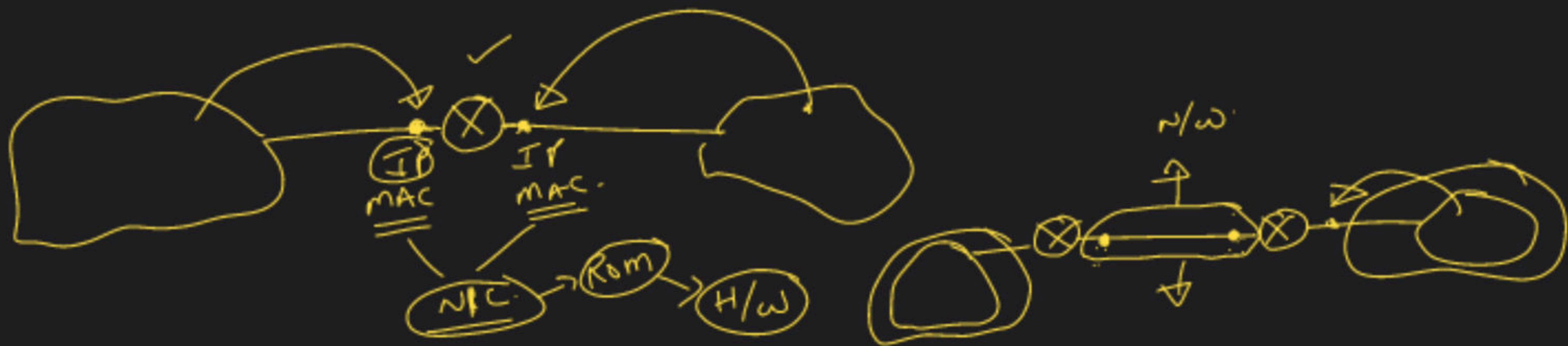
Computer Networks

Session Layer

Functions of Session Layer ✓

Authentication and Authorisation

Checkpointing

Synchronisation

Dialog control

SA
NA

N'C

Scripts   NIC

TL
NL
PLL
PL

end sep

logs

NIC
CPU
POW
Switch.

Functions of Session Layer

Authentication and Authorization ✓ ✗

Checkpointing

Synchronisation

Dialog control

Passwords.

fail

AL
PY
sem
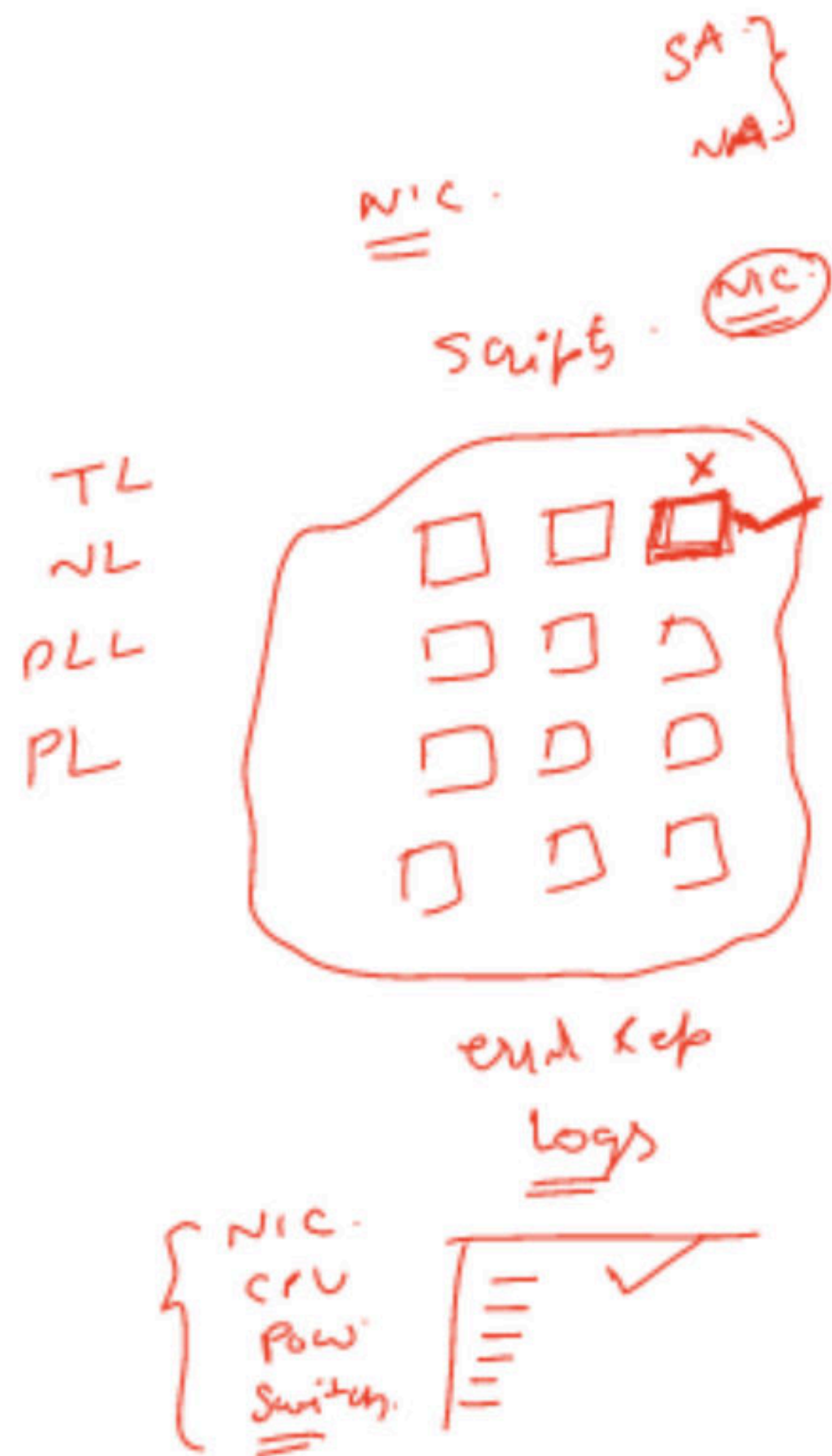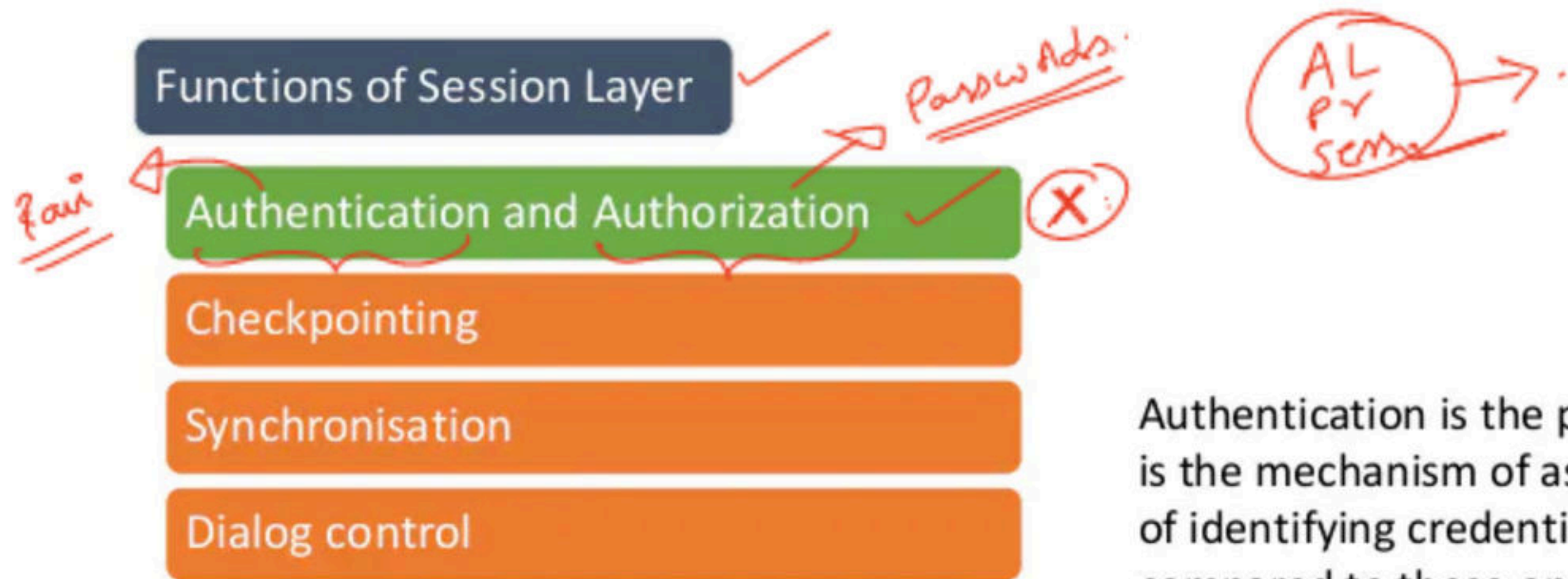
Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

Authorization is is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

Functions of Session Layer

- Authentication and Authorisation
- Checkpointing ✓
- Synchronisation
- Dialog control

Checkpoints

Video file

Even if the internet
Connection is lost,
Downloading will resume
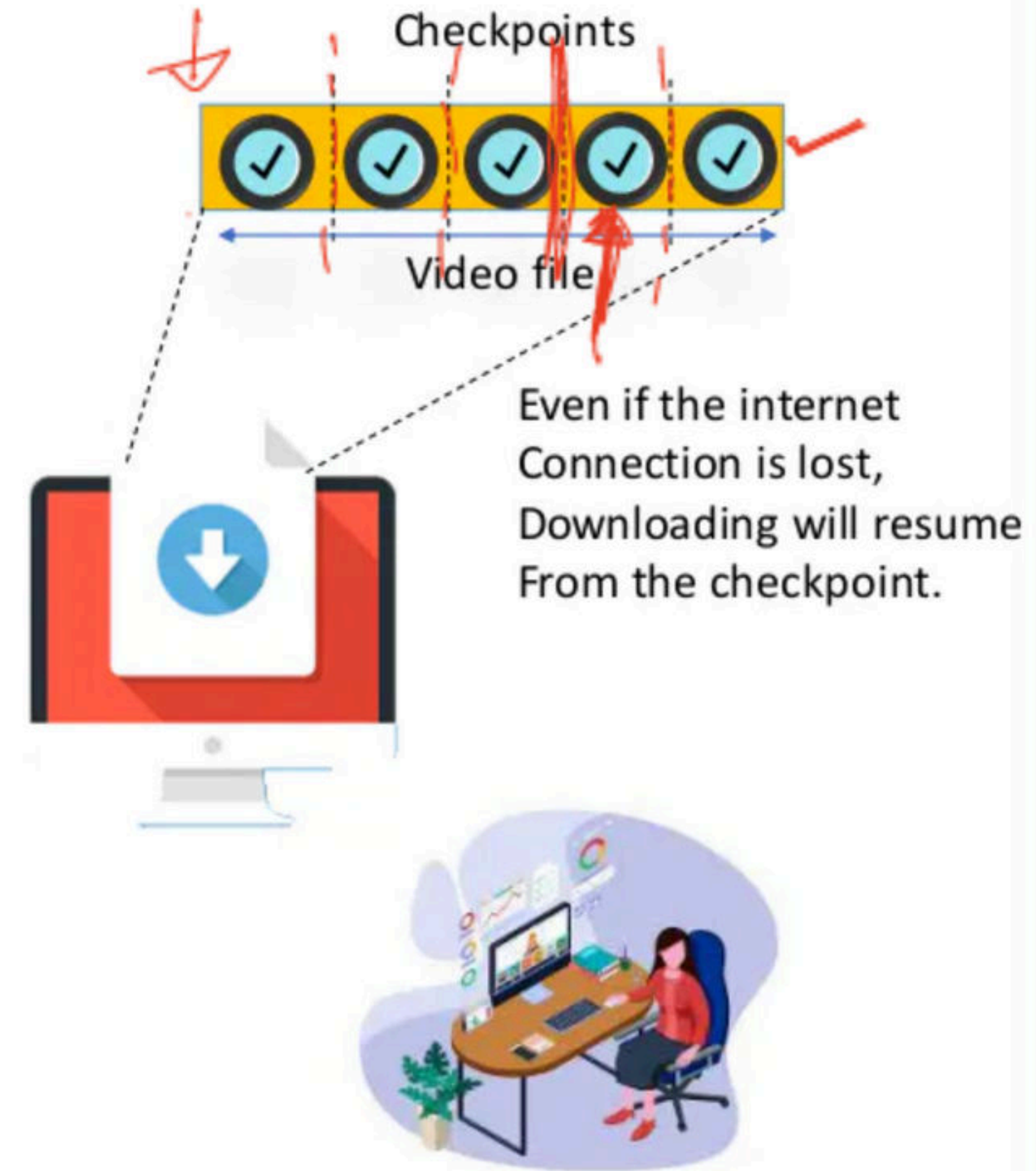From the checkpoint.

Functions of Session Layer

- Authentication and Authorisation
- Checkpointing
- Synchronisation
- Dialog control

Functions of Session Layer

Authentication and Authorisation

Checkpointing

Synchronisation

Dialog control

Video conferencing – Only one person must speak at once

Computer Networks

Presentation Layer and GATE 2014 question

Functions of Presentation Layer

Data Translation

Encryption and Decryption
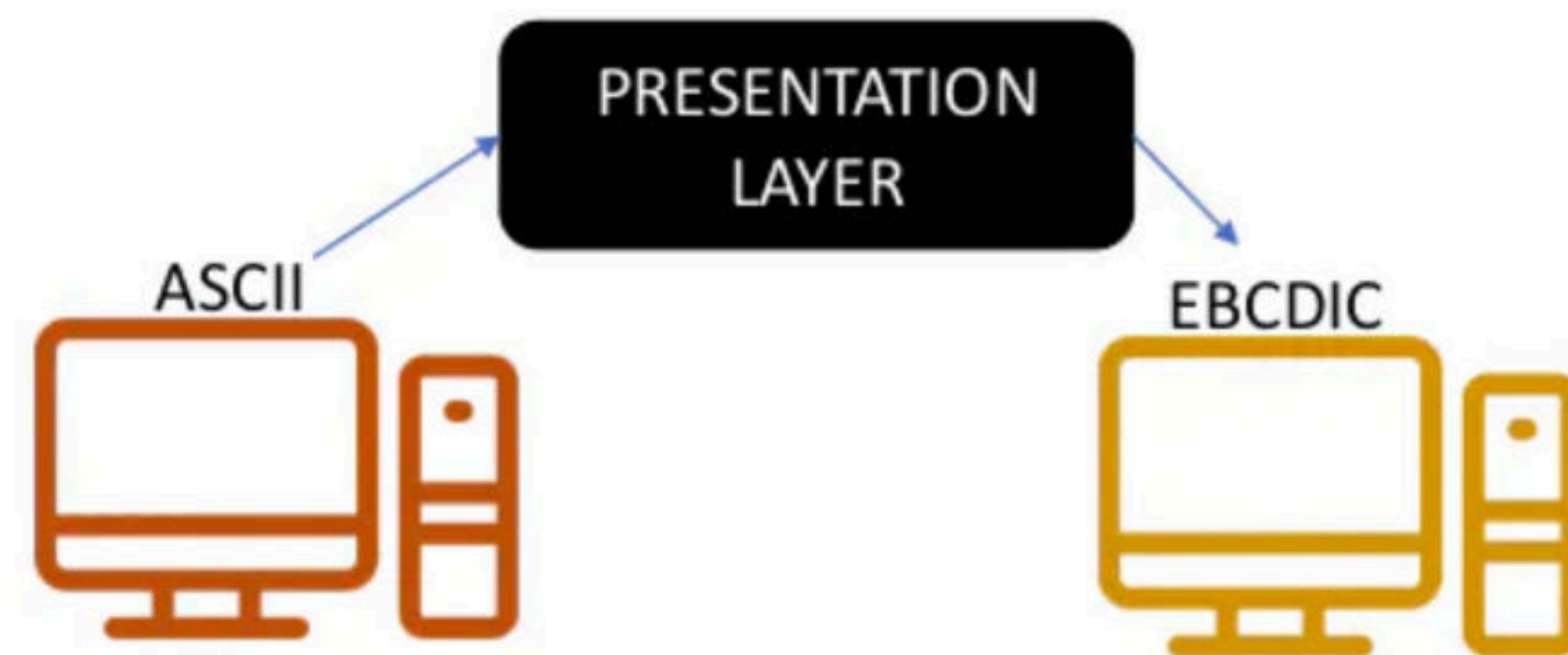
Data compression

Functions of Presentation Layer

Data Translation

Encryption and Decryption

Data compression

Encryption & Decryption

Plaintext   Encryption   Ciphertext   Decryption   Plaintext

Functions of Presentation Layer

Data Translation

Encryption and Decryption

Data compression

GATE 2014

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.

Q—R1—R2—R3—H

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

[I1] The URL of the file downloaded by Q

[I2] The TCP port numbers at Q and H

[I3] The IP addresses of Q and H

[I4] The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?

A) Only I1 and I2
B) Only I1
C) Only I2 and I3
D) Only I3 and I4

GATE 2014

An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.

Q—R1—R2—R3—H

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

[I1] The URL of the file downloaded by Q

[I2] The TCP port numbers at Q and H

[I3] The IP addresses of Q and H

[I4] The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?

A) Only I1 and I2

B) Only I1

C) Only I2 and I3

D) Only I3 and I4

Answer:

An Intruder can't learn [I1] through sniffing at R2 because URLs and Download are functioned at Application layer of OSI Model.

An Intruder can learn [I2] through sniffing at R2 because Port Numbers are encapsulated in the payload field of IP Datagram.

An Intruder can learn [I3] through sniffing at R2 because IP Addresses and Routers are functioned at network layer of OSI Model.

An Intruder can't learn [I4] through sniffing at R2 because it is related to Data Link Layer of OSI Model.

Computer Networks

Ethernet

Ethernet is one of the standard LAN technologies used for building wired LANs.
It is defined under IEEE 802.3.

Ethernet uses bus topology.In bus topology, all the stations are connected to a single half duplex link.

Ethernet uses CSMA / CD as access control method to deal with the collisions.

Ethernet uses Manchester Encoding Technique for converting data bits into signals.

For Normal Ethernet, operational bandwidth is 10 Mbps.

For Fast Ethernet, operational bandwidth is 100 Mbps.

For Gigabit Ethernet, operational bandwidth is 1 Gbps.

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header   DLL header   DLL tail
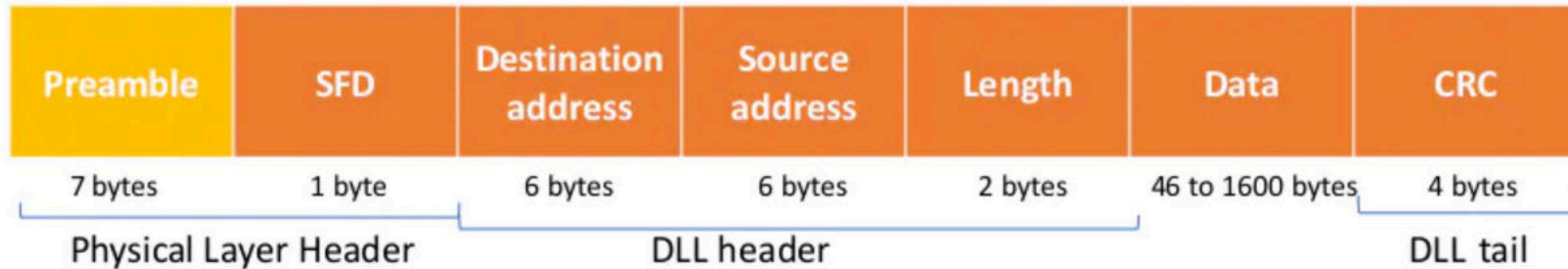
1. Preamble-

• It is a 7 byte field that contains a pattern of alternating 0's and 1's.

• It alerts the stations that a frame is going to start.

• It also enables the sender and receiver to establish bit synchronization.

Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header — DLL header — DLL tail
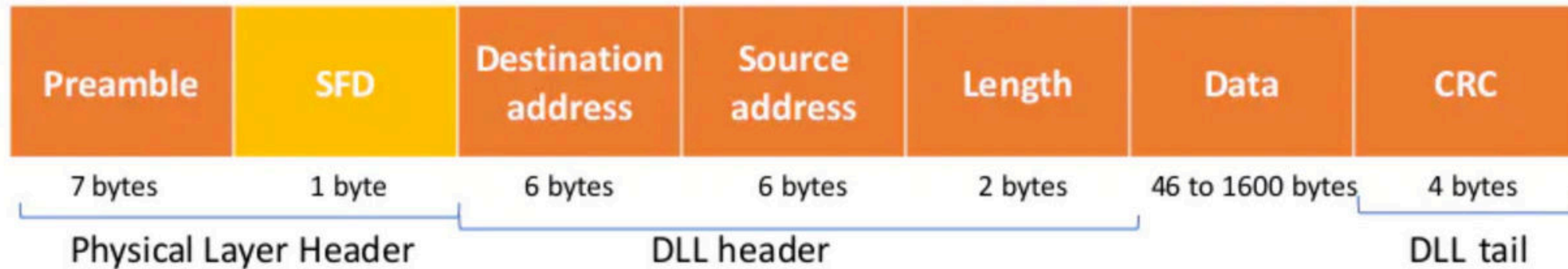
2. Start Frame Delimiter (SFD)-

•It is a 1 byte field which is always set to 10101011.
•The last two bits "11" indicate the end of Start Frame Delimiter and marks the beginning of the frame.

Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header · DLL header · DLL tail
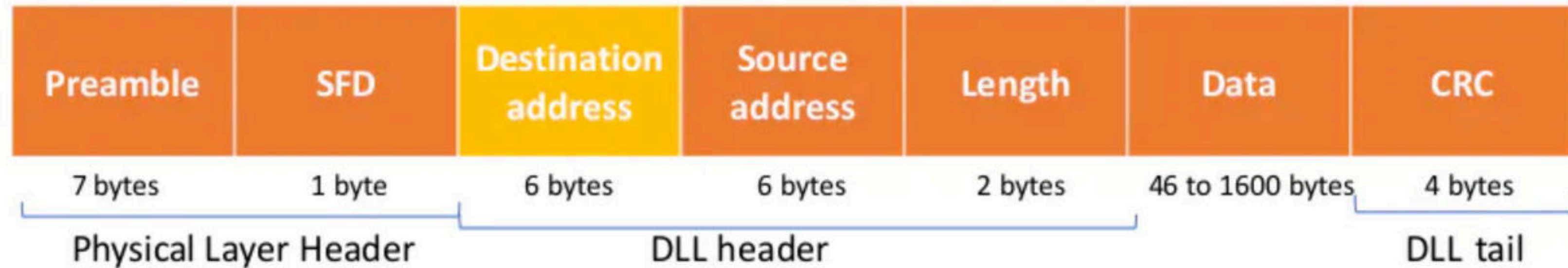
3. Destination Address-

•It is a 6 byte field that contains the MAC address of the destination for which the data is destined.

Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header   DLL header   DLL tail
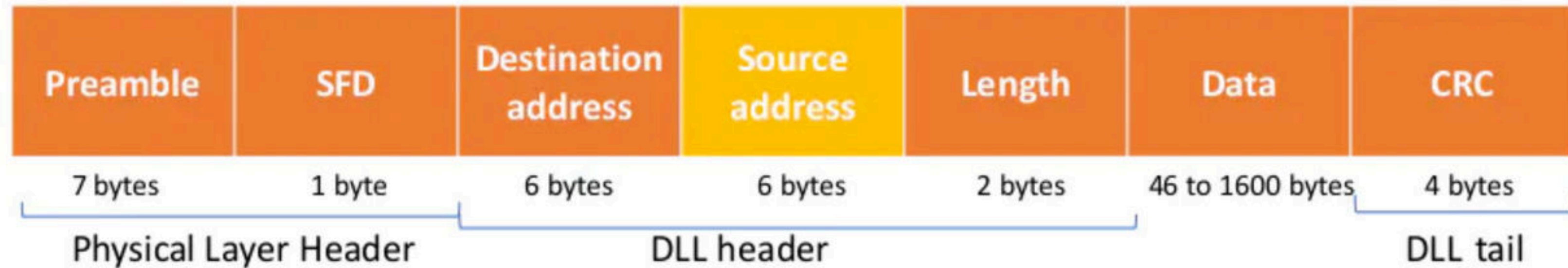
4. Source Address-

•It is a 6 byte field that contains the MAC address of the source which is sending the data.

Types of MAC address :-

There are three types of MAC addresses, which are:

1. Unicast MAC Address
2. Multicast MAC address
3. Broadcast MAC address

1.)Unicast MAC address:

The Unicast MAC address represents the specific NIC on the network.
A Unicast MAC address frame is only sent out to the interface which is assigned to a specific NIC and hence transmitted to the single destination device. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one destination NIC.

2.)Multicast MAC Address:

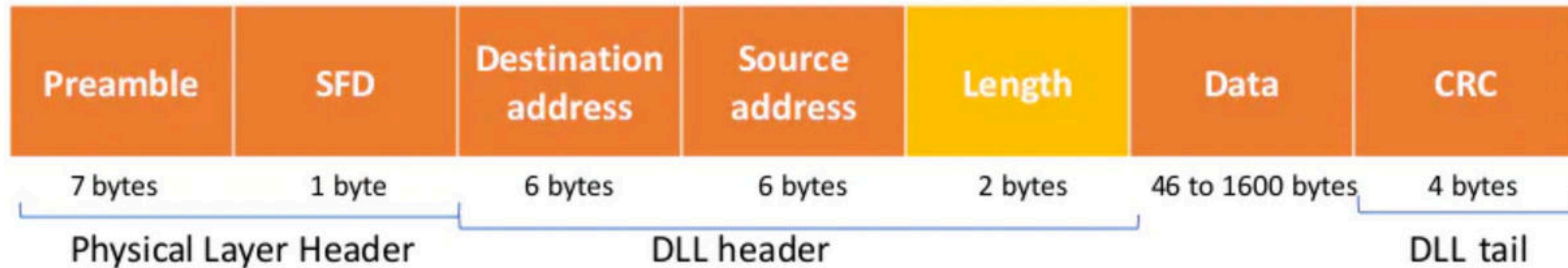Multicast addresses enables the source device to transmit a data frame to multiple devices or NICs.
In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) or first 3 bytes of the first octet of an address is set to one and reserved for the multicast addresses.

3.)Broadcast MAC address

It represents all devices within a Network. In broadcast MAC address, Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are known as a broadcast address.
All these bits are the reserved addresses for the broadcast. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belong to that LAN segment. Hence if a source device wants to send the data to all the devices within a network, that can use the broadcast address as the destination MAC address.
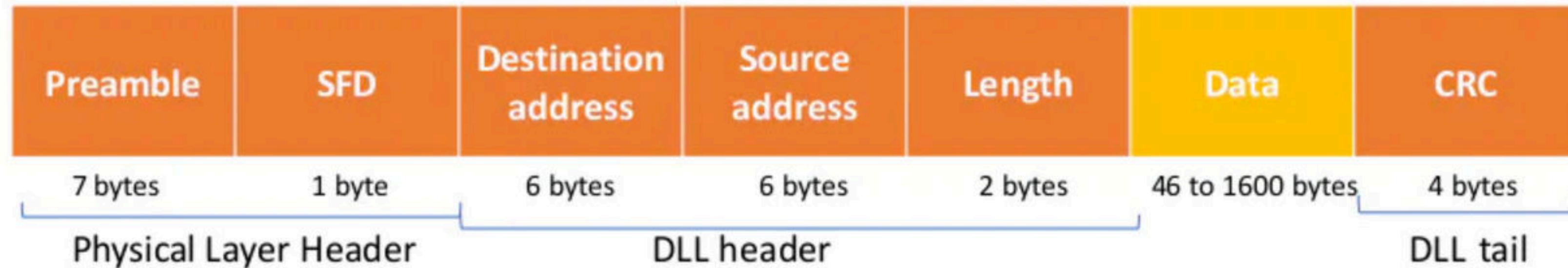
Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header — DLL header — DLL tail

5. Length-

• It is a 2 byte field which specifies the length (number of bytes) of the data field.
• This field is required because Ethernet uses variable sized frames.

• The maximum value that can be accommodated in this field $= 2^{16} - 1 = 65535$.
• But it does not mean maximum data that can be sent in one frame is 65535 bytes.
• The maximum amount of data that can be sent in a Ethernet frame is 1500 bytes.
• This is to avoid the monopoly of any single stati

Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header — DLL header — DLL tail

Minimum Length of Data Field

6. Data-

•It is a variable length field which contains the actual data.

•It is also called as a **payload field**.

•The length of this field lies in the range [46 bytes , 1500 bytes].

•Thus, in a Ethernet frame, minimum data has to be 46 bytes and maximum data can be 1500 bytes.

•Ethernet uses CSMA / CD as access control method to deal with collisions.
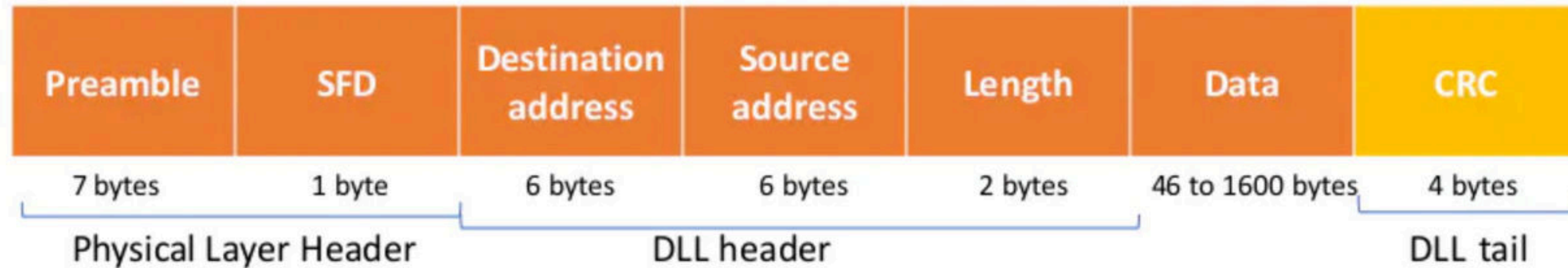
•For detecting the collisions, CSMA / CD requires-

   Minimum length of data packet = 2 x Propagation delay x Bandwidth

•Substituting the standard values of Ethernet, it is found that minimum length of the Ethernet frame has to be 64 bytes starting from the destination address field to the CRC field and 72 bytes including the Preamble and SFD fields.

•Therefore, minimum length of the data field has to be = 64 bytes − (6+6+2+4) bytes = 46 bytes

Maximum Length of Data Field

•The maximum amount of data that can be sent in a Ethernet frame is 1500 bytes.

•This is to avoid the monopoly of any single station.

•If Ethernet allows the frames of big sizes, then other stations may not get the fair chance to send their data.

Ethernet Frame Format

Preamble	SFD	Destination address	Source address	Length	Data	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 to 1600 bytes	4 bytes

Physical Layer Header   DLL header   DLL tail

7. Frame Check Sequence (CRC)-

• It is a 4 byte field that contains the CRC code for error detection.

Advantages of Using Ethernet-

It is simple to understand and implement.

Its maintenance is easy.

It is cheap.

Limitations of Using Ethernet-

Point-01:

It can not be used for real time applications.

Real time applications require the delivery of data within some time limit.

Ethernet is not reliable because of high probability of collisions.

High number of collisions may cause a delay in delivering the data to its destination.

Point-02:

It can not be used for interactive applications.

Interactive applications like chatting requires the delivery of even very small amount of data.

Ethernet requires that minimum length of the data must be 46 bytes.

Point-03:

It can not be used for client server applications.

Client server applications require that server must be given higher priority than clients.

Ethernet has no facility to set priorities.