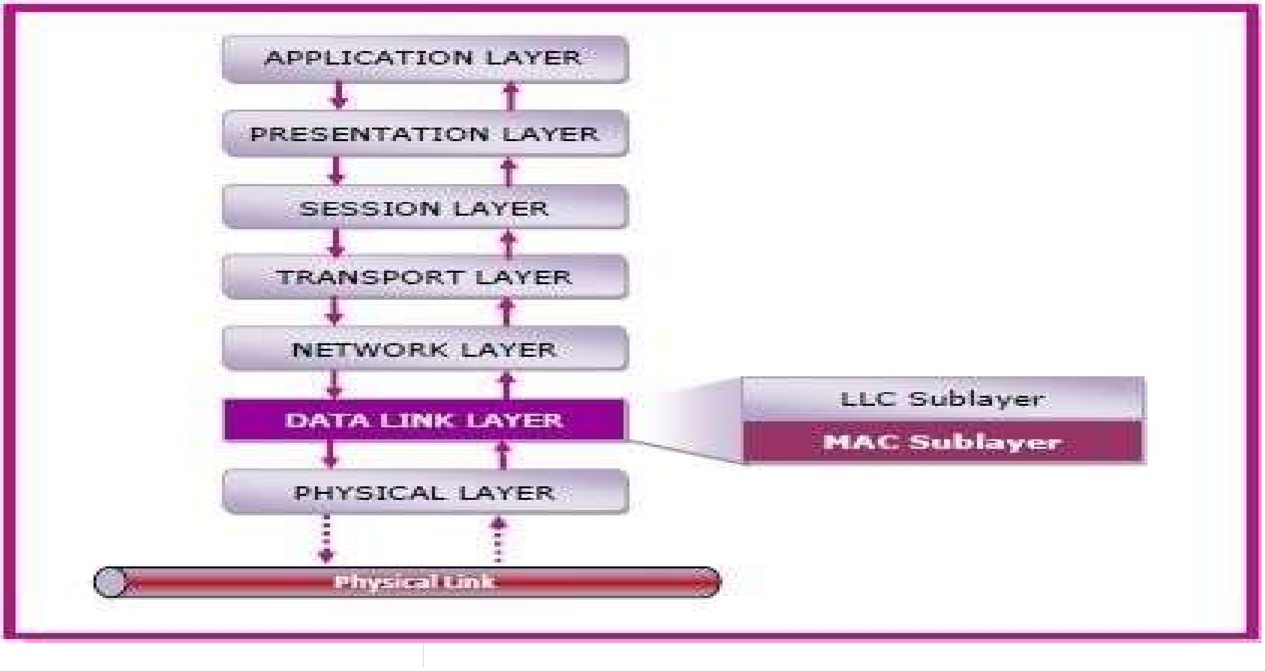
UNIT-3 Medium Access Sub Layer

3.1 Medium Access Sub Layer

The medium access control (MAC) is a sub layer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.



Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.

- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into a network card (known as a **Network Interface Card**) during the time of manufacturing. MAC Address is also known as the **Physical Address** of a network device.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

3.2 Channel Allocation

When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users. The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.

Channel Allocation Schemes

Channel Allocation may be done using two schemes −

- Static Channel Allocation
- Dynamic Channel Allocation

Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment.

In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimizes bandwidth usage and result is faster transmissions.

Dynamic channel allocation is further divided into centralized and distributed allocation.

3.3 LAN PROTOCOLS

A LAN is a high-speed, fault-tolerant data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.

LAN protocols typically use one of two methods to access the physical network medium:

- carrier sense multiple access collision detect (CSMA/CD) and
- token passing.

In the **CSMA/CD media-access scheme,** network devices contend for use of the physical network medium. CSMA/CD is therefore sometimes called contention access. Examples of LANs that use the CSMA/CD media-access scheme are **Ethernet/IEEE 802.3** networks, including 100BaseT.

In the **token-passing media-access scheme**, network devices access the physical medium based on possession of a token. Examples of LANs that use the token-passing media-access scheme are **Token Ring/IEEE 802.5** and **FDDI**.

LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

- In a **unicast transmission**, a single packet is sent from the source to a destination on a network.

- A **multicast transmission** consists of a single data packet that is copied and sent to a specific subset of nodes on the network.
- A **broadcast transmission** consists of a single data packet that is copied and sent to all nodes on the network

LAN Topologies

LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

- A **bus topology** is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations.
- A **ring topology** is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology.
- A **tree topology** is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case.
- A **star topology** is a LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology.

LAN Devices

Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches, and routers.

- A **repeater** is a physical layer device used to interconnect the media segments of an extended network. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment. These actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices. Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified. The total number of repeaters and network segments that can be connected is limited due to timing and other issues.
- A **hub** is a physical-layer device that connects multiple user stations, each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network while maintaining the logical bus or ring configuration of the LAN. In some respects, a hub functions as a multiport repeater.
- A **LAN extender** is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network-layer protocols (such as IP, IPX, and AppleTalk), and filter traffic based on the MAC address or network-layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts. LAN extenders, however, are not capable of segmenting traffic or creating security firewalls.
- **Bridges** analyze incoming frames, make forwarding decisions based on information contained in the frames, and forward the frames toward the destination. In some cases, such as **source-route bridging**, the entire path to the destination is contained in each frame. In other cases, such as **transparent bridging**, frames are forwarded one hop at a time toward the destination.
- **Switches** are data link layer devices that, like bridges, enable multiple physical LAN segments to be interconnected into a single larger network. Similar to bridges, switches forward

and flood traffic based on MAC addresses. Because switching is performed in hardware instead of in software, however, it is significantly faster. Switches use either store-and-forward switching or cut-through switching when forwarding traffic. Many types of switches exist, including ATM switches, LAN switches, and various types of WAN switches.

- **Routers** perform two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an internetwork. In the context of the routing process, the latter of these is referred to as switching. Although switching is relatively straightforward, path determination can be very complex.

3.4 ALOHA PROTOCOLS

ALOHA is a multiple access protocol for transmission of data via a shared network channel. It operates in the medium access control sublayer (MAC sublayer) of the open systems interconnection (OSI) model. Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.

In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy. If the channel is idle, then the frames will be successfully transmitted. If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded. These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

Aloha is the type of Random access protocol it was developed at the University of Hawaii in early 1970, it is a LAN-based protocol in this type there are more chances of occurrence of collisions during the transmission of data from any source to the destination

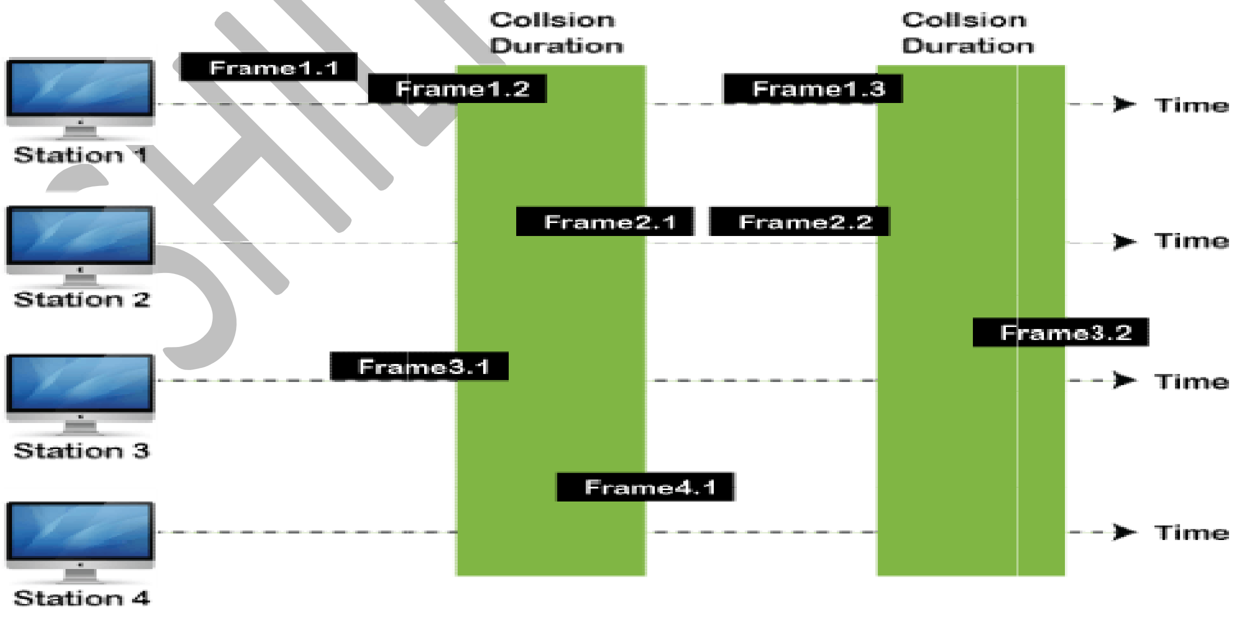
Versions/Types of ALOHA Protocols

Pure ALOHA

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.

In pure ALOHA, the time of transmission is continuous. Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.

When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.



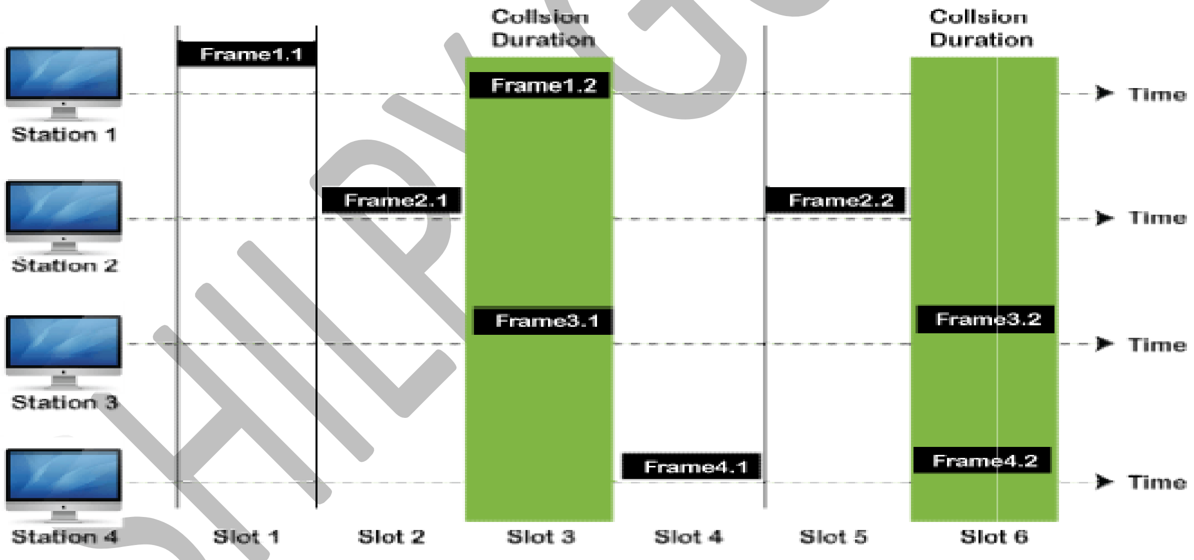
Frames in Pure ALOHA

Slotted ALOHA

The slotted Aloha is designed to overcome the pure Aloha's deficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called slots.

So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time.

However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.



Frames in Slotted ALOHA

Differences between Pure ALOHA and Slotted ALOHA

Pure Aloha	Slotted Aloha
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, Probability of successful transmission of the data packet $= G x e^{-2G}$reduce	In Slotted Aloha, Probability of successful transmission of the data packet $= G x e^{-G}$
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduces the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

3.5 FDDI (Fiber Distributed Data Interface)

Fiber Distributed Data Interface, or FDDI, is a high-speed network technology which runs at 100 Mbps over fiber-optic cabling, often used for network backbones in a local area network (LAN) or metropolitan area network (MAN).

How FDDI Works?

Fiber Distributed Data Interface (FDDI) is usually implemented as a dual token-passing ring within a ring topology (for campus networks) or star topology (within a building). The dual ring consists of a primary and secondary ring. The primary ring carries data. The counter-rotating secondary ring can carry data in the opposite direction, but is more commonly reserved as a backup in case the primary ring goes down. This provides FDDI with the degree of fault tolerance necessary for network backbones. In the event of a failure on the primary ring, FDDI automatically reconfigures itself to use the secondary ring as shown in the illustration. Faults can be located and repaired using a fault isolation technique called beaconing. However, the secondary ring can also be configured for carrying data, extending the maximum potential bandwidth to 200 Mbps.

Stations connect to one (or both) rings using a media interface connector (MIC). Its two fiber ports can be either male or female, depending on the implementation. There are two different FDDI implementations, depending on whether stations are attached to one or both rings:

Single-attached stations (Class B stations): Connect to either the primary or secondary ring using M ports. Single-attached FDDI uses only the primary ring and is not as commonly deployed for network backbones as dual-attached FDDI. Single-attached stations are used primarily to connect Ethernet LANs or individual servers to FDDI backbones.

Dual-attached stations (Class A stations): Connect to both rings. The A port is the point at which the primary ring enters and the secondary ring leaves; the B port is the reverse. M ports provide attachment points for single-attached stations. Dual-attached FDDI uses both rings, with the secondary ring serving as a backup for the primary. Dual-attached FDDI is used primarily for network backbones that require fault tolerance. Single-attached stations can be connected to dual-attached FDDI backbones using a dual-attached device called a concentrator or multiplexer.

FDDI makes a great network backbone for an Ethernet or Token Ring network. Put your servers directly on the FDDI ring to increase server performance. When bridging between Ethernet LANs and FDDI backbones, be aware that there are two different types of bridges:

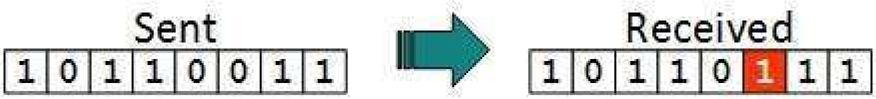
- **Encapsulating bridges**: Encapsulate Ethernet frames into FDDI frames
- **Translating bridges:** Translate source and distension MAC addresses into FDDI addresses

3.6 Error Detection and Correction

There are many reasons such as noise, cross-talk etc., which may get data corrupted during transmission. An error occurs when the output information does not match the input information. Digital signals suffer from noise during transmission, which can create errors in binary bits travelling from one system to another. That is, a 0 bit may become a 1 bit, or a 1 bit may become a 0.

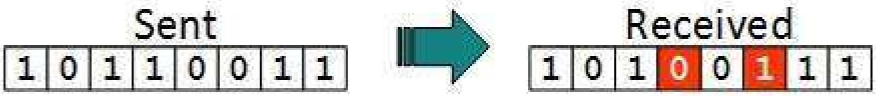
Types of Errors

- **Single bit error**



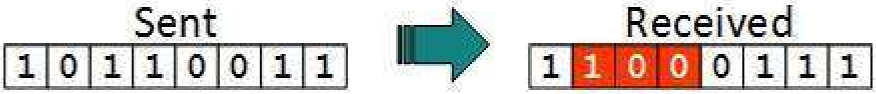
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

3.6.1 Error Detection Techniques:

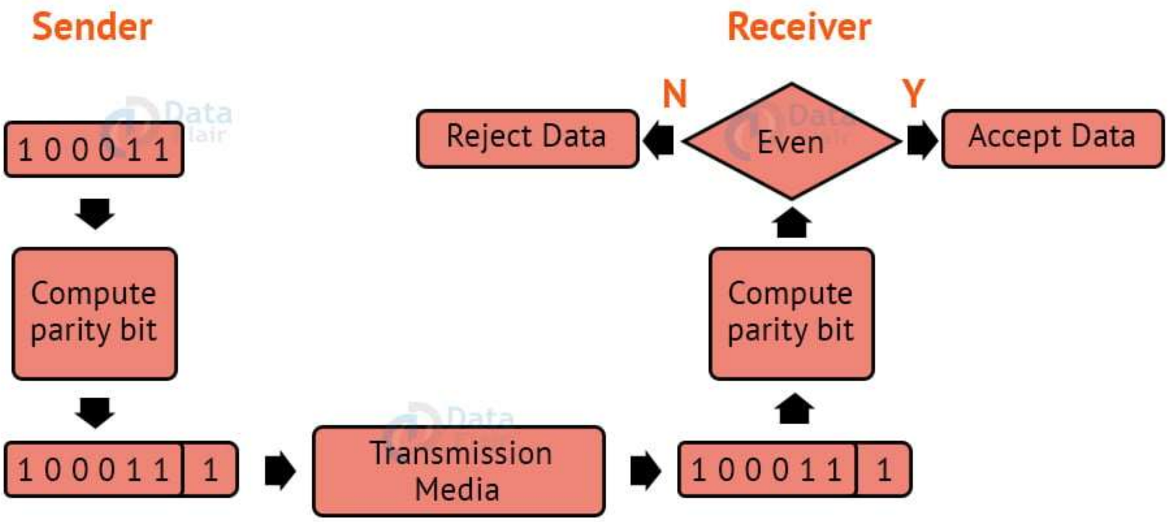
Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

1. Simple Parity Check:

- One extra bit is transmitted in addition to the original bits to make the number of 1s even in the case of even parity or odd in the case of odd parity.
- While creating a frame, the sender counts the amount of 1s in it. If even parity is utilised and the number of 1s is even, one bit with the value 0 is added. In this manner, the number of 1s remains even. If the number of 1s is odd, a value 1 is added to make it even.
- The receiver just counts how many 1s are in a frame. If the number of 1s is even and even parity is utilised, the frame is regarded as uncorrupted and approved. Even if the number of 1s is odd and odd parity is utilised, the frame is not damaged.
- The receiver can identify a single bit flip in transit by counting the number of 1s. However, when more than one bit is

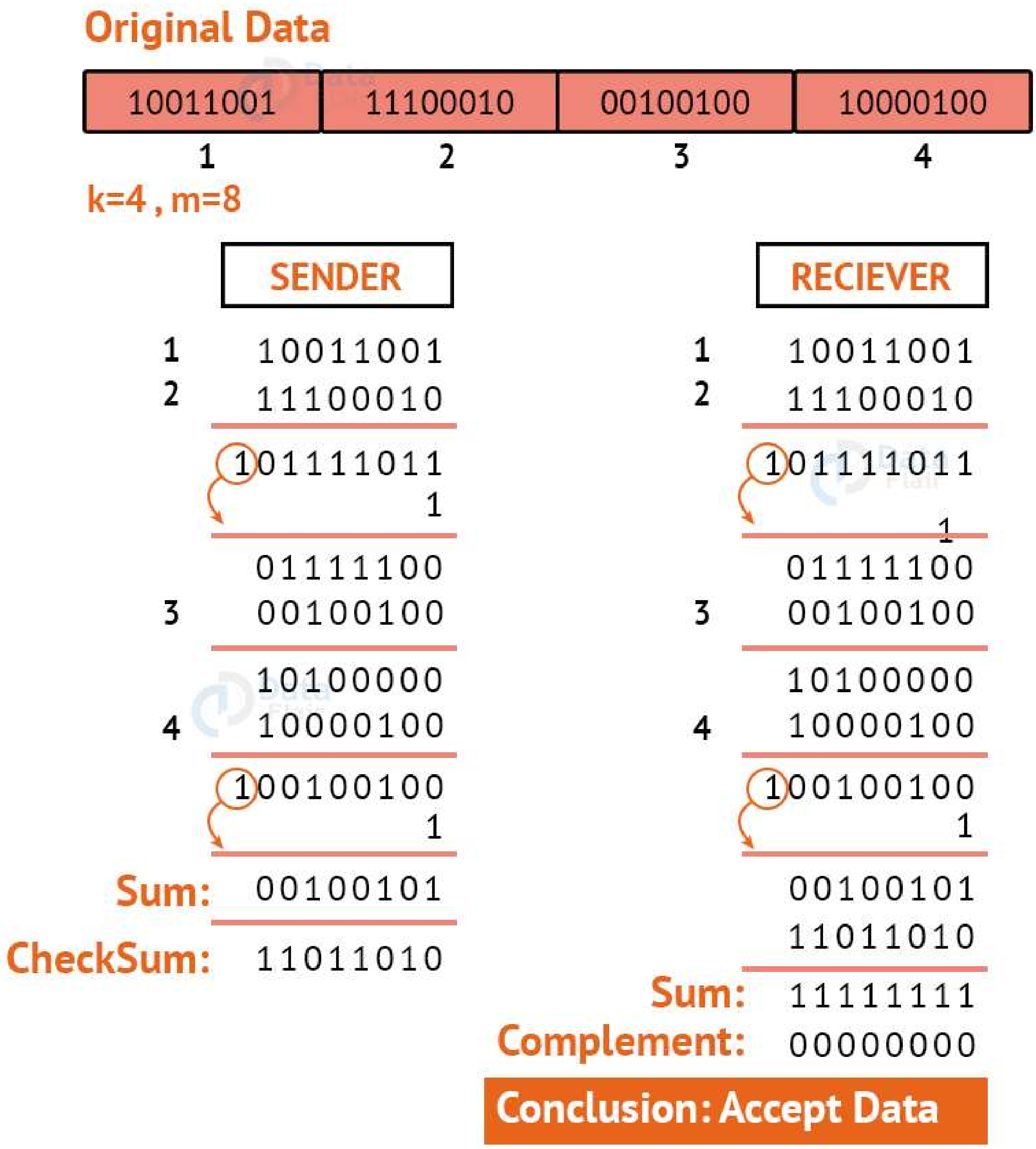
incorrect, it is extremely difficult for the receiver to identify the problem.

Example of Simple Even Parity Check



2. Checksum:

- The data is split into k segments of m bits each in the checksum error detection technique.
- To get the total, the segments are summed at the sender's end using 1's complement arithmetic. To obtain the checksum, a complement of the sum is taken.
- The checksum segment is sent with the data segments.
- To obtain the total, all received segments are summed using 1's complement arithmetic at the receiver's end. The sum is then calculated.
- If the result is 0, the data is accepted; otherwise, it is rejected.

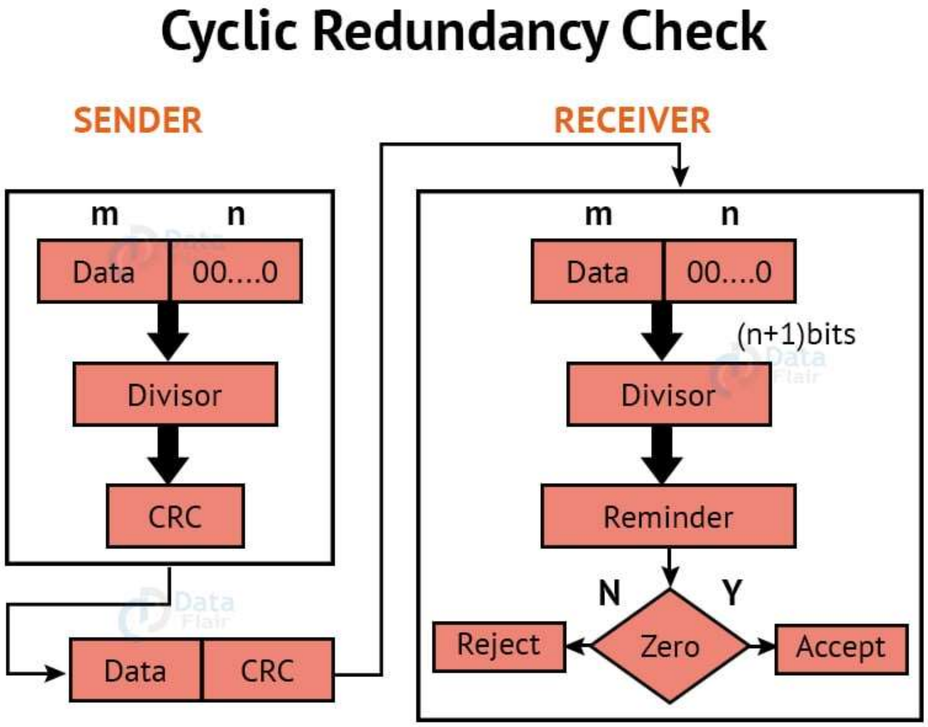


4. Cyclic Redundancy Check:

CRC is an alternative method for determining whether or not a received frame includes valid data. The binary division of the data bits being delivered is used in this approach. Polynomials are used to generate the divisor.

The sender divides the bits that are being transferred and calculates the remainder. The sender inserts the remainder at the end of the original bits before sending the actual bits. A codeword is made up of the actual data bits plus the remainder. The transmitter sends data bits in the form of codewords.

The receiver, on the other hand, divides the codewords using the same CRC divisor. If the remainder consists entirely of zeros, the data bits are validated; otherwise, it is assumed that some data corruption happened during transmission.



3.6.2 Error Correction:

Error Correction codes are used to detect and repair mistakes that occur during data transmission from the transmitter to the receiver.

There are two approaches to error correction:

1. Backward Error Correction:

When a backward mistake is detected, the receiver requests that the sender retransmit the complete data unit.

2. Forward Error Correction:

In this scenario, the error-correcting code is used by the receiver, which automatically corrects the mistakes.

A single extra bit can identify but not repair the mistake.

To correct the mistakes, the specific location of the error must be known. If we wish to compute a single-bit mistake, for example, the error correcting algorithm will identify which one of seven bits is incorrect. We will need to add some more redundant bits to do this.

Error Correction Techniques:

1. Hamming Code:

Parity bits: A bit that is added to the original binary data to make sure the total number of 1s is even or odd (in case of even or odd parity respectively).

Even parity: To check for even parity, if the total number of 1s is even, the parity bit value is 0. If the total number of occurrences of 1s is odd, the parity bit value is 1.

Odd Parity: To test for odd parity, if the total number of 1s is even, the parity bit value is 1. If the total number of 1s is odd, the parity bit value is 0.

To produce d+r, an information of ‘d’ bits is added to the redundant bits ‘r’.

Each (d+r) digit's position is assigned a decimal value.

The 'r' bits are assigned to locations 1, 2,....2k-1.

The parity bits are recalculated at the receiving end. The position of an error is determined by the decimal value of the parity bits.

Example: If the data to be transmitted is 1011001

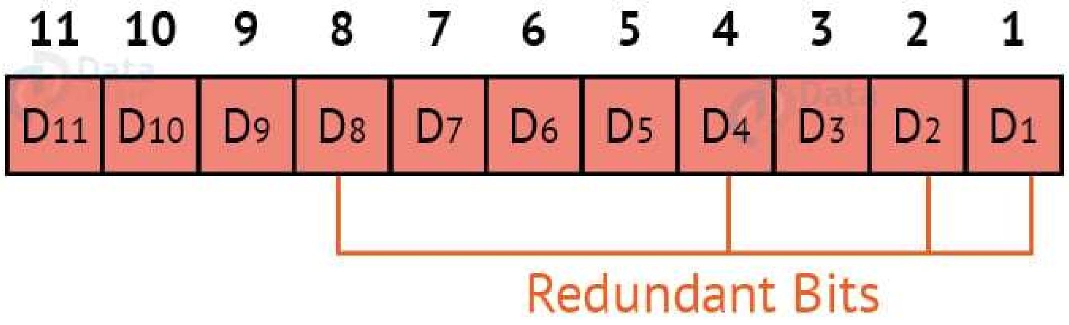
Number of data bits = 7

Thus, number of redundancy bits = 4

Total bits = 7+4 = 11

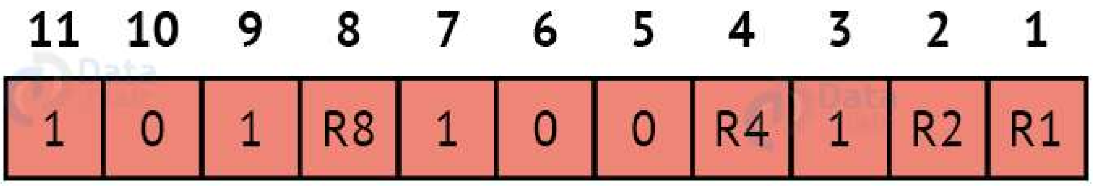
Redundant bits are always placed at positions that correspond to the power of 2, so the redundant bits will be placed at positions: 1,2,4 and 8.

Redundant bits will be placed here:



11	10	9	8	7	6	5	4	3	2	1
D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1

Thus now, all the 11 bits will look like this:

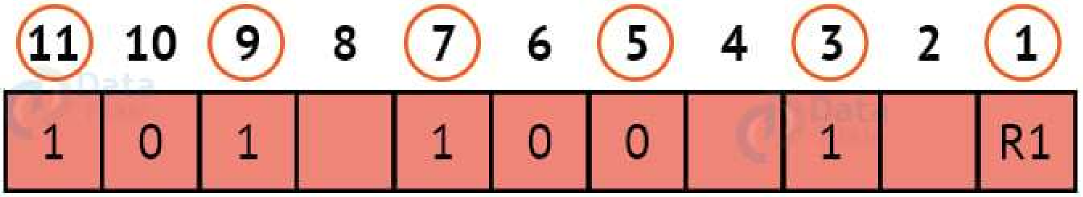


11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	R4	1	R2	R1

Here, R1, R2, R4 and R8 are the redundant bits.

Determining the parity bits:

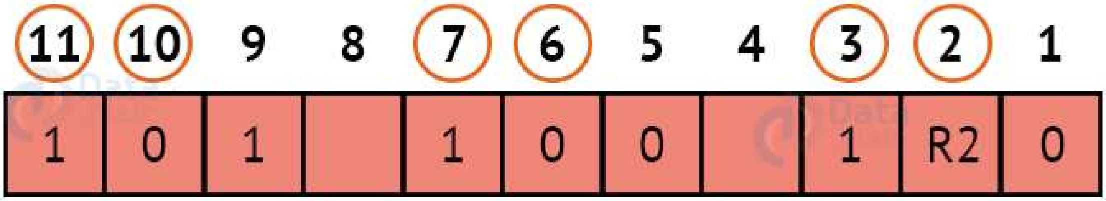
R1:



11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1		R1

We look at bits 1,3,5,7,9,11 to calculate R1. In this case, because the number of 1s in these bits together is even, we make the R1 bit equal to 0 to maintain even parity.

R2:



11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1	R2	0

We look at bits 2,3,6,7,10,11 to calculate R2. In this case, because the number of 1s in these bits together is odd, we make the R2 bit equal to 1 to maintain even parity.

R4:

11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0	R4	1	1	0

We look at bits 4,5,6,7 to calculate R4. In this case, because the number of 1s in these bits together is odd, we make the R4 bit equal to 1 to maintain even parity.

R8:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	1	1	1	0

We look at bits 8,9,10,11 to calculate R8. In this case, because the number of 1s in these bits together is even, we make the R8 bit equal to 0 to maintain even parity.

Thus, the final block of data which is transferred looks like this:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

3.7 Sliding Window protocols

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

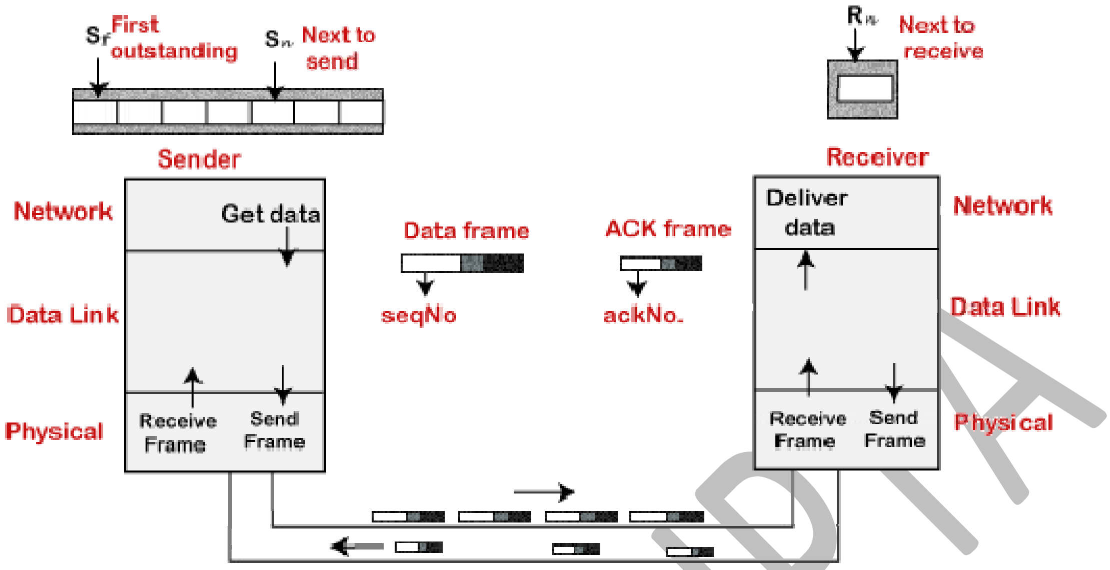
1. Go-Back-N ARQ
2. Selective Repeat ARQ

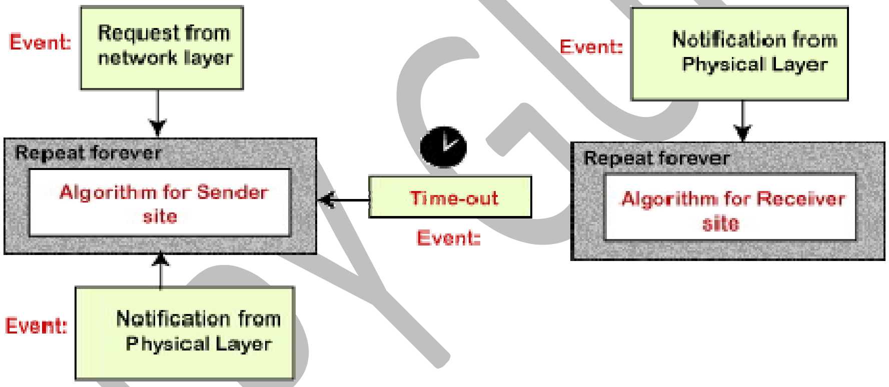
Go-Back-N ARQ

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.

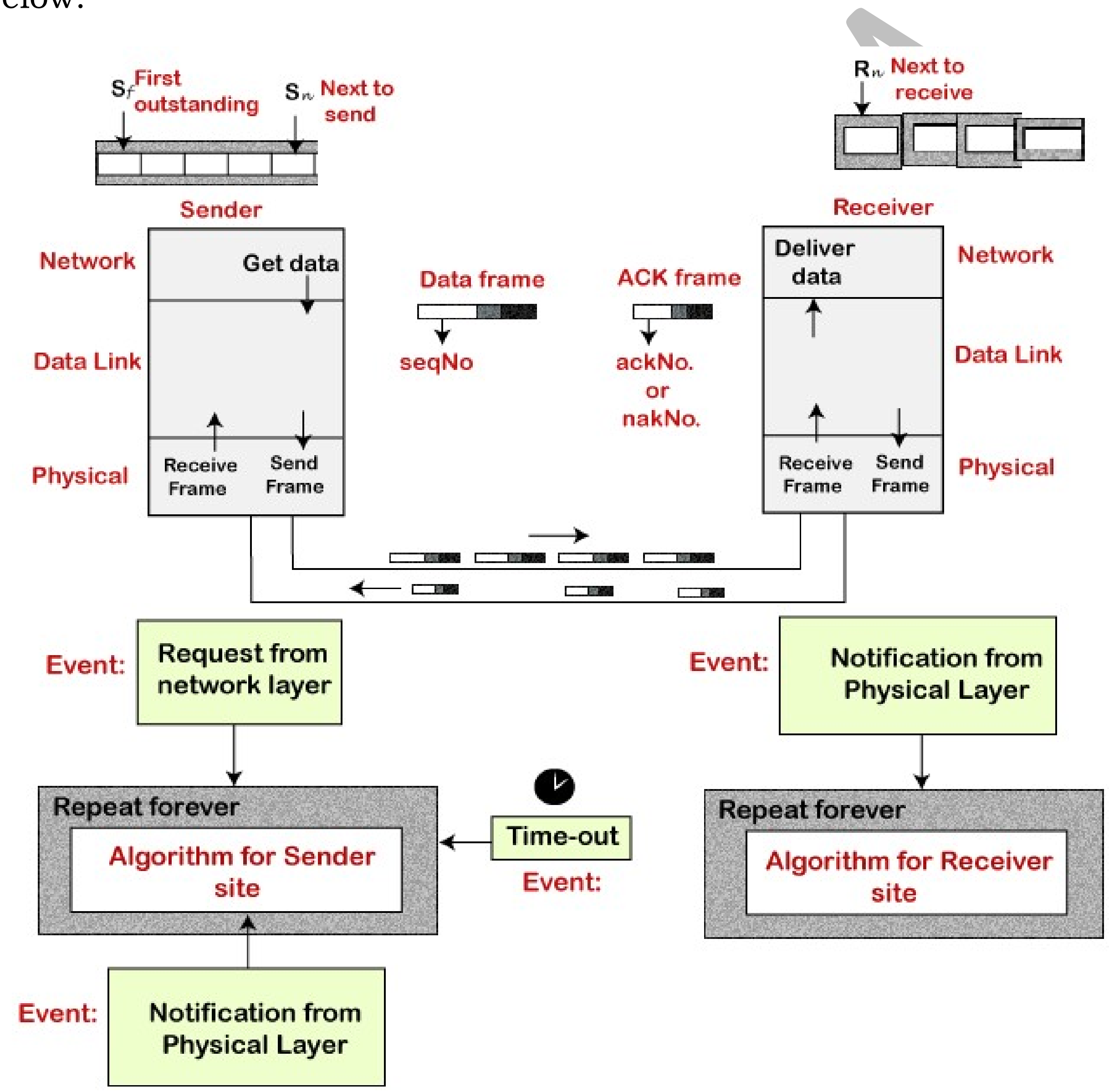



Event:
Request from network layer
Repeat forever
Algorithm for Sender site
Time-out
Event:
Event:
Notification from Physical Layer
Event:
Notification from Physical Layer
Repeat forever
Algorithm for Receiver site

Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.