Term paper: Role of Datalink Layer in communication and its protocols

Kanisha Shah
CSE, Institute of Technology
Nirma University
Ahmedabad, India
19BCE253@nirmauni.ac.in

ABSTRACT

Data Link layer is one of the protocol layers in OSI model which transfers the data from its above layer i.e. from Network to Physical layer. Here the vital role of this layer is that to free the data from error, while Network layer works on Source to Destination point of view. The specialty of this layer is that its “framing” assembly. It also provides the means to rectify the errors and usually correct it by one of its roles. Studying and simulating protocols to analyze and the drawbacks and addons present while transmitting payload or packets from one network to other in same LAN. The protocols are taken into consideration as their loopholes can be studied thoroughly and coming with a new idea. There are certain protocols used which enhances the facility provided by the specific layer

KEYWORDS

Payload, Transmission, Encapsulation, MAC, Automatic Repeat Request, Protocol, Acknowledgement, Redundancy, Synchronous, Network Interface Card.

INTRODUCTION

There are two types of protocol suites developed and they are:

1. TCP/IP Protocol Suite
2. OSI Model

Originally TCP/IP Protocol suite was defined of 4 layers and they are host-to-network, internet, transport and application. However, while upgrading to OSI Model host-to-network is equivalent to Physical + Data Link Layer, internet to Network Layer, application layer to Session + Presentation + Application Layer and transport layer takes care of duties of Session Layer.

OSI Model comprises of 7 layers as shown in the fig.
While Data Link Layer is subdivided into 2 parts as:

1. LLC/DLC (Logical /Data Link layer)
2. MAC (Multiple Access Control)

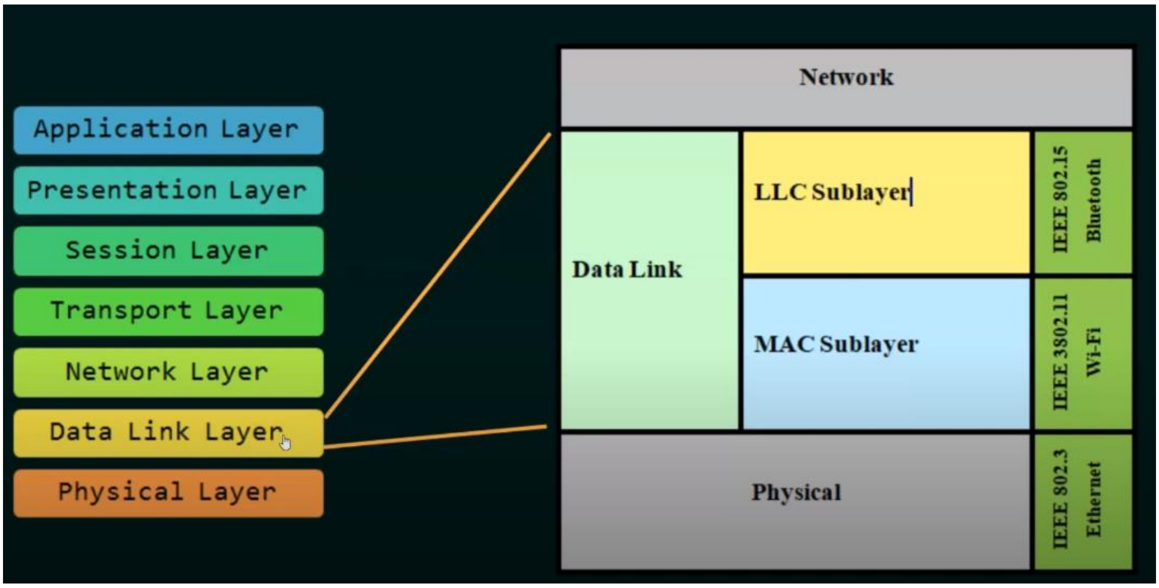
1. LLC/DLC

It handles communication between upper and lower layers i.e. Network and Physical layers.
It takes network protocol data and adds control information to help deliver the packet to the destination. (Flow Control)

2. MAC

It is implemented by the hardware, typically in the computer by NIC (Network Interface Card). As it is near to physical layer it works more on hardware concept. While a single company can’t issue more than 1 NIC on a single LAN connection.
It is subdivided into

a. Data Encapsulation
b. Media Access Control



Description

Data Link layer transforms the physical layer, a raw transmission facility, to a reliable link. By this physical layer appears Error-free from the network layer.

Roles of Data Link Layer:

1. Hop to Hop/ Node to Node Delivery
2. Flow Control
3. Error Control
4. Access Control
5. Physical Address

Hop to Hop/ Node to Node Delivery

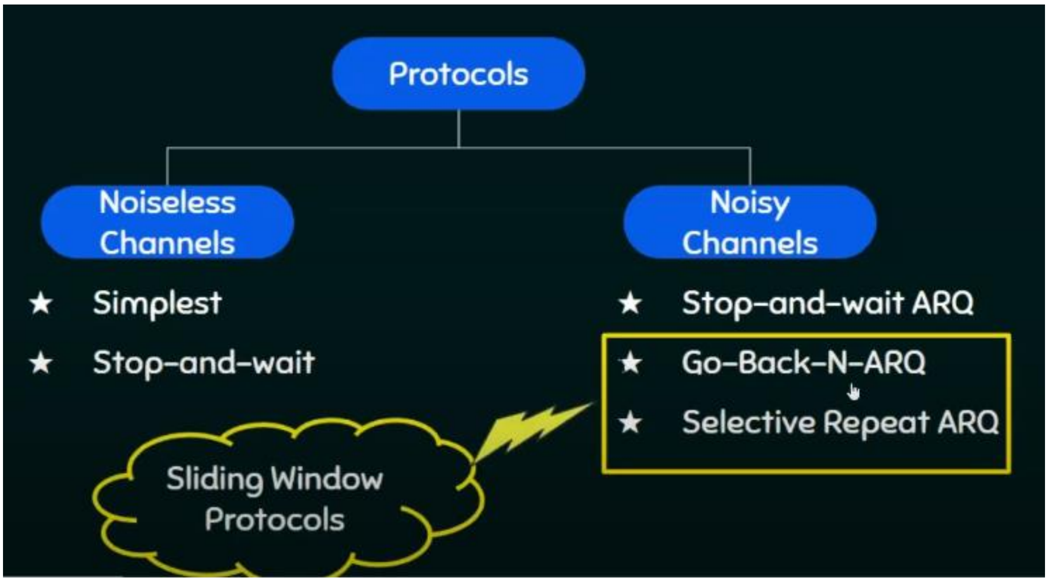
It works on the same LAN within a Network i.e. using a MAC/Physical Address. Like the Network layer works on the same point of view but it works on the basis of Source to destination hence it is more reliable when the network changes. It even works on a different LAN connection but probably used in same LAN hence between the networks present into them. For eg. Passing a data from A--B--C--D, Now suppose B and C are acting as routers thus data link appends headers in every passage of data. Likewise moving in consecutive systems datalink changes.

Flow Control

As the name suggest it works on the speed to transfer the data. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender system, here datalink imposes the flow control mechanism to avoid overwhelming the receiver side. Hence if some router gets overloaded, then we have to must delete our buffer.
Same is done by Network layer but under the view of whole system, but here at every node it works.

Protocols undertaken are:

1. Stop-and-Wait
2. Go-Back-N
3. Selective Repeat


Protocols

Noiseless Channels

★ Simplest

★ Stop-and-wait

Noisy Channels

★ Stop-and-wait ARQ

★ Go-Back-N-ARQ

★ Selective Repeat ARQ

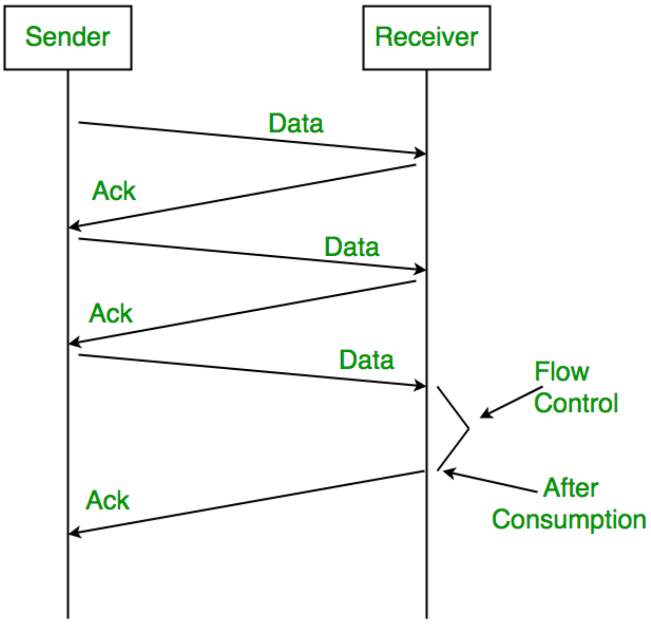
Sliding Window Protocols

Stop-and-Wait

- It is unidirectional in nature.
- Here only 1 frame transmits at a time and other is transmited after receiving the acknowledgement. It is the case that utilises the lowest bandwith and eficiency.
- Sender window i.e. capacity is 1 and samefor the receiver side. Here retransmission is the lowest that is 1 as only one frame is sent at a time.

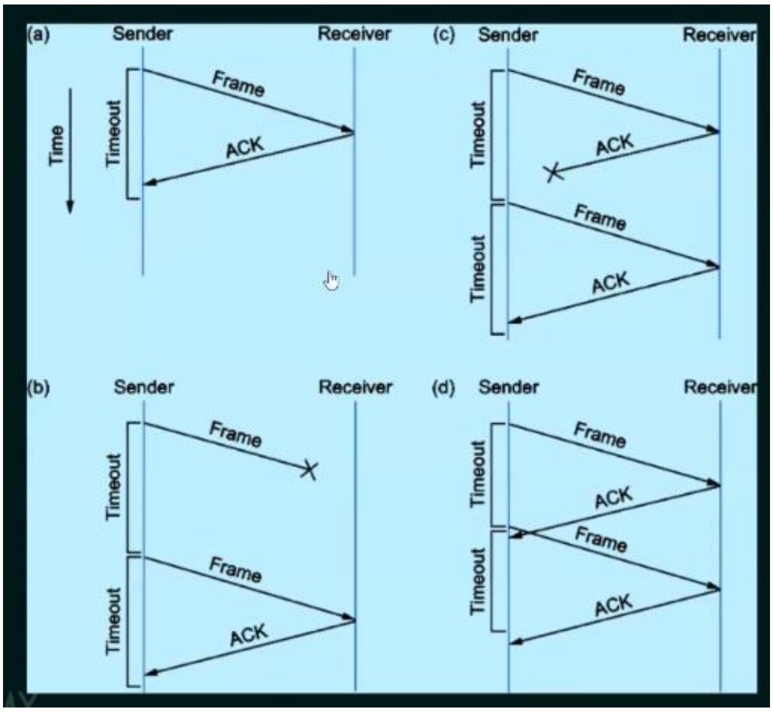
Drawback:

- Sender waits for the acknowledgement for an infinite amount of time.
- It can be a case like where the acknowledgement may lost or delay.
- Size of window is too small, thus can't be used in daily basis.



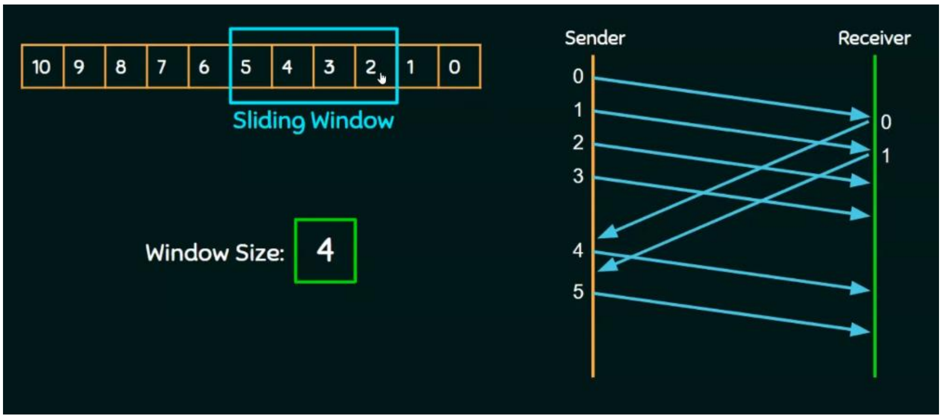
Stop-and-Wait-ARQ

Here the same approach is followed as above but it won't wait for timeout timer to end. It will directly send the data packet again.



Stop-and-Wait ARQ = Stop-and-Wait + Timeout Timer + Sequence number

Sliding Window Protocols

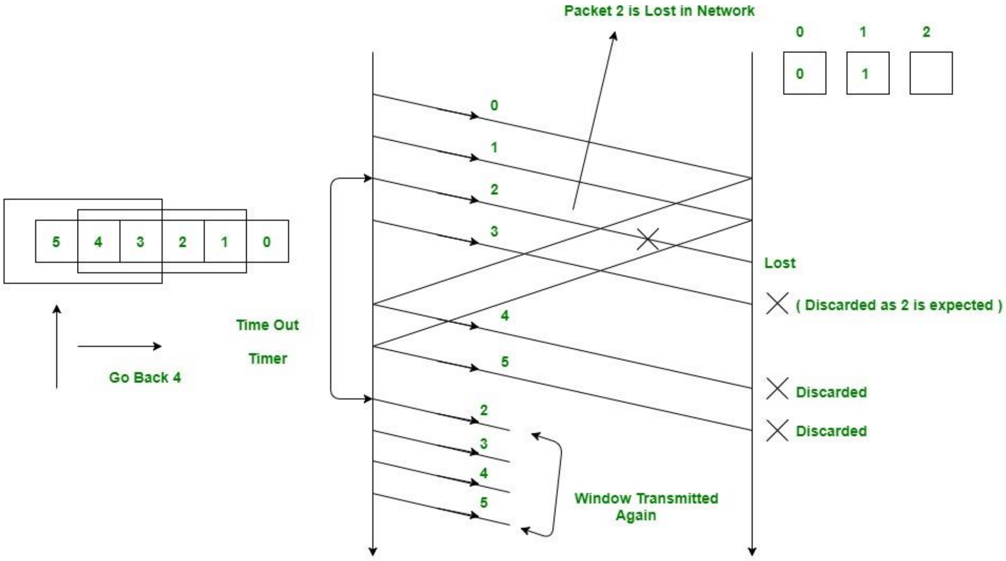


Go-Back-N-ARQ

It transfers multiple frames. Here sender window is larger comapred to the previous one, while the receiver window remains the same. It is one of the sliding approach. As the receiver accepts only one at a time thus packets are accepted in order. It possess cummulative acknowledgement i.e. if 3 packets are received it sends 4 as an acknowledgement. Here retransmission is maximum as if the receiver wants a specific packet it will retransmit all of the rest.

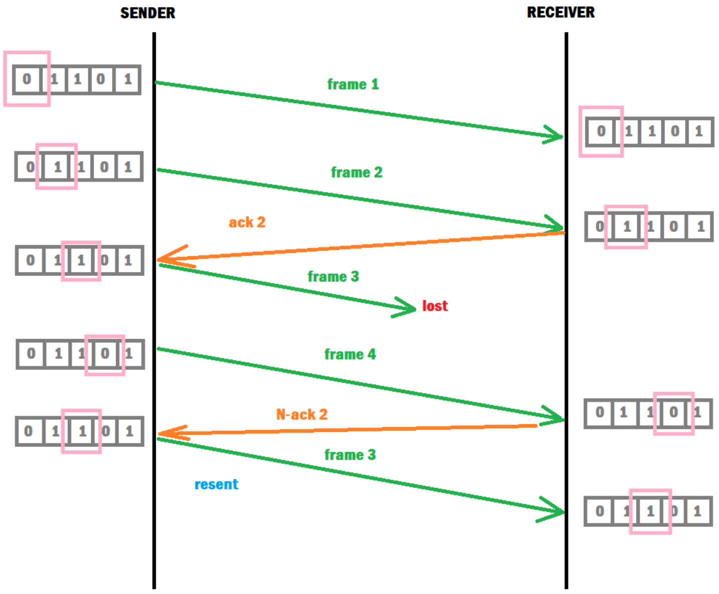
Drawback:

Retransmission is more.



Selective Repeat ARQ

It is same as above, a multiple frames handler. It is combination of both thus possess some of the characteristics of each of them. Like sender and receiver window size is same but more is size i.e. 2^{k-1}. While it accepts out of order packets. Hence less retransmission occurs i.e. 1. It possess both cummulative an independent acknowlegdement. Hence addition of searching + sorting. One more addon then above two is Negative acknowlegdement (where it do not wait till time out timer)



Error Detection & Correction/ Error Control

Error

As we know error can occur while transmitting the packet due to certain reasons like attenuation, distortion and noise. Error can be Single bit and Burst error. While talking about single bit, a single bit is changed and while burst error occurs when a series of bits are modulated during the transmission.
Eg. 101 ----- 100
Eg. 101010 ----- 111011

Detection

It is subdivided as:

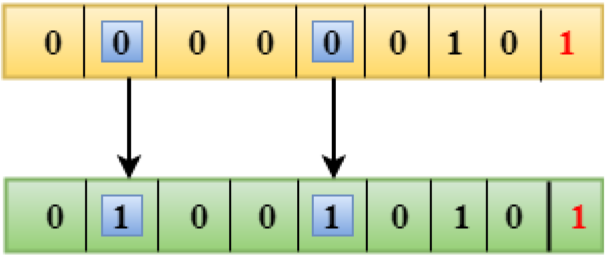
1. Simple Parity/Single Parity
2. 2-D Parity Check
3. Check Sum
4. Cyclic Redundancy Check

1. Single Parity

Here data bits are more compared to redundant bits which are used for detecting the errors. Here audio is transferred it is least expensive and possess (m+1) bits.
It works on even parity. It can detect all the single bit error in a code word. While detect all odd no. of error also.

Drawbacks

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.

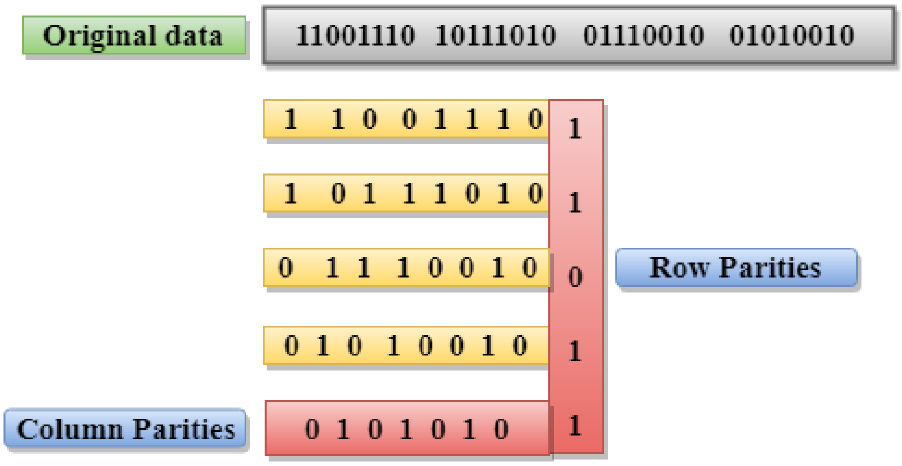


2. 2-D Parity Check

Here it organises in form of a table, i.e. it divides into row and column. Parity check bits are computed for each row, hence it equals to single parirt check. Here redundant row of bits is added to the whole block. Parity bits are checked at the receiving end.

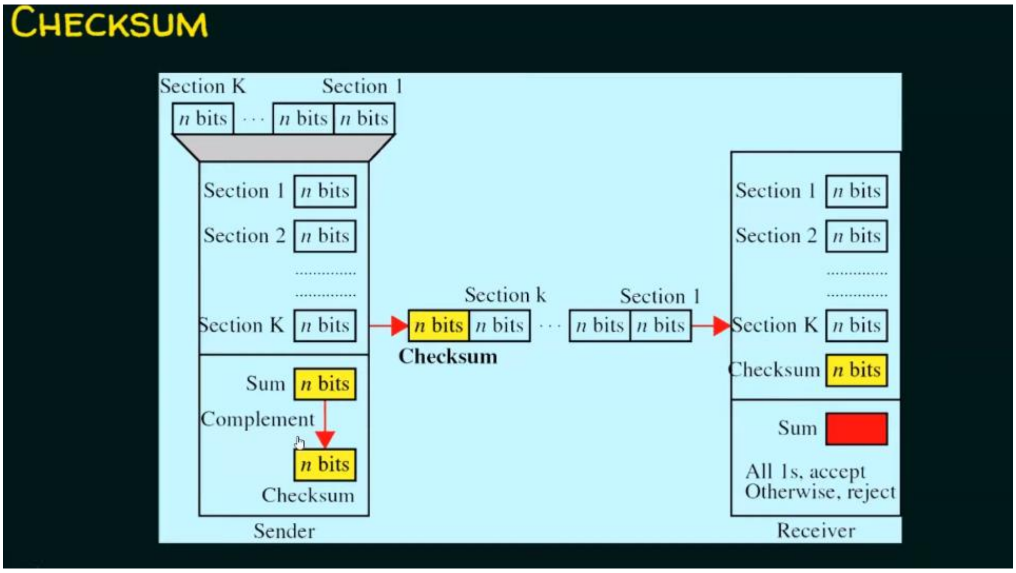
Drawbacks

- This technique can't detect error for 4-bit
- If two bits at same position are corrupted and the bits at exactly same position is corrupted, then it is not capable to detect the error



3. Check Sum

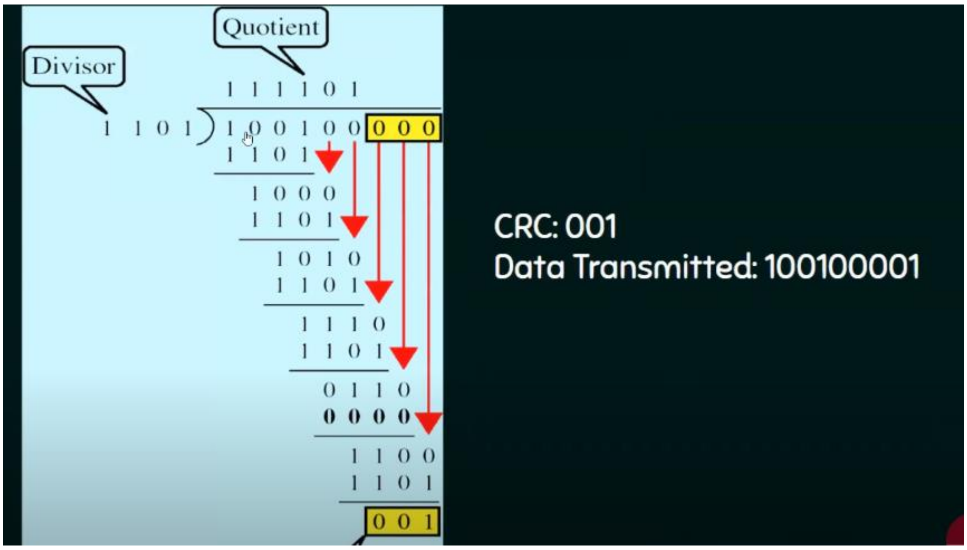
- As the name suggest it is addition of check and sum, thus checks the data and adds up them. Here we have to break the data into ‘k’ blocks, sum up all data bits then adding them all with the carry finally doing 1’s compliment.
- Detects all errors involving an odd no. of bits.
- Similarly detects most errors involving an even no. of bits.



CHECKSUM

4. Cyclic Redundancy Check

It is more powerful. Most widely used methods in real life environment. This can detect all odd no. of errors, single bit, burst error of length equal to polynomial degree. Here total bits are (m+r) where m are original data bits and r is redundant (maximum power of polynomial).



CRC: 001
Data Transmitted: 100100001

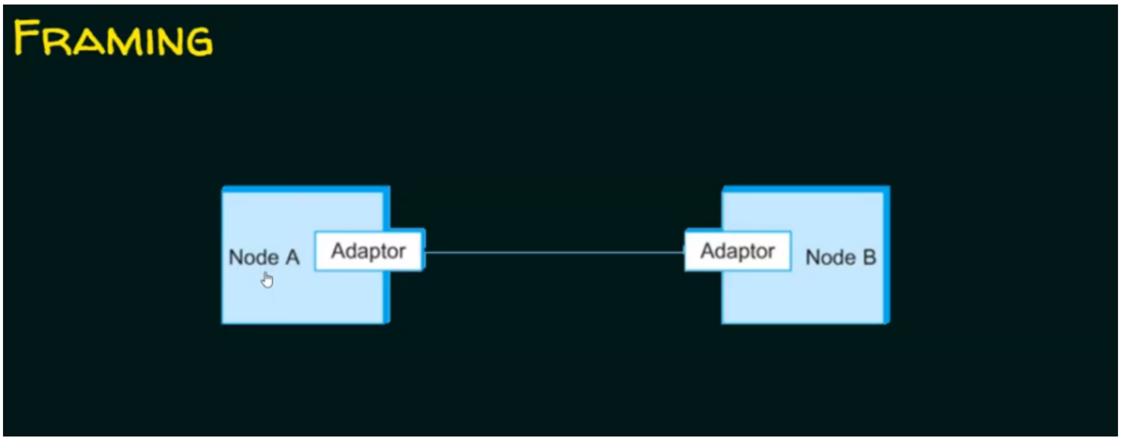
ADDITIONAL INFORMATION AND CONTENT

Data Encapsulation

Frame is assembled before transmission and frame is disassembled upon reception.
Here it adds the header and trailer to the network layer packet.
While header comprises of the information of receiver's address and trailer only controls in the phase of error detection. It undergoes the functionalities as:

a. Framing
b. Physical Address/Media Access Control
c. Error Control

It is responsible for the placement of frames on the media and the removal of frames from the media.
Communicates directly with the physical layer.



Here bits flow between adaptors while frames flow between hosts.
Frame comprises of Header + Network Layer packet + Trailer.
Framing on basis of Size is subdivided into two parts i.e.

1. Fixed Size
2. Variable Size

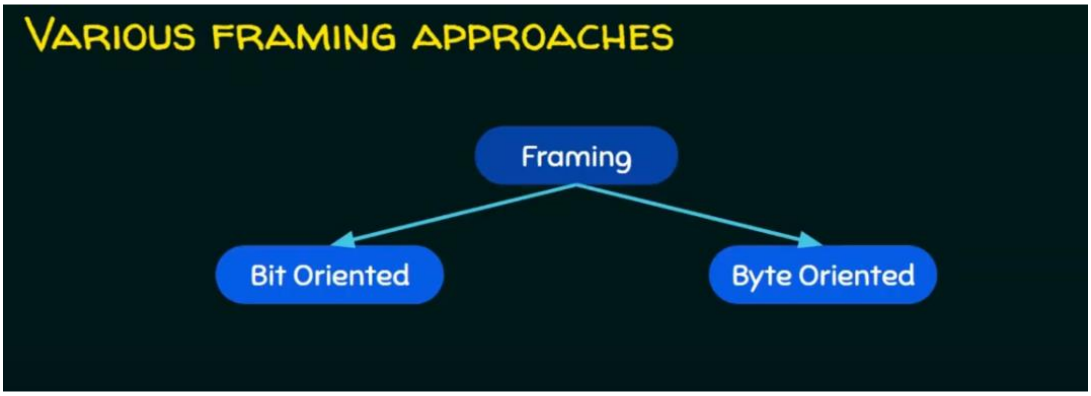
1. Fixed Size

Length is delimeter of frames

2. Variable Size

Additional mechanism is used for beginning and ending of frame.
More frequently used as frame size is more transmitted in variable size.

Framing Approaches



Bit Oriented

Frames comprises of bits
They can be interpreted as text as well as multimedia data.

Byte/ Character Oriented

It is one of the oldest approaches
Frame composed of bytes which is equal to 8 bits.

Clock Oriented

Eg. Sonet

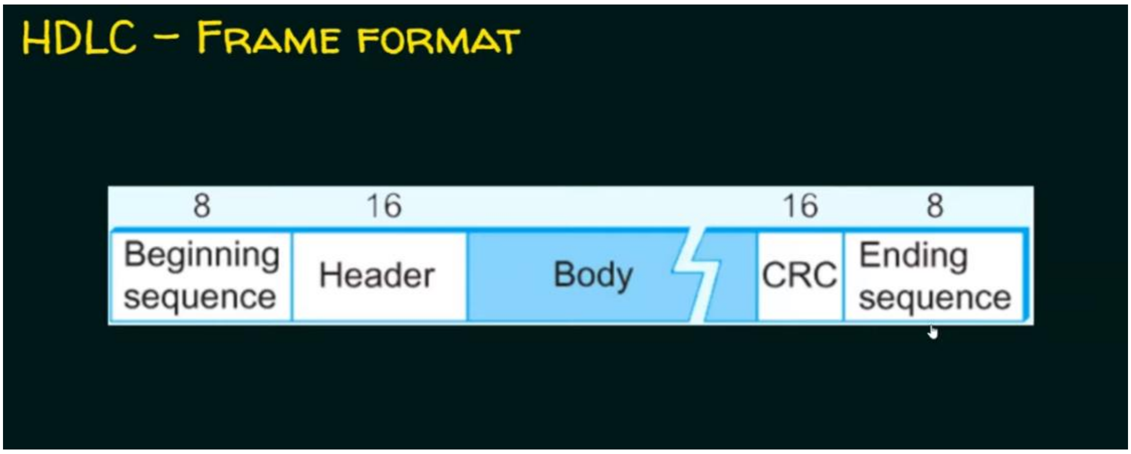
Protocols followed in framing approaches are as follows:

1. HDLC (High Level Data Link Control)
2. BISYNC/BSC (Binary Synchronous Communication)
3. Point to Point
4. DDCMP(Digital Data Communication Message Protocol)

1. High Level Data Link Control

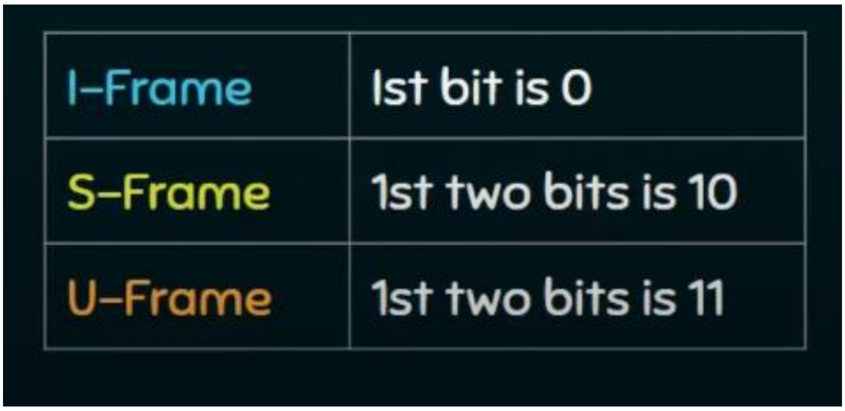
It is a bit oriented protocol. Being Synchronous datalink control protocol developed by IBM. It has transformed from SDLC TO HDLC. While start and end sequence remains the same. The main motto of this protocol is that it transmitts during any times when the link idle so that the sender and receiver can keep their clocks synchronised.

Header: Address and Control Field
Body: Payload (Variable Size)
CRC: Cyclic Redundancy Check,trailer



HDLC – FRAME FORMAT

8	16		16	8
Beginning sequence	Header	Body	CRC	Ending sequence

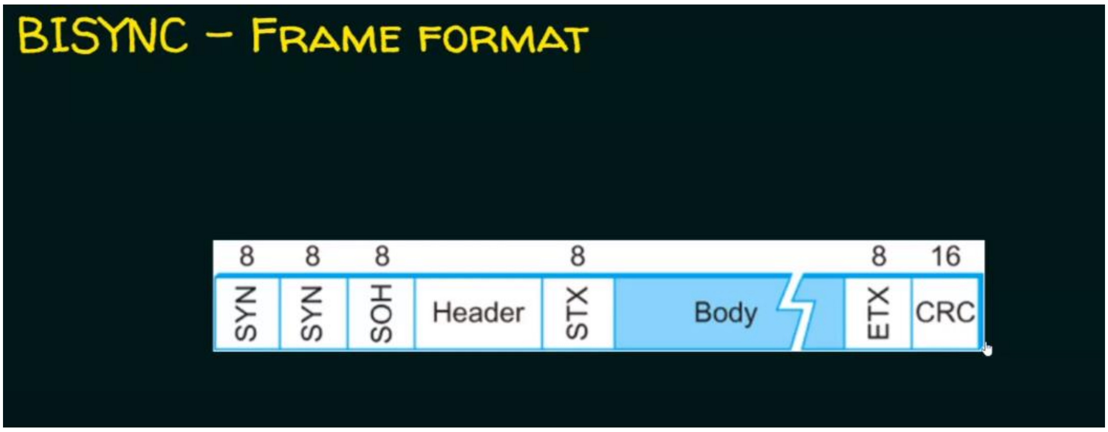


I-Frame	Ist bit is 0
S-Frame	1st two bits is 10
U-Frame	1st two bits is 11

2. Binary Synchronous Communication

It is a sentinal approach. Developed by IBM. Here character stuffing occurs by adding 1 extra byte whenever there is a flag or escape in text which is done by DLE. It is half-duplex link protocol, announced in 1967 after the introduction of System/360. It replaced the synchronous transmit-receive (STR) protocol used with second generation computers.

SOH – Start of Header
ETX – End of Text
STX – Start of Text
Body – Payload



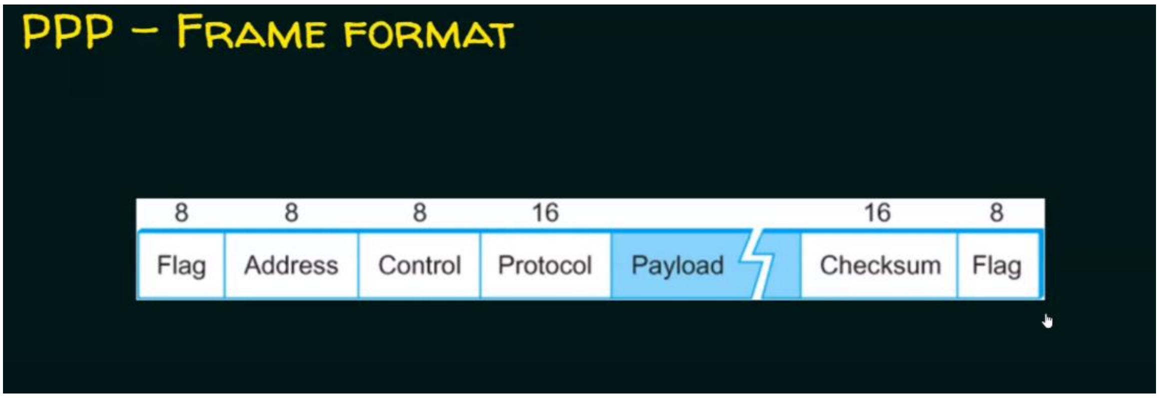
BISYNC – FRAME FORMAT

8	8	8		8		8	16
SYN	SYN	SOH	Header	STX	Body	ETX	CRC

3. Point to Point

It is one of WAN protocol. Runs over Internet Links and widely used in braodband communicationhaving heavy loads and hogh speeds. There ia Multiprotocol data between 2 directly connected component. Character/ Byte stuffing occurs for redundancy. The main cause to provide unique data with some backups is that if during transmission the data gets hampered extra bits are available which signifies that.

Flag - 01111110 , it is fixed
Address – all 1's in case of broadband.
Control – Constant Value

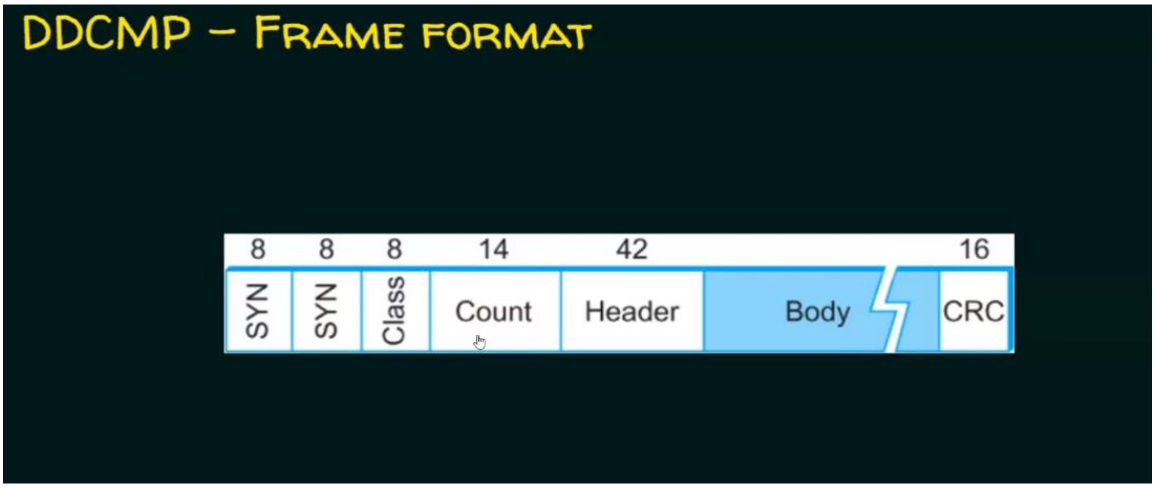


PPP – FRAME FORMAT

8	8	8	16		16	8
Flag	Address	Control	Protocol	Payload	Checksum	Flag

4. Digital Data Communication Message Protocol

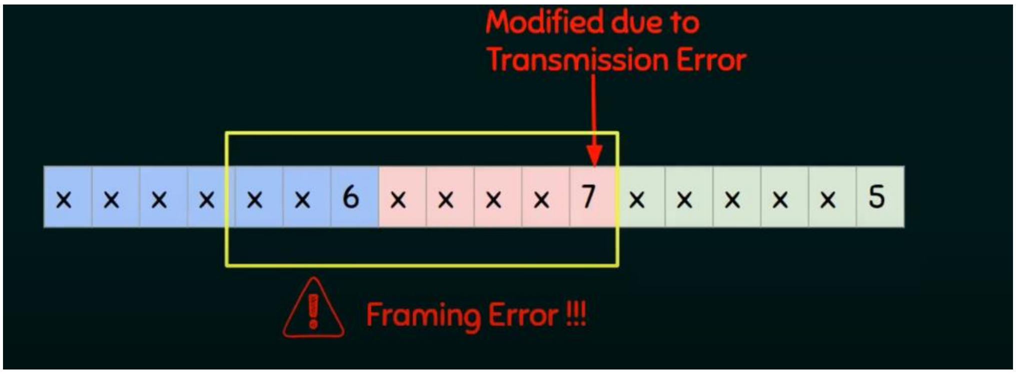
Devised by digital equipment corporation. It is Byte-counting approach. Here "count" signifies how many bytes are contained in frame body. If the countfield gets disturbed it generates a huge error.



DDCMP – FRAME FORMAT

8	8	8	14	42		16
SYN	SYN	Class	Count	Header	Body	CRC

Like here the digits signifies the count, while if any digit is distorted in between the whole data is interpreted wrong.



Multiple Access Control

If there is a dedicated link between the sender and receiver then the datalink control is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.
Hence multiple access protocols are required to decrease collision and avoid crosstalk.
It is similar to broadcasting like at the same time more than one system want to send the data which the data gets distorted in whole hence some protocols must be followed and they are as:

1. **Random Access**
   a. Aloha (Pure , Slotted)
   b. CSMA (Carrier Sense Multilpe Access)
   c. CSMA/CD (Carrier Sense Multilpe Access/ Collision Detection)
   d. CSMA/CA (Carrier Sense Multilpe Access/ Collision Avoidance)
2. **Control Access**
   a. Polling
   b. Token Passing
   c. Reservation
3. **Channelization Protocols**
   a. FDMA (Frequency Division Multiple Access)
   b. TDMA (Time Division Multiple Access)
   c. CDMA (Code Division Multiple Access)

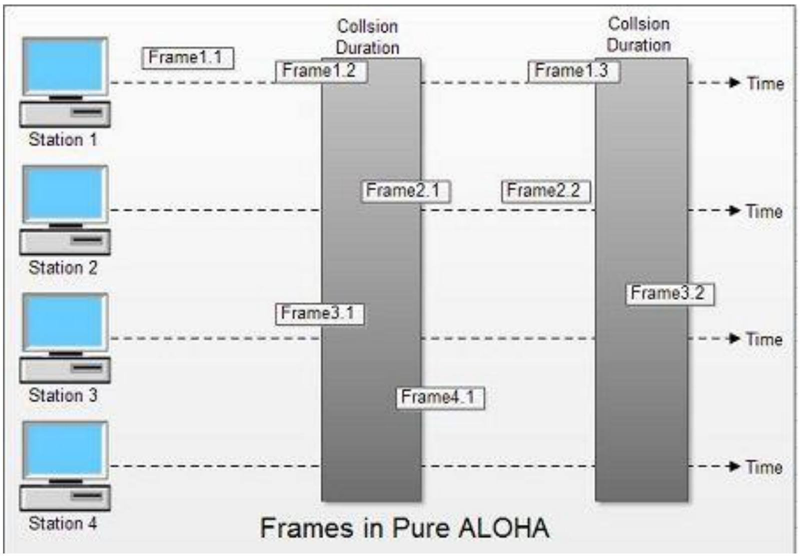
Random Access Protocol

Here all stations are superior in nature. Hence any station can send data anytime, thus leads to collision. Here each station has a right to the medium without being controlled by any other station. Collision leads to distortion or modification of data.

Pure Aloha

Any station can start transmission whenever the data arrives, henec it is very flexible. It needs an acknowledgement. It is LAN based in nature. Retransmission process occurs n collision. Here only transmission time is seen not propogation time.

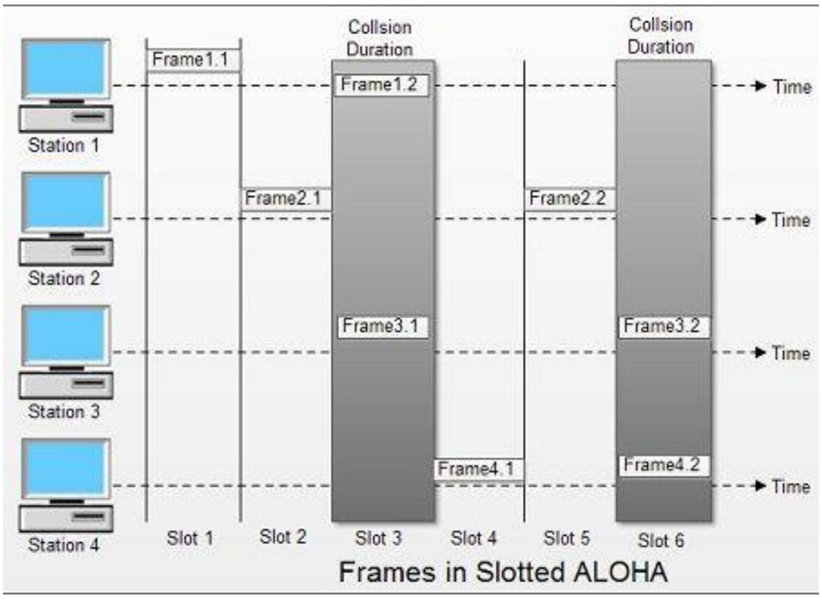
Vulnerable Time: 2 x Transmission time



Slotted Aloha

It always starts transmission at the beginning, as they are divided into blocks of Transmission time duration. Here collision do occur when two or more frames start the same time. More efficient compared to pure one.

Vulnerable Time: Transmission time



CSMA (Carrier Sense Multilpe Access)

It is prior to the Aloha methods. Here to minimize the chance of collision and therefore, increase the performance, the CSMA methods were developed. It's priciple is "Sense Before Transmit" or "Listen Before Talk". Carrier may be busy or idle hence mustbe seen before. The possibility of collision still exists because of propogation delay; a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

CSMA/CD (Carrier Sense Multilpe Access/Collision Detection)

- It is effective after a collision.
- It is used in wired networks.
- Reduces recovery time.
- It resends the data frame in case a conflict occurs during transmission.

CSMA/CA (Carrier Sense Multilpe Access/Collision Avoidance)

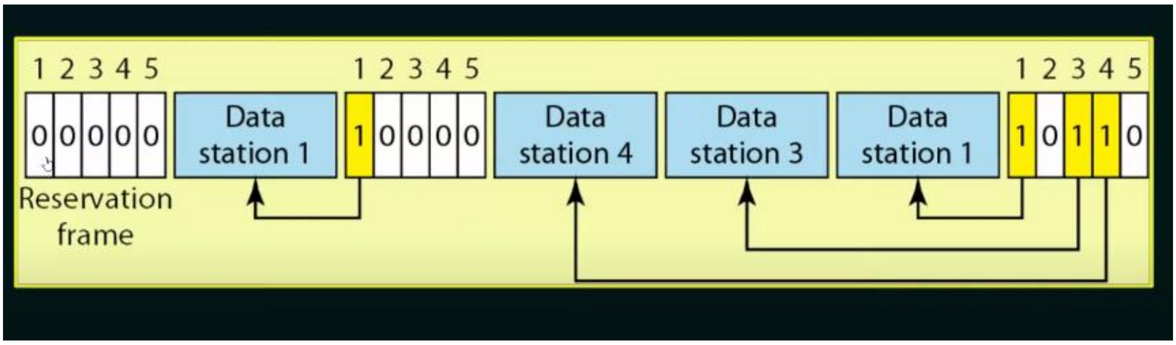
- It is effective before a collision
- It is generally used in wireless networks
- It minimises the risk of collision
- It initially transmits the intent to send the data, once an acknowledgment is received, the sender sends the data.

Control Access

Here no-one is superior or inferior, they consult one another to find which is the perfect station to send the packet. A station can't send unless it gets authorised by other station. Thus when station gets authorised it is superior at that vary moment.

Reservation

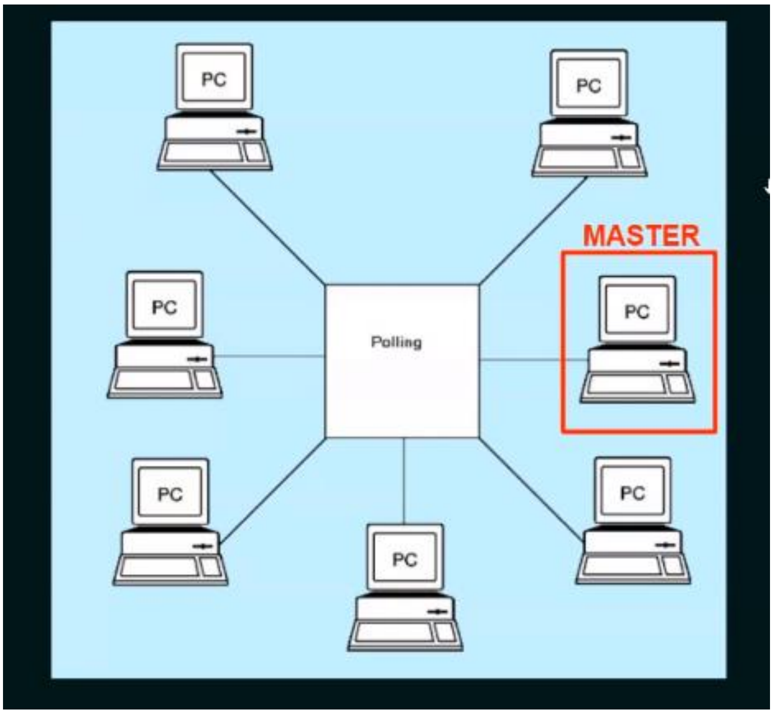
A station always needs to make a reservation before sending the data. In each interval a reservation frame precedes the data frames sent in each interval. As there are N stations thus leads to N minislots in reservation frame, thus minislot belongs to a specific station. So, wherever the station wants to send the data it first needs to reserve its place in th slot.



Polling

It requires one of the nodes to be designated as a Master node(Primary Station). It polls each of the node ina round-robin fashion. If master node selects 1st node, it can transmit according to the limit fixed by master node. Likewise nextly it selects the 2nd node and thus the process repeats.

Here polling protocol eliminates the collisin. This achieves much more higher efficiency.

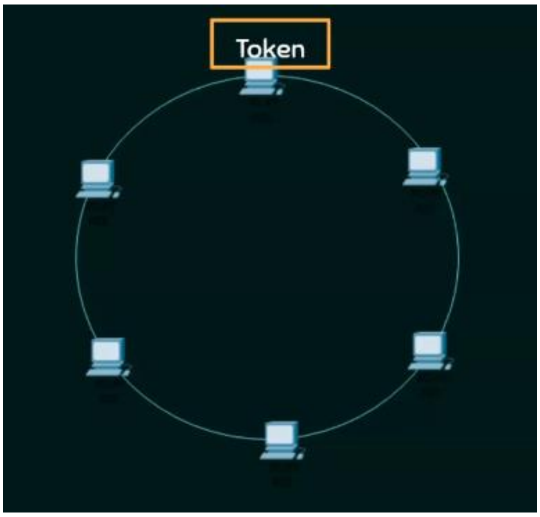


Drawback

- This protocol introduces a polling delay that is the amount of time required to notify a node that it can transmit.
- If the master node fails, the entire channel becomes inoperative.

Token Passing

Here there is no master node. Hence here the anology follows is like you send or pass a token to the next station when your whole or maximum fixed data is transmitted. A station is authorised to send the data when it receives the token or a special frame. A “Special frame” is a small, special-purpose frame known as a token is exchanged among the nodes in some fixed order. While completing the transmission it have to pass the token to the next upcoming node.
Here token passing is decentralised and highly efficient.



Drawbacks

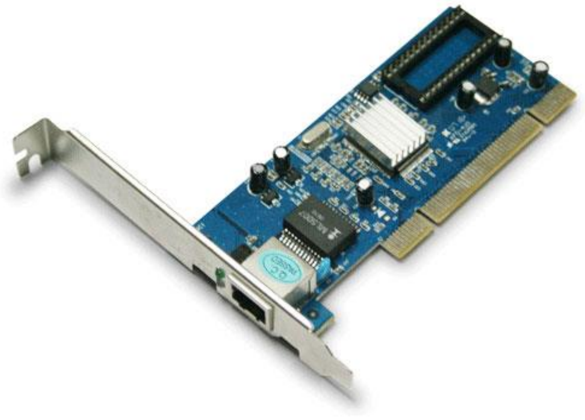
If the failure of one node which holds the token can crash the entire channel.
If the node accidentally neglects to release the token then some recovery procedure must be invoked to get back the token.

Channelization Protocols

Here the available bandwidth of a link possessing different channels is shared among the stations in terms of time, frequency or by phase of code.

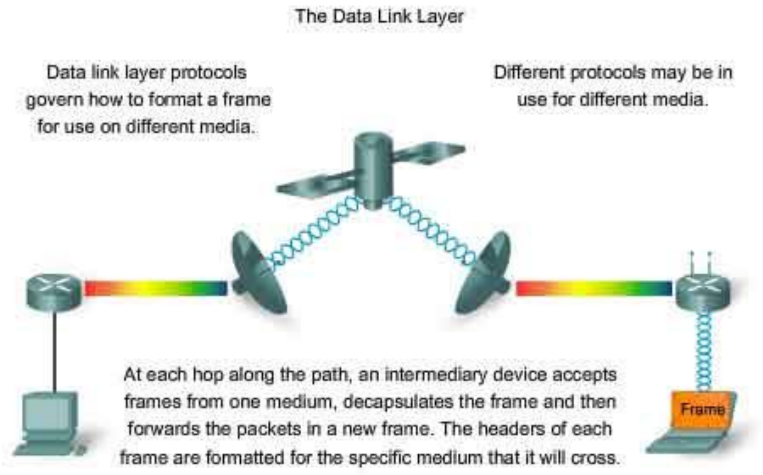
RELATED APPLICATIONS AND EXAMPLES

- The NIC (Network Interface Card) operates in the data link layer of the OSI reference model for networking which is inserted into the system bus of the computer and connect the software processes and physical that is hardware media.



(Network Interface Card)

- The IEEE 802.11 standards which is an upgraded version of IEEE 802, includes the physical layer and medium access control layer (MAC) of the data link layer specifications for implementing the Wireless local area network (WLAN) to support infrastructure.
- Once the request from your web browser has been created it is sent to the network card. Once it reaches your network card it must be converted into a message that is sent from your computer to the default gateway which will forward the message to the Internet. At the DATA LINK layer, the web request is inserted inside a network request to the default gateway.


The Data Link Layer
Data link layer protocols govern how to format a frame for use on different media.
Different protocols may be in use for different media.
At each hop along the path, an intermediary device accepts frames from one medium, decapsulates the frame and then forwards the packets in a new frame. The headers of each frame are formatted for the specific medium that it will cross.
Frame

ACKNOWLEDGMENT

I would like to humbly express my gratitude towards my teacher, Prof. Sharada Valiveti and Prof. Umesh Bodkhe for giving me this amazing opportunity to explore and learn new things. The project helped me in doing a lot of research about the topic and even more related topics which increased my interest into the field.

REFERENCES

[1] https://www.tutorialspoint.com/difference-between-csma-ca-and-csma-cd
[2] https://www.tutorialspoint.com/reservation-protocols-in-computer-network
[3] Behrouz A Forozan, “Data Communications and Networking”, Fourth Edition.
[4] https://ukdiss.com/examples/physical-layer-data-link-layer.php
[5] https://www.inetdaemon.com/tutorials/basic_concepts/network_models/osi_model/real_world_example.shtml