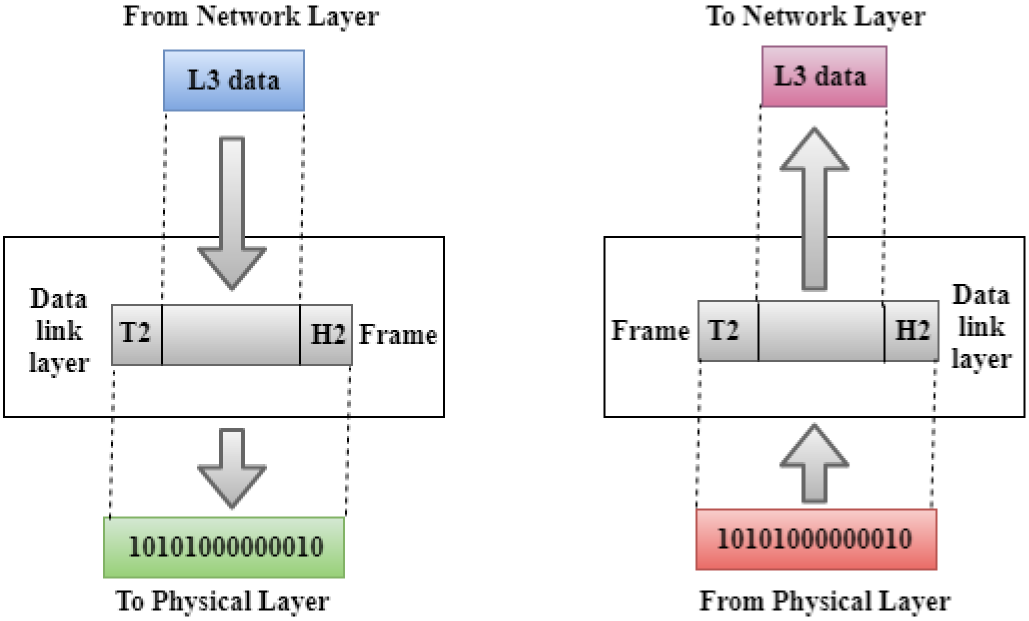
C Data link layer

Design issues:

2.Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
  - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
  - It identifies the address of the network layer protocol from the header.
  - It also provides flow control.
  - **Media Access Control Layer**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

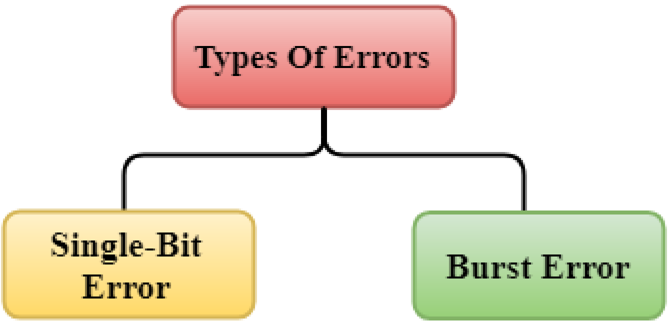
Header
Packet
Trailer

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

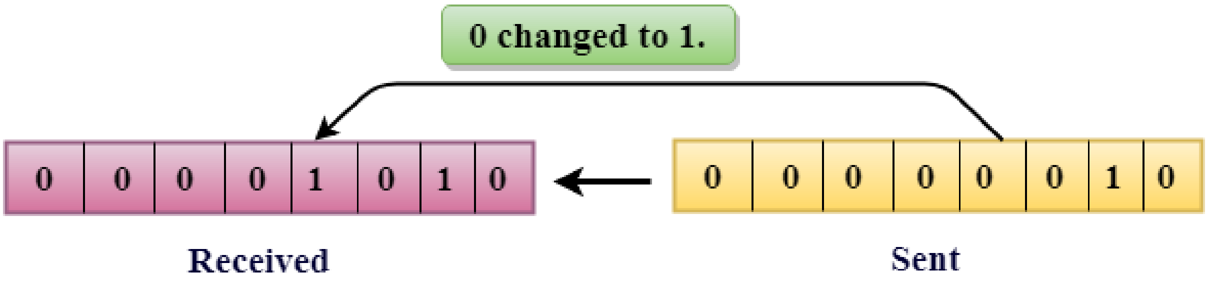


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



0 0 0 0 1 0 1 0

0 0 0 0 0 0 1 0

In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

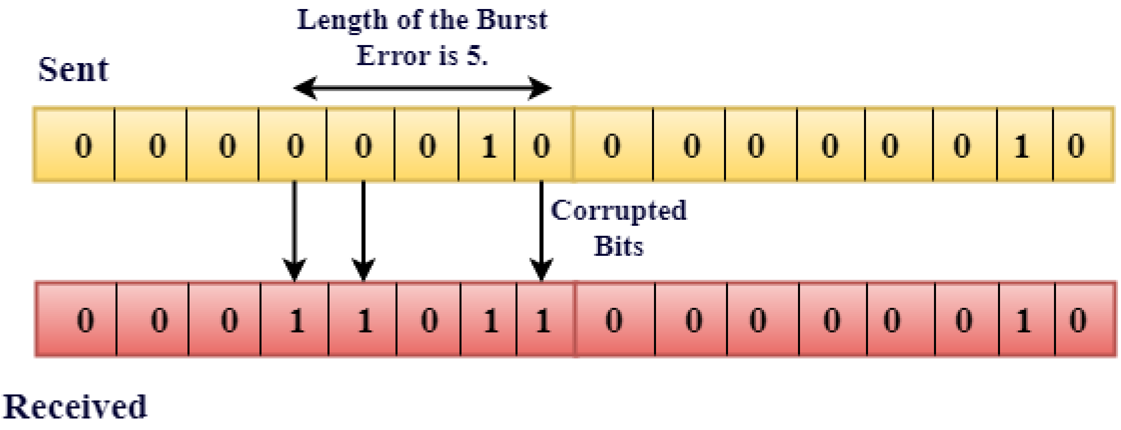
single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 0

0 0 0 1 1 0 1 1 0 0 0 0 0 0 1 0

The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

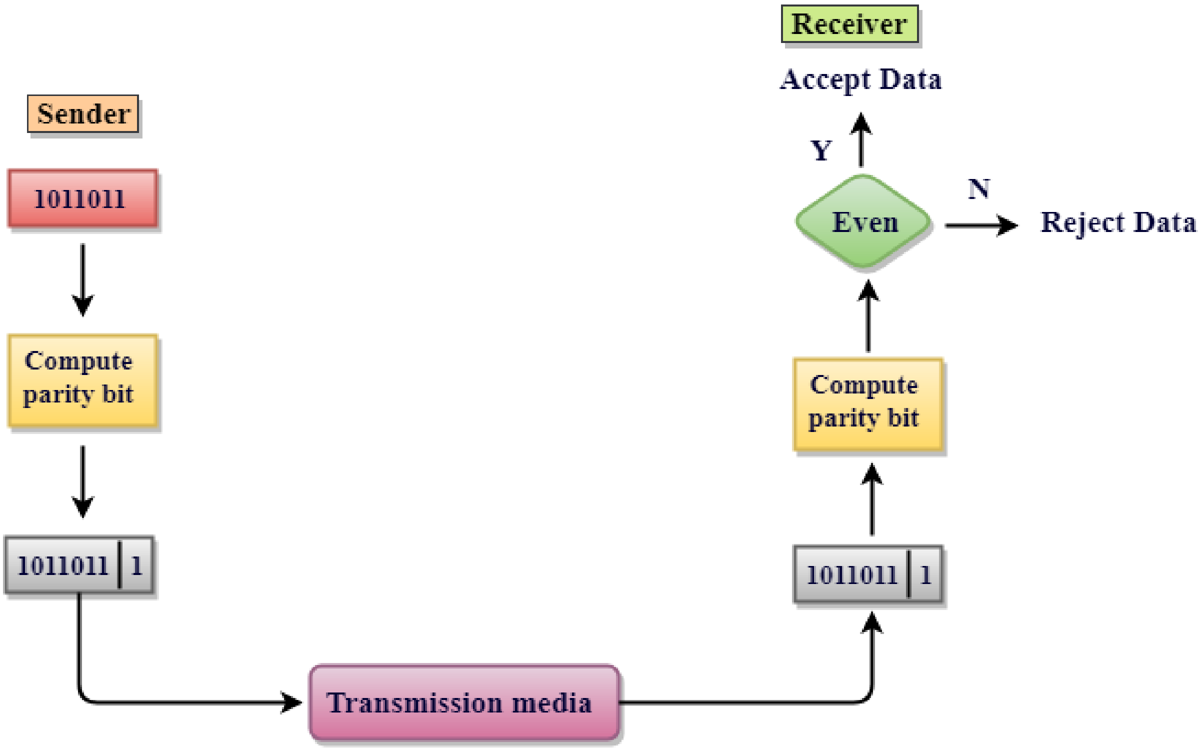
Error Detecting Techniques:

The most popular Error Detecting Techniques are

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

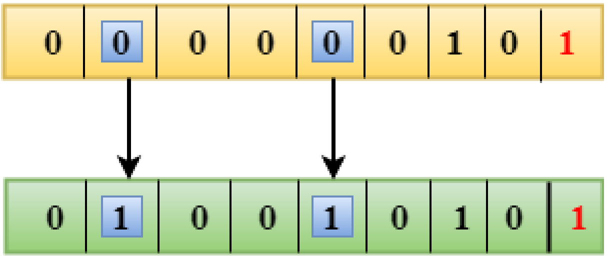
Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



Drawbacks Of Single Parity Checking

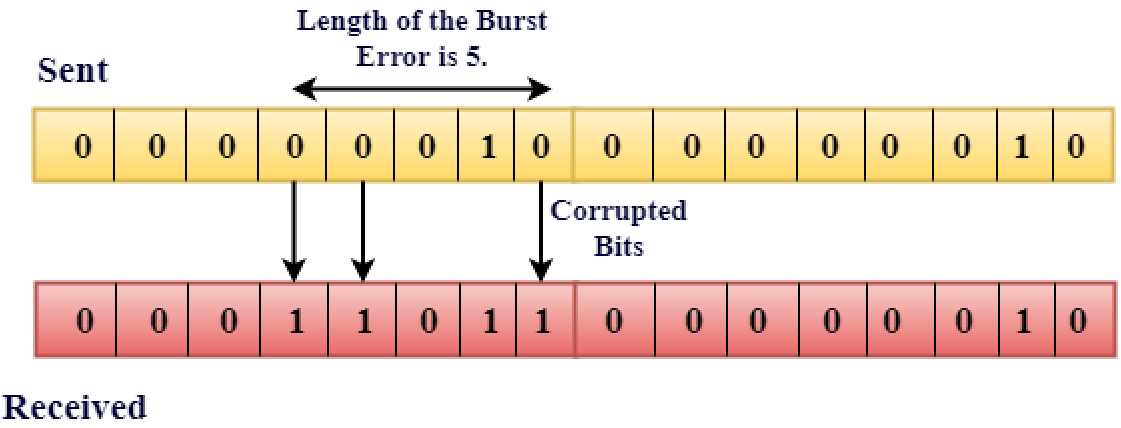
- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



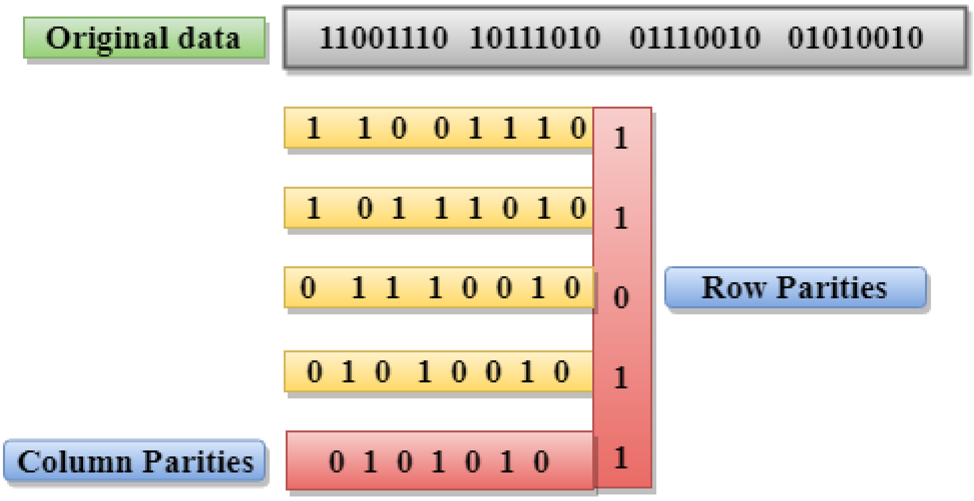
The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

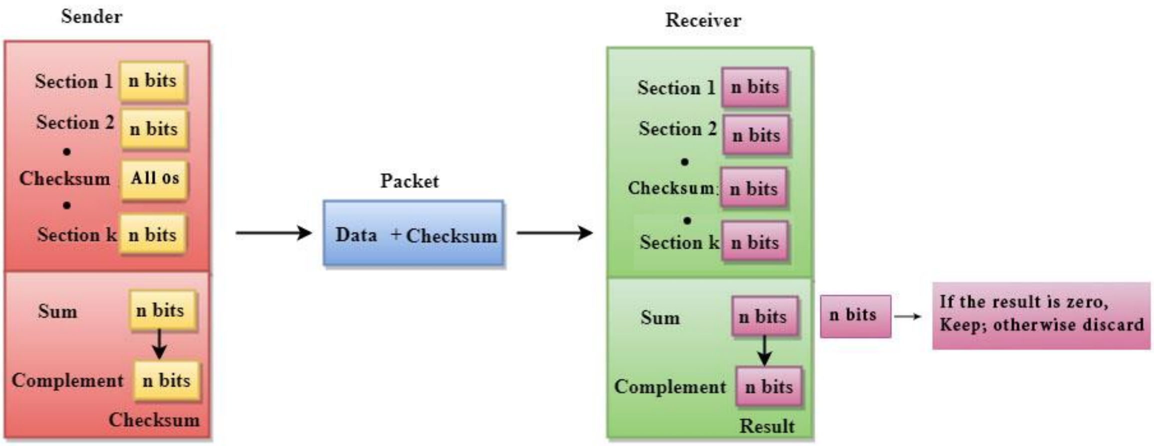
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be ?L



Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

Cyclic Redundancy Check (CRC)

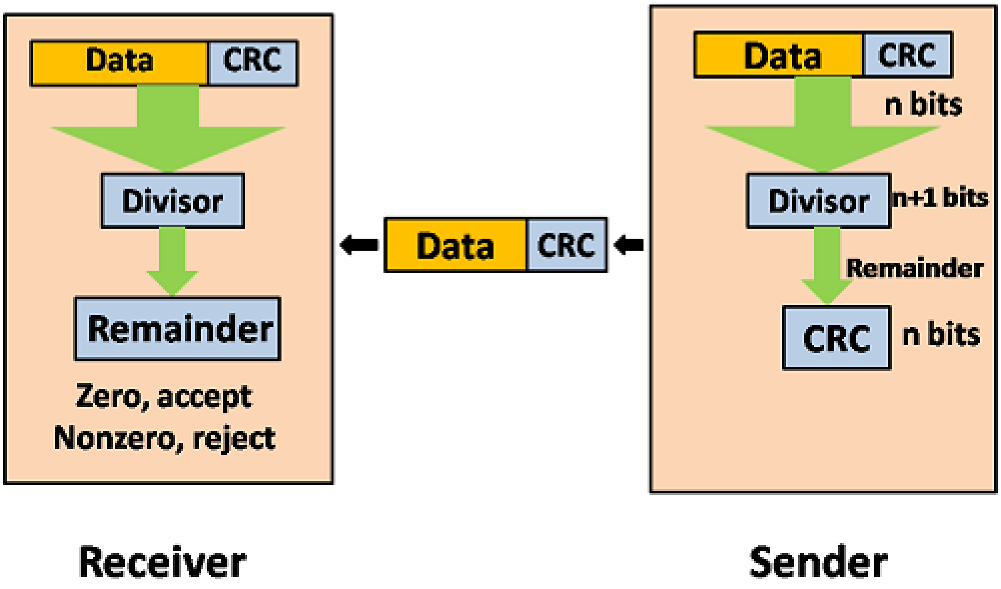
CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

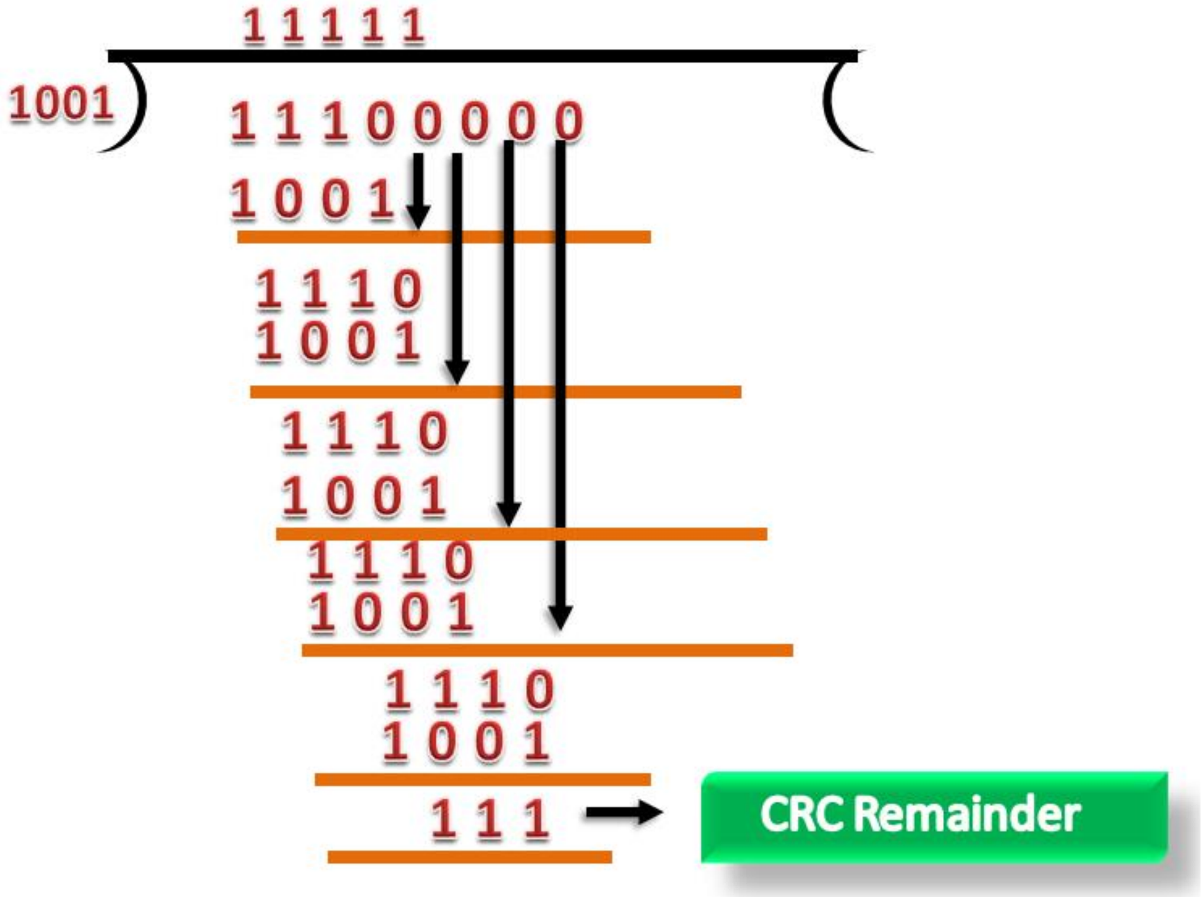


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

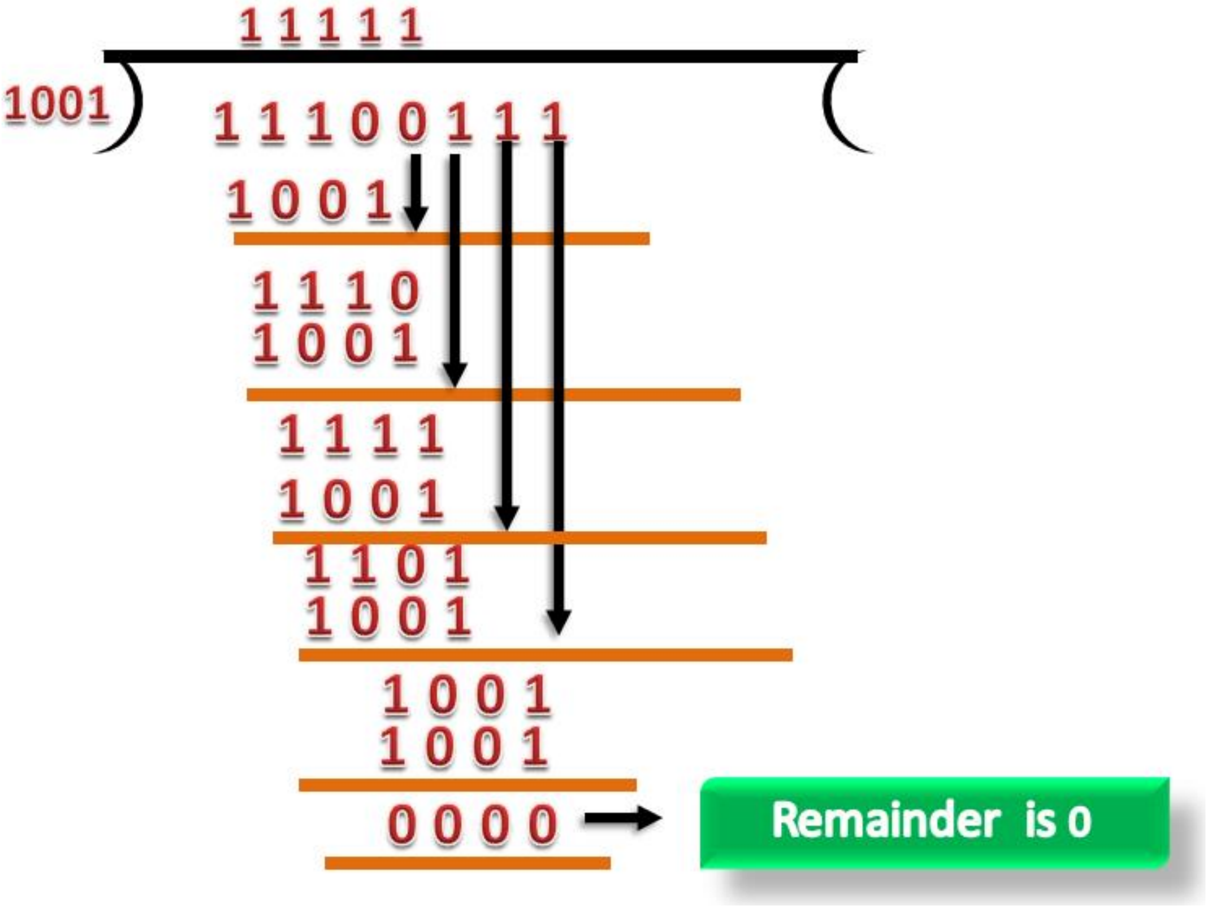
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



Stop and Wait Protocol

Before understanding the stop and Wait protocol, we first know about the error control mechanism. The error control mechanism is used so that the received data should be exactly same whatever sender has sent the data. The error control mechanism is divided into two categories, i.e., Stop and Wait ARQ and sliding window. The sliding window is further divided into two categories, i.e., Go Back N, and Selective Repeat. Based on the usage, the people select the error control mechanism whether it is **stop and wait** or **sliding window**.

What is Stop and Wait protocol?

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

The primitives of stop and wait protocol are:

Sender side

Rule 1: Sender sends one data packet at a time.

Rule 2: Sender sends the next packet only when it receives the acknowledgment of the previous packet.

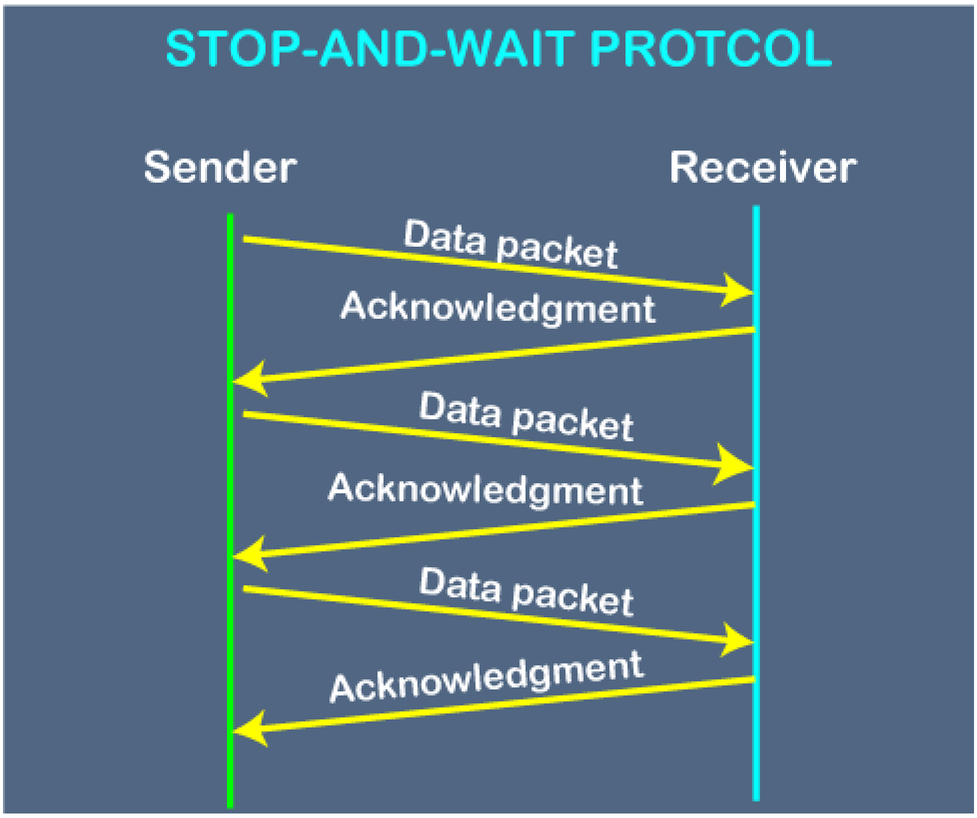
Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

Receiver side

Rule 1: Receive and then consume the data packet.

Rule 2: When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.


STOP-AND-WAIT PROTCOL
Sender
Receiver
Data packet
Acknowledgment
Data packet
Acknowledgment
Data packet
Acknowledgment

What is noiseless protocol?

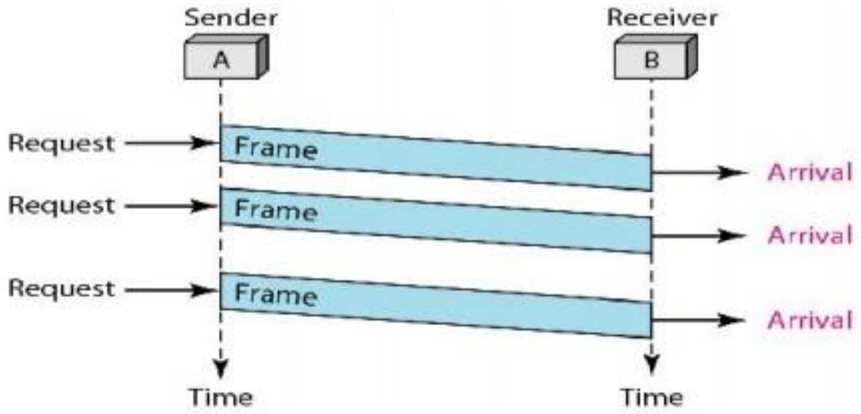


Figure 2.7 Flow diagram for Example 2.1

It is a **unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver**. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

Sliding Window Protocol

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.

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:

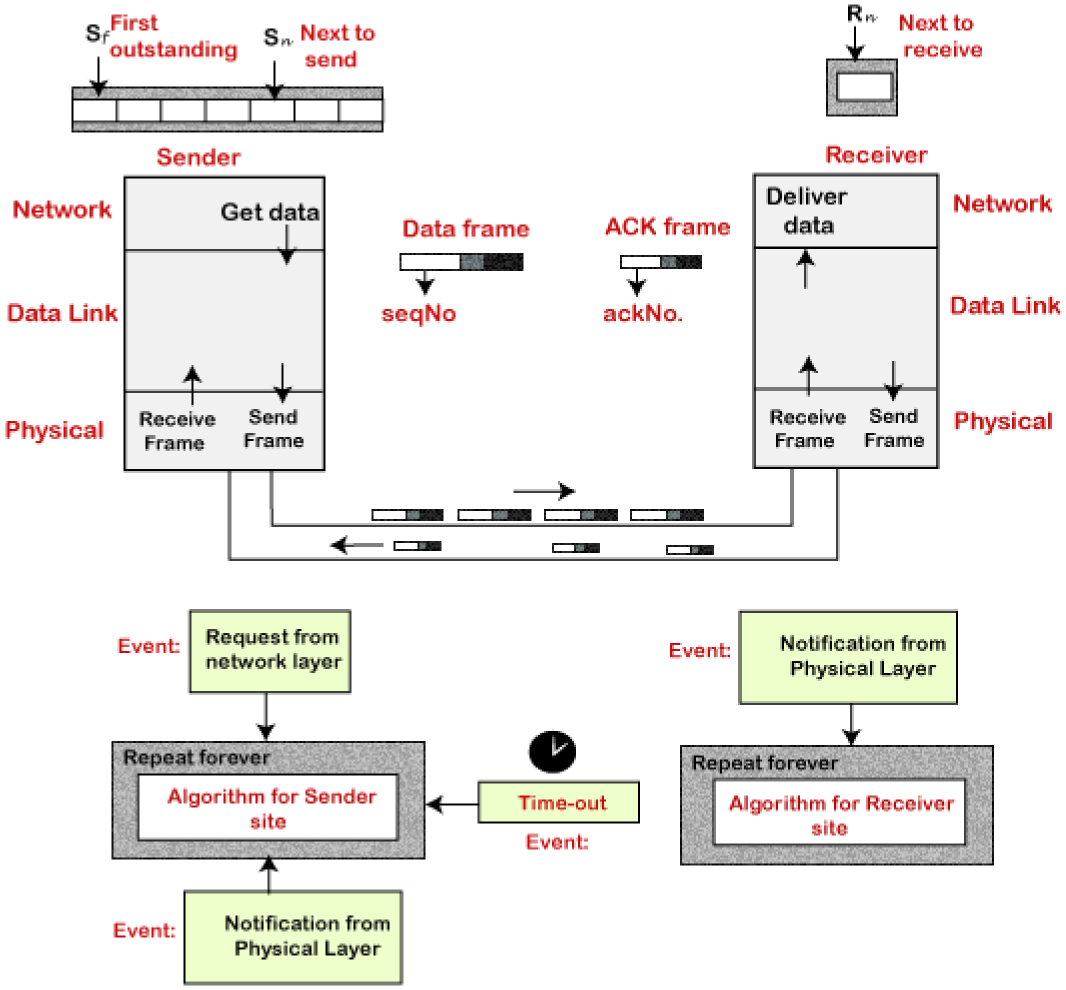
1. Go-Back-N ARQ(Automatic Repeat Request)
2. Selective Repeat ARQ(Automatic Repeat Request)

Go-Back-N ARQ(Automatic Repeat Request)

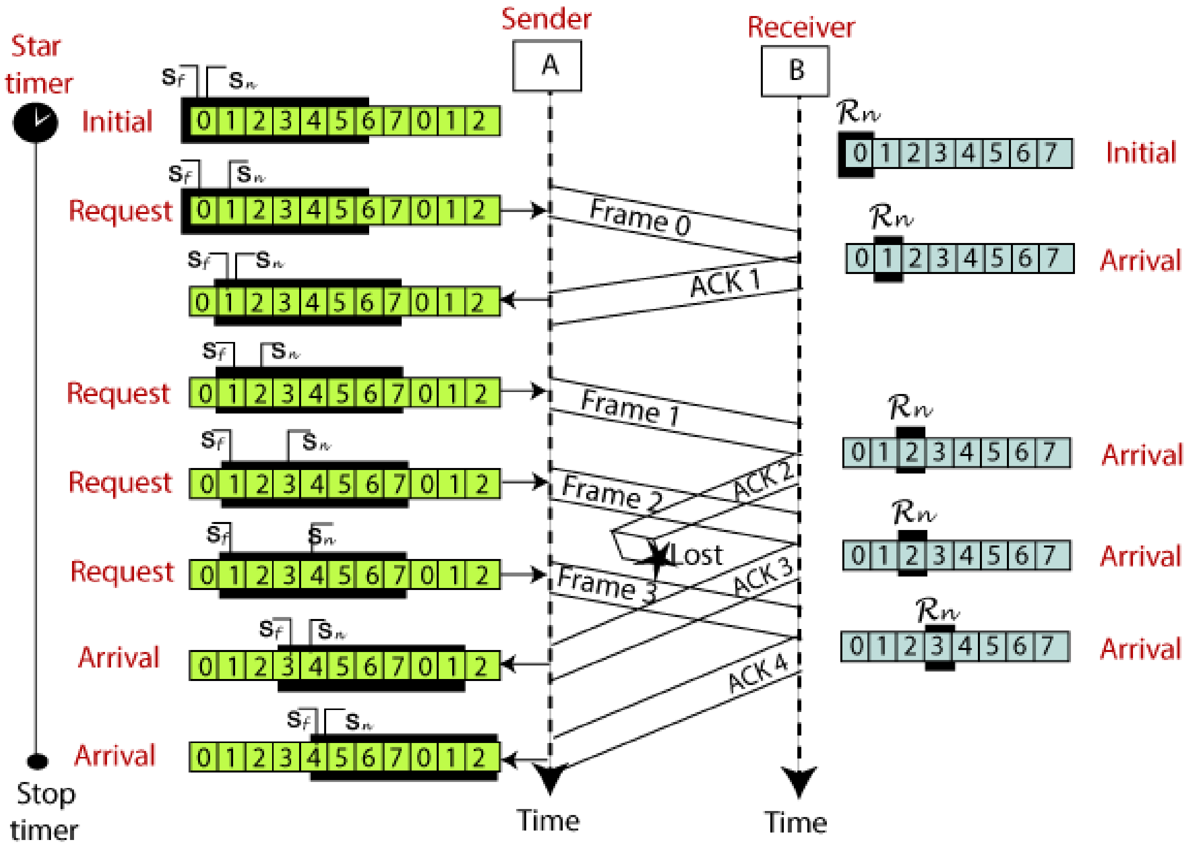
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

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



The example of Go-Back-N ARQ is shown below in the figure.

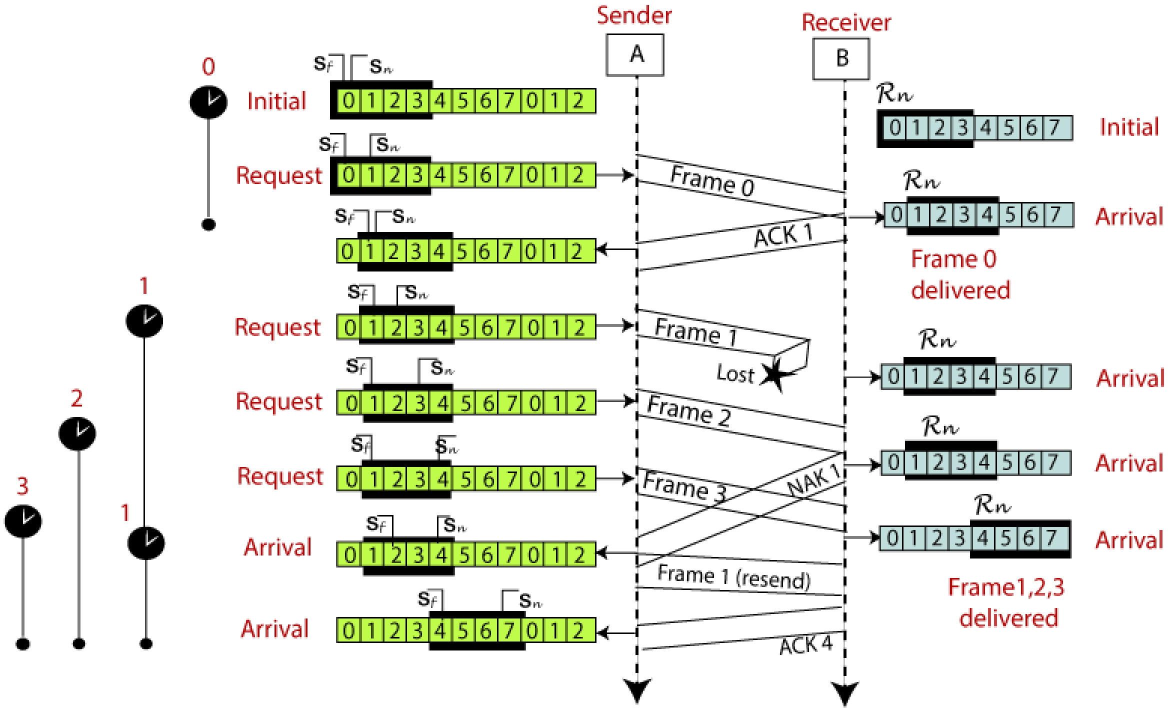


Selective Repeat ARQ

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.

The example of the Selective Repeat ARQ protocol is shown below in the figure



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.

Multiple Access protocols

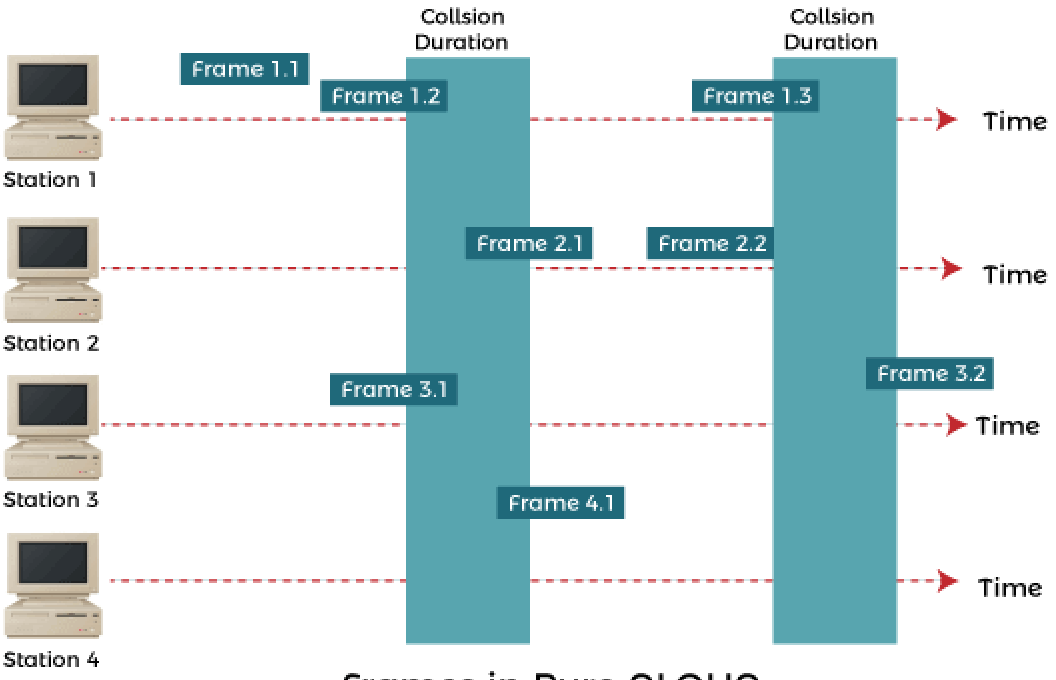
1. Aloha
2. CSMA(carrier sense multiple access)

What is aloha?

Aloha is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. In aloha, any station can transmit data to a channel at any time. It does not require any carrier sensing.

ı.Pure Aloha

Pure aloha is used when data is available for sending over a channel at stations. 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.

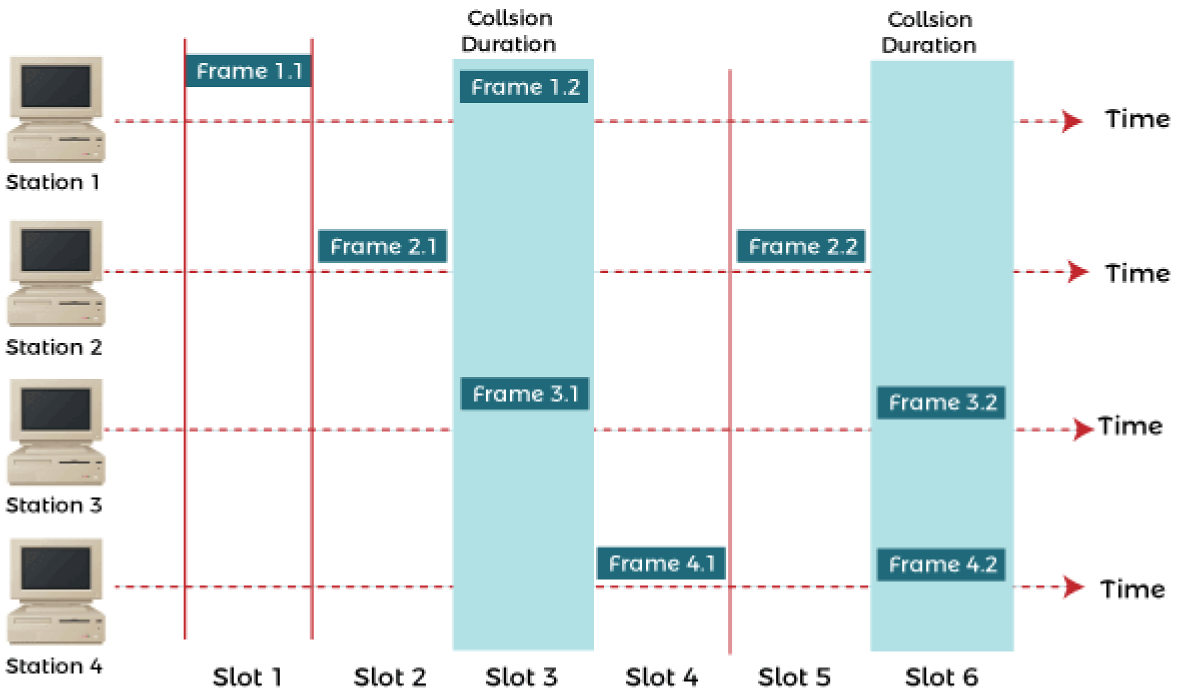


Frames in Pure ALOHA

When a station transmits the data frame to a channel without checking whether the channel is free or not, there will be a possibility of the collision of data frames. Station expects the acknowledgement from the receiver, and if the acknowledgement of the frame is received at the specified time, then it will be OK; otherwise, the station assumes that the frame is destroyed. Then station waits for a random amount of time, and after that, it retransmits the frame until all the data are successfully transmitted to the receiver.

Slotted Aloha

There is a high possibility of frame hitting in pure aloha, so slotted aloha is designed to overcome it. Unlike pure aloha, slotted aloha does not allow the transmission of data whenever the station wants to send it.



Frames in Slotted ALOHA

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. If the station is failed to send the data, it has to wait until the next slot.

However, there is still a possibility of a collision because suppose if two stations try to send a frame at the beginning of the time slot.

Wireless LAN

Introduction to Wireless LAN

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is Switching Concept required?

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.

- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

ANALOG AND DIGITAL SIGNALS

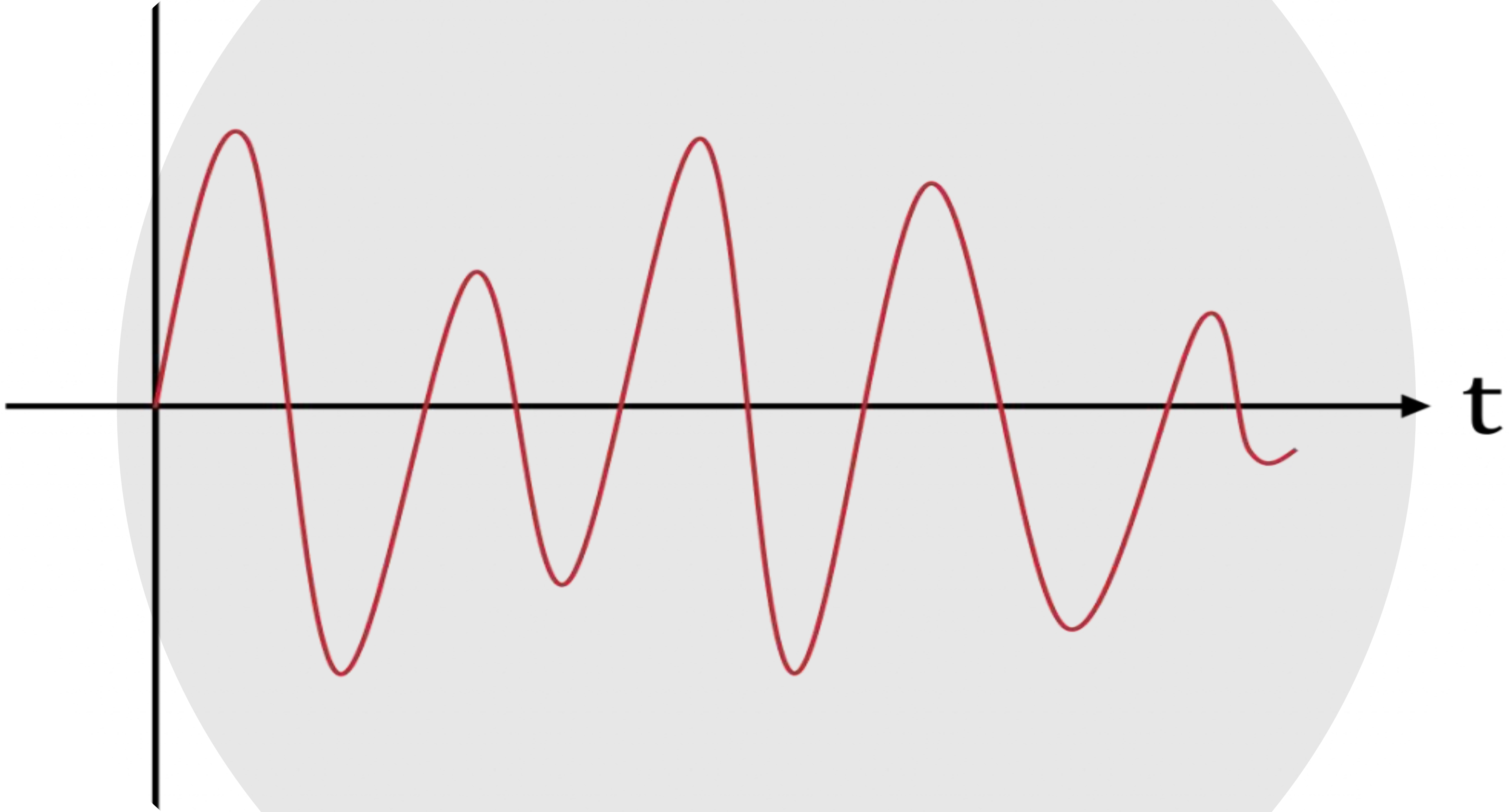
- To be transmitted, data must be transformed to electromagnetic signals.
- Data is transmitted from one point to another point by means of electrical signals that may be in digital and analog form.
- Analog data refers to information that is continuous; For example, sounds made by a human voice.
- Digital data refers to information that has discrete states. Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s.

Signal Propagation:

- Movement of signal through the channel wired or wireless is called as signal propagation.
- If we apply a signal at one end of the conducting medium then eventually this signal gets propagated to the other end of the medium.
- Signals which repeat itself after a fixed time period are called periodic signals. Signals which do not repeat itself after a fixed time period are called non-periodic signals.
- The signal containing the data or information is in the electric form and it is applied at point X of the conducting medium.
- The electrons in the conducting medium will transfer the charge to the adjacent electrons and the signal at point X gets transferred to Y and then to Z which is the receiving point
- The shape of the signal at the receiver i.e. point Z is almost same as that at the source i.e. point X, but the signal reaches point Z after a finite delay called propagation delay.

Analog Signal

- An analog signal is a continuous wave form that changes smoothly over time.
- Analog signal is usually represented by sine wave.
- An analog signal can take on any value in a specified range of values. As the wave moves from value A to B, it passes through and includes an infinite number of values along its path.
- A simple example is Alternating Current (AC), which continually varies between about +110 volts and -110 volts in a sine wave fashion 60 times per second.
- A more complex example of an analog signal is the time-varying electrical voltage generated when a person speaks into a dynamic microphone or telephone.


t

- Analog signals are usually specified as a continuously varying voltage over time and can be displayed on a device known as an oscilloscope.
- The maximum voltage displacement of a periodic (repeating) analog signal is called its amplitude, and the shortest distance between crests of a periodic analog wave is called its wavelength.

Advantages of analog signals:

- 1. The main advantage is the fine definition of the analog signal which has the potential for an infinite amount of signal resolution.
- 2. Compared to digital signals, analog signals are of higher density.
- 3. Best suited for the transmission of audio and video.
- 4. Consumes less bandwidth than digital signals to carry the same information.
- 5. Analog signal is less susceptible to noise.

Disadvantages of analog signals:

- 1. The primary disadvantage of analog signaling is that any system has noise - i.e., random unwanted variation.
- 2. The effects of noise create signal loss and distortion.
- 3. Most of the analog systems also suffer from generation loss.

Analog Transmission

- Analog transmission means of transmitting only analog signals. Data could be analog or digital; signal is always analog. Propagation could be over guided or unguided medium (space, atmosphere).

- Analog (or analogue) transmission is a transmission method of conveying voice, data, image, signal or video information using a continuous signal which varies in amplitude, phase, or some other property in proportion to that of a variable.

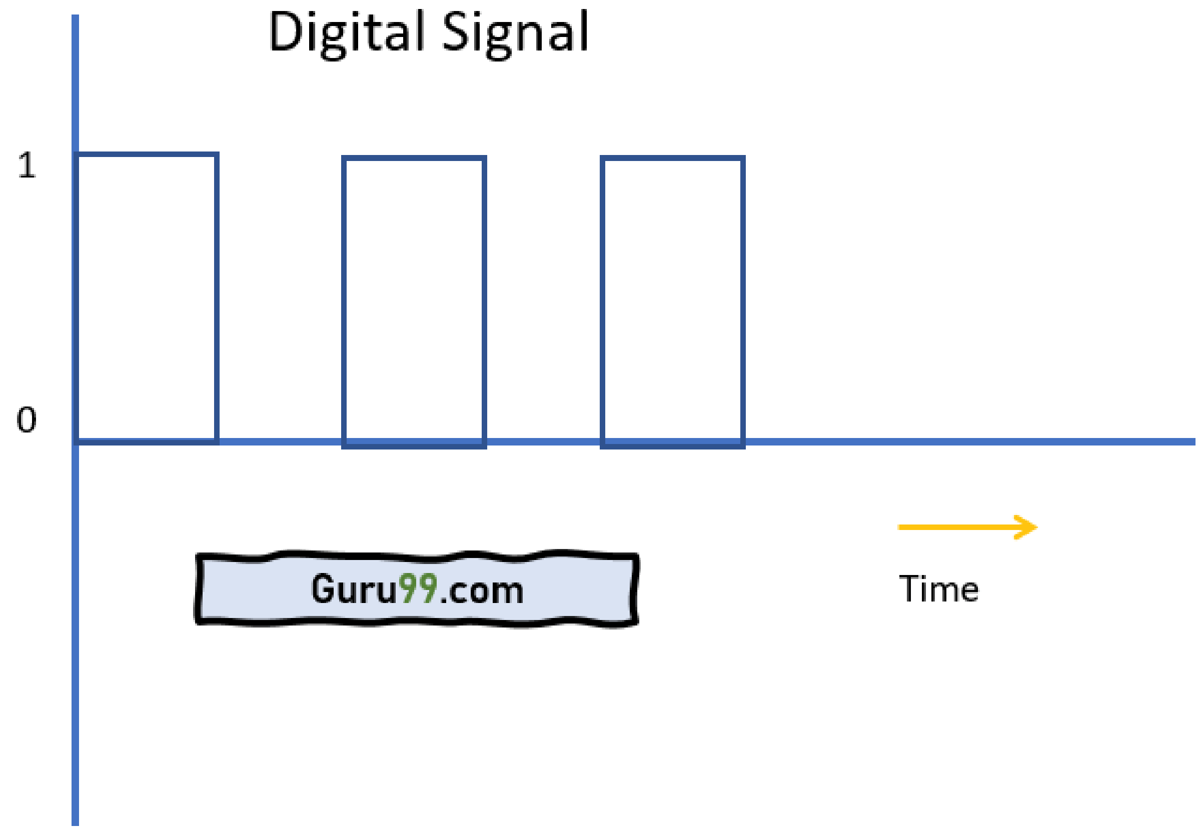
- It could be the transfer of an analog source signal, using an analog modulation method such as Frequency Modulation (FM) or Amplitude Modulation (AM) etc.

- Analogue data transmission consists of sending information over a physical transmission medium in the form of a wave.

- Three types of analogue transmission are defined depending on which parameter of the carrier wave is being varied:
  - 1. Transmission by amplitude modulation of the carrier wave.
  - 2. Transmission by frequency modulation of the carrier wave.
  - 3. Transmission by phase modulation of the carrier wave.

Digital Signal

- A digital signal is discrete in nature. Digital signal can have only a limited number of definite values, often as simple as 1 and 0.
- Transmission of signals that vary discretely with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.
- Digital signals use discrete values for the transmission of binary information over a communication medium such as a network cable or a telecommunications link.
- On a serial transmission line, a digital signal is transmitted 1-bit at a time.


Digital Signal
1
0
Guru99.com
Time

Advantages of digital signals

- 1. Digital signals are more secure - it is easier to encrypt digital signals making internet shopping less risky .
- 2. Digital signals suffer less from noise because any errors can be detected and corrected using regenerators.
- 3. Optical fibres can transmit digital signals and optical fibres are cheap.
- 4. Digital signals can be compressed so more channels can be transmitted along the same fibre.
- 5. Can connect several different users to the same line - such as video conferencing.

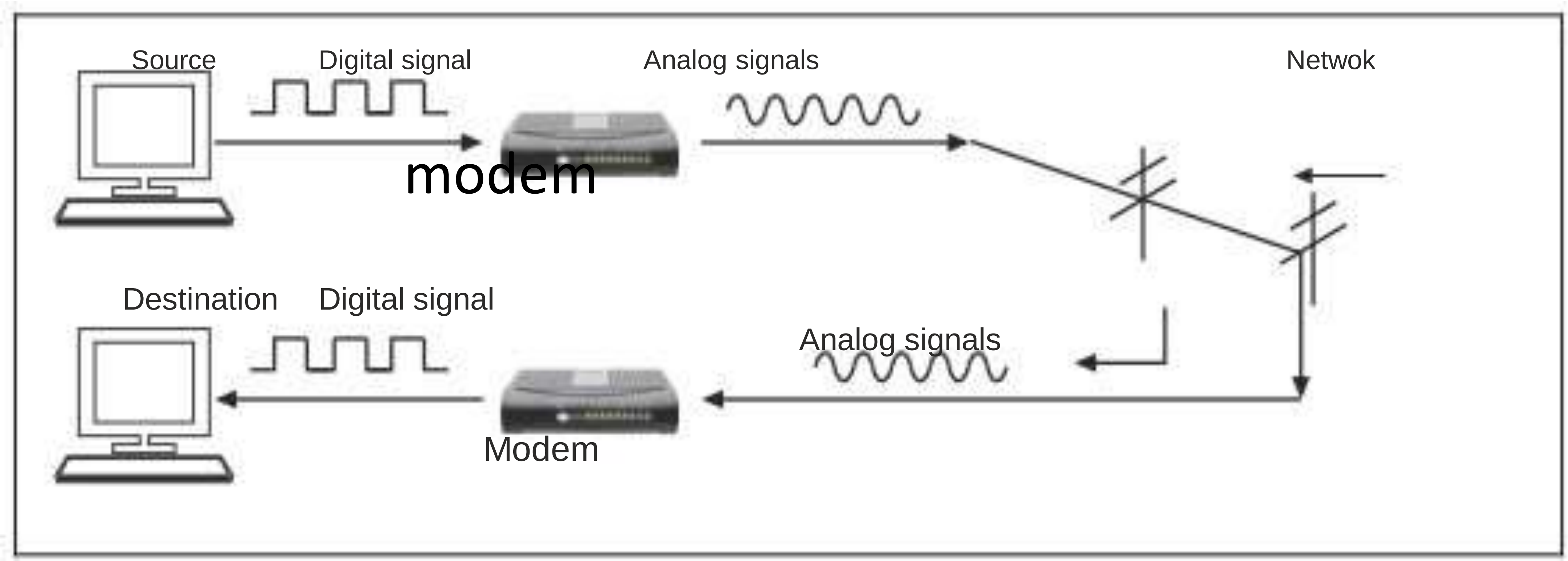
Disadvantages of Digital Signals:

- 1. Digital signals need more bandwidth to transmit the same information.
- 2. The transmitter and receiver have to synchronise very carefully so that the information makes sense.

Digital Transmission

- Digital transmission means of transmitting both digital and analog signals. Usually assume the signal is carrying digital (or digitized) data.
- A repeater retrieves the (digital) signal; recovers the (digital) data, e.g., a pattern of 1's and 0's; retransmits a new signal.
- A similar technique used for the analog signal where we assume that the data is digital or digitized; repeater recovers the (digital or digitized) data and amplifies only the data and retransmits.

Digital Signal, Analog Transmission



- For the problem of how to send digital signal over an analog network, some codification techniques are required to convert to digital signal to analog signal in telephone networks.
- For this purpose modem is used. Modem stands for modulator and demodulator.
- A modulator uses some coding scheme and converts a digital signal into an analog signal and demodulator converts the analog signal back into the digital signal.
- When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data, i.e. binary data.
- An analog is characterized by its amplitude, frequency and phase. There are three kinds of digital-to-analog conversions possible