Introduction

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

Serial and Parallel Data Transmission

The process of sending data between two or more digital devices is known as *data transmission*. Data is transmitted between digital devices using one of the two methods – *serial transmission* or *parallel transmission*.

Serial Data Transmission

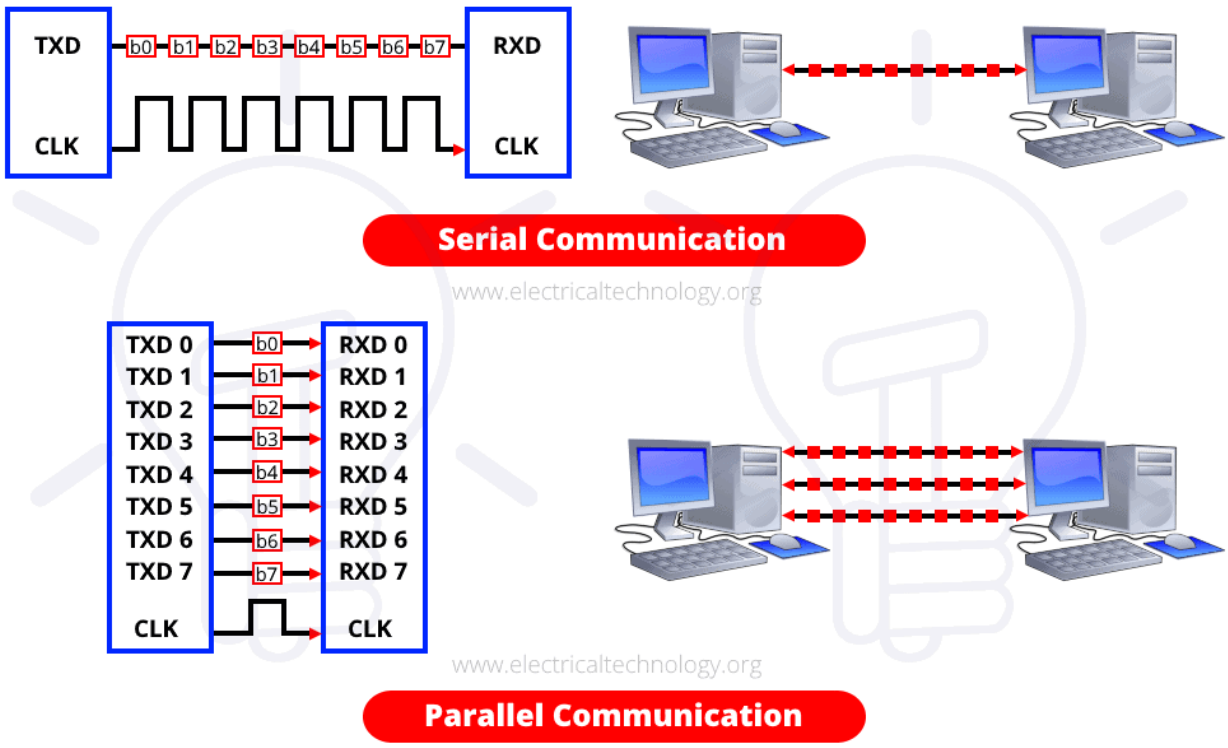
A serial transmission transfers data one bit at a time, consecutively, via a communication channel or computer bus in telecommunication and data transmission. On the other hand, parallel communication delivers multiple bits as a single unit through a network with many similar channels.

- 8-bits are conveyed at a time in serial transmission, with a start bit and a stop bit.
- All long-distance communication and most computer networks employ serial communication.
- Serial computer buses are becoming more common, even across shorter distances, since newer serial technologies' greater signal integrity and transmission speeds have begun to outperform the parallel bus's simplicity advantage.
- The majority of communication systems use serial mode. Serial networks may be extended over vast distances for far less money since fewer physical wires are required.

Parallel Data Transmission

Parallel communication is a means of transmitting multiple binary digits (bits) simultaneously in data transmission. It differs from serial communication, which sends only one bit at a time; this distinction is one method to classify a communication channel.

- A parallel interface comprises parallel wires that individually contain data and other cables that allow the transmitter and receiver to communicate. Therefore, the wires for a similar transmission system are put in a single physical thread to simplify installation and troubleshooting.
- A large amount of data must be delivered across connection lines at high speeds that match the underlying hardware.
- The data stream must be transmitted through "n" communication lines, which necessitates using many wires. This is an expensive mode of transportation; hence it is usually limited to shorter distances.



Difference between Serial and Parallel Data Transmission

Key	Serial Transmission	Parallel Transmission
Definition	Serial Transmission is the type of transmission in which a single communication link is used to transfer the data from one end to another.	Parallel Transmission is the mode of transmission in which multiple parallel links are used that transmit each bit of data simultaneously.
Bit transmission	In case of Serial Transmission, only one bit is transferred at one clock pulse.	In case of Parallel Transmission, 8-bits transferred at one clock pulse.
Cost Efficiency	As single link is used in Serial Transmission, it can be implemented easily without having to spend a huge amount. It is cost efficient.	Multiple links need to be implemented in case of Parallel Transmission; hence it is not cost efficient.
Performance	As single bit gets transmitted per clock in case of Serial Transmission, its performance is	8-bits get transferred per clock in case of Parallel transmission, hence it is more efficient in performance.

Prepared by: Er. Bigyan Bhattarai

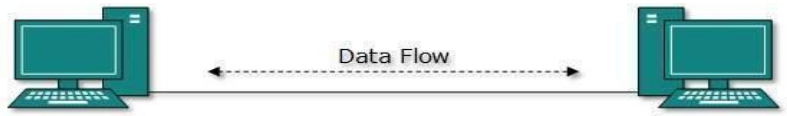
Key	Serial Transmission	Parallel Transmission
	comparatively lower as compared to Parallel Transmission.	
Preference	Serial Transmission is preferred for long distance transmission.	Parallel Transmission is preferred only for short distance.
Complexity	Serial Transmission is less complex as compared to that of Parallel Transmission.	Parallel Transmission is more complex as compared to that of Serial Transmission.

Data Communication Topologies

A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.

Network topologies describe the arrangement of networks and the relative location of traffic flows. Administrators can use network topology diagrams to determine the best placements for each node and the optimal path for traffic flow. With a well-defined and planned-out network topology, an organization can more easily locate faults and fix issues, improving its data transfer efficiency.

Network geometry can be defined as the *physical topology* and the *logical topology*. Network topology diagrams are shown with devices depicted as network nodes and the connections between them as lines. The type of network topology differs depending on how the network needs to be arranged.



The way in which devices are interconnected to form a network is called network topology. Some of the factors that affect choice of topology for a network are −

- Cost − Installation cost is a very important factor in overall cost of setting up an infrastructure. So, cable lengths, distance between nodes, location of servers, etc. have to be considered when designing a network.
- Flexibility − Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.

- Reliability – Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- Scalability – Network topology should be scalable, i.e. it can accommodate load of new devices and nodes without perceptible drop in performance.
- Ease of installation – Network should be easy to install in terms of hardware, software and technical personnel requirements.
- Ease of maintenance – Troubleshooting and maintenance of network should be easy.

1. Bus Topology

Data network with bus topology has a linear transmission cable, usually coaxial, to which many network devices and workstations are attached along the length. Server is at one end of the bus. When a workstation has to send data, it transmits packets with destination address in its header along the bus.

Advantages of Bus Topology

These are the advantages of using bus topology –

- Easy to install and maintain
- Can be extended easily
- Very reliable because of single transmission line

Disadvantages of Bus Topology

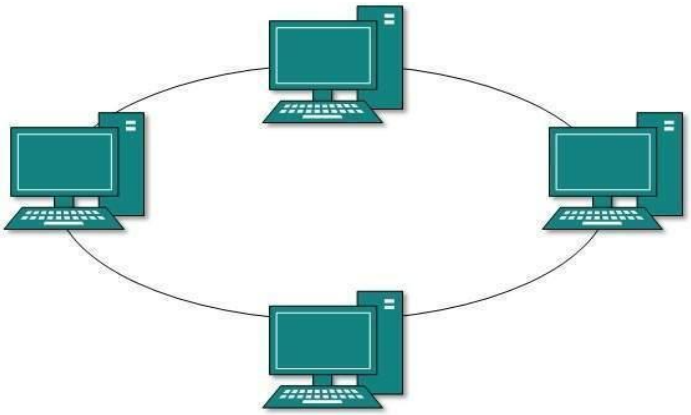
These are some disadvantages of using bus topology –

- Troubleshooting is difficult as there is no single point of control
- One faulty node can bring the whole network down
- Dumb terminals cannot be connected to the bus

2. Ring Topology

In ring topology each terminal is connected to exactly two nodes, giving the network a circular shape. Data travels in only one pre-determined direction.

When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one. Before further transmission data may be amplified. In this way, data reverses the network and reaches the destination node, which removes it from the network. If the data reaches the sender, it removes the data and resends it later.



Advantages of Ring Topology

`These are the advantages of using ring topology –`

- Small cable segments are needed to connect two nodes
- Ideal for optical fibers as data travels in only one direction
- Very high transmission speeds possible

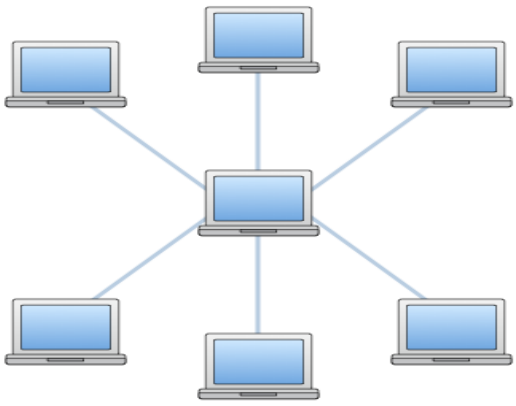
Disadvantages of Ring Topology

`These are some the disadvantages of using ring topology –`

- Failure of single node brings down the whole network but now routing can be done at any two nodes.
- Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified.
- Difficult to remove one or more nodes while keeping the rest of the network intact.

3. Star Topology

In star topology, server is connected to each node individually. Server is also called the central node. Any exchange of data between two nodes must take place through the server. It is the most popular topology for information and voice networks as central node can process data received from source node before sending it to the destination node.



Advantages of Star Topology

These are the advantages of using star topology −

- Failure of one node does not affect the network
- Troubleshooting is easy as faulty node can be detected from central node immediately
- Simple access protocols required as one of the communicating nodes is always the central node

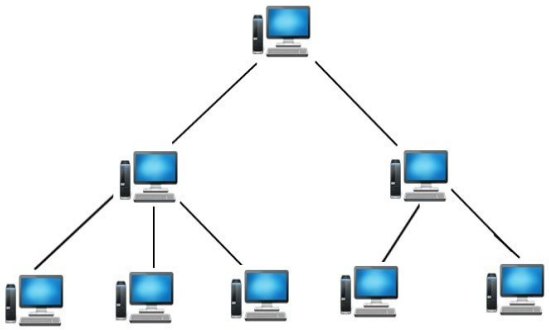
Disadvantages of Star Topology

These are the disadvantages of using star topology −

- Long cables may be required to connect each node to the server
- Failure of central node brings down the whole network

4. Tree Topology

Tree topology has a group of star networks connected to a linear bus backbone cable. It incorporates features of both star and bus topologies. Tree topology is also called hierarchical topology.



Advantages of Tree Topology

These are some of the advantages of using tree topology −

- Existing network can be easily expanded
- Point-to-point wiring for individual segments means easier installation and maintenance
- Well suited for temporary networks

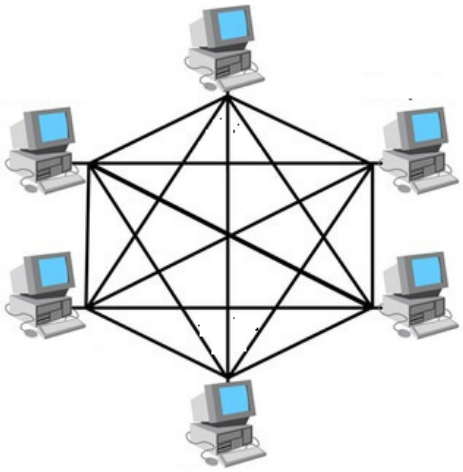
Disadvantages of Tree Topology

These are some of the disadvantages of using tree topology −

- Technical expertise required to configure and wire tree topology
- Failure of backbone cable brings down entire network
- Insecure network
- Maintenance difficult for large networks

5. Mesh Topology

In a mesh topology, each computer is connected to every other computer in point-to-point mode as shown in the image below. For example, if we have four computers, we must have six links. If we have n computers, we must have n(n-1)/2 links.



Advantages

The advantages of mesh topology are:

- Message delivery is more reliable.
- Network congestion is minimum due to large number of links.

Disadvantages

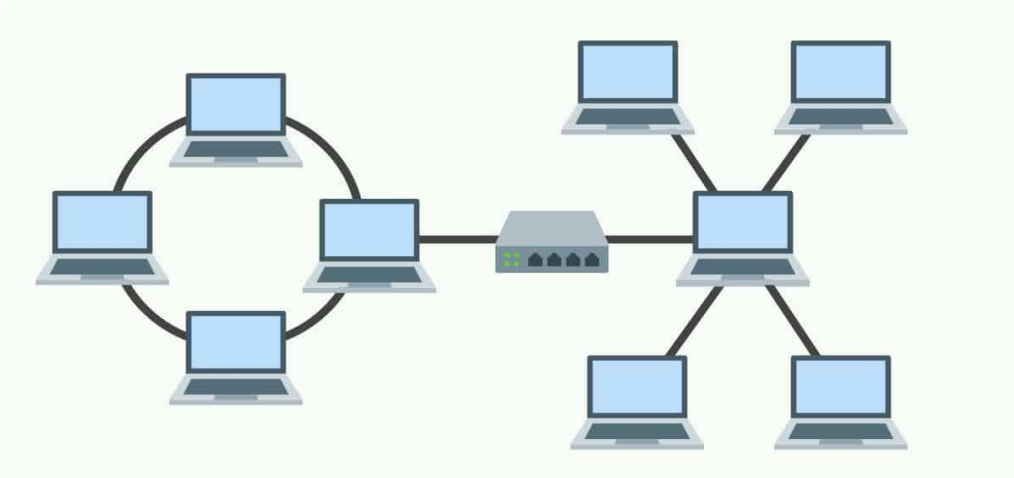
The disadvantages of mesh topology are:

- It is very expensive to implement.
- It is very difficult to configure and install.

6. Hybrid Topology

The hybrid topology is the combination of multiple topologies, used for constructing a single large topology. A hybrid topology is created when two different network topologies are interconnected.

If two ring topologies are connected then the resultant topology is not the hybrid topology. On the other hand, if the ring topology is connected to the bus topology, then the resulting topology is called the hybrid topology. This topology generally combines the features of the two topologies and is therefore more effective and efficient than the individual topologies.



Advantages

The advantages of hybrid topology are:

- The hybrid topology is more effective as it uses multiple topologies.
- The hybrid topology contains the best and efficient features of the combined topologies from which it is constructed.

Disadvantages

The disadvantages of hybrid topology are:

- The hybrid topology is relatively more complex than the other topologies.
- The hybrid topology is difficult to install and configure.

7. Daisy Chain

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Serial Interface and Parallel Interface

Serial Interface

A serial interface is a communication interface that transmits data as a single stream of bits, typically using a wire-plus-ground cable, a single wireless channel or a wire-pair.

The serial interface acts as a communication interface between two digital systems that sends data as a series of voltage pulses over a wire. In contrast, a parallel interface transmits multiple bits simultaneously using different wires.

Some devices that use the serial interface include the Universal Serial Bus (USB), Recommended Standard No. 232 (RS-232), 423, 422 and 485 1-Wire and I2C

There are two types of serial interface:

- Asynchronous serial interface (commonly abbreviated as SCI): With the SCI, data is sent in well-defined frames. A frame refers to the total, non-divisible packet of bits. Included within the frame are certain information (for example, data) and some overhead (for example, control bits).

  The frames used in an asynchronous serial protocol usually include a single start bit, parity bits, seven or eight data bits, and, sometimes, a stop bit. SCI is often used to establish communication between two computer systems. SCI is considered asynchronous because neither system needs to synchronize its clock prior to communicating.

- Synchronous serial interface (commonly abbreviated as SPI): In SPI, the receiver does not have any internal clock, which indicates that the receiver is unable to individually synchronize its data line reading with the transmission rate of the transmitter. The receiver requires some assistance and that support is available in the form of a clock signal, which is shared by the receiver and transmitter. The clock signal serves as a control line that informs the receiver about the best time to read from the data line. This implies that the receiver and transmitter should synchronize their accessibility to the data line to successfully send data.

  SPI is generally used if a microcontroller needs to send data to a device with no internal clock.

  Recommended Standard No. 232

  DB9 and DB25 connector is used in RS 232

  DB9 used in COM1 port and DB25 used in COM2 Port in serial communication USB is used in COM3, COM4, COM5 and more.

Parallel Interface

A parallel interface refers to a multiline channel, with each line capable of transmitting several bits of data simultaneously. Before USB ports became common, most personal computers (PCs) had at least one parallel interface for connecting a printer using a parallel port. In contrast, a "serial interface" uses a serial port, a single line capable of only transmitting one bit of data at a time; a computer mouse connection is a good example.

The first parallel interface was the Centronics parallel interface developed and used in the Centronics 101 model printer in 1970. This became the standard; but a variety of cables were required.

The IEEE 1284 standard specified five modes of operations, each specifying a direction of data flow, i.e., toward or away from the computer or bi-directional. These are:

- Compatibility Mode: This is the original Centronics parallel interface.
- Nibble Mode: This allowed data transfer back to the computer.
- Byte Mode: This allows data to be sent back to the computer at the same speed that data is sent from the computer to the printer or other device.
- ECP Mode: This stands for “enhanced capability port” and allows bidirectional data flow for printers and scanners.
- EPP Mode: This uses data cycles to quickly transfer data in both directions at speeds of 500 kilobytes to 2 megabytes per second.

One of the latest parallel interface technologies is known as “high-performance parallel interface” or HIPPI.

IEEE 1284 Cables and connectors

An IEEE-compliant cable must meet several standards of wiring and quality. Three types of connectors are defined:

- Type A: DB-25 25 pins, for the host connection.
- Type B: Centronics (officially called "Micro Ribbon") 36-pin, for the printer or device connection.
- Type C: Mini-Centronics (MDR36 or HPCN36) 36-pin, a half-pitch, smaller alternative for the device connection that has not proven popular.

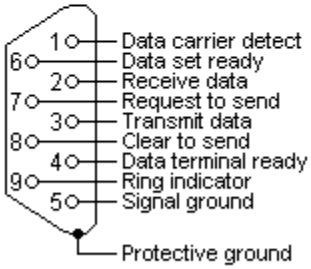
There are two kinds of IEEE 1284 cables:

- IEEE 1284-I: uses IEEE 1284-A and IEEE 1284-B connectors.
- IEEE 1284-II: uses IEEE 1284-C connectors.

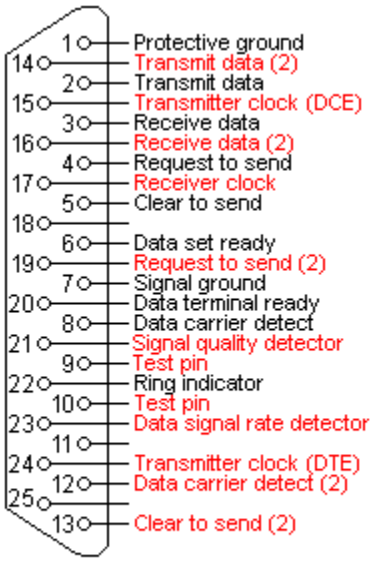
RS-232

In telecommunications, RS-232 or Recommended Standard 232 is a standard originally introduced in 1960 for serial communication transmission of data. It formally defines signals connecting between a *DTE* (*data terminal equipment*) such as a computer terminal, and a *DCE* (*data circuit-terminating equipment* or *data communication equipment*), such as a modem. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pinout of connectors. The current version of the standard is *TIA-232-F Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, issued in 1997. The RS-232 standard had been commonly used in computer serial ports and is still widely used in industrial communication devices

RS232 connector is a port used for data exchange between equipment's. It was designed for data exchange between DTE (Data Terminal Equipment) or PC and DCE (Data Communication Equipment) or MODEM. The need for RS232 came from limitations raised by parallel data exchange. RS232 uses serial communication protocol where data exchange is done bit by bit. Although RS232 is later replaced by faster USB (Universal Serial Bus); it is still popular in some areas. RS232 used to have 25 pins, now it is shrunk to just 9 pins.



RS 232 9 pin



RS 232 25 pin

DTE			DCE	
DB9	DB25		DB9	DB25
-	1	Protective GND	-	1
3	2	TxD →	3	2
2	3	← RxD	2	3
7	4	RTS →	7	4
8	5	← CTS	8	5
6	6	← DSR	6	6
5	7	Signal GND	5	7
1	8	← DCD	1	8
4	20	DTR →	4	20
9	22	← RI	9	22

Prepared by: Er. Bigyan Bhattarai

Pin Number	Pin Name	Description
DATA pins (Data flow takes through these pins)		
2	RXD	Receive Data (Data is received though this pin)
3	TXD	Transmit Data (Data is transmitted through this pin)
CONTROL pins (These pins are for establishing interface and to avoid data loss)		
1	CD	Carrier Detect (Set by MODEM when answer is received by remote MODEM)
4	DTR	Data Terminal Ready (Set by PC to prepare MODEM to be connected to telephone circuit)
6	DSR	Data Set Ready (Set by MODEM to tell PC it is ready to receive and send data)
7	RTS	Request To Send (Set by PC to tell MODEM that MODEM can begin sending data)
8	CTS	Clear To send (Set by MODEM to tell PC that it is ready to receive data)
9	RI	Set by MODEM to tell PC a ringing condition has been detected.
REFERENCE		
5	GND	Ground (Used as reference for all pin voltage pulses)

A serial port complying with the RS-232 standard was once a standard feature of many types of computers. Personal computers used them for connections not only to modems, but also to printers, computer mice, data storage, uninterruptible power supplies, and other peripheral devices.

Compared with later interfaces such as RS-422, RS-485 and Ethernet, RS-232 has lower transmission speed, shorter maximum cable length, larger voltage swing, larger standard connectors, no multipoint capability and limited multidrop capability. In modern personal computers, USB has displaced RS-232 from most of its peripheral interface roles. Thanks to their simplicity and past ubiquity, however, RS-232

interfaces are still used—particularly in industrial CNC machines, networking equipment and scientific instruments where a short-range, point-to-point, low-speed wired data connection is fully adequate.

RS232 Pin Configuration

New RS232 has nine pins as mentioned earlier. These nine pins are arranged in the port as shown in RS232 Connector Pinout. The DCE and DTE ports are exactly similar except for the direction of data flow. These nine pins are roughly divided in to three categories and we will discuss each category below.

RS232 Features and Specifications

1. RS232 uses Asynchronous communication so no clock is shared between PC and MODEM.
2. Logic '1' on pin is stated by voltage of range '-15V to -3V' and Logic '0' on pin is stated by voltage of range '+3V to +15V'. The logic has wide voltage range giving convenience for user.
3. MAX232 IC can be installed easily to establish RS232 interface with microcontrollers.
4. Full duplex interface of RS232 is very convenient.
5. Two pin simplex RS232 interface can also be established easily if required.
6. A maximum data transfer speed of 19 Kbps (Kilobits per second) is possible through RS232
7. A maximum current of 500mA can be drawn from pins of RS232
8. The interface can be established up to a distance of 50 feet.

Disadvantages of RS232

1. There is no pin dedicated for powering devices (No VCC)
2. More communication pins
3. Switching voltages between +15v and -15v is difficult at higher speeds
4. A maximum speed of 19 Kbps
5. A maximum distance of 50 feet
6. More pins lead to higher noise
7. Only a single device can be connected to RS232 connector unlike I2C
8. Need hardware to convert high voltage logic of RS232 to be compatible to TTL (controller and processor units)

Telephone Networks

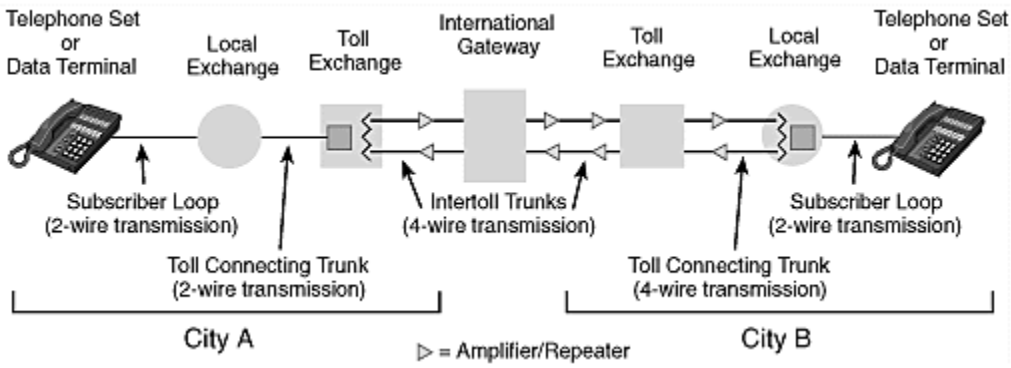
A telephone network is a telecommunications network that connects telephones, which allows telephone calls between two or more parties.

A landline network where the telephones must be directly wired into a single telephone exchange. This is known as the public switched telephone network or PSTN.

PSTN is a circuit switch network whereas, now-a-days business VoIP phone systems use digital packet switching.

The entire network was originally an analog system using analog system to transmit voice.

Telephone network is made up of three major components: local loops, trunk and switching offices.



1. Local Loops

A twisted pair cable that connects the subscriber telephone to the nearest end office or local central office. The local loop when used for voice has a bandwidth of 4Khz.

In telephony, a local loop is a wired connection from a telephone companies end office to customers houses or small business. It is also referred as last mile. The local loop or local or subscriber line is a physical link or circuit that connects from the demarcation point of the customer premises to the edge of a common carrier or telecommunications services provider's network.

2. Trunks

Transmission is usually through optical fiber or microwave links. Handles hundreds and thousands of connections through multiplexing. A transmission media that handles the communication between offices. A trunk is a communication line or link designed to carry multiple signals simultaneously to provide network access between two points. It typically connects switching centers in a communication system. An interconnecting transmission channel between a switching machine in one location and a switching machine in an adjacent node.

3. Switching

Connects several trunks line and used to switch the different call.

Direct Distance Dialing

Direct distance dialing (DDD) is a telecommunication service feature in North America by which a caller may, without operator assistance, call any other user outside the local calling area. Direct dialing by subscribers typically requires extra digits to be dialed as prefixes to the directory telephone number of the destination. International Direct Distance Dialing (IDDD) extends the system beyond the geographic boundaries of the National Public Telephone Network. This is also known as national wise dialing.

Successful operation of DDD program depends primarily on three factors:

A standard national wise numbering.

A method of charging the customer.

A fundamental plan for automatic toll switching.

What is the difference between STD ISD and PCO?

The full STD form is Subscriber Trunk Dialing. The full form of ISD is International Subscriber Dialing. The full form of PCO is Public Call Office.

Dedicated line service

A point-to-point hardware connection between the two-service location by using a physical link.

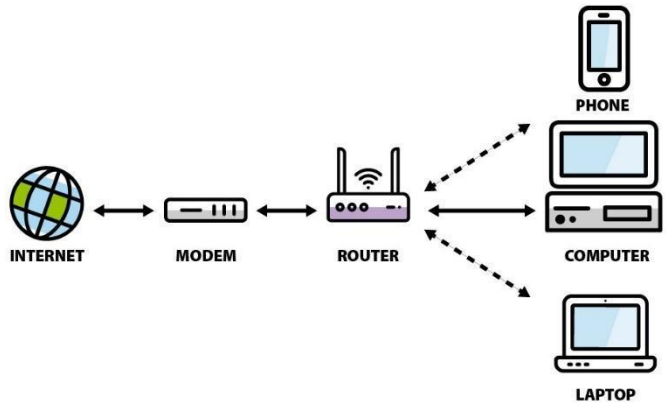
Intranet or Internet any network can be used.

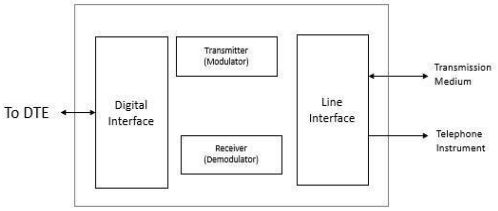
Shared resources: have some dedicated bandwidth (speed) and a defined a certain IP address and VLAN for a user. The IP address may be public or private and used a telecommunication network.

Data Modems

A modulator-demodulator or modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio. A modem transmits data by modulating one or more carrier wave signals to encode digital information, while the receiver demodulates the signal to recreate the original digital information. The goal is to produce a signal that can be transmitted easily and decoded reliably. Modems can be used with almost any means of transmitting analog signals, from light-emitting diodes to radio.

Short for modulator/demodulator, a modem is a hardware device that allows a computer to send and receive information over telephone lines. When sending a signal, the device converts ("modulates") digital data to an analog audio signal, and transmits it over a telephone line. Similarly, when an analog signal is received, the modem converts it back ("demodulates" it) to a digital signal.





Types of modems

Categorization is usually based on the following basic modem features:

1. Directional capacity: half duplex modem and full duplex modem.
2. Connection to the line: 2-wire modem and 4-wire modem.
3. Transmission mode: asynchronous modem and synchronous modem.

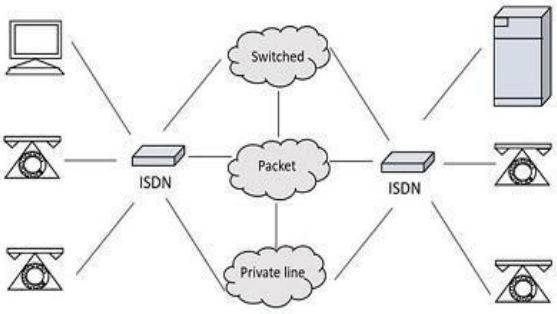
ISDN

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the digitalized circuits of the public switched telephone network. By the time the standard was released, newer networking systems with much greater speeds were available, and ISDN saw relatively little uptake in the wider market. ISDN has largely been replaced with digital subscriber line (DSL) systems of much higher performance. DSL is replaced by FTTH technology.

SDN supports a variety of services. A few of them are listed below −

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Block diagram of ISDN



The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

Basic Rate Interface
The entry level interface to ISDN is the Basic Rate Interface (BRI), a 128 kbit/s service delivered over a pair of standard telephone copper wires. The 144 kbit/s overall payload rate is divided into two 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel or data channel). This is sometimes referred to as 2B+D.
2*64+D=144 kbit/s

Primary Rate Interface

The other ISDN access available is the Primary Rate Interface (PRI), which is carried over T-carrier (T1) with 24 time slots (channels) in North America, and over E-carrier (E1) with 32 channels in most other countries. Each channel provides transmission at a 64 kbit/s data rate.

With the E1 carrier, the available channels are divided into 30 bearer (*B*) channels, one data (*D*) channel, and one timing and alarm channel. This scheme is often referred to as 30B+2D and speed of 2.048 Mbits/s.

In North America, PRI service is delivered via T1 carriers with only one data channel, often referred to as 23B+D, and a total data rate of 1.544 Mbit/s.

Advantages of ISDN

ISDN is a telephone network–based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as –

- As the services are digital, there is less chance for errors.
- The connection is faster.
- The bandwidth is higher.
- Voice, data and video – all of these can be sent over a single ISDN line.

Disadvantages of ISDN

The disadvantage of ISDN is that it requires specialized digital services and is costlier.

However, the advent of ISDN has brought great advancement in communications. Multiple transmissions with greater speed are being achieved with higher levels of accuracy.

Ethernet

Ethernet is a family of wired computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3.

Different types of Ethernets according to speed

10BASE speed of 10Mbps

100BASE speed of 100Mbps

1000BASE speed of 1Gbps

10GBASE speed of 10Gbps

Most popular packet switched LAN technology.

Maximum length up to 2500m (500m segments with 4 repeaters)

Bus and star topology are used to connect hosts.

Host attach to network via ethernet transceiver or hub or switch.

Hubs are used to facilitate shared connection.

All the hosts on an ethernet are competing for access to the medium.

Problem: Distributed algorithm that provides fair access.

Ethernet uses mac addresses that are 48 bits in length and expressed as twelve hexadecimal digits.

On a network, when one device sends data it can open a communication pathway to the other device by using the destination MAC addresses.

FF: FF: FF: FF: FF: FF (Broadcast)

Ethernet standard defines both the layer 2 protocols and the layer 1 technologies.

Data Communications Protocol

In telecommunication, a communication protocol is a system of digital rules for data exchange within or between computers.

Communicating system use well defined formats for exchanging messages. Some network protocols are:

A. Open System Interconnections (OSI)
B. Transmission control protocol / Internet Protocol (TCP/IP)

Basic requirements of protocols

1. Data formats for data exchange
2. Address formats for data exchange
3. Address mapping
4. Routing
5. Detection of transmission errors
6. Acknowledgement
7. Loss of information timeout and retries
8. Detection of information flow
9. Sequence control
10. Flow control

Packet Format

Most network packets are split into three parts:

1. Header
   Contains instructions about the data carried by the packet
   Length of packet
   Synchronization
   Packet number
   Protocol
   Originating address and destination address
2. Payload
   Body or data of a packet
   If a packet is fixed length, then the payload may be padded with blank information to make it the right size.
3. Trailer
   Sometimes called a footer, typically contains a couple of bits that tell the receiving device that it has reached the end of the packet.
   It may also have some types of error checking.

Packet Transport Network

PTN is an integrated transport network technology featuring both packet and transmission. It becomes a mainstream solution for IP based mobile backhaul networks in 3G and LTE system due to several key technologies.

Packet Switching and Private Switching

Circuit switching is a communication method where a dedicated communication path, or circuit, is established between two devices before data transmission begins. The circuit remains dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress. Circuit switching is commonly used in voice communication and some types of data communication.

Advantages of Circuit Switching:

- Guaranteed bandwidth: Circuit switching provides a dedicated path for communication, ensuring that bandwidth is guaranteed for the duration of the call.
- Low latency: Circuit switching provides low latency because the path is predetermined, and there is no need to establish a connection for each packet.
- Predictable performance: Circuit switching provides predictable performance because the bandwidth is reserved, and there is no competition for resources.
- Suitable for real-time communication: Circuit switching is suitable for real-time communication, such as voice and video, because it provides low latency and predictable performance.

Disadvantages of Circuit Switching:

- Inefficient use of bandwidth: Circuit switching is inefficient because the bandwidth is reserved for the entire duration of the call, even when no data is being transmitted.
- Limited scalability: Circuit switching is limited in its scalability because the number of circuits that can be established is finite, which can limit the number of simultaneous calls that can be made.
- High cost: Circuit switching is expensive because it requires dedicated resources, such as hardware and bandwidth, for the duration of the call.

What is Packet Switching?

Packet switching is a communication method where data is divided into smaller units called packets and transmitted over the network. Each packet contains the source and destination addresses, as well as other information needed for routing. The packets may take different paths to reach their destination, and they may be transmitted out of order or delayed due to network congestion.

Advantages of Packet Switching:

- Efficient use of bandwidth: Packet switching is efficient because bandwidth is shared among multiple users, and resources are allocated only when data needs to be transmitted.
- Flexible: Packet switching is flexible and can handle a wide range of data rates and packet sizes.
- Scalable: Packet switching is highly scalable and can handle large amounts of traffic on a network.
- Lower cost: Packet switching is less expensive than circuit switching because resources are shared among multiple users.

Disadvantages of Packet Switching:

- Higher latency: Packet switching has higher latency than circuit switching because packets must be routed through multiple nodes, which can cause delay.
- Limited QoS: Packet switching provides limited QoS guarantees, meaning that differentypes of traffic may be treated equally.
- Packet loss: Packet switching can result in packet loss due to congestion on the network or errors in transmission.
- Unsuitable for real-time communication: Packet switching is not suitable for real-time communication, such as voice and video, because of the potential for latency and packet loss.

Similarities:

- Both methods involve the transmission of data over a network.
- Both methods use a physical layer of the OSI model for transmission of data.
- Both methods can be used to transmit voice, video, and data.
- Both methods can be used in the same network infrastructure.
- Both methods can be used for both wired and wireless networks.

Circuit Switching	Packet Switching
In-circuit switching has there are 3 phases: i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In-circuit switching, each data unit knows the entire path address which is provided by the source.	In Packet switching, each data unit just knows the final destination address intermediate path is decided by the routers.
In-Circuit switching, data is processed at the source system only	In Packet switching, data is processed at all intermediate nodes including the source system.
The delay between data units in circuit switching is uniform.	The delay between data units in packet switching is not uniform.
Resource reservation is the feature of circuit switching because the path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.

Circuit Switching	Packet Switching
Wastage of resources is more in Circuit Switching	Less wastage of resources as compared to Circuit Switching
It is not a store and forward technique.	It is a store and forward technique.
Transmission of the data is done by the source.	Transmission of the data is done not only by the source but also by the intermediate routers.
Congestion can occur during the connection establishment phase because there might be a case where a request is being made for a channel but the channel is already occupied.	Congestion can occur during the data transfer phase, a large number of packets comes in no time.
Circuit switching is not convenient for handling bilateral traffic.	Packet switching is suitable for handling bilateral traffic.
In-Circuit switching, the charge depends on time and distance, not on traffic in the network.	In Packet switching, the charge is based on the number of bytes and connection time.
Recording of packets is never possible in circuit switching.	Recording of packets is possible in packet switching.
In-Circuit Switching there is a physical path between the source and the destination	In Packet Switching there is no physical path between the source and the destination
Circuit Switching does not support store and forward transmission	Packet Switching supports store and forward transmission
Call setup is required in circuit switching.	No call setup is required in packet switching.
In-circuit switching each packet follows the same route.	In packet switching packets can follow any route.
The circuit switching network is implemented at the physical layer.	Packet switching is implemented at the data link layer and network layer

Prepared by: Er. Bigyan Bhattarai

Circuit Switching	Packet Switching
Circuit switching requires simple protocols for delivery.	Packet switching requires complex protocols for delivery.

Error

Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with a certain level of accuracy. But to understand how errors are controlled, it is essential to know what types of errors may occur.

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits lead to spurious data being received by the receiver and are called errors.

Error control mechanism may involve two possible ways and error detection error correction.

Error detection techniques are responsible for checking whether any error has occurred or not in the frame that has been transmitted via network. It does not take into account the number of error bits and the type of error.

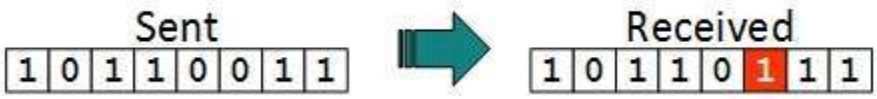
For error detection, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

Types of Errors

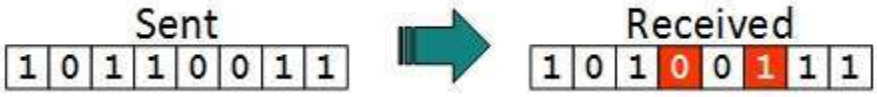
There may be three types of errors:

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 Detection Techniques

1. Parity Generator and Parity Check

Majority of modern communication is Digital in nature i.e.; it is a combination of 1's and 0's. The digital data is transmitted either through wires (in case of wired communication) or wireless. Even in an advanced mode of communication, there will be errors while transmitting data (due to noise).

The simplest of errors is corruption of a bit i.e., a 1 may be transmitted as a 0 or vice-versa. To confirm whether the received data is the intended data or not, we should be able to detect errors at the receiver.

In this tutorial, we will learn about Parity Bit, Even Parity, Odd Parity, Parity Generator and Parity Checker with a practical example and practical circuit.

What is Parity Bit?

The parity generating technique is one of the most widely used error detection techniques for the data transmission. In digital systems, when binary data is transmitted and processed, data may be subjected to noise so that such noise can alter 0s (of data bits) to 1s and 1s to 0s.

Hence, a Parity Bit is added to the word containing data in order to make number of 1s either even or odd. The message containing the data bits along with parity bit is transmitted from transmitter to the receiver.

At the receiving end, the number of 1s in the message is counted and if it doesn't match with the transmitted one, it means there is an error in the data. Thus, the Parity Bit it is used to detect errors, during the transmission of binary data.

Parity Generator and Checker

A Parity Generator is a combinational logic circuit that generates the parity bit in the transmitter. On the other hand, a circuit that checks the parity in the receiver is called Parity Checker. A combined circuit or device of parity generators and parity checkers are commonly used in digital systems to detect the single bit errors in the transmitted data.

Even Parity and Odd Parity

The sum of the data bits and parity bits can be even or odd. In even parity, the added parity bit will make the total number of 1s an even number, whereas in odd parity, the added parity bit will make the total number of 1s an odd number.

The basic principle involved in the implementation of parity circuits is that sum of odd number of 1s is always 1 and the sum of even number of 1s is always 0. Such error detecting and correction can be implemented by using Ex-OR gates (since Ex-OR gate produce zero output when there are even number of inputs).

Parity Generator

It is a combinational circuit that accepts an n-1 bit data and generates the additional bit that is to be transmitted with the bit stream. This additional or extra bit is called a Parity Bit.

In an even parity bit scheme, the parity bit is '0' if there are even numbers of 1s in the data stream and the parity bit is '1' if there are odd numbers of 1s in the data stream.

In the odd parity bit scheme, the parity bit is '1' if there are even numbers of 1s in the data stream and the parity bit is '0' if there are odd numbers of 1s in the data stream. Let us discuss both even and odd parity generators.

Even Parity Generator

Let us assume that a 3-bit message is to be transmitted with an even parity bit. Let the three inputs A, B and C are applied to the circuit and output bit is the parity bit P. The total number of 1s must be even, to generate the even parity bit P.

The figure below shows the truth table of even parity generator in which 1 is placed as parity bit in order to make all 1s as even when the number of 1s in the truth table is odd.

3-bit message			Even parity bit generator (P)
A	B	C	Y
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Odd Parity Generator

Let us consider that the 3-bit data is to be transmitted with an odd parity bit. The three inputs are A, B and C and P is the output parity bit. The total number of bits must be odd in order to generate the odd parity bit.

In the given truth table below, 1 is placed in the parity bit in order to make the total number of bits odd when the total number of 1s in the truth table is even.

3-bit message			Odd parity bit generator (P)
A	B	C	Y
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Parity Check

It is a logic circuit that checks for possible errors in the transmission. This circuit can be an even parity checker or odd parity checker depending on the type of parity generated at the transmission end. When this circuit is used as even parity checker, the number of input bits must always be even.

Even Parity Checker

Consider that three input messages along with even parity bit is generated at the transmitting end. These 4 bits are applied as input to the parity checker circuit, which checks the possibility of error on the data. Since the data is transmitted with even parity, four bits received at circuit must have an even number of 1s.

If any error occurs, the received message consists of odd number of 1s. The output of the parity checker is denoted by PEC (Parity Error Check).

The below table shows the truth table for the Even Parity Checker in which PEC = 1 if the error occurs, i.e., the four bits received have odd number of 1s and PEC = 0 if no error occurs, i.e., if the 4-bit message has even number of 1s.

4-bit received message				Parity error check C_p
A	B	C	P	
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	0
0	1	0	0	1
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

Odd Parity Checker

Consider that a three-bit message along with odd parity bit is transmitted at the transmitting end. Odd parity checker circuit receives these 4 bits and checks whether any error is present in the data.

If the total number of 1s in the data is odd, then it indicates no error, whereas if the total number of 1s is even then it indicates the error since the data is transmitted with odd parity at transmitting end.

The below figure shows the truth table for odd parity generator where PEC =1 if the 4-bit message received consists of even number of 1s (hence the error occurred) and PEC= 0 if the message contains odd number of 1s (that means no error).

4-bit received message				Parity error check C_p
A	B	C	P	
0	0	0	0	1
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	0
1	1	0	0	1
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

2. Checksums

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data. When the receiver gets this data, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error.

Error Detection by Checksums

For error detection by checksums, data is divided into fixed sized frames or segments.

Sender's End – The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.

Receiver's End – The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

If the result is zero, the received frames are accepted; otherwise, they are discarded.

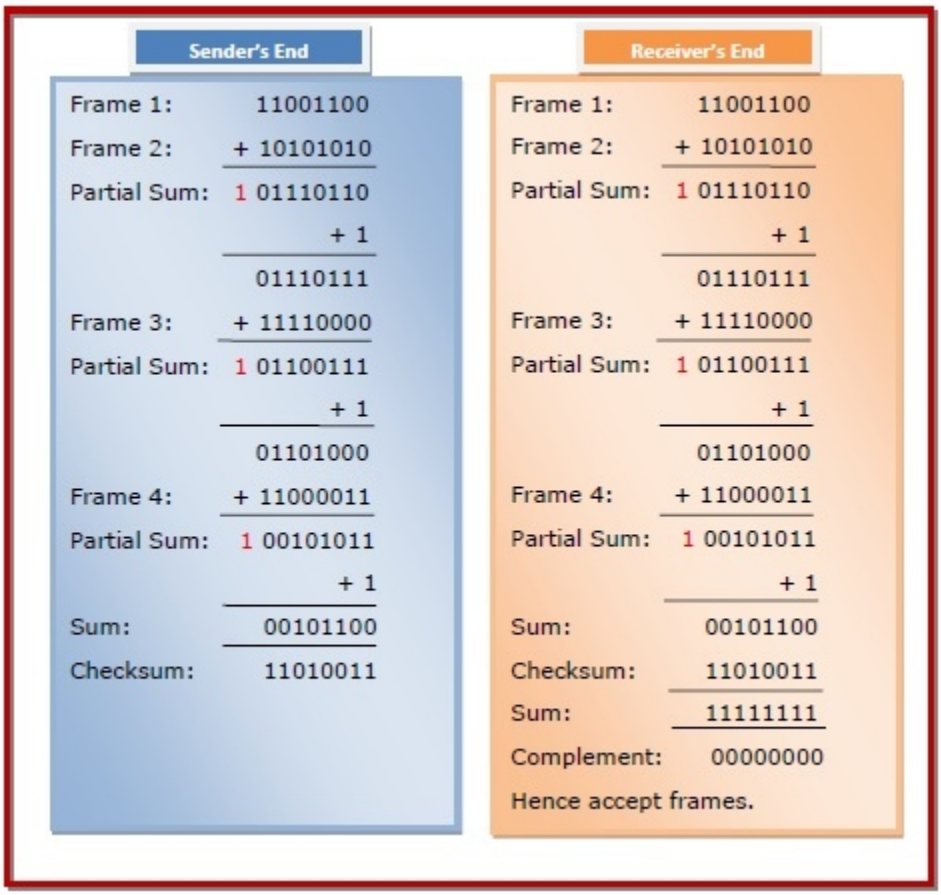
Example

Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.

The sender adds the bits using 1s complement arithmetic. While adding two numbers using 1s complement arithmetic, if there is a carry over, it is added to the sum.

After adding all the 4 frames, the sender complement the sum to get the checksum, 11010011, and sends it along with the data frames.

The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.



3. Cyclic Redundancy Check (CRC)

CRC or Cyclic Redundancy Check is a method of detecting accidental changes/errors in the communication channel.

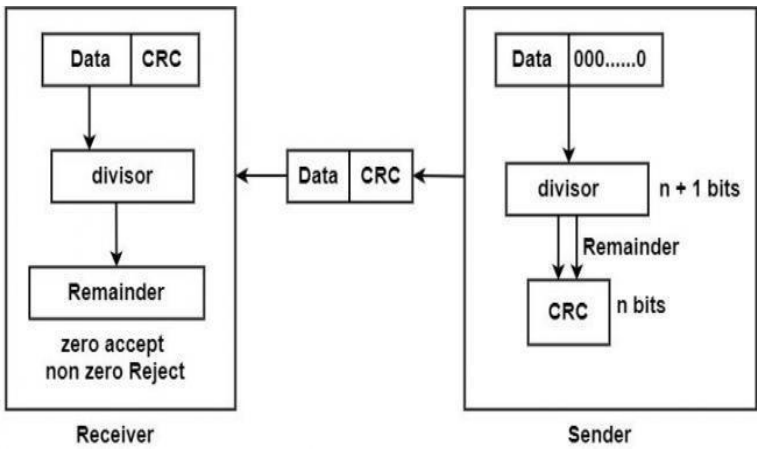
The Cyclic Redundancy Checks (CRC) is the most powerful method for Error-Detection and Correction. It is given as a kbit message and the transmitter creates an (n – k) bit sequence called frame check sequence. The out coming frame, including n bits, is precisely divisible by some fixed number. Modulo 2 Arithmetic is used in this binary addition with no carries, just like the XOR operation.

Redundancy means duplicity. The redundancy bits used by CRC are changed by splitting the data unit by a fixed divisor. The remainder is CRC.

Qualities of CRC

- It should have accurately been one less bit than the divisor.
- Joining it to the end of the data unit should create the resulting bit sequence precisely divisible by the divisor.

.



CRC uses Generator Polynomial which is available on both sender and receiver side
An example generator polynomial is of the form like $x^3 + x + 1$. This generator polynomial represents key 1011. Another example is $x^2 + 1$ that represents key 101.

Sender Side (Generation of Encoded Data from Data and Generator Polynomial (or Key)):

1. The binary data is first augmented by adding k-1 zeros in the end of the data
2. Use *modulo-2 binary division* to divide binary data by the key and store remainder of division.
3. Append the remainder at the end of the data to form the encoded data and send the same

Receiver Side (Check if there are errors introduced in transmission)
Perform modulo-2 division again and if the remainder is 0, then there are no errors.

In this article we will focus only on finding the remainder i.e., check word and the code word.

Modulo 2 Division:
The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. Just that instead of subtraction, we use XOR here.

- In each step, a copy of the divisor (or data) is XORed with the k bits of the dividend (or key).
- The result of the XOR operation (remainder) is (n-1) bits, which is used for the next step after 1 extra bit is pulled down to make it n bits long.
- When there are no bits left to pull down, we have a result. The (n-1)-bit remainder which is appended at the sender side.

n : Number of bits in data to be sent

from the sender side.

k : Number of bits in the key obtained

from generator polynomial

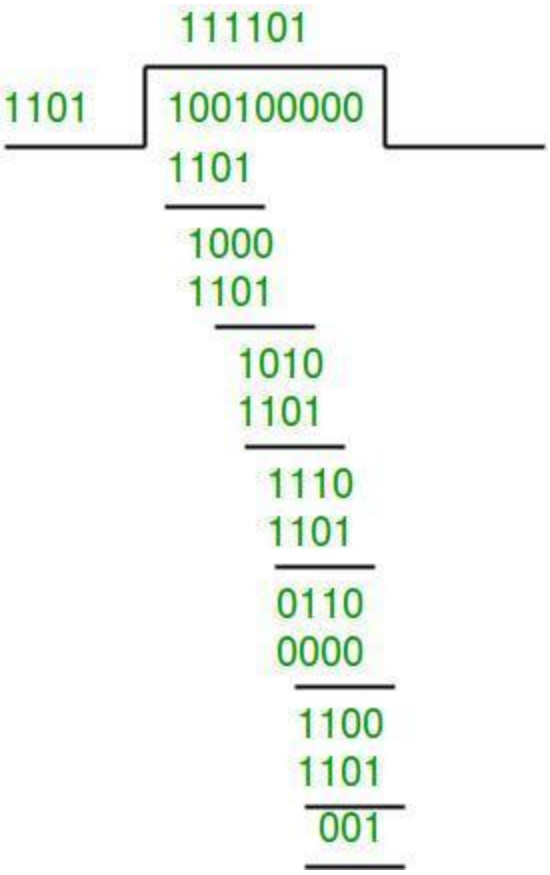
- Illustration:

Example 1 (No error in transmission):

- Data word to be sent = 100100
- Predetermined P = 1101 [Or generator polynomial $x^3 + x^2 + 1$]

Message D or K = 6, Predetermined P = 4 and R = 4-1 = 3 and n = K + R = 9

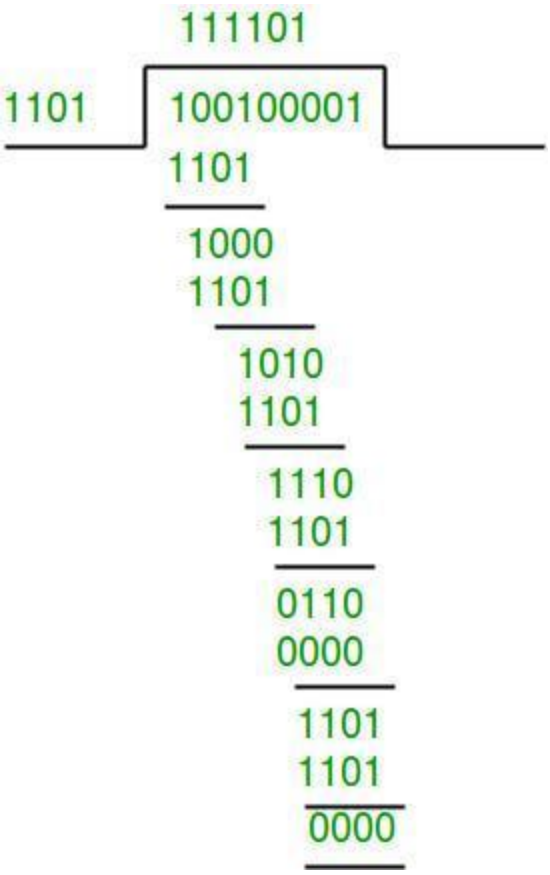
Sender Side:



- Therefore, the remainder is 001 and hence the encoded
- data sent is 100100001.

Receiver Side:

- Code word received at the receiver side 100100001

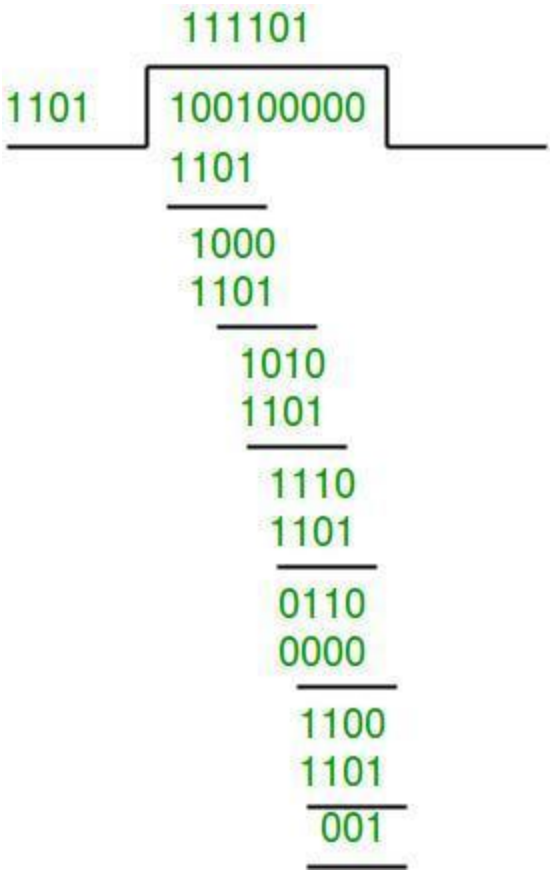


- Therefore, the remainder is all zeros. Hence, the
- data received has no error.

Example 2: (Error in transmission)
Data word to be sent - 100100

Key - 1101

Sender Side:

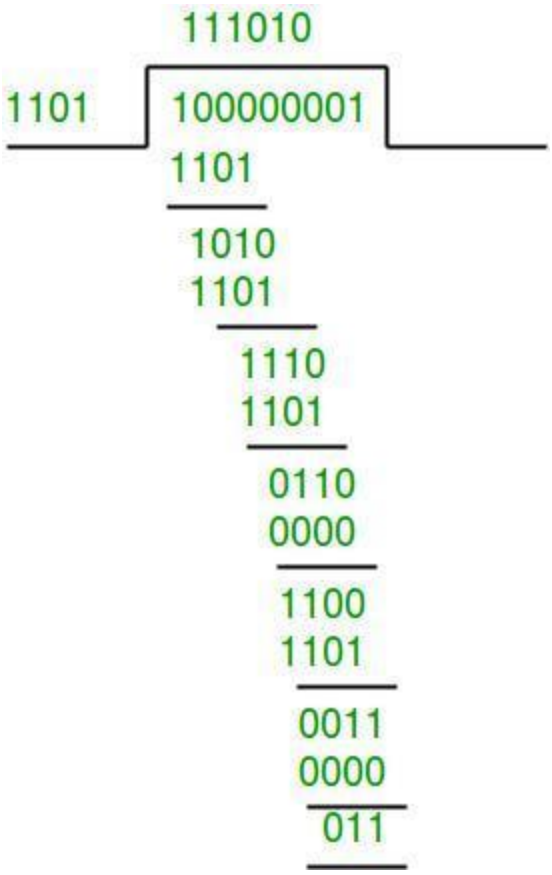


Therefore, the remainder is 001 and hence the code word sent is 100100001.

Receiver Side

Let there be an error in transmission media

Code word received at the receiver side - 100000001



Since the remainder is not all zeroes, the error is detected at the receiver side.

Error Correction Techniques

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits lead to spurious data being received by the receiver and are called errors.

Error-correcting codes (ECC) are a sequence of numbers generated by specific algorithms for detecting and removing errors in data that has been transmitted over noisy channels. Error correcting codes ascertain the exact number of bits that has been corrupted and the location of the corrupted bits, within the limitations in the algorithm.

ECCs can be broadly categorized into two types -

1. Block codes - The message is divided into fixed-sized blocks of bits, to which redundant bits are added for error detection or correction.
2. Convolutional codes - The message consists of data streams of arbitrary length and parity symbols generated by the sliding application of a Boolean function to the data stream.

Hamming Codes

Hamming code is an error correction system that can detect and correct errors when data is stored or transmitted. It requires adding additional parity bits with the data. It is commonly used in error correction code (ECC). It's named after its inventor, Richard W. Hamming.

Whenever data is transmitted or stored, it's possible that the data may become corrupted. This can take the form of bit flips, where a binary 1 becomes a 0 or vice versa. Error correcting codes seek to find when an error is introduced into some data. This is done by adding parity bits, or redundant information, to the data.

If enough parity data is added, it enables forward error correction (FEC), where errors can be automatically fixed when read back. FEC can increase the data

transmission rate for noisy channels by reducing the amount of necessary retransmits.

Hamming code uses a block parity mechanism. The data is divided into blocks, and parity is added to the block. Hamming code can correct single-bit errors and detect the presence of two-bit errors in a data block.

The amount of parity data added to Hamming code is given by the formula $2^{*}_{p} \geq d + p + 1$, where *p* is the number of parity bits and *d* is the number of data bits. For example, if you wanted to transmit 7 data bits, the formula would be $2^{*}_{4} \geq 7 + 4 + 1$, so 4 parity bits are required.

Hamming codes are linear block codes. The family (n, k) Hamming codes for q≥3 is defined by,

Block diagram : n= 2^q - 1

Number of message bit : k= 2^q - 1 - q

Number of parity bits : (n-k) = q

where, q ≥ 3 i.e. maximum number of parity bit is 3.

minimum distance, dmin =3

code rate or code efficiency = k/n

code word length, n = 2^q - 1

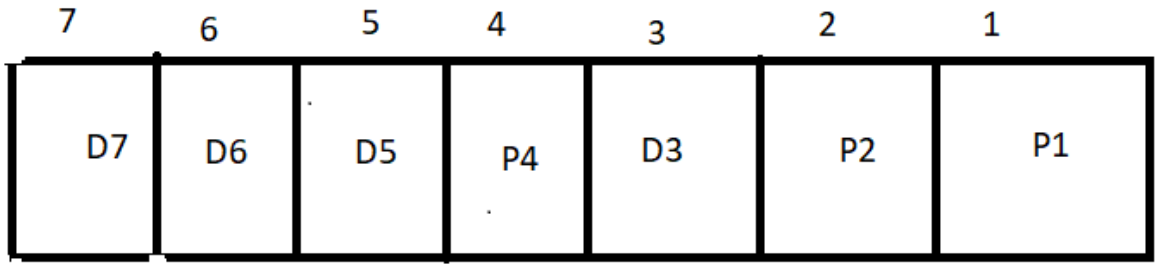
k = 2^q - 1 - q	q= (n - k)

message bits parity bits

Examples of Hamming Codes

If the received hamming code is 1110101 with even parity then detect and correct error.

D7	D6	D5	P4	D3	P2	P1



For P1 Check 1 bit and skip one bit

P1 = 2^0 = 1

For P2 Check 2 bit and skip two bit

P2 = 2^1 = 2

For P1 Check 4 bit and skip four bit

P4 = 2^2 = 4

P1=D3⊕D5⊕D7

1=1⊕1⊕1 This is true so P1=0

P2=D3⊕D6⊕D7

0=1⊕1⊕1 This is false so P2=1

P4=D7⊕D6⊕D5

0=1⊕1⊕1 This is false so P4=1

P4P2P1 = 110 (which is 6th bit error)

Error syndrome (E) =

0	1	0	0	0	0	0

Received data (D) =

1	1	1	0	1	0	1

Corrected Data = R ⊕ E

1	0	1	0	1	0	1

Hence, the corrected data becomes: 1010101

The main advantage of using a hamming code is cost-effective if a data stream contains single-bit errors. It can provide error detection and also indicates the bit which contains an error for correction. Hamming codes are very easy and best to use in computer memory and single-bit error correction and detection.