Explain CSMA Protocols. Explain how collisions are handled in CSMA/CD.

CSMA Protocols stands for Carrier Sense Multiple Access Protocols. CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network. Devices attached to the network cable listen (carrier sense) before transmitting. If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

Types of CSMA Protocols:

1.**Persistent CSMA**

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called I-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over again.

Advantages:

- Due to carrier sense property 1-persistent CSMA gives better performance than the ALOHA systems.

Disadvantages:

- Propagation Delay

2.**Non-Persistent CSMA**

- In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
- After this time, it again checks the status of the channel and if the channel is free it will transmit.
- A station that has a frame to send senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantages:

- It reduces the chance of collision and leads to better channel utilization,

Disadvantages:

- It reduces the efficiency of network because the channel remains idle and it leads to longer delays than 1-persistent CSMA.

3.**P-Persistent CSMA**

- Used for slotted channels.
- When a station becomes ready to send, it senses the channel.
- In this method after the station finds the line idle, it may or may not send.
- If a station senses an idle channel it transmits with a probability p and refrains from sending by probability (1-p).

4.**CSMA/CD**

Ethernet (IEEE 802.3) sends data using CSMA/CD (CSMA with Collision Detection). CSMA was an improvement over ALOHA as the channel was sensed before transmission begins. Now a further improvised CSMA, in the form of CSMA/CD has been brought about. In this stations abort their transmission as soon as they detect a collision.

Working:

- If two stations sense the channel to be idle they begin transmitting simultaneously and cause a collision.

-A collision is indicated by a high voltage.

- Both the stations monitor the channel for a collision and stop transmitting as soon as a collision is detected.
- Now the stations wait for a random amount of time and check if channel is free.
- The process continues.

How long will it take a station to realize that a collision has taken place?

- Let the time for a signal to propagate between the two farthest stations be τ

- .

- Assume that at time t0, one station begins transmitting.

- Let's call the most distant station B.

- At time τ

– ε, which is an instant before the signal arrives at B, B itself senses an idle channel and begins transmitting. A collision occurs one instant later at timeτ

- .

- B detects the collision almost instantly and stops, but little noise burst caused by the collision does not get back to the original station until timeτ

+ τ = 2τ

- In other words, in the worst case a station cannot be sure that it has seized the channel until it has transmitted for 2 τ

without hearing a collision.

IEEE 802 Standards

The IEEE 802 Standards comprises a family of networking standards that cover the physical layer specifications of technologies.

IEEE (Institute of Electrical and Electronics Engineers) 802 committee defines and publishes standards for wired Ethernet Local Area Networks, Metropolitan Area Networks (MAN), Wireless networks etc.

IEEE (Institute of Electrical and Electronics Engineers) Working Groups work to create and write the standard and IEEE working group focus for individual area.

The following tables show the most popular IEEE 802 Standards.

Standard	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token ring
802.6	Metropolitan area network (MAN)
802.7	Broadband technology
802.8	Fiber-optic technology
802.9	Voice and data integration
802.10	Network security
802.11	Wireless networking
802.12	Demand priority networking
IEEE 802.15	Wireless Personal Area Network (PAN)

Ethernet Standards

Standard	Description
802.3	Ethernet CSMA /CD (10 Mbps)
802.3u	Fast Ethernet (100 Mbps)
802.3z	Gigabit Ethernet over fiber-optic cabling or coaxial cabling
802.3ab	Gigabit Ethernet over twisted-pair cabling
802.3ae	10-Gigabit Ethernet

Token Bus Network:

Ethernet applies the CSMA/CD method for solving the channel allocation problem. This method works well in sensing the channel, sending frame when it is idle and also if the collision is sensed then in retransmitting the frame after a random amount of time. This results in a repeated attempt of transmission and thereby causing a delay in sending a single frame especially when the channel is loaded with traffic. This method is called a **Token Bus System**. Token bus system applies the physical architecture of the Ethernet system.

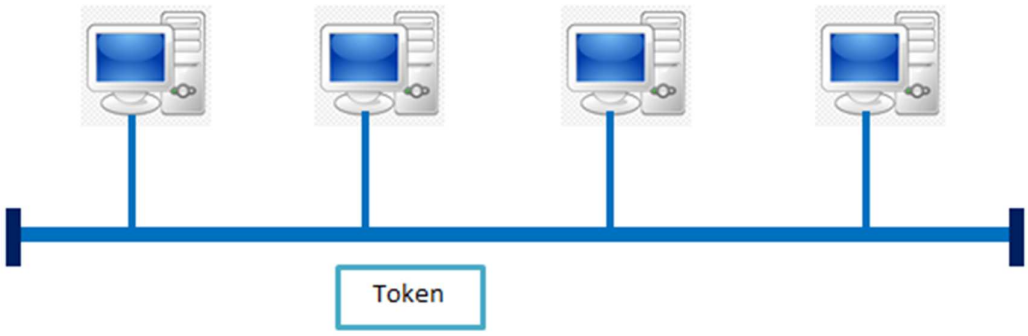


Fig: Token Bus Network

In the Token bus system, the stations are physically organized in bus topology but logically organized in a ring topology. A token passes by the stations. Any station that wants to send a frame must capture the token first, it must be in the possession of the token. Once the data frame is received by the receiver properly and it comes back to the sender, the sender destroys the frame and releases the free token.

Token Ring Network:

In Communication Network, Token ring is the preferred architecture rather than the token bus. The token bus is limited only to process control and automation systems. The token ring also removes the uncertainty in predicting the delay of transmission of a frame occurring in an Ethernet system.

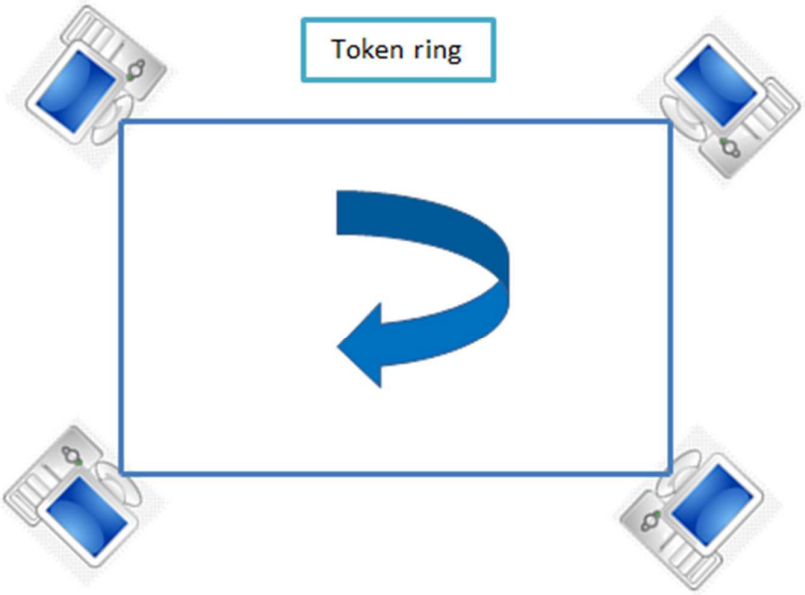


Fig: Token Ring Network

In a token ring system, a free token revolves around the ring usually in a unidirectional way. Any station can transmit only one frame when its turn comes. The basic idea behind the allocation of a shared channel in this system that is called **Token Passing Method.** A token is simply a short frame that is passed from one station to another. A station can send a frame only if it is in possession of the token.

Token Bus vs Token Ring:

Token Bus	Token Ring
1. The token bus network is defined by the IEEE 802.4 standard	1. The token ring network is defined by the IEEE 802.5 standard
2. Token bus network provides better bandwidth than token ring.	2.Token ring network does not provide better bandwidth than token bus.
3. Token Bus networks are unreliable	3. Token Ring networks are reliable
4. In token bus network, Bus topology is used.	4. In token ring network, Star topology is used.
5. Token bus is cheaper than Token Ring	5. Token Ring is expensive than Token Bus
6. Token bus network is designed for the large industries.	6. Token ring network is designed for the offices.

Data Link Layer Design Issues

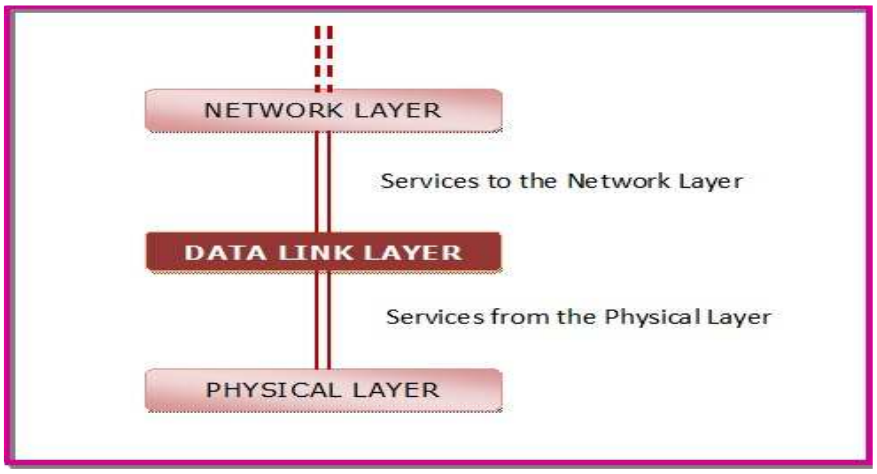
The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

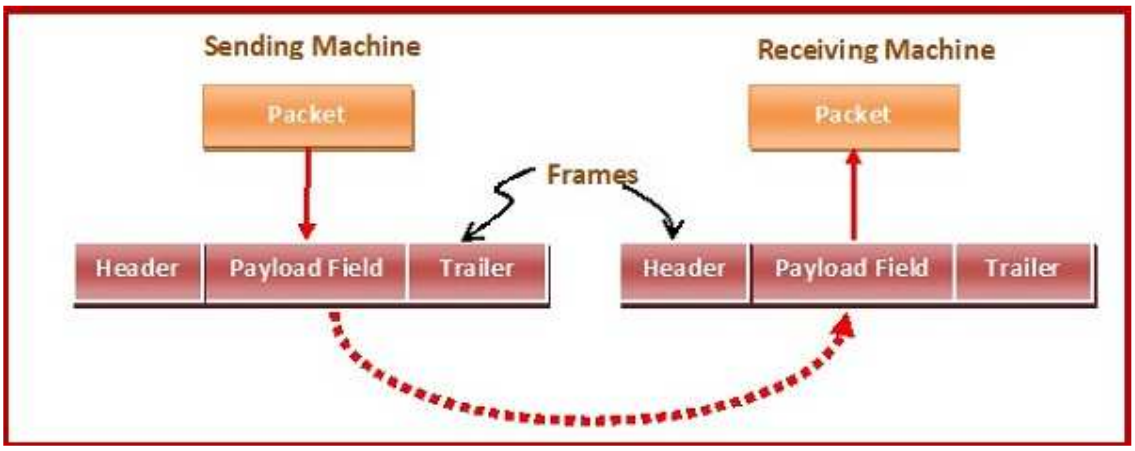
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

The Data Link Layer uses two methods to control the error.

1. Error Detecting Code

   Whenever a message is transmitted, the data gets corrupted many times due to noise. To remove this problem, we use the Error Detection Code. In this process, it sends a digital data with Messege so that it can understand if there is an error in this Messege. With the help of Redundancy Bit, we can easily understand error detection because extra bits are inserted in this process so that we can understand the error.

2. Error Correction Code

We use this Process to remove the correct Messege from the corrupt Messege. We know such code by the name of Error Correcting Code. It also works to identify the correct location of corrupt Bit. Parity check is very useful for us in this process because it is very helpful in correcting the error. As soon as we get to know the location of corrupt Bit, it changes the value and gives us the right Messege.

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

Link Management

In some cases, the data link layer service must be ``opened" before use:

- The data link layer uses open operations for allocating buffer space, control blocks, agreeing on the maximum message size, etc.
- Synchronize and initialize send and receive sequence numbers with its peer at the other end of the communications channel.

Error Detection and Correction

In data communication, line noise is a fact of life (e.g., signal attenuation, natural phenomenon such as lightning, and the telephone repairman). Moreover, noise usually occurs as bursts rather than independent, single bit errors. For example, a burst of lightning will affect a set of bits for a short time after the lightning strike.

Detecting and correcting errors requires *redundancy* -- sending additional information along with the data.

There are two types of attacks against errors:

Error Detecting Codes:

Include enough redundancy bits to *detect* errors and use ACKs and retransmissions to recover from the errors.

Error Correcting Codes:

Include enough redundancy to detect *and* correct errors.

To understand errors, consider the following:

1. Messages (frames) consist of *m* data (message) bits and *r* redundancy bits, yielding an *n* = (*m*+*r*)-bit *codeword*.

2. *Hamming Distance*. Given any two codewords, we can determine how many of the bits differ. Simply exclusive or (XOR) the two words, and count the number of 1 bits in the result.
3. Significance? If two codewords are *d* bits apart, *d* errors are required to convert one to the other.
4. A code's *Hamming Distance* is defined as the minimum Hamming Distance between any two of its legal codewords (from all possible codewords).
5. In general, all 2^m possible data words are legal. However, by choosing check bits carefully, the resulting codewords will have a large Hamming Distance. The larger the Hamming distance, the better able the code can detect errors.

To detect *d* 1-bit errors requires having a Hamming Distance of at least *d*+1 bits. Why?

To correct *d* errors requires 2*d*+1 bits. Intuitively, after *d* errors, the garbled messages is still closer to the original message than any other legal codeword.

Design Issues in Network Layer

Network layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

Before learning about design issues in the network layer, let's learn about it's various functions.

- **Addressing:**
  Maintains the address at the frame header of both source and destination and performs addressing to detect various devices in network.
- **Packeting:**
  This is performed by Internet Protocol. The network layer converts the packets from its upper layer.
- **Routing:**
  It is the most important functionality. The network layer chooses the most relevant and best path for the data transmission from source to destination.
- **Inter-networking:**
  It works to deliver a logical connection across multiple devices.

Network layer design issues:
The network layer comes with some design issues they are described as follows:

1. Store and Forward packet switching:
The host sends the packet to the nearest router. This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination. This mechanism is called "Store and Forward packet switching."

2. Services provided to Transport Layer:
Through the network/transport layer interface, the network layer transfers it's services to the transport layer. These services are described below.
But before providing these services to the transfer layer following goals must be kept in mind :-

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.

- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.

Based on the connections there are 2 types of services provided :

- **Connectionless –** The routing and insertion of packets into subnet is done individually. No added setup is required.
- **Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

3. Implementation of Connectionless Service:
Packet are termed as “datagrams” and corresponding subnet as “datagram subnets”. When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.Each data packet has destination address and is routed independently irrespective of the packets.

4. Implementation of Connection Oriented service:
To use a connection-oriented service, first we establishes a connection, use it and then release it. In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.

It can be done in either two ways :

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver. A virtual path is established here. While, other connections may also be using the same path.

Network Layer Design Issues

The network layer or layer 3 of the OSI (Open Systems Interconnection) model is concerned delivery of data packets from the source to the destination across multiple hops or links. It is the lowest layer that is concerned with end − to − end transmission. The designers who are concerned with designing this layer needs to cater to certain issues. These issues encompasses the services provided to the upper layers as well as internal design of the layer.

The design issues can be elaborated under four heads −

- Store − and − Forward Packet Switching
- Services to Transport Layer
- Providing Connection Oriented Service
- Providing Connectionless Service

Store – and – Forward Packet Switching

The network layer operates in an environment that uses store and forward packet switching. The node which has a packet to send, delivers it to the nearest router. The packet is stored in the router until it has fully arrived and its checksum is verified for error detection. Once, this is done, the packet is forwarded to the next router. Since, each router needs to store the entire packet before it can forward it to the next hop, the mechanism is called store − and − forward switching.

Services to Transport Layer

The network layer provides service its immediate upper layer, namely transport layer, through the network − transport layer interface. The two types of services provided are −

- Connection − Oriented Service − In this service, a path is setup between the source and the destination, and all the data packets belonging to a message are routed along this path.
- Connectionless Service − In this service, each packet of the message is considered as an independent entity and is individually routed from the source to the destination.

The objectives of the network layer while providing these services are −

- The services should not be dependent upon the router technology.
- The router configuration details should not be of a concern to the transport layer.
- A uniform addressing plan should be made available to the transport layer, whether the network is a LAN, MAN or WAN.

Providing Connection Oriented Service

In connection − oriented services, a path or route called a **virtual circuit** is setup between the source and the destination nodes before the transmission starts. All the packets in the message are sent along this route. Each packet contains an identifier that denotes the virtual circuit to which it belongs to. When all the packets are transmitted, the virtual circuit is terminated and the connection is released. An example of connection − oriented service is MultiProtocol Label Switching (MPLS).

Providing Connectionless Service

In connectionless service, since each packet is transmitted independently, each packet contains its routing information and is termed as datagram. The network using datagrams for transmission is called datagram networks or datagram subnets. No prior setup of routes are needed before transmitting a message. Each datagram belong to the message follows its own individual route from the source to the destination. An example of connectionless service is Internet Protocol or IP. It is www system service.