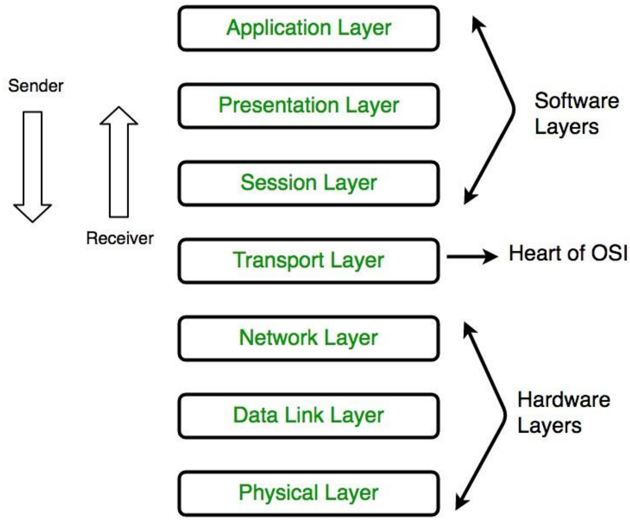
UNIT-2 OSI LAYERS

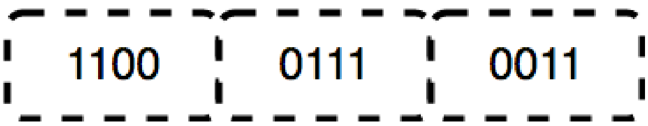
communication layers and its applications

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization for Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. **Physical Layer (Layer 1)** :
The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.**

It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are as follows:

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

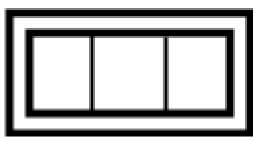
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

2. Data Link Layer (DLL) (Layer 2) :
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. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.



The functions of the Data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

3. Network Layer (Layer 3) :

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

4. Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender's side: Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are as follows:

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

A. Connection-Oriented Service: It is a three-phase process that includes

– Connection Establishment
– Data Transfer
– Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

B. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

5. Session Layer (Layer 5) :

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security. The functions of the session layer are :

1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*
***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

6. Presentation Layer (Layer 6):

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :
At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

communication media

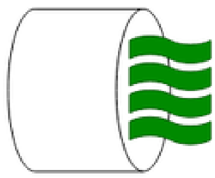
communication media is the medium over which information travels from the sender to the receiver.

different types of wired media are:
- Twisted pair cables
- Coaxial cables
- Optical fiber cables

In wired media the signal is guided within solid wires like coaxial cables, twisted pair cables, optical fibers etc.

(i) Twisted Pair Cable –
It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):**
  UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

Advantages:

⇢ Least expensive

⇢ Easy to install

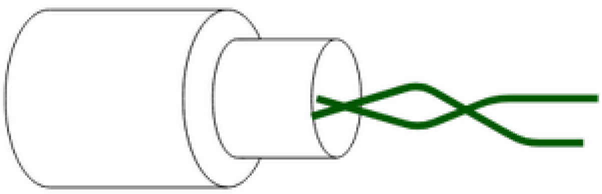
⇢ High-speed capacity

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

⇢ Short distance transmission due to attenuation

- **Shielded Twisted Pair (STP):**
  This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

(ii) Coaxial Cable –
It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

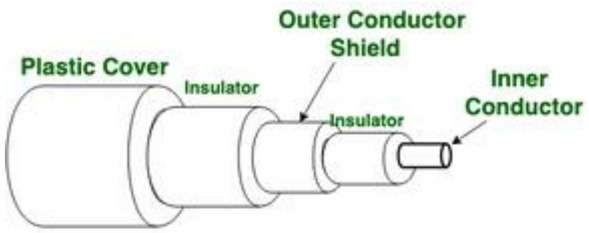


Figure of Coaxial Cable

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

(iii) Optical Fiber Cable –
It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

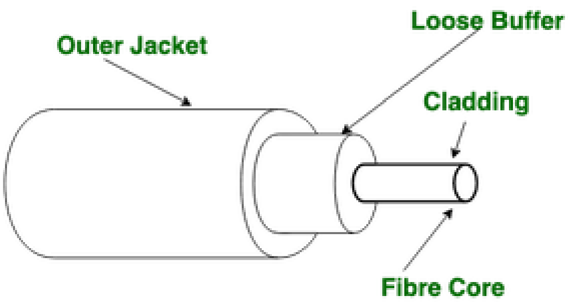


Figure of Optical Fibre Cable

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Introduction to Errors:

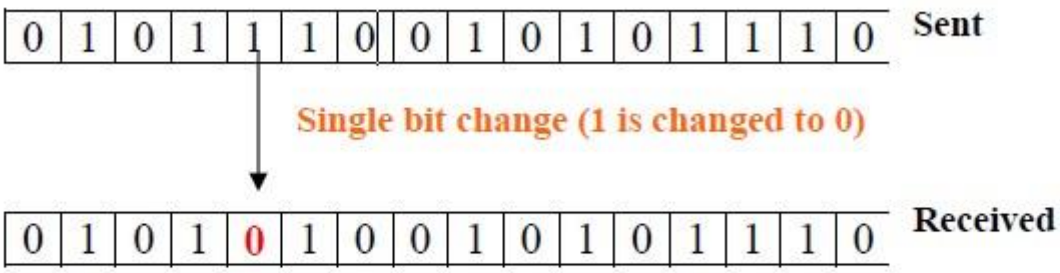
Environmental interference and physical defects in the communication medium can cause random bit errors during data transmission.

Types of errors

These interferences can change the timing and shape of the signal. If the signal is carrying binary encoded data, such changes can alter the meaning of the data.
These errors can be divided into two types :
1. Single-bit error
2. Burst error.

Single-bit Error

The term single-bit error means that only one bit of given data unit (such as a byte, character, or data unit) is changed from 1 to 0 or from 0 to 1



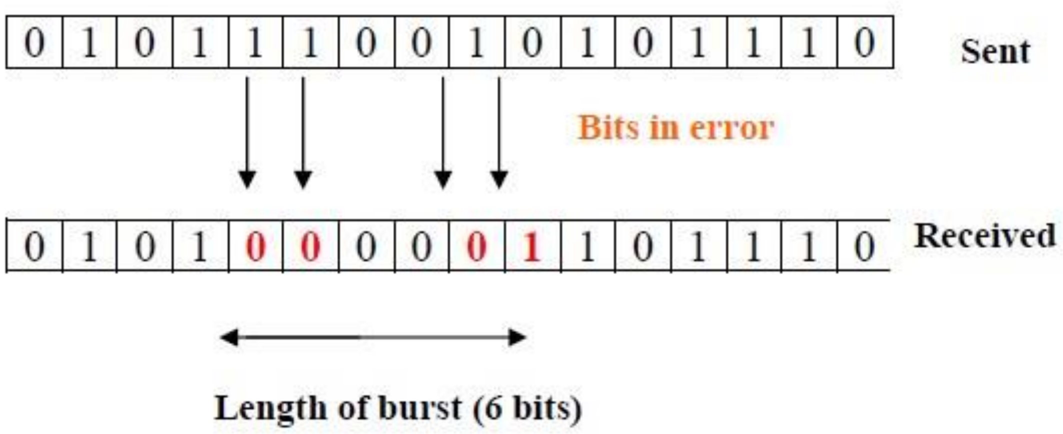
Single bit error

Single bit errors are least likely type of errors in serial data transmission. To see why, imagine a sender sends data at 10 Mbps. This means that each bit lasts only for 0.1 µs (micro-second).

For a single bit error to occur noise must have duration of only 0.1 µs (micro-second), which is very rare. However, a single-bit error can happen if we are having a parallel data transmission. For example, if 16 wires are used to send all 16 bits of a word at the same time and one of the wires is noisy, one bit is corrupted in each word.

Burst Error

The term burst error means that two or more bits in the data unit have changed from 0 to 1 or vice-versa. Note that burst error doesn't necessary means that error occurs in consecutive bits. The length of the burst error is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not be corrupted.



Burst Error

Burst errors are mostly likely to happen in serial transmission. The duration of the noise is normally longer than the duration of a single bit, which means that the noise affects data; it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

Error detection and correction

Error detection is the detection of errors caused by *noise or other impairments* during transmission from the transmitter to the receiver.

Error correction is the detection of errors and reconstruction of the original error free data.

Error detection and correction are implemented at the data link layer or the transport layer of the open system interconnection model (OSI)

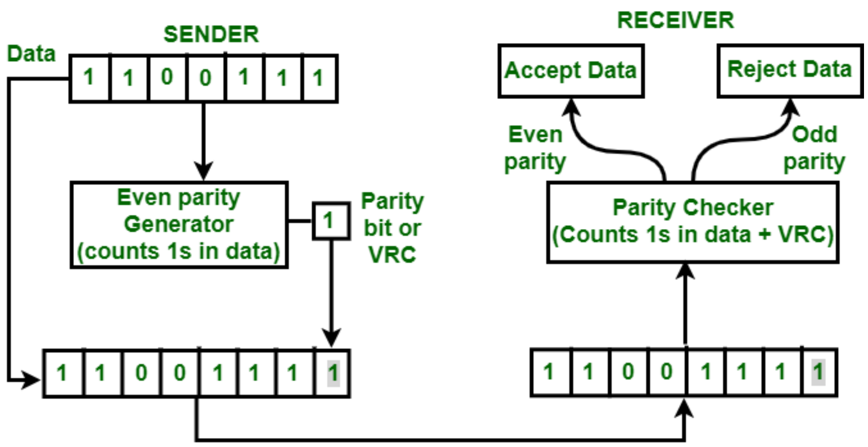
METHODS OF ERROR DETECTION

1. **VRC** (vertical redundancy check)

In *VRC* a parity bit is added to every data unit so that the total number of 1s become even.It can detect all single bit error. It can detect burst error only if total number of errors in the data unit is odd.

Example –

If the source wants to transmit data unit 1100111 using even parity to the destination. The source will have to pass through Even Parity Generator.



Even parity VRC

Parity generator will count number of 1s in data unit and will add parity bit. In the above example, number of 1s in data unit is 5, parity generator appends a parity bit 1 to this data unit making the total number of 1s even i.e 6 which is clear from above figure.

Data along with parity bit is then transmitted across the network. In this case, 11001111 will be transmitted. At the destination, This data is passed to parity checker at the destination. The number of 1s in data is counted by parity checker.

If the number of 1s count out to be odd, e.g. 5 or 7 then destination will come to know that there is some error in the data. The receiver then rejects such an erroneous data unit.

2. LRC (Longitudinal redundancy check)

In LRC, block of bits are divided into rows and a redundant rows of bits is then added to the whole block.

Example :
If a block of 32 bits is to be transmitted, it is divided into matrix of four rows and eight columns which as shown in the following figure :

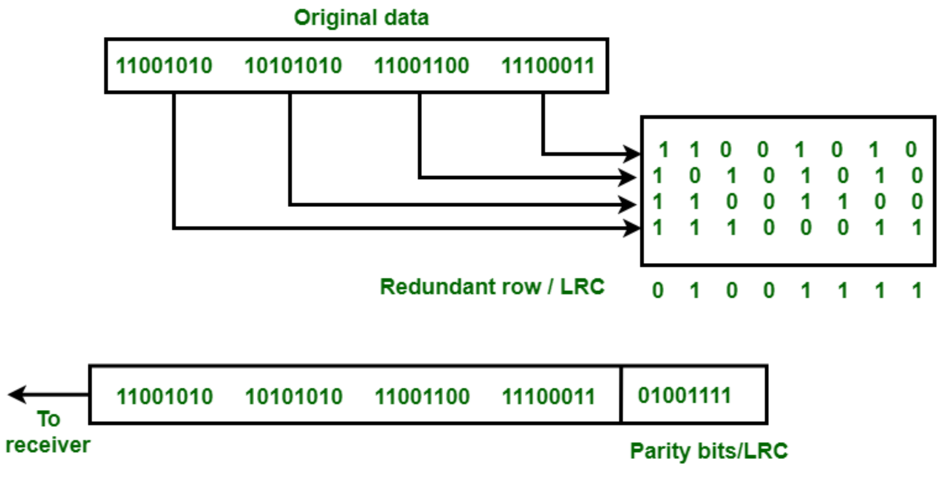


Figure: LRC

In this matrix of bits, a parity bit (odd or even) is calculated for each column. It means 32 bits data plus 8 redundant bits are transmitted to receiver. Whenever data reaches at the destination, receiver uses LRC to detect error in data.

4. checksum

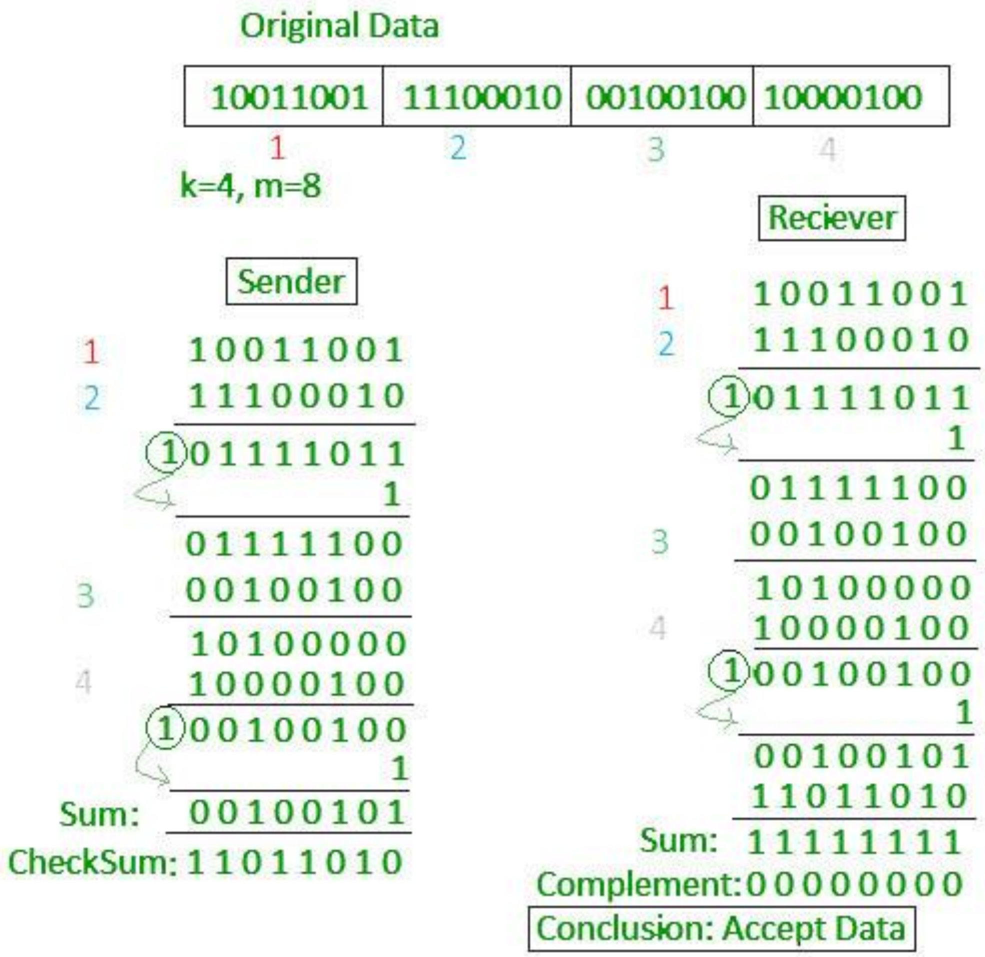
In checksum error detection scheme, the data is divided into k segments each of m bits.

In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.

The checksum segment is sent along with the data segments.

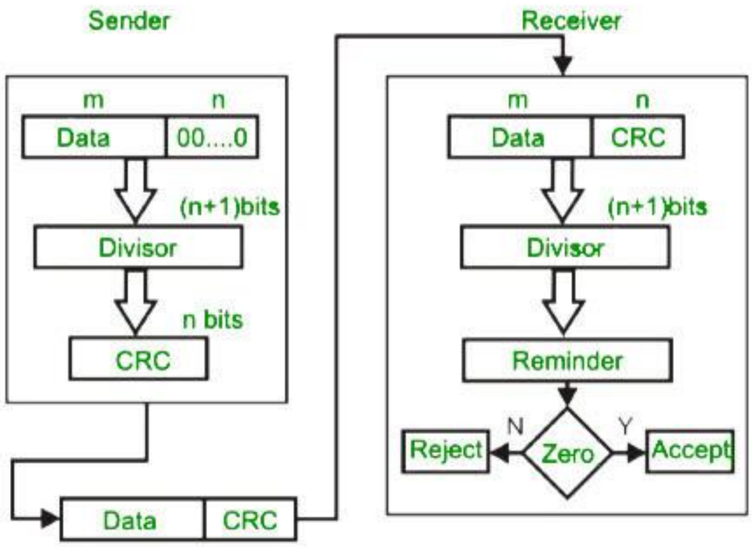
At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.

If the result is zero, the received data is accepted; otherwise discarded.



4. The fourth and most efficient method of error detection is **CRC** that is cyclic redundancy check.

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



ERROR CORRECTION

Error correction is the process of detecting errors in transmitted messages and reconstructing the original error-free data. Error correction ensures that corrected and error-free messages are obtained at the receiver side.

Two methods of error correction are-

1. reverse error correction (REC).

2. Forward error correction(FEC)

In the first approach the receiver requests for the retransmission of the code word whenever it detects an error after that the receiver locates the error by analyzing the received code and revers the erroneous bits.

In the second approach the code set is so designed that it is possible for the receiver to detect and correct error as well by itself.

Flow control and its applications:

In a network, the sender sends the data and the receiver receives the data. But suppose a situation where the sender is sending the data at a speed higher than the receiver is able to receive and process it, then the data will get lost.

Flow-control methods will help in ensuring this. The flow control method will keep a check that the senders send the data only at a speed that the receiver is able to receive and process. So, let's get started with the blog and learn more about flow control.

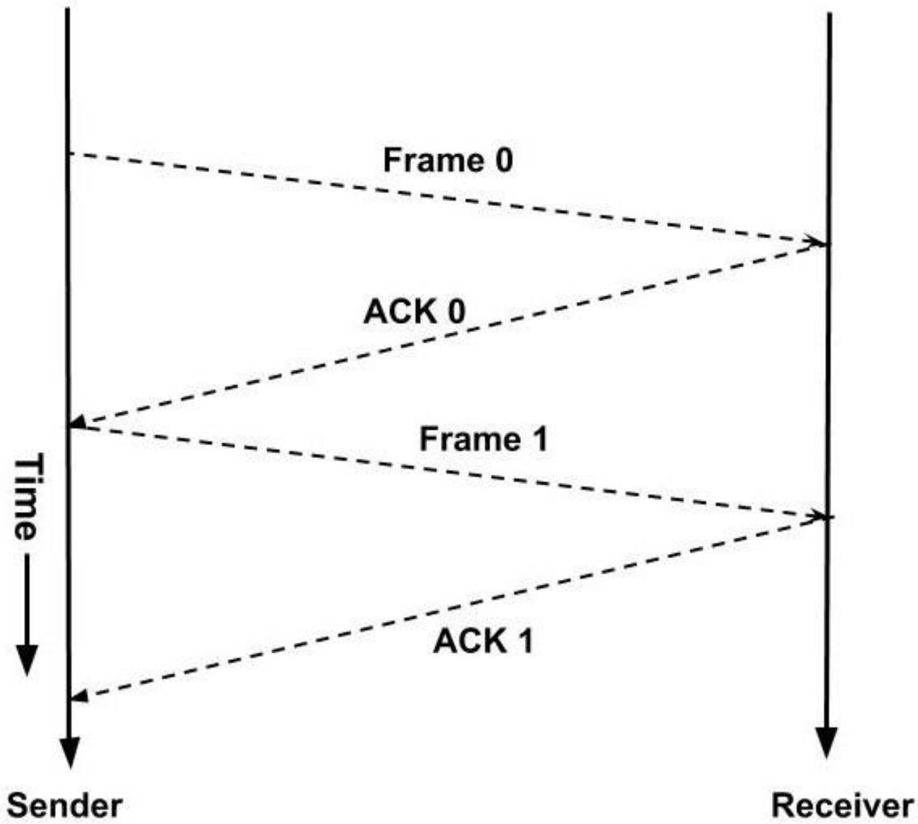
Flow Control

Flow control tells the sender how much data should be sent to the receiver so that it is not lost. This mechanism makes the sender wait for an acknowledgment before sending the next data. There are two ways to control the flow of data:

1. Stop and Wait Protocol
2. Sliding Window Protocol

Stop and Wait Protocol

It is the simplest flow control method. In this, the sender will send one frame at a time to the receiver. Until then, the sender will **stop and wait** for the acknowledgment from the receiver. When the sender gets the acknowledgment then it will send the next data packet to the receiver and wait for the acknowledgment again and this process will continue. This can be understood by the diagram below.



Suppose if any frame sent is not received by the receiver and is lost. So the receiver will not send any acknowledgment as it has not received any frame. Also, the sender will not send the next frame as it will wait for the acknowledgment for the previous frame which it had sent.

So a deadlock situation can be created here. To avoid any such situation there is a time-out timer. The sender will wait for this fixed amount of time for the acknowledgment and if the acknowledgment is not received then it will send the frame again.

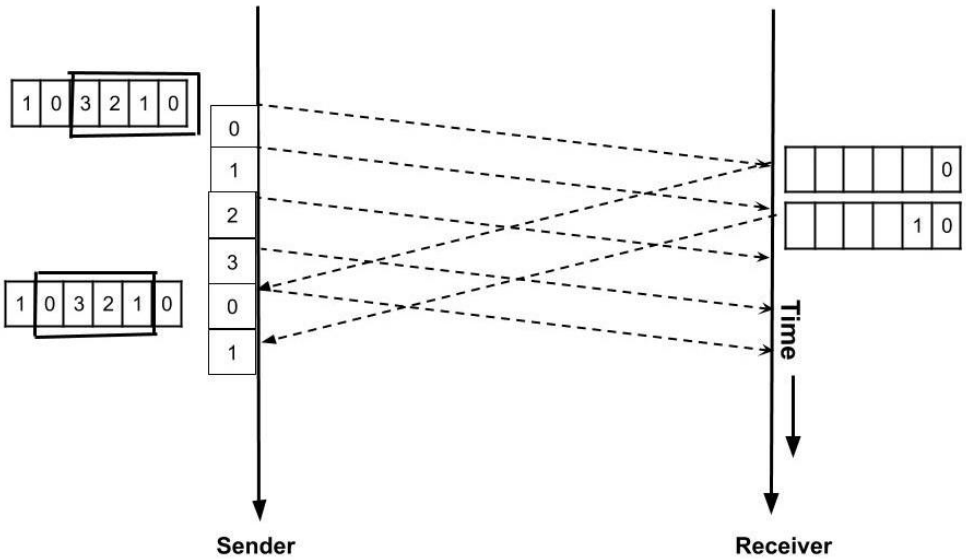
Sliding Window Protocol

As we saw that the disadvantage of the stop and wait protocol is that the sender waits for the acknowledgment and during that time the sender is idle. In sliding window protocol we will utilize this time. We will change this waiting time into transmission time.

A **window** is a buffer where we store the frames. Each frame in a window is numbered. If the window size is **n** then the frames are numbered from the number 0 to n-1. A sender can send n frames at a time. When the receiver sends the acknowledgment of the frame then we need not store that frame in our window as it has already been received by the receiver.

So, the window in the sender side **slides** to the next frame and this window will now contain a new frame along with all the previous unacknowledged frames of the window. **At any instance of time window will only contain the unacknowledged frames.** This can be understood with the ***example*** below:

1. Suppose the size of the window is 4. So, the frames would be numbered as 0,1,2,3,0,1,2,3,0,... so on.
2. Initially, the frames in the window are 0,1,2, 3. Now, the sender starts transmitting the frames. The first frame is sent, then second and so on.
3. When the receiver receives the first frame i.e. frame 0. Then it sends an acknowledgment.
4. When the acknowledgment is received by the sender then it knows that the first frame has been received by the receiver and it need not keep its record. So, the **window slides** to the next frame.
5. The new window contains the frame 1, 2, 3, 0. In this way, the window slides hence the name sliding window protocol.



Sliding Window Protocol