MID-I IMP QUESTIONS

1. Define computer networks. Explain the different types of network Examples.

2. OSI Reference Model

3. TCP/IP Reference Model, Differences between OSI Reference Model and TCP/IP Reference Model

4. Write brief notes on the following network devices

- **Repeaters**
- **Transceivers**
- **Bridges**
- **Hubs**
- **Switches**
- **Routers**
- **Modems**
- **Firewalls**
- **WAP**
- **NIC**
- **Gateways**

5. Framing

6. Error Detection Algorithms

7. Error Correction Algorithms

8. Sliding Window Protocols

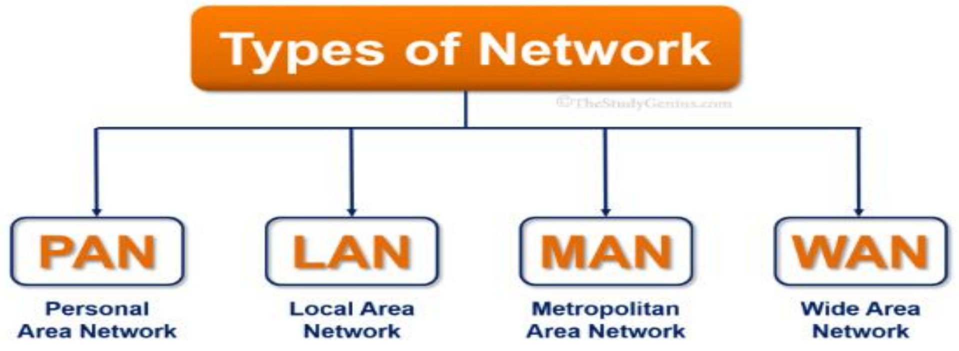
9. MAC Addressing

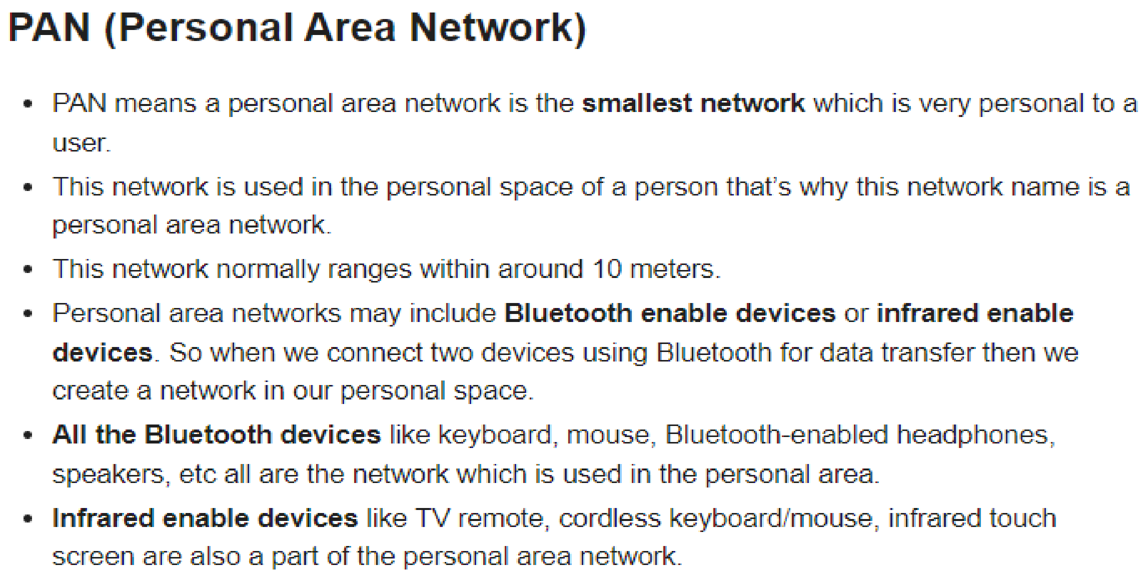
10. Routing Protocols

1. Define computer networks. Explain the different types of network Examples.

Def:- A computer network is a set of devices connected through links. A **node** can be computer, printer, or any other device capable of sending or receiving the data. The **links** connecting the nodes are known as communication channels.

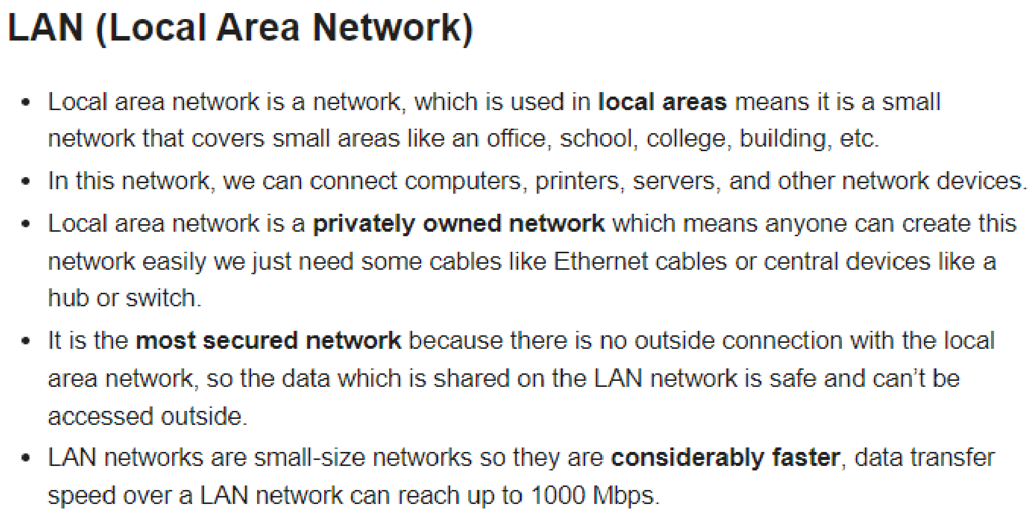
Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset.





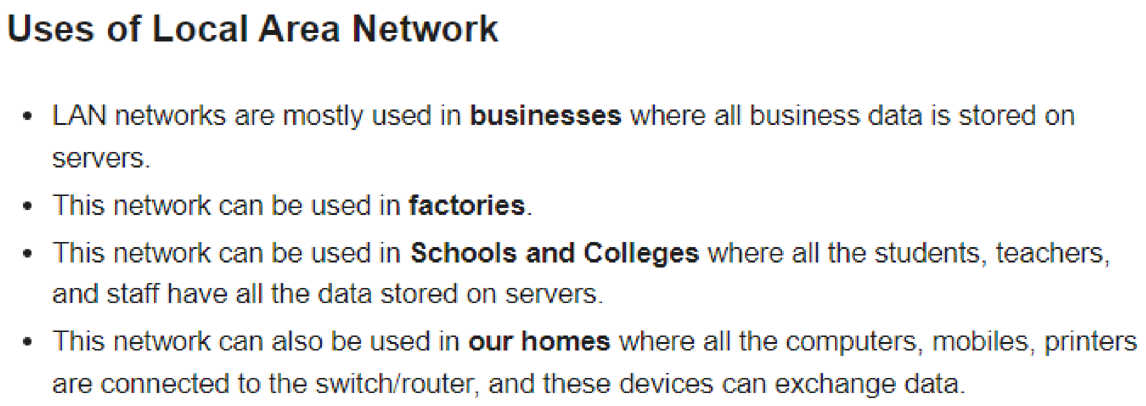
PAN (Personal Area Network)

- PAN means a personal area network is the **smallest network** which is very personal to a user.
- This network is used in the personal space of a person that's why this network name is a personal area network.
- This network normally ranges within around 10 meters.
- Personal area networks may include **Bluetooth enable devices** or **infrared enable devices**. So when we connect two devices using Bluetooth for data transfer then we create a network in our personal space.
- **All the Bluetooth devices** like keyboard, mouse, Bluetooth-enabled headphones, speakers, etc all are the network which is used in the personal area.
- **Infrared enable devices** like TV remote, cordless keyboard/mouse, infrared touch screen are also a part of the personal area network.



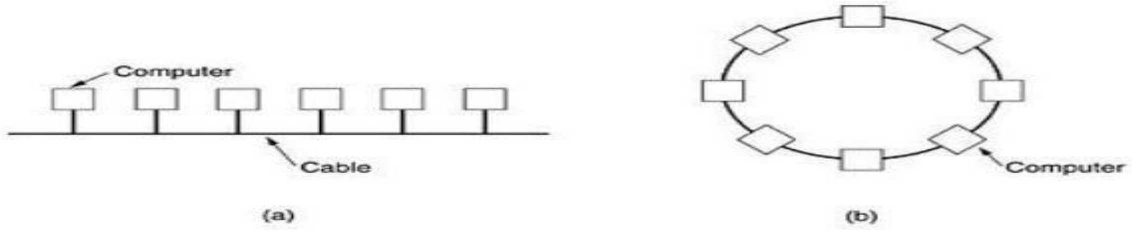
LAN (Local Area Network)

- Local area network is a network, which is used in **local areas** means it is a small network that covers small areas like an office, school, college, building, etc.
- In this network, we can connect computers, printers, servers, and other network devices.
- Local area network is a **privately owned network** which means anyone can create this network easily we just need some cables like Ethernet cables or central devices like a hub or switch.
- It is the **most secured network** because there is no outside connection with the local area network, so the data which is shared on the LAN network is safe and can't be accessed outside.
- LAN networks are small-size networks so they are **considerably faster**, data transfer speed over a LAN network can reach up to 1000 Mbps.

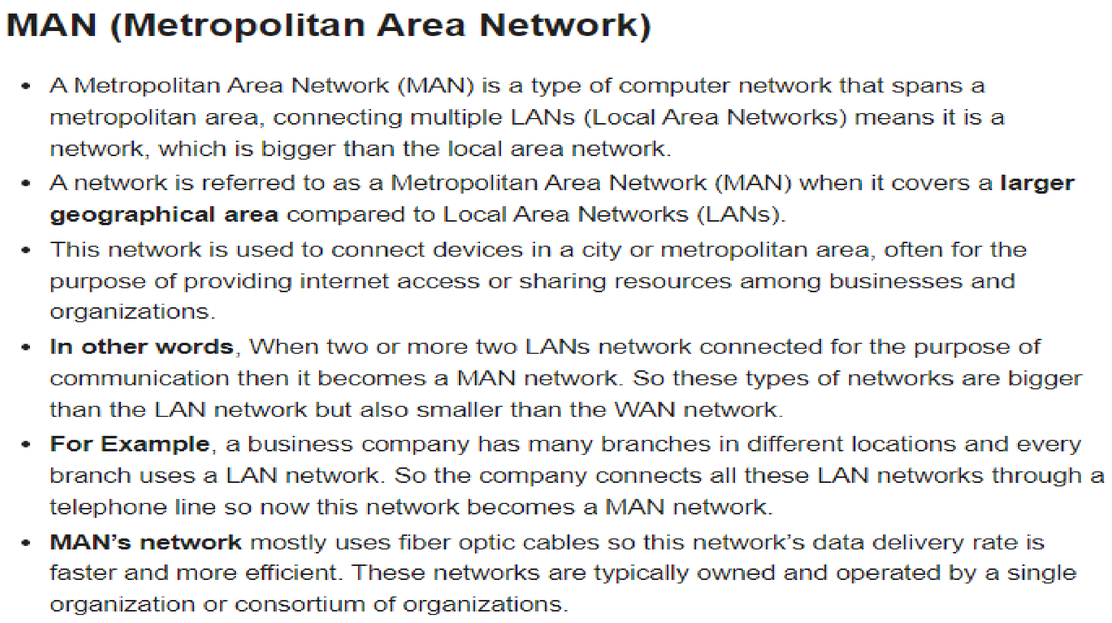


Uses of Local Area Network

- LAN networks are mostly used in **businesses** where all business data is stored on servers.
- This network can be used in **factories**.
- This network can be used in **Schools and Colleges** where all the students, teachers, and staff have all the data stored on servers.
- This network can also be used in **our homes** where all the computers, mobiles, printers are connected to the switch/router, and these devices can exchange data.

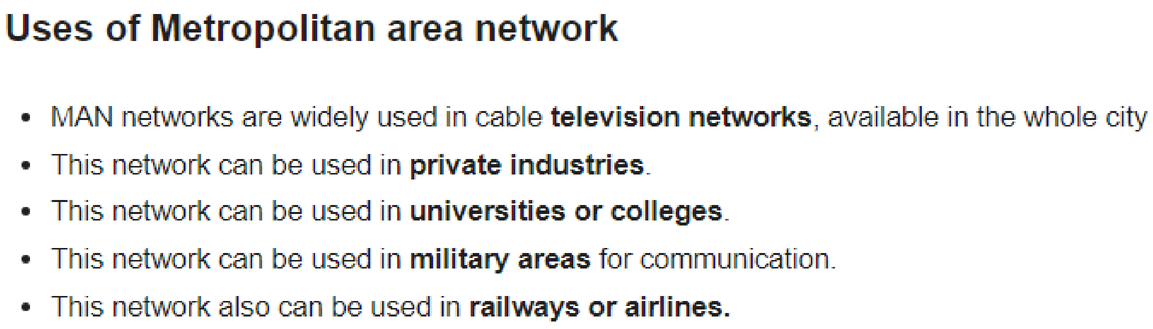


Two broadcast networks . (a) Bus. (b) Ring



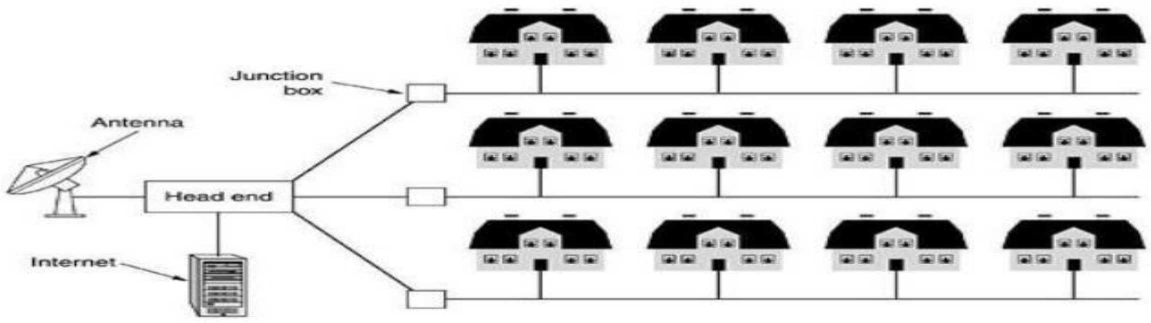
MAN (Metropolitan Area Network)

- A Metropolitan Area Network (MAN) is a type of computer network that spans a metropolitan area, connecting multiple LANs (Local Area Networks) means it is a network, which is bigger than the local area network.
- A network is referred to as a Metropolitan Area Network (MAN) when it covers a **larger geographical area** compared to Local Area Networks (LANs).
- This network is used to connect devices in a city or metropolitan area, often for the purpose of providing internet access or sharing resources among businesses and organizations.
- **In other words**, When two or more two LANs network connected for the purpose of communication then it becomes a MAN network. So these types of networks are bigger than the LAN network but also smaller than the WAN network.
- **For Example**, a business company has many branches in different locations and every branch uses a LAN network. So the company connects all these LAN networks through a telephone line so now this network becomes a MAN network.
- **MAN's network** mostly uses fiber optic cables so this network's data delivery rate is faster and more efficient. These networks are typically owned and operated by a single organization or consortium of organizations.



Uses of Metropolitan area network

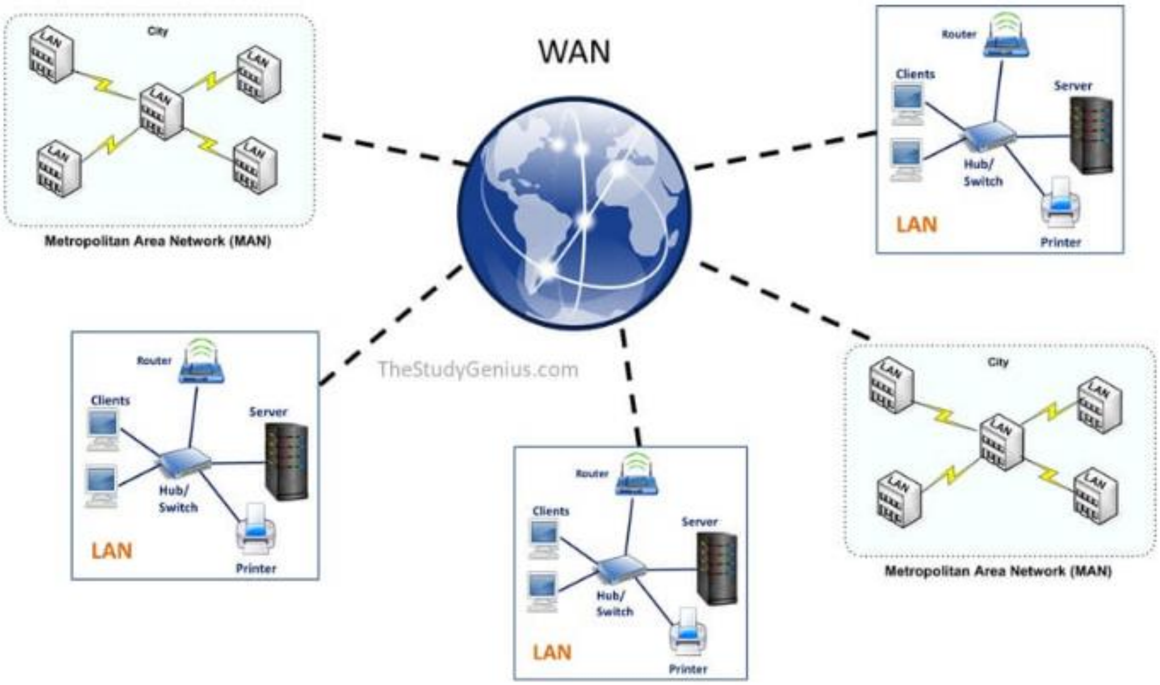
- MAN networks are widely used in cable **television networks**, available in the whole city
- This network can be used in **private industries**.
- This network can be used in **universities or colleges**.
- This network can be used in **military areas** for communication.
- This network also can be used in **railways or airlines.**



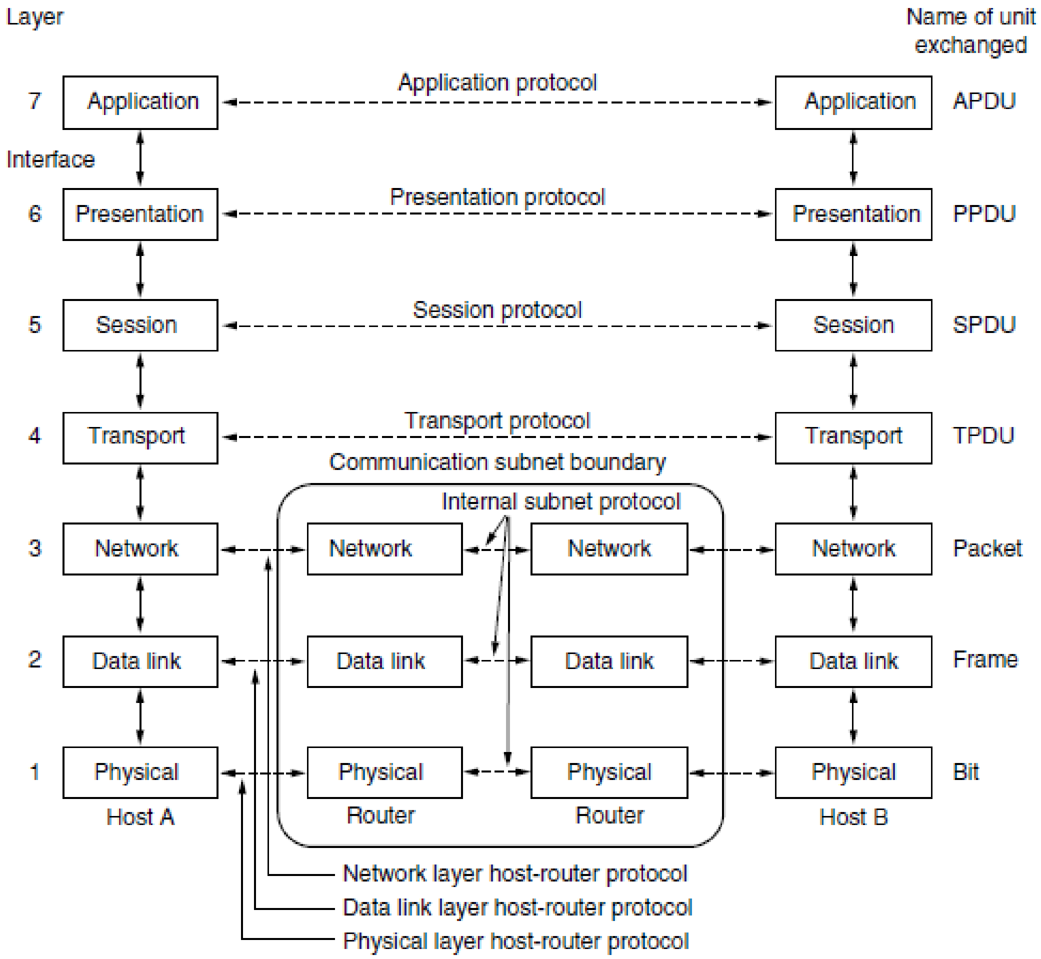
Metropolitan area network based on cable TV

WAN (Wide Area Network)

- WAN means a wide area network is a wide network that means this network is used in **large geographical areas** like in the whole country or continent and uses common carriers like – satellite systems, telephone lines, etc.
- In other words, when many LANs and MAN's networks are connected to each other for the purpose of communication then it's become WAN network because now the area of the network is too wide so it is called a wide area network.
- This network generally covers larger distance areas (like states, countries, continents).
- Actually, the largest WAN network in the world, where thousands of LAN and MAN networks are connected to each other.



2. OSI Reference Model



PHYSICAL LAYER

- The **physical layer** is concerned with transmitting raw bits over a communication channel.
- The design issues have to do with making sure that when one side sends a 1 bit it is received by the other side as a 1 bit, not as a 0 bit.
- Typical questions here are

what electrical signals should be used to represent a 1 and a 0,

how many nanoseconds a bit lasts,

whether transmission may proceed simultaneously in both directions,

how the initial connection is established, how it is torn down when both sides are finished,

how many pins the network connector has, and

what each pin is used for.

- These design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium, which lies below the physical layer.

DATALINK LAYER

- The main task of the data link layer is to transform a **raw transmission facility** into a line that appears free of undetected transmission errors. It does so by masking the real errors so the network layer does not see them.
- It accomplishes this task by having the sender break up the input data into **data frames** (typically a few hundred or a few thousand bytes) and transmit the frames sequentially.
- If the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement frame**.
- Another issue that arises in the data link layer is how to keep a fast transmitter from drowning a slow receiver in data. Some **traffic regulation mechanism** may be needed to let the transmitter know when the receiver can accept more data.
- Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sublayer of the data link layer, the **medium access control** sublayer, deals with this problem.
- **NETWORK LAYER**
- The network layer controls the **operation of the subnet**.

- A key design issue is determining how packets are **routed from source to destination**.
- Routes can be determined by
- Static tables.
- Highly dynamic
- If too many packets are present in the subnet at the same time, they will get in one another's way, forming **bottlenecks**.
- Handling **congestion** is also a responsibility of the network layer, in conjunction with higher layers that adapt the load they place on the network.
- More generally, the **quality of service** provided (delay, transit time, jitter, etc.) is also a network layer issue.
- The network layer allow **heterogeneous networks** to be interconnected.
- In **broadcast networks**, the routing problem is simple, so the network layer is often thin or even non existent.

TRANSPORT LAYER

- The basic function of the transport layer is to accept data from above it, **split it up into smaller units** if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.
- The transport layer also determines **what type of service to provide** to the session layer, and, ultimately, to the users of the network.
- The most popular type of transport connection is **an error-free point-to-point channel** that delivers messages or bytes in the order in which they were sent.

- However, other possible kinds of transport service exist, such as the transporting of isolated messages with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations.
- The type of service is determined when the connection is established.
- The transport layer is a true end-to-end layer.

SESSION LAYER

- The session layer allows users on different machines to **establish sessions** between them.
- Sessions offer various services, including
  - **Dialog control** (keeping track of whose turn it is to transmit),
  - **Token management** (preventing two parties from attempting the same critical operation simultaneously), and
  - **Synchronization** (checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

PRESENTATION LAYER

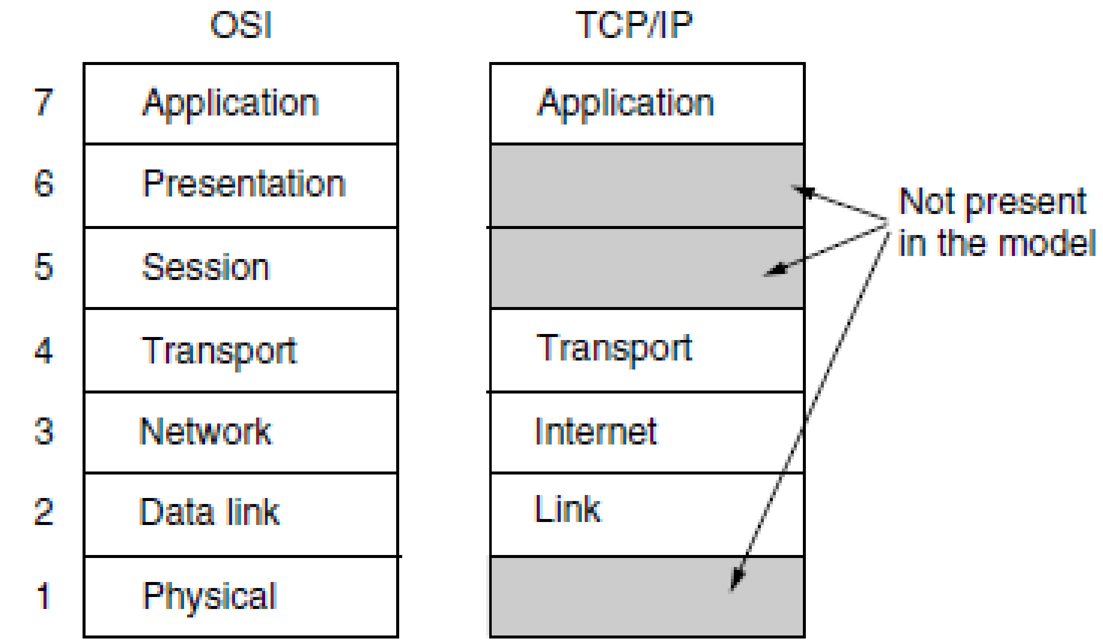
- Presentation layer is concerned with the **syntax and semantics** of the information transmitted.
- In order to make it possible for computers with different internal data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ‘‘on the wire.’’
- The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged.

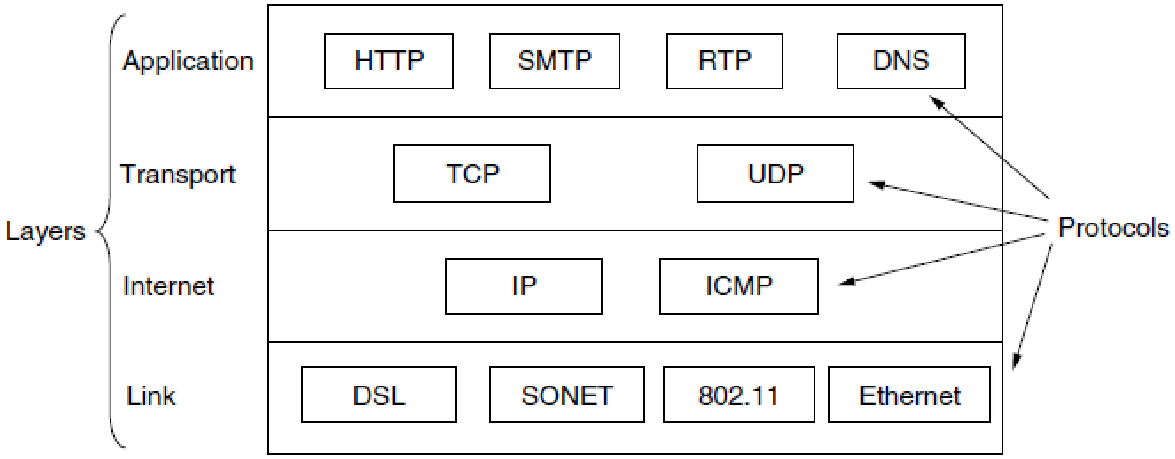
APPLICATION LAYER

- The application layer contains a **variety of protocols** that are commonly needed by users.
- One widely used application protocol is **HTTP** (**HyperText Transfer Protocol**), which is the basis for the World Wide Web.
- When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.
- Other application protocols are used for **file transfer, electronic mail, and network news.**

3. TCP/IP Reference Model, Differences between OSI Reference Model and TCP/IP Reference Model

TCP/IP Reference Model:





LINK LAYER

- The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.

- It is not really a layer at all, but rather an interface between hosts and transmission links.

INTERNET LAYER

- Permit hosts to inject packets into any network and have them travel independently to the destination.
- They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- The internet layer defines an official packet format and protocol called **IP**(**Internet Protocol**), plus a companion protocol called **ICMP (Internet Control Message Protocol**) that helps it function.
- The job of the internet layer is to deliver IP packets where they are supposed to go.
- Packet routing is clearly a major issue here, as is congestion.

TRANSPORT LAYER

- Allow peer entities on the source and destination hosts to carry on a conversation.
- Two end-to-end transport protocols have been defined here.

1.**TCP** (**Transmission Control Protocol**), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.

- It segments the incoming byte stream into discrete messages and passes each one on to the internet layer.

- At the destination, the receiving TCP process reassembles the received messages into the output stream.
- TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

2.**UDP** (**User Datagram Protocol**), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.

APPLICATION LAYER

- It contains all the higher- level protocols.
- The protocols included
  - Virtual terminal (TELNET),
  - File transfer (FTP)
  - Electronic mail (SMTP)
  - Domain Name System (DNS), for mapping host names onto their network addresses,
  - HTTP, the protocol for fetching pages on the World Wide Web,
  - RTP, the protocol for delivering real-time media such as voice or movies.

Comparison of the OSI and TCP/IP Reference Models:

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented users of the transport service. Despite these fundamental similarities, the two models also have many differences Three concepts are central to the OSI model:

1. Services. 2. Interfaces. 3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicit. Each layer performs some services for the layer above it. The service definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.

A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, says nothing about how the layer works inside.

Finally, the peer protocols used in a layer are the layer's own business. It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services). It can also change them at will without affecting software in higher layers.

The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like. For example, the only real services offered by the internet layer are SEND IP PACKET and RECEIVE IP PACKET.

As a consequence, the protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes. Being able to make such changes is one of the main purposes of having layered protocols in the first place. The OSI reference model was devised before the corresponding protocols were invented. This ordering means that the model was not biased toward one particular set of protocols, a fact that made it quite general. The downside of this ordering is that the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.

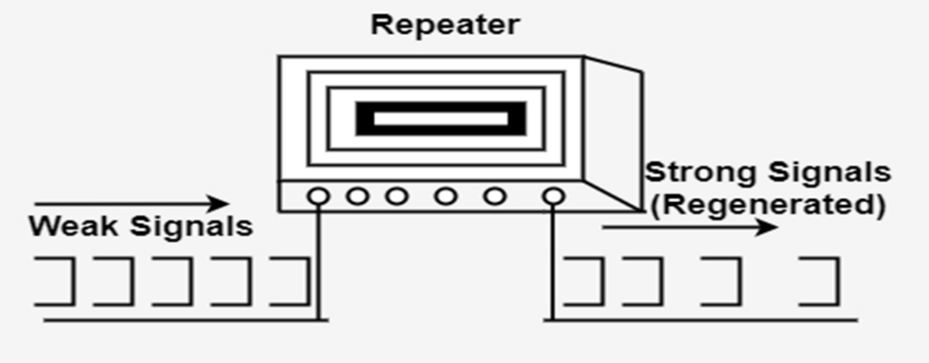
Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer, where it counts (because the transport service is visible to the users). The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer, givingthe users a choice. This choice is especially important for simple request-response protocols.

4. Write brief notes on the following network devices

Repeaters,Transceivers,Bridges,Hubs,Switches

Routers,Modems,Firewalls,WAP,NIC,Gateways.

Repeaters



- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it.
- When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength.
- It is a 2-port device.
- Large office buildings, warehouses, laboratories and campuses are all locations that can benefit from repeaters.

Transceivers

- A transceiver is a combination transmitter/receiver in a single package.
- While the term typically applies to wireless communications devices, it can also be used for transmitter/receiver devices in cable or optical fiber systems.
- The main functionality of this electronic device is to transmit, as well as receive, different signals.
- In local area networks, the transceiver is a part of the network interface card.
- It can both transmit signals over the network wire and detect electrical signals flowing through the wire.

Bridges

- **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

Transparent Bridges:

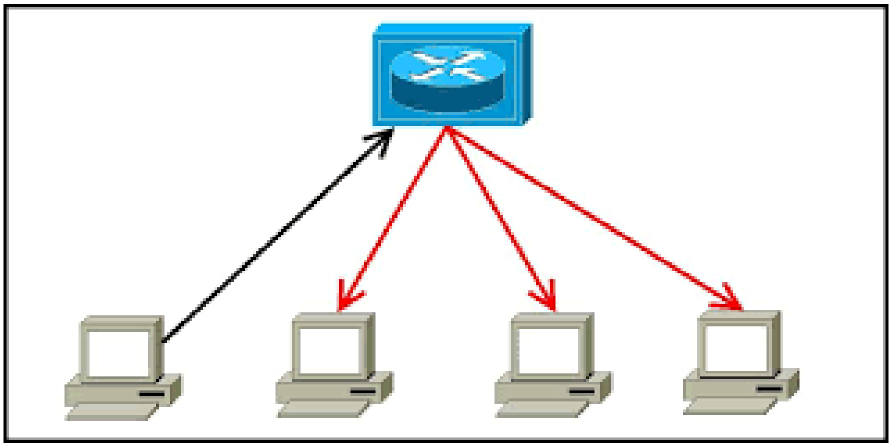
- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary.
- These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges:

- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow.
- The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Hubs

- A hub is a basically multi-port repeater.
- A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.



Active Hub:- These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

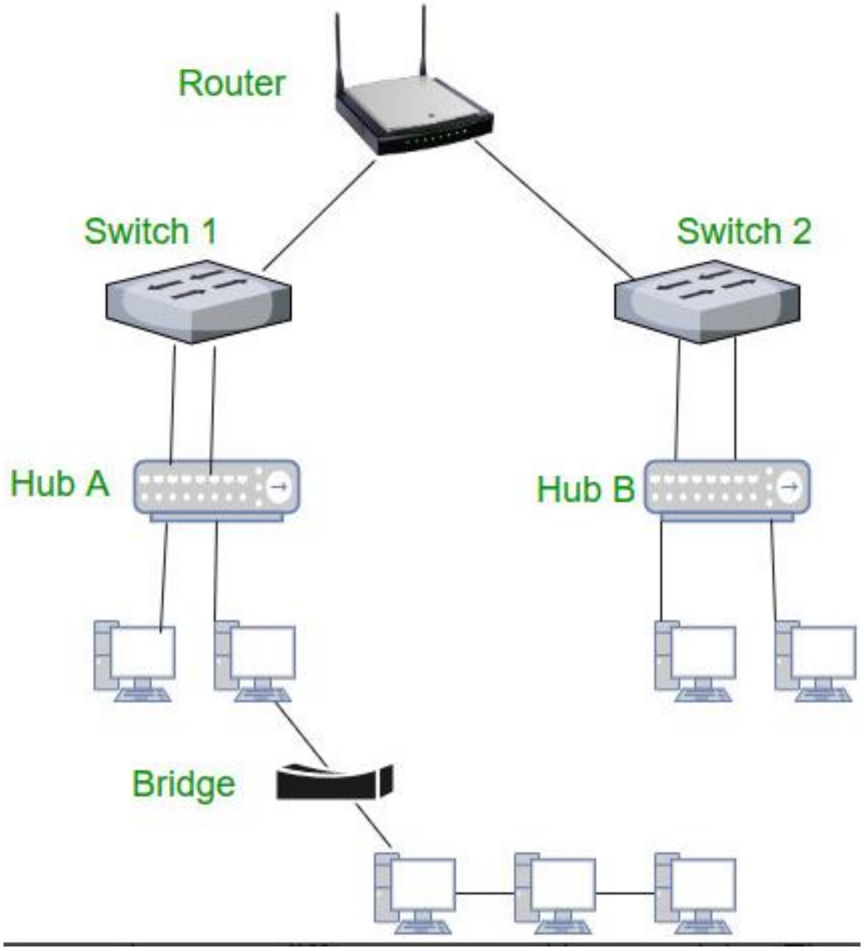
Passive Hub:- These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

Intelligent Hub:- It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Routers

- A router is a device like a switch that routes data packets based on their IP addresses.
- The router is mainly a Network Layer device.
- Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.

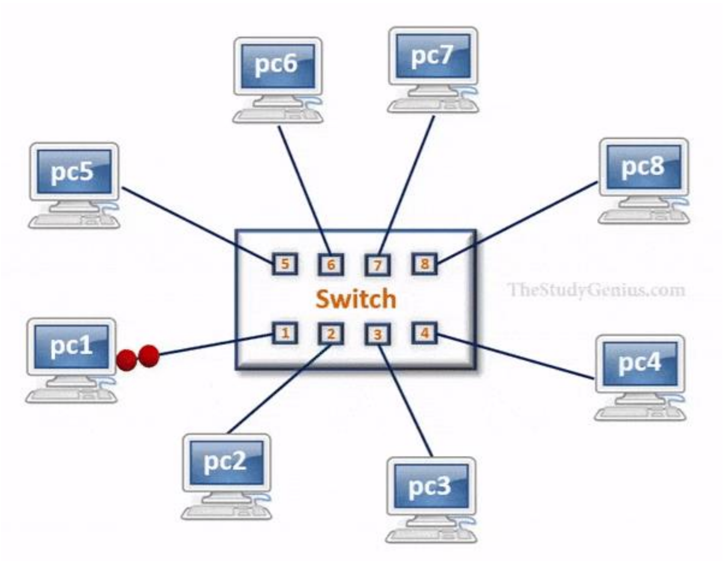
- The router divides the broadcast domains of hosts connected through it.



Switches

- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

- In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.



Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.

Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.

Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.

Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.

Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.

PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.

Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.

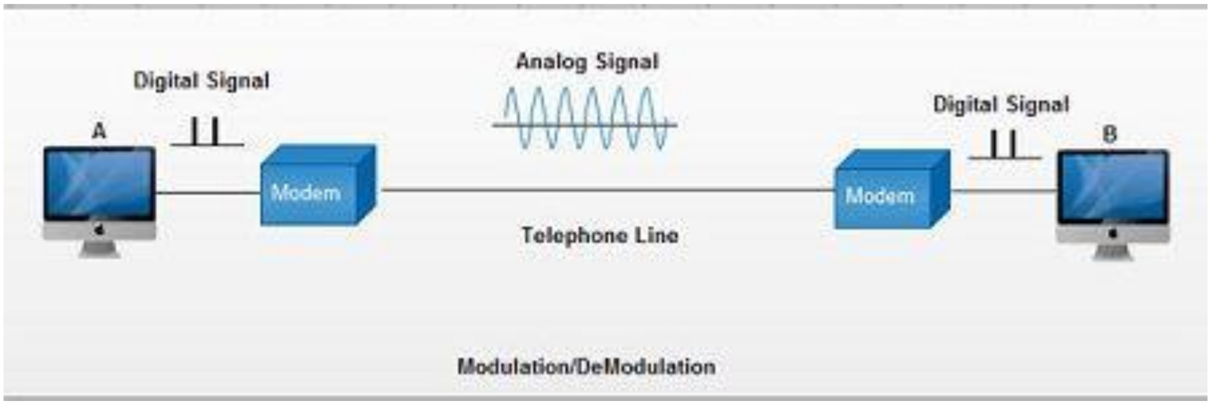
Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.

Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.

Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

Modems

- A modem (modulator-demodulator) converts digital signals into analog signals of different frequencies and transmits them to a modem at the receiving location.
- The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer.
- The digital data is usually transferred to or from the modem over a serial line through an industry-standard interface, RS-232.

- 

- There are three main types of modems:
- A **DSL modem** uses telephone cables and is considered the slowest connection.
- A **cable modem** transmits information over TV lines and is faster than DSL.
- A **wireless modem** transfers information between the local network and an internet service provider; it is the fastest transmitter.

Firewalls

- A firewall restricts the internet traffic of a private network, controlling what goes in and out.
- They analyze and restrict data packets based on programmed parameters, either whitelists or blacklists.
- Whitelists only allow information that falls within a certain set of parameters.
- Blacklists deny all information that falls inside the parameters.
- Firewalls are essential for private networks, especially those operating with sensitive information.

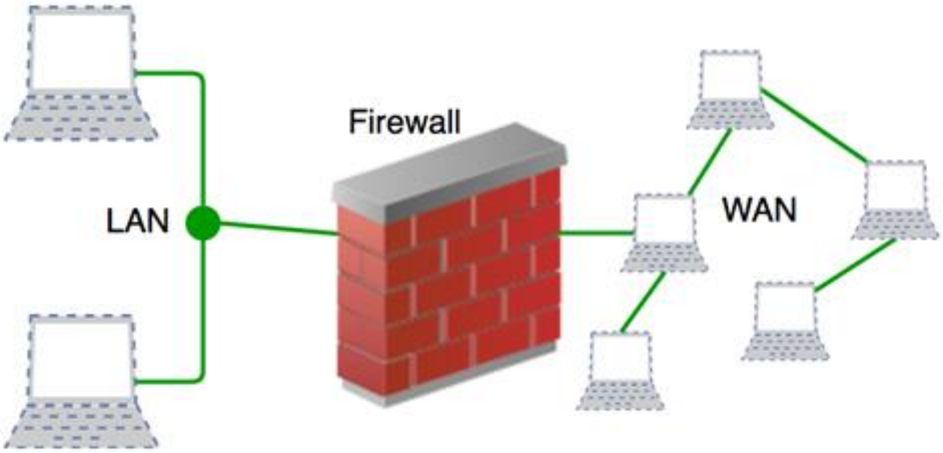
- They are also used within internal networks to block access between subgroups, such as a sales department being denied access to files pertaining to IT or HR.
- Several types of firewalls exist, and which one is right for you depends on your operation.

Firewall types :

Packet filtering: Acts as a network layer checkpoint, analyzing data packets by IP address, packet type, port number or network protocols

Stateful inspection: Analyzes data at network and transport layers, inspecting source IP, destination IP, source port and destination port

Next-generation: Analyzes actual packet content and all TCP handshake checks, checking for malware, and detects advanced threats (see the section on IDS and IPS below)



Host- based Firewalls :

•Host-based firewall is installed on each network node which controls each incoming and outgoing packet.

•It is a software application or suite of applications, comes as a part of the operating system.

•Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

Network-based Firewalls :

•Network firewall function on network level.

•In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall.

•A Network firewall might have two or more network interface cards (NICs).

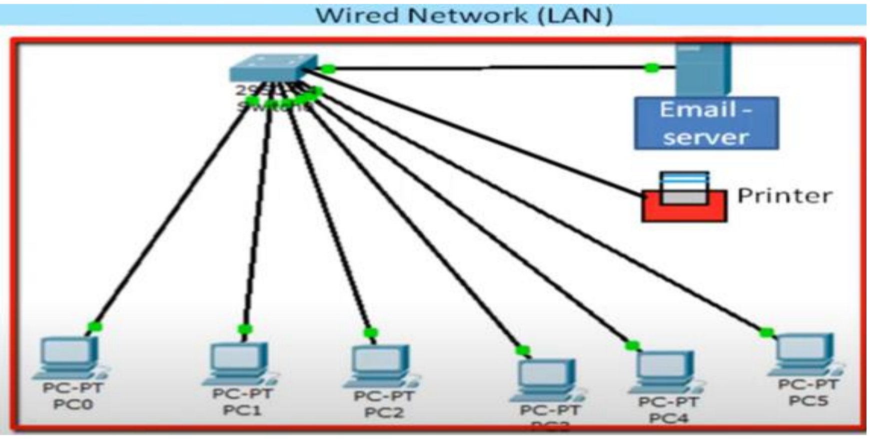
•A network-based firewall is usually a dedicated system with proprietary software installed.

WAP

- A wireless access point is a device used to create a wireless LAN (WLAN).
- WAPs are separate network devices with a built-in antenna, transmitter and adapter.
- WAPs use the wireless infrastructure network mode to provide a connection point between WLANs and a wired ethernet LAN.
- They also have several ports, allowing you to expand the network to support additional clients.
- Each WAP is limited by its transmission range — the distance a client can be from an WAP and still obtain a reasonable signal and data process speed.
- The distance depends on the wireless standard, the obstructions and the environmental conditions between the client and the WAP.

- Higher-end WAPs have high-powered antennas, enabling them to extend how far the wireless signal can travel.

- WAPs might also provide many ports for increasing a network’s size, firewall capabilities and Dynamic Host Configuration Protocol (DHCP) service.
- Therefore, an WAPs can be a switch, DHCP server, router and firewall.
- A service set identifier (SSID) name is necessary to connect to a wireless network.
- The SID is used to identify all systems belonging to the same network, and client stations must be configured with the SSID to be authenticated to the WAP.
- The WAP might broadcast the SSID, allowing all wireless clients in the area to see the WAP’s SSID.



- For security reasons, APs can be configured not to broadcast the SSID, meaning an administrator needs to give client systems the SSID instead of allowing it to be discovered automatically.

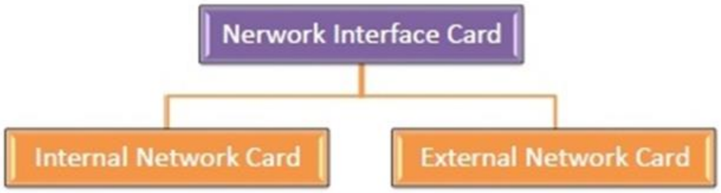
- Wireless devices ship with default SSIDs, security settings, channels, passwords and usernames.
- For security reasons, changing these default settings as soon as possible is strongly recommended because many internet sites list the default settings used by manufacturers.
- WAPs can be fat or thin.
    - Fat APs, sometimes called autonomous FAPs, must be manually configured with network and security settings. They are left alone to serve clients until they can no longer function.
    - Thin APs allow remote configuration using a controller. Since thin clients are not manually configured, they can be easily reconfigured and monitored.

NIC

- NIC or network interface card is a network adapter that is used to connect the computer to the network.
- It is installed in the computer to establish a LAN.
- It has a unique id that is written on the chip, and it has a connector to connect the cable to it.
- The cable acts as an interface between the computer and the router or modem.
- ISO-OSI:NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

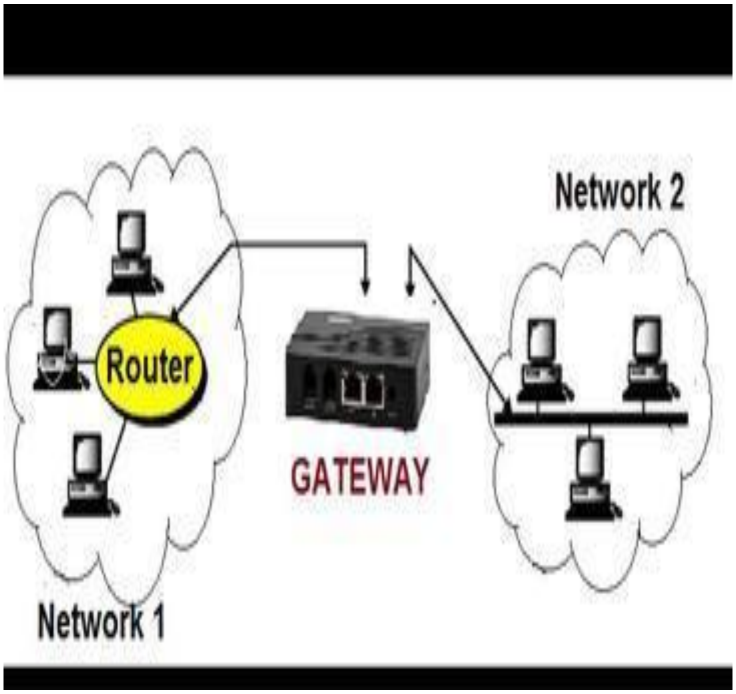
- TCP/IP:At the TCP/IP layer, the NIC connects a device to a network.
- At the physical layer, the NIC transmits a signal that sends information to the network layer.

There are two main types of NICs:



- An Ethernet NIC comes with an 8P8C socket for connecting an ethernet cable.
- A Wi-Fi NIC connects to a wireless network.
- Mobile devices have only a wireless NIC, but most computers still incorporate an Ethernet chip.
- Ethernet ports are more reliable but limit a user’s mobility while handling the device.

Gateways



- A gateway is a passage to connect two networks that may work upon different networking models.
- They work as messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switches or routers.
- Gateways translate between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP).
- Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies.
- They perform all of the functions of routers and more.
- A router with added translation functionality is a gateway.

5. Framing :

Framing:

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. This bit stream is not guaranteed to be error free. The number of bits received may be less than, equal to, or more than the number of bits transmitted, and they may have different values. It is up to the data link layer to detect and, if necessary, correct errors. The usual approach is for the data link layer to break the bit stream up into discrete frames and compute the checksum for each frame. When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it (e.g., discarding the bad frame and possibly also sending back an error report).

Breaking the bit stream up into frames is more difficult than it at first appears. One way to achieve this framing is to insert time gaps between frames, much like the spaces between words in ordinary text. Since it is too risky to count on timing to mark the start and end of each frame, other methods have been devised. We will look at four methods:

1. Character count.
2. Flag bytes with byte stuffing.
3. Starting and ending flags, with bit stuffing.
4. Physical layer coding violations.

The first framing method uses a field in the header to specify the number of characters in the frame. When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is

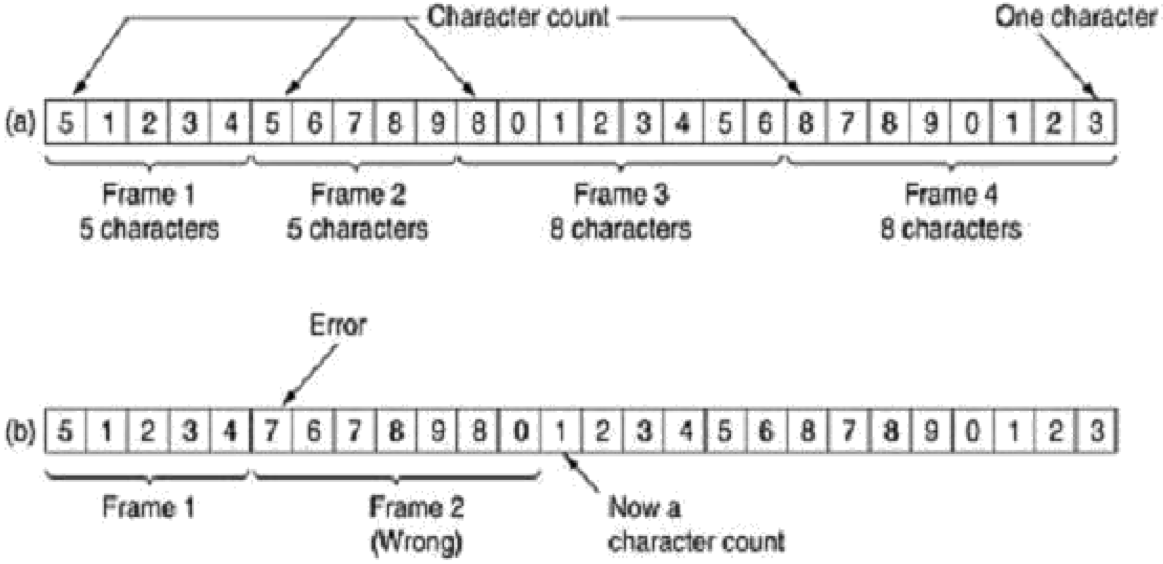


Fig: A character stream. (a) Without errors. (b) With one error.

The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the character count of 5 in the second frame of Fig(b) becomes a 7, the destination will get out of synchronization and will be unable to locate the start of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts. Sending a frame back to the source asking for a retransmission does not help either, since the destination does not know how many characters to skip over to get to the start of the retransmission. For this reason, the character count method is rarely used anymore.

The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. In the past, the starting and ending bytes were different, but in recent years most protocols have used the same byte, called a flag byte, as both the starting and ending delimiter, as shown in Fig2.2.(a) as FLAG. In this way, if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame. Two consecutive flag bytes indicate the end of one frame and start of the next one.

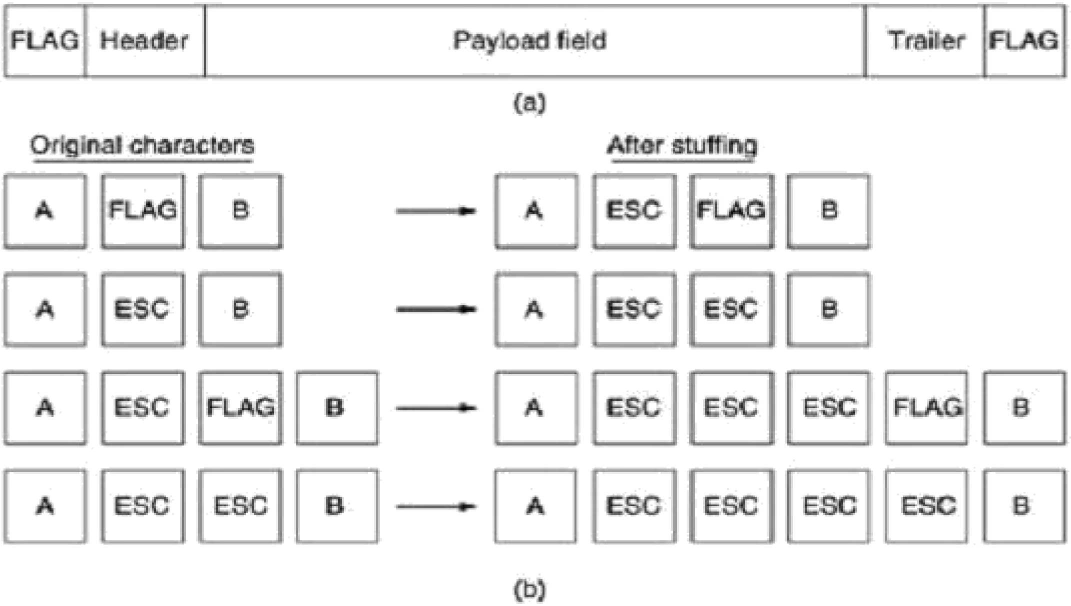


Fig: (a) A frame delimited by flag bytes (b) Four examples of byte sequences before and after byte stuffing.

A serious problem occurs with this method when binary data, such as object programs or floating-point numbers, are being transmitted. It may easily happen that the flag byte's bit pattern occurs in the data. This situation will usually interfere with the framing. One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data. The data link layer on the receiving end removes the escape byte before the data are given to the network layer. This technique is called byte stuffing or character stuffing. Thus, a framing flag byte can be distinguished from one in the data by the absence or presence of an escape byte before it.

Of course, the next question is: What happens if an escape byte occurs in the middle of the data? The answer is that it, too, is stuffed with an escape byte. Thus, any single escape byte is part of an escape sequence, whereas a doubled one indicates that a single escape occurred naturally in the data. In all cases, the byte sequence delivered after de stuffing is exactly the same as the original byte sequence.

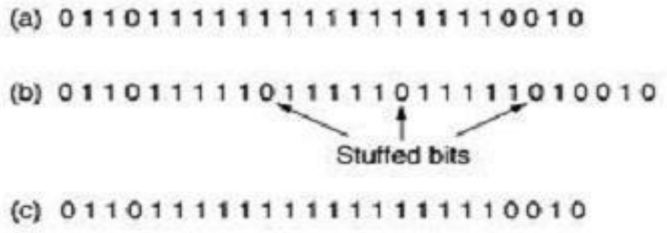
The byte-stuffing scheme depicted is a slight simplification of the one used in the PPP

protocol that most home computers use to communicate with their Internet service provider.

A major disadvantage of using this framing method is that it is closely tied to the use of 8-bit characters. Not all character codes use 8-bit characters. For example UNICODE uses 16-bit characters, As networks developed, the disadvantages of embedding the character code length in the framing mechanism became more and more obvious, so a new technique had to be developed to allow arbitrary sized characters.

The new technique allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. It works like this. Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte). Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream. This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.

When the receiver sees five consecutive incoming 1 bits, followed


(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0
(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0
Stuffed bits
(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

by a 0 bit, it automatically de stuffs (i.e., deletes) the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110.

Figure: Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data. The last method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy. For example, some LANs encode 1 bit of data by using 2 physical bits. Normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit

boundaries. The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.

As a final note on framing, many data link protocols use combination of a character count with one of the other methods for extra safety. When a frame arrives, the count field is used to locate the end of the frame. Only if the appropriate delimiter is present at that position and the checksum is correct is the frame accepted as valid. Otherwise, the input stream is scanned for the next delimiter.

6. Error Detection Algorithms :

Error – Detection and Correction – Parity – LRC – CRC and checksum , Hamming code.

The data can be corrupted during transmission (from source to receiver). It may be affected by external noise or some other physical imperfections. In this case, the input data is not same as the received output data. This mismatched data is called “Error”.

The data errors will cause loss of important / secured data. Even one bit of change in data may affect the whole system’s performance. Generally the data transfer in digital systems will be in the form of ‘Bit – transfer’. In this case, the data error is likely to be changed in positions of 0 and 1 .

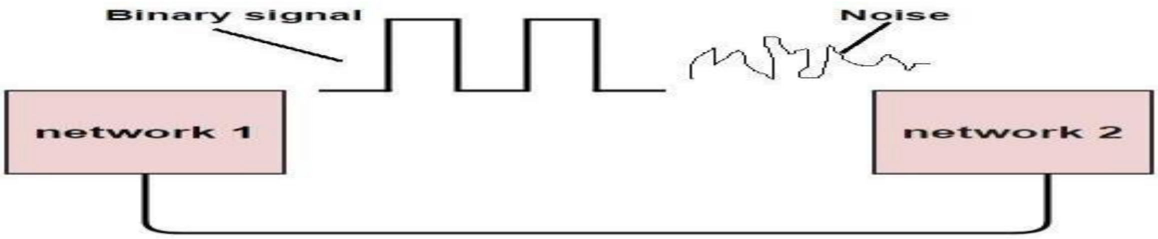


Fig : Error

Types Of Errors

In a data sequence, if 1 is changed to zero or 0 is changed to 1, it is called “Bit error”.

There are generally 3 types of errors occur in data transmission from transmitter to receiver. They are

- Single bit errors
- Multiple bit errors
- Burst errors

Single Bit Data Errors

The change in one bit in the whole data sequence , is called “Single bit error”. Occurrence of single biterror is very rare in serial communication system. This type of error occurs only in parallel communication system, as data is transferred bit wise in single line, there is chance that single line to benoisy.

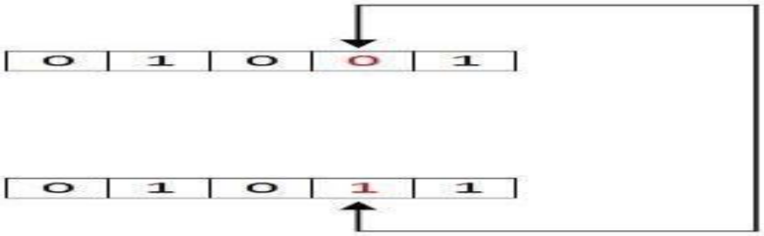


Fig : Single Bit Data Errors

Multiple Bit Data Errors

If there is change in two or more bits of data sequence of transmitter to receiver, it is called “Multiple biterror”. This type of error occurs in both serial type and parallel type data communication networks.

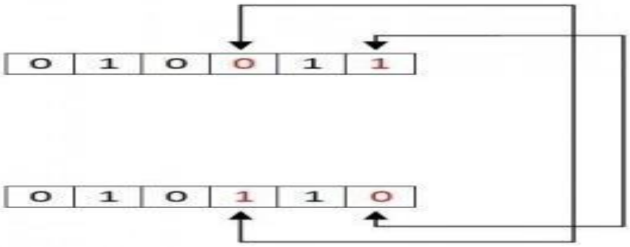


Fig : Multiple Bit Data Errors

Burst Errors

The change of set of bits in data sequence is called “Burst error”. The burst error is calculated in from thefirst bit change to last bit change.

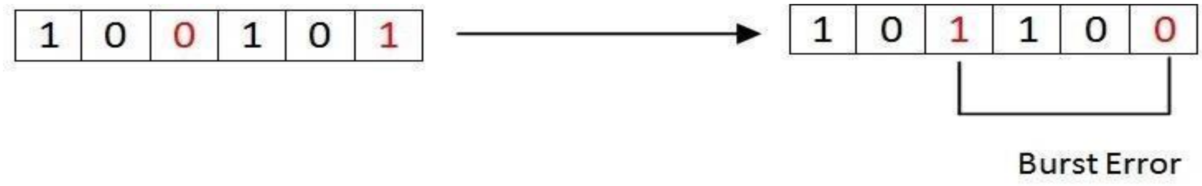


Fig : Burst Errors

Here we identify the error form fourth bit to 6th bit. The numbers between 4th and 6th bits are also considered as error. These set of bits are called "Burst error". These burst bits changes from transmitter to receiver, which may cause a major error in data sequence. This type of errors occurs in serial communication and they are difficult to solve.

Error Detecting Codes

Error detection is the process of detecting the errors that are present in the data transmitted from transmitter to receiver, in a communication system. We use some redundancy codes to detect these errors, by adding to the data while it is transmitted from source (transmitter). These codes are called “Error detecting codes”.

Types of Error detection

□ Parity Checking

□ Cyclic Redundancy Check (CRC)

□ Longitudinal Redundancy Check (LRC)

□ Check Sum

Parity Checking :

Parity bit means nothing but an additional bit added to the data at the transmitter before transmitting the data. Before adding the parity bit, number of 1’s or zeros is calculated in the data. Based on this calculation of data an extra bit is added to the actual information / data. The addition of parity bit to the data will result in the change of data string size.

This means if we have an 8 bit data, then after adding a parity bit to the data binary string it will become a 9 bit binary data string.

Parity check is also called as “Vertical

Redundancy Check (VRC)”. There is two

types of parity bits in error detection,

they are

1. Even parity 2.Odd parity

Even Parity

If the data has even number of 1’s, the parity bit is 0.

Ex: data is 10000001 -> parity bit 0 Odd number of

1’s, the parity bit is 1. Ex: data is 10010001 -> parity

bit 1

Odd Parity

If the data has odd number of 1’s, the parity bit is 0.

Ex: data is 10011101 -> parity bit 0 Even number of

1’s, the parity bit is 1. Ex: data is 10010101 -> parity

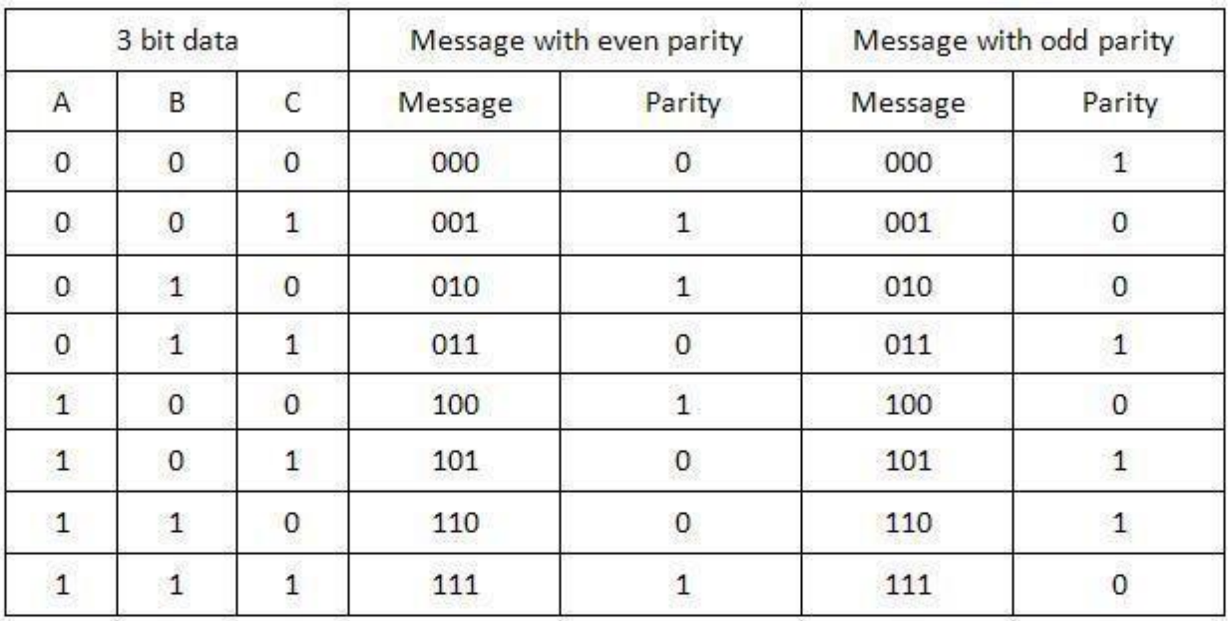
bit 1

NOTE:

The counting of data bits will include the parity bit also.

The circuit which adds a parity bit to the data at transmitter is called “Parity generator”. The parity bits are transmitted and they are checked at the receiver. If the parity bits sent at the transmitter and the parity bits received at receiver are not equal then an error is detected. The circuit which checks the parity at receiver is called “Parity checker”.

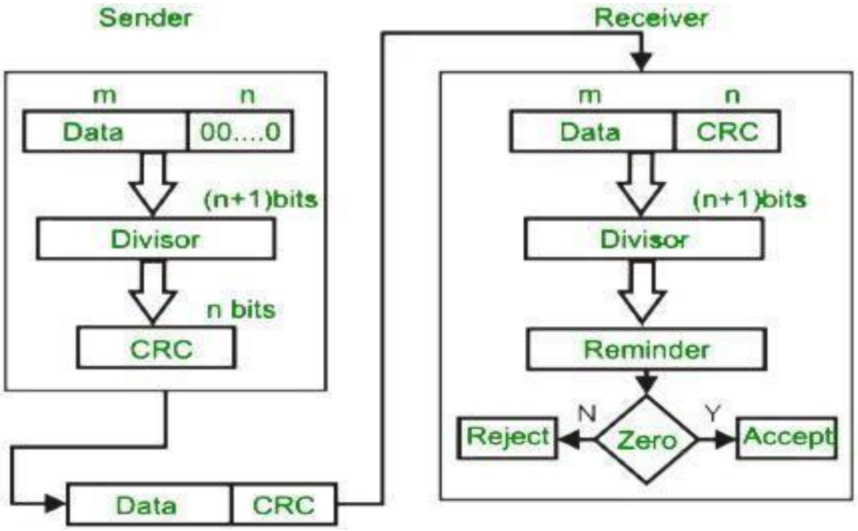
Messages with even parity and odd parity



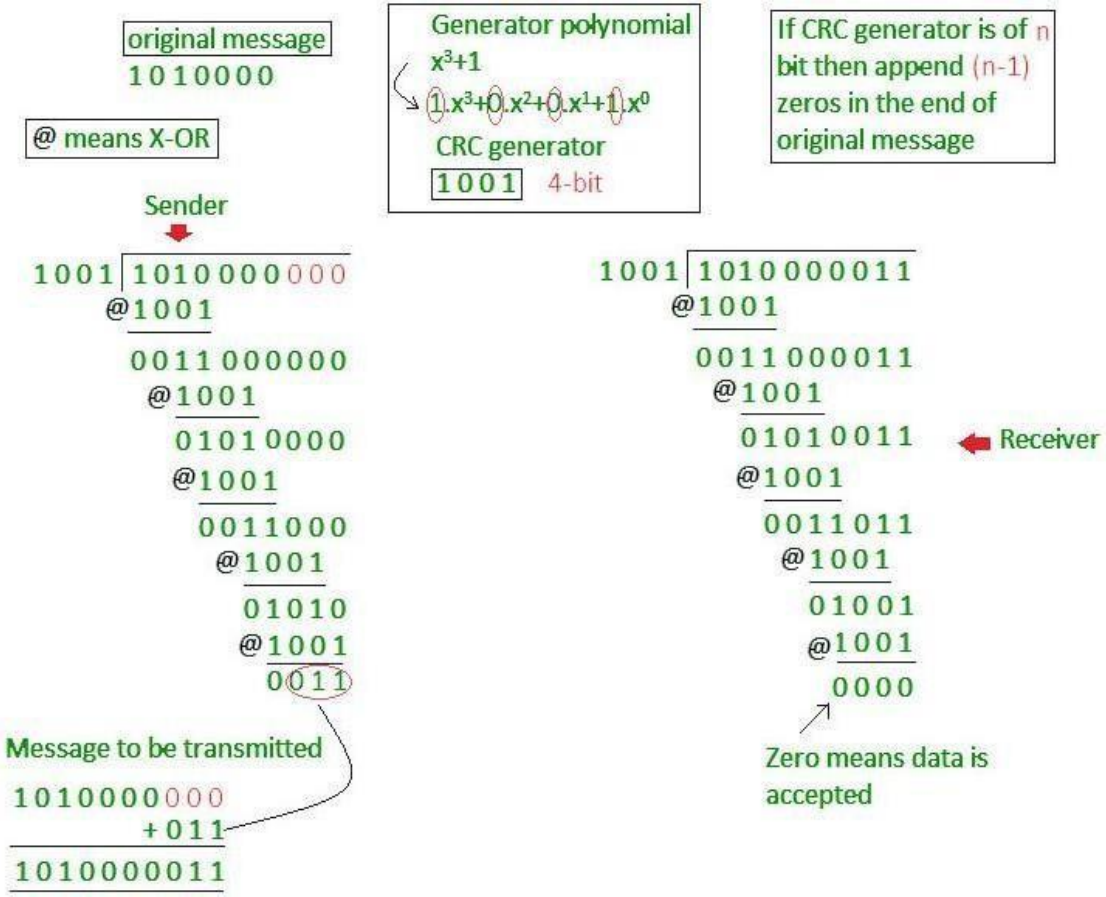
3 bit data			Message with even parity		Message with odd parity	
A	B	C	Message	Parity	Message	Parity
0	0	0	000	0	000	1
0	0	1	001	1	001	0
0	1	0	010	1	010	0
0	1	1	011	0	011	1
1	0	0	100	1	100	0
1	0	1	101	0	101	1
1	1	0	110	0	110	1
1	1	1	111	1	111	0

Cyclic Redundancy Check (CRC):

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



Example :



original message
1010000

@ means X-OR

Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1001 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001 | 1010000000
      @1001
       0011000000
         @1001
          01010000
          @1001
           0011000
            @1001
             01010
             @1001
              0011
```

Message to be transmitted

```
 1010000000
      + 011
 1010000011
```

```
1001 | 1010000011
      @1001
       0011000011
         @1001
          01010011      Receiver
          @1001
           0011011
            @1001
             01001
             @1001
              0000
```

Zero means data is accepted

Longitudinal Redundancy Check (LRC):

In longitudinal redundancy method, a BLOCK of bits are arranged in a table format (in rows and columns) and we will calculate the parity bit for each column separately. The set of these parity bits are also sent along with our original data bits.

Longitudinal redundancy check is a bit by bit parity computation, as we calculate the parity of each column individually.

This method can easily detect burst errors and single bit errors and it fails to detect the 2 bit errors occurred in same vertical slice.

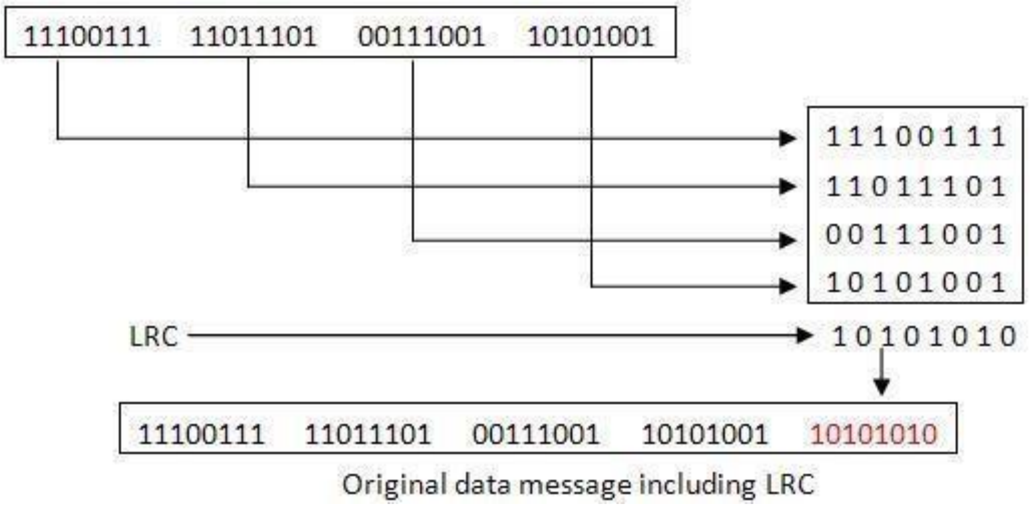


Fig : Longitudinal Redundancy Check

Check Sum:

The checksum method includes parity bits, check digits and longitudinal redundancy check (LRC). For example, if we have to transfer and detect errors for a long data sequence (also called as Data string) then we divide that into shorter words and we can store the data with a word of same width. For each another incoming bit we will add them to the already stored data. At every instance, the newly added word is called “Checksum”.

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

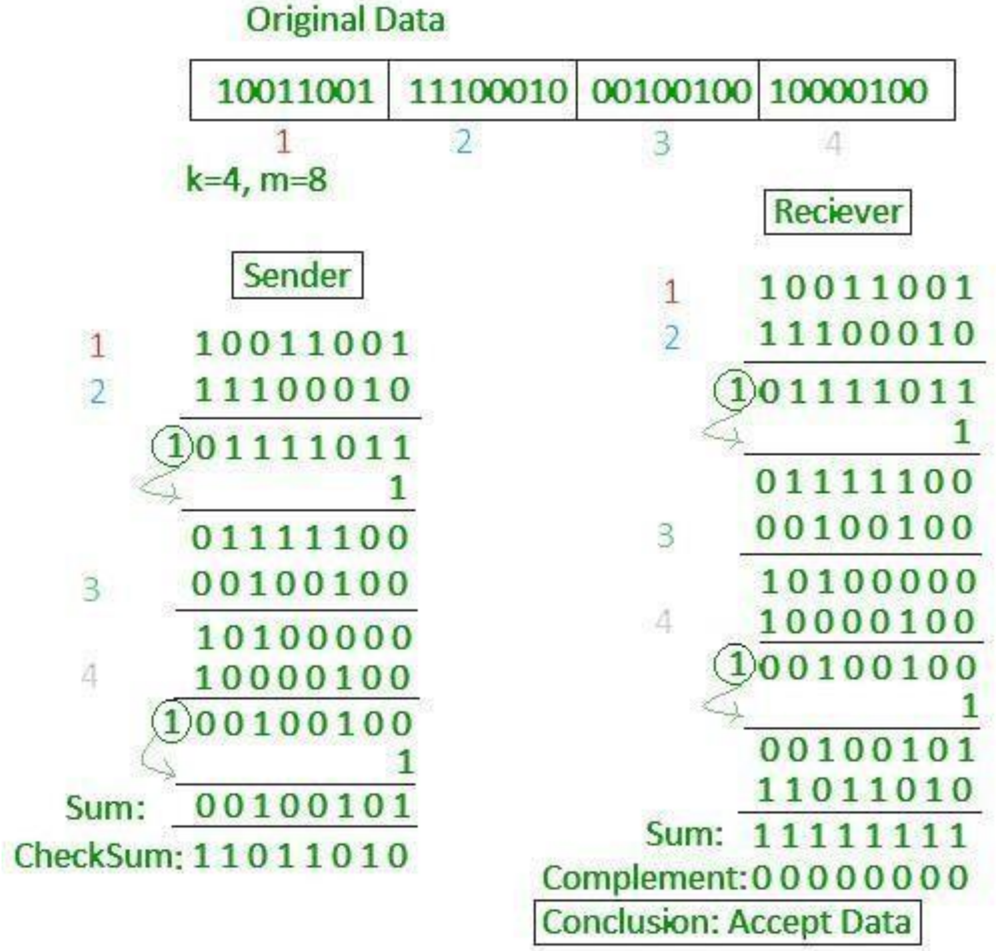


Fig : Check Sum

7. Error Correction Algorithms

Error-Correcting Codes :(Hamming code)

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

Redundant bits –

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.

```
2^r > m + r + 1
where, r = redundant bit, m = data bit
```

The number of redundant bits can be calculated using the following formula

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:

= 2^4 > 7 + 4 + 1

Thus, the number of redundant bits= 4

Parity bits –

A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1’s in the data are even or odd. Parity bits are used for error detection. There are two types of parity bits:

- Even parity bit:
  In the case of even parity, for a given set of bits, the number

of 1’s are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1’s an even number. If the total number of 1’s in a given set of bits is already even, the parity bit’s value is 0.

- Odd Parity bit :

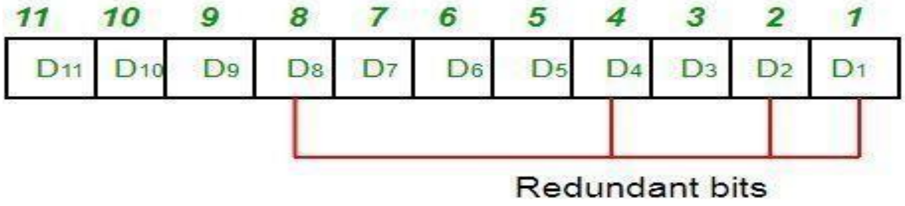
  In the case of even parity, for a given set of bits, the number of 1’s are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1’s an odd number. If the total number of 1’s in a given set of bits is already odd, the parity bit’s value is 0.

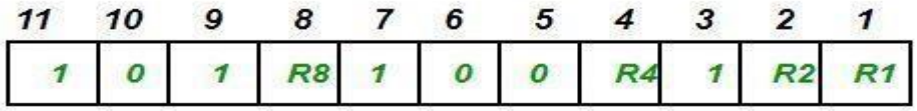
General Algorithm of Hamming code –
The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
   a. Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
   b. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
   c. Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).
   d. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).
   e. In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Determining the position of redundant bits:
These redundancy bits are placed at the positions which correspond to the power of 2. As in the above example:

1. The number of data bits = 7
2. The number of redundant bits = 4
3. The total number of bits = 11
4. The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8

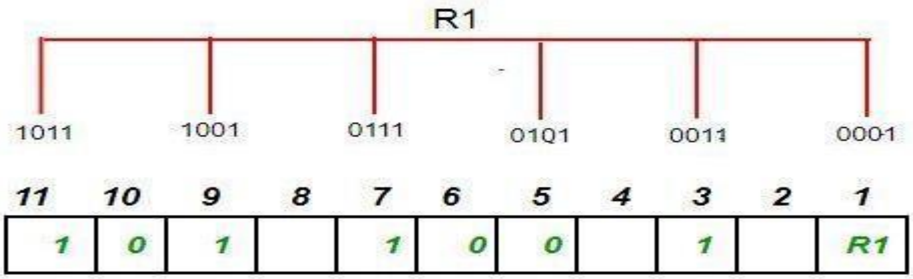




Suppose the data to be transmitted is 1011001, the bits will be placed as follows:

Determining the Parity bits –

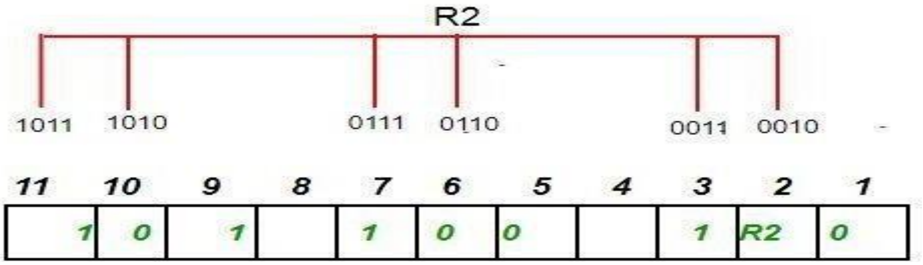
1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.
   R1: bits 1, 3, 5, 7, 9, 11



To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions

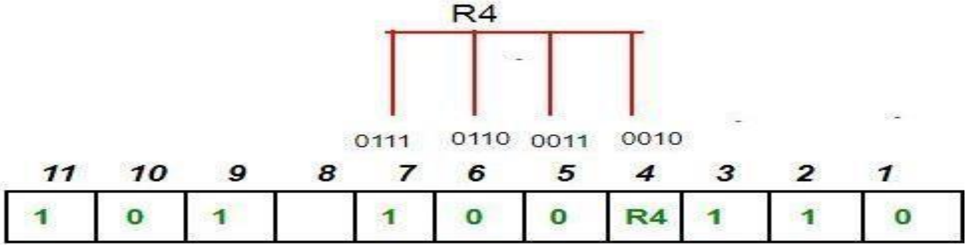
corresponding to R1 is an even number the value of R1 (parity bit's value)
= 0

2. R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.
R2: bits 2,3,6,7,10,11



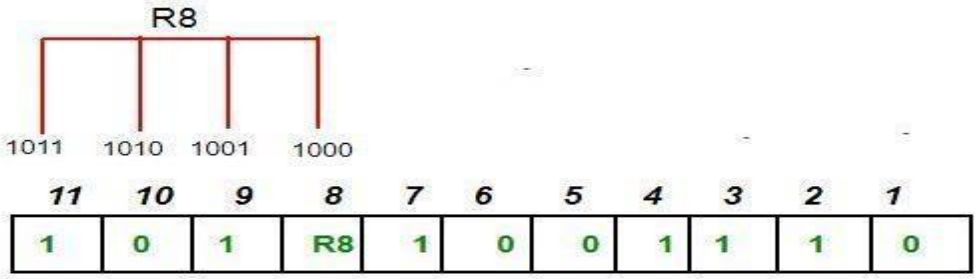
To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is an odd number the value of R2(parity bit's value)=1

3. R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.
R4: bits 4, 5, 6, 7



To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is an odd number the value of R4(parity bit's value) = 1

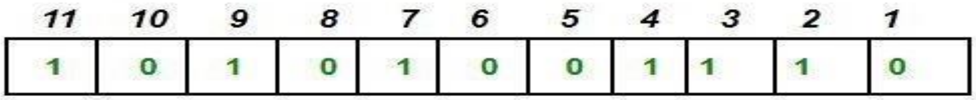
4. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.
R8: bit 8,9,10,11



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

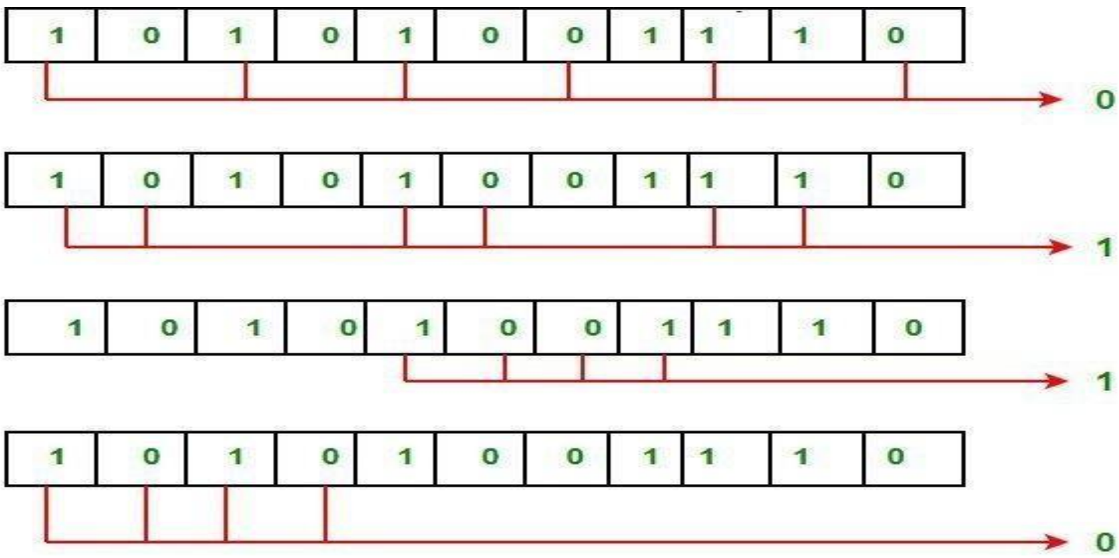
To find the redundant bit R8, we check for even parity. Since the total number of 1’s in all the bit positions corresponding to R8 is an even number the value of R8(parity bit’s value)=0.

Thus, the data transferred is:



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

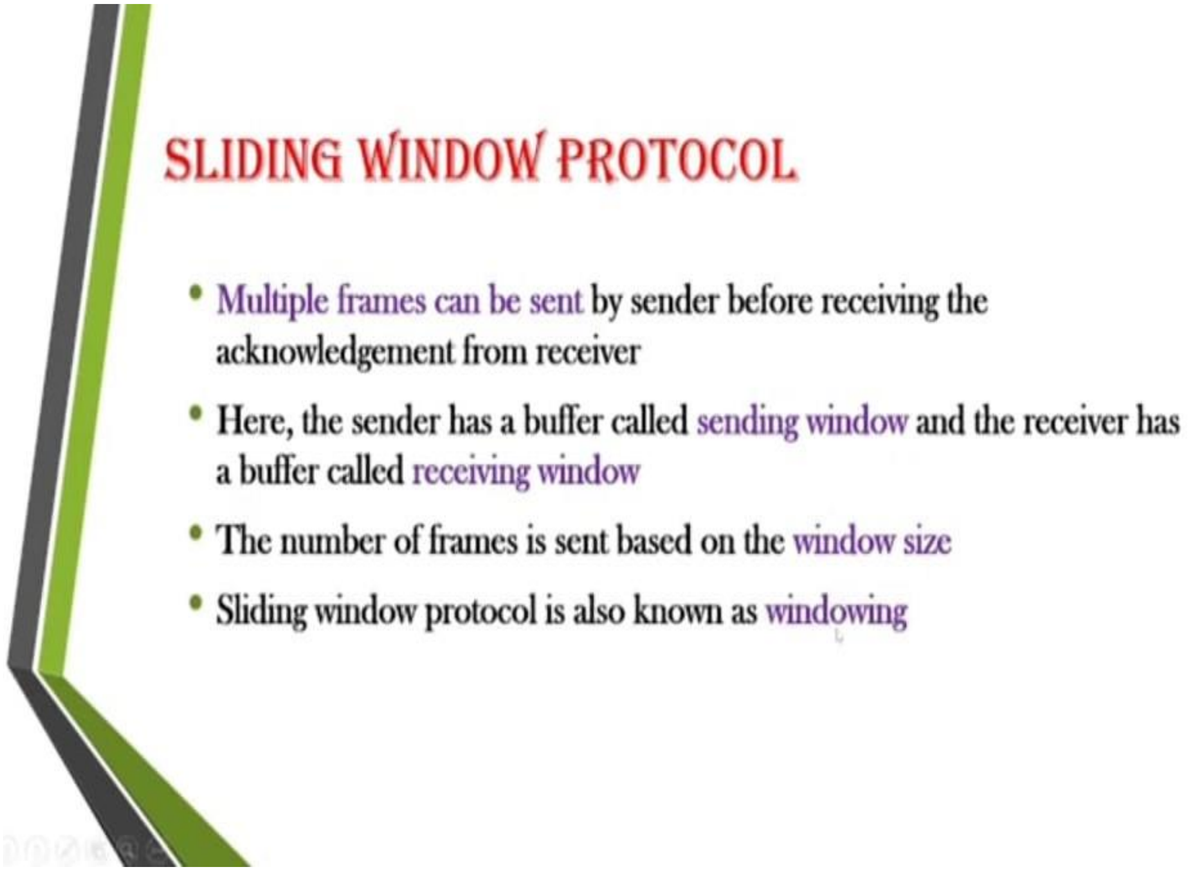
Error detection and correction –
Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then itgives new parity values in the binary number:



The bits give the binary number as 0110 whose decimal representation is 6. Thus, the bit 6contains an error. To correct the error the 6th bit is changed from 1 to 0.

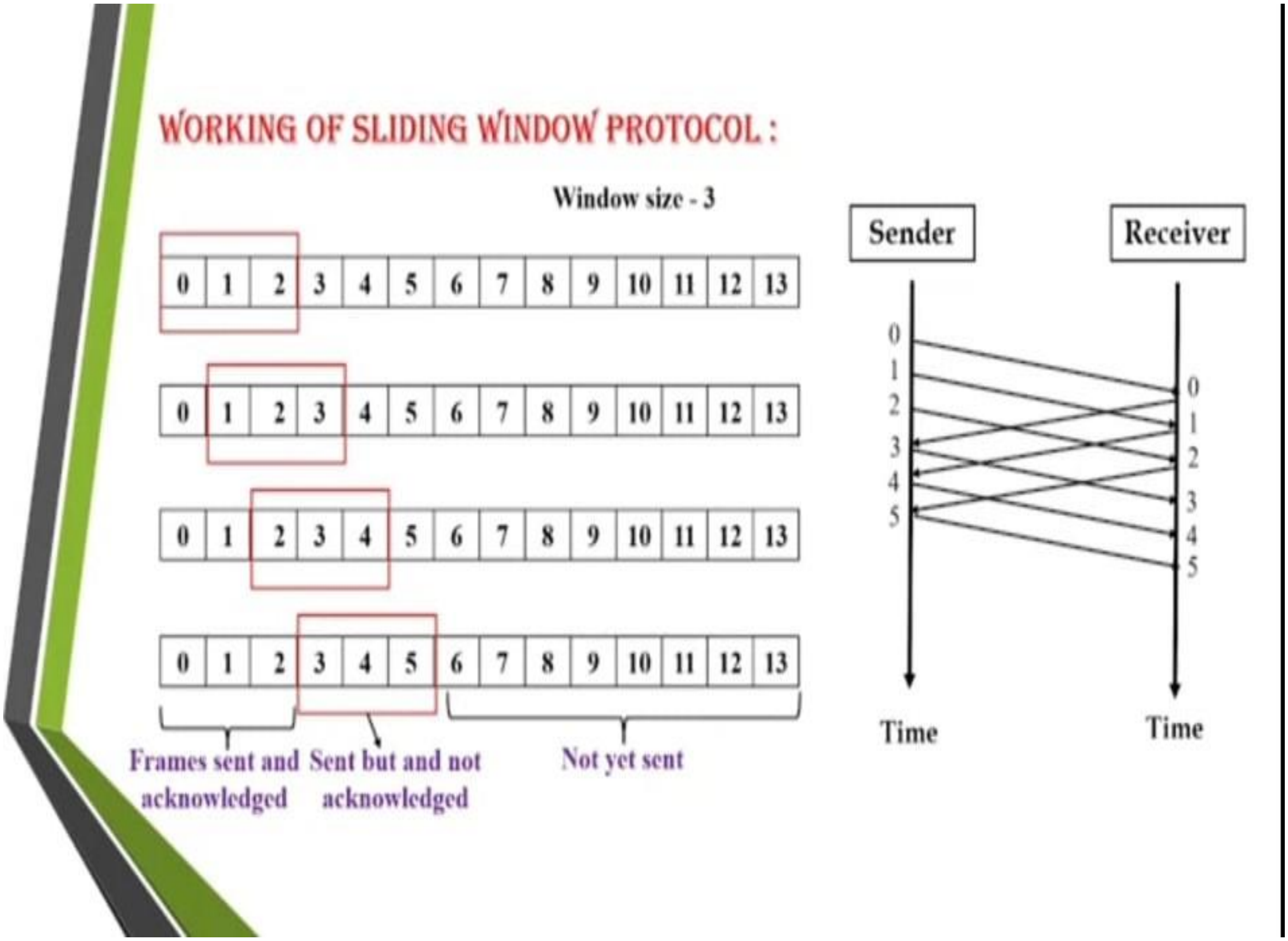
- **8. Sliding Window Protocols**
- The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

- In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.
- *Sliding window protocols apply Pipelining :*
- *Go-Back-N ARQ*
- *Selective Repeat ARQ*
- *Sliding window protocols improve the efficiency*
- *multiple frames should be in transition while waiting for ACK. Let more than one frame to be outstanding.*
- *Outstanding frames: frames sent but not acknowledged*
- *Pipelining:* **Pipelining** is a process of sending multiple data packets serially without waiting for the previous acknowledgement.
- *There is no pipelining in stop and wait ARQ because we need to wait for a frame to reach the destination and be acknowledged before the next frame can be sent*
- *Pipelining improves the efficiency of the transmission*



SLIDING WINDOW PROTOCOL

- Multiple frames can be sent by sender before receiving the acknowledgement from receiver
- Here, the sender has a buffer called sending window and the receiver has a buffer called receiving window
- The number of frames is sent based on the window size
- Sliding window protocol is also known as windowing



WORKING OF SLIDING WINDOW PROTOCOL :

Go-Back-N Automatic Repeat Request:(GBN)

Stop and wait ARQ mechanism does not utilize the resources at their best.When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

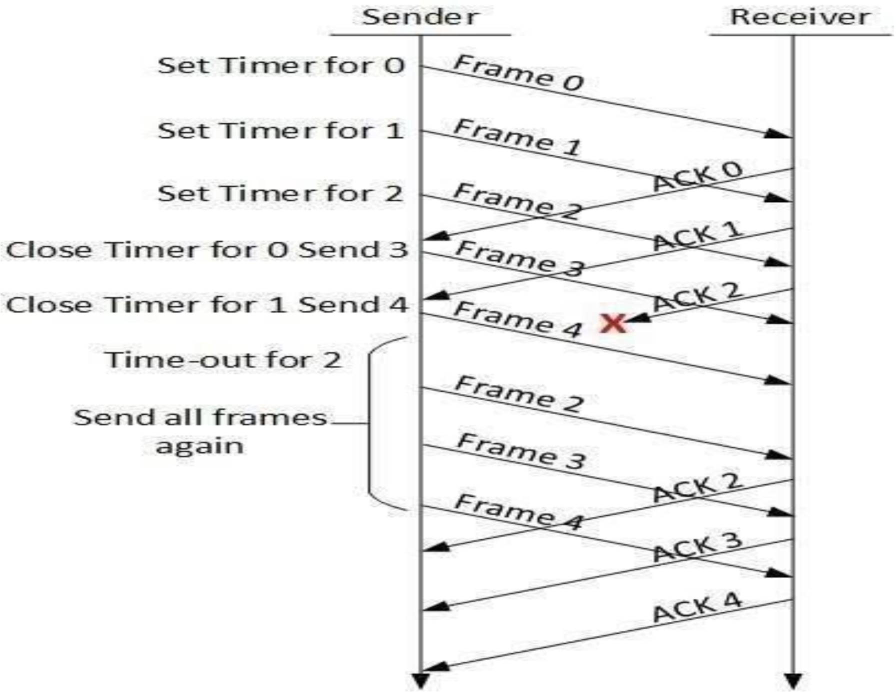
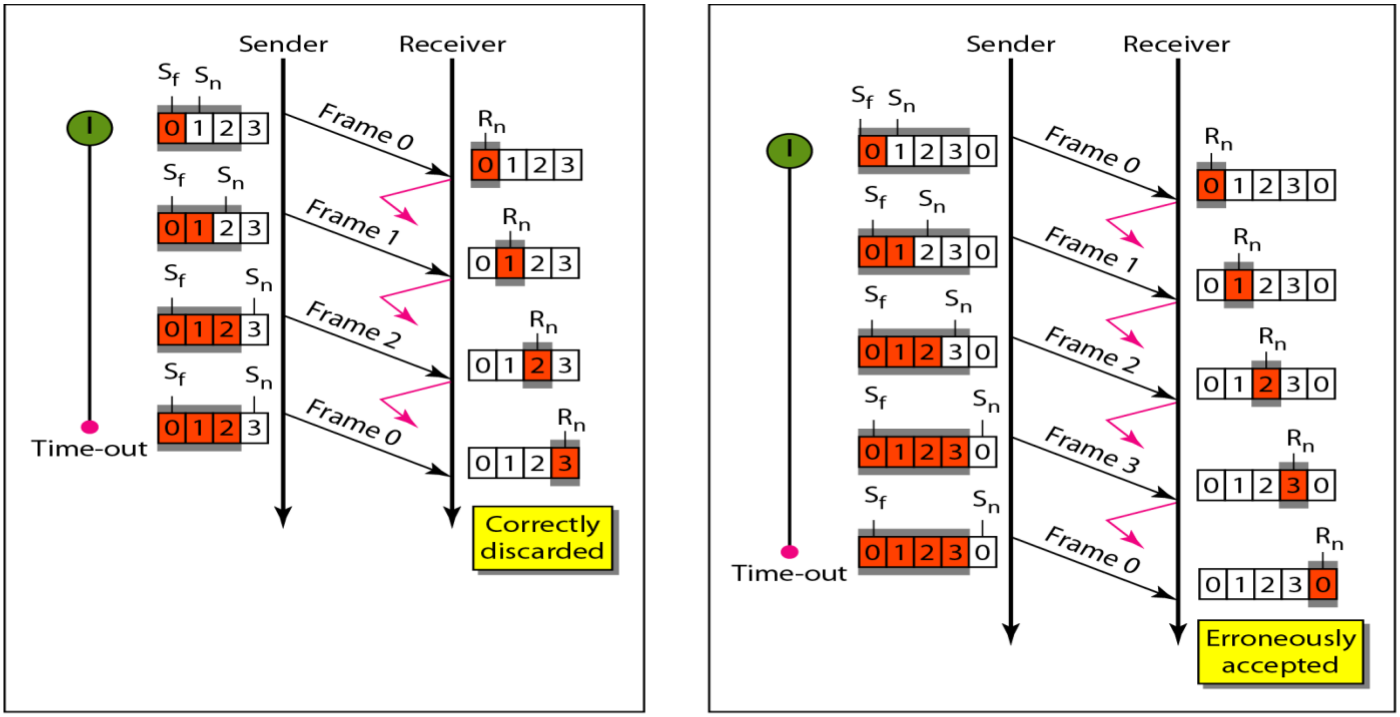


Fig 2.13 Go-Back-N Automatic Repeat Request



a. Window size < 2^m

b. Window size = 2^m

The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame’s sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its windowsize and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.

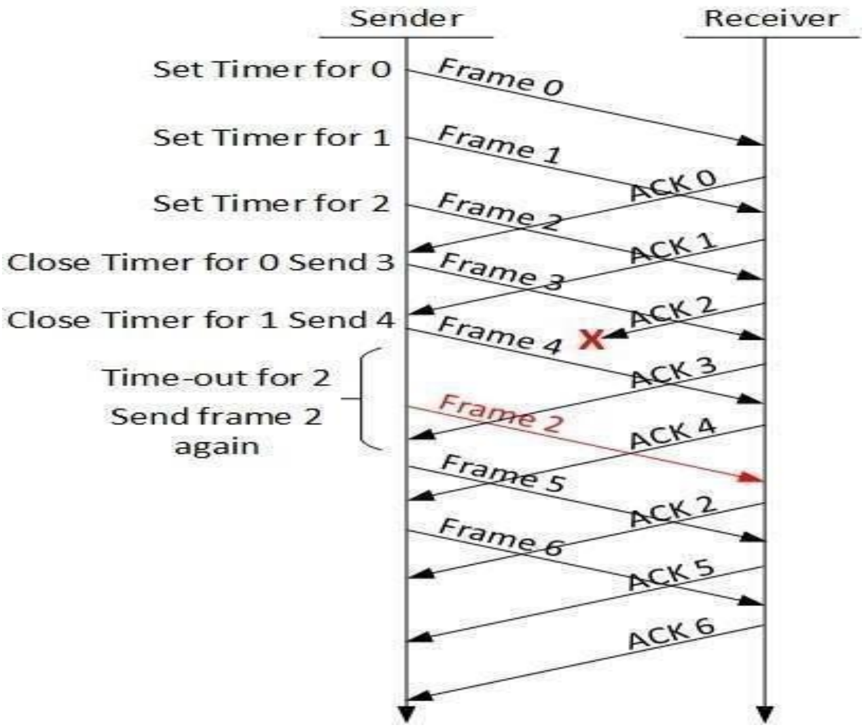
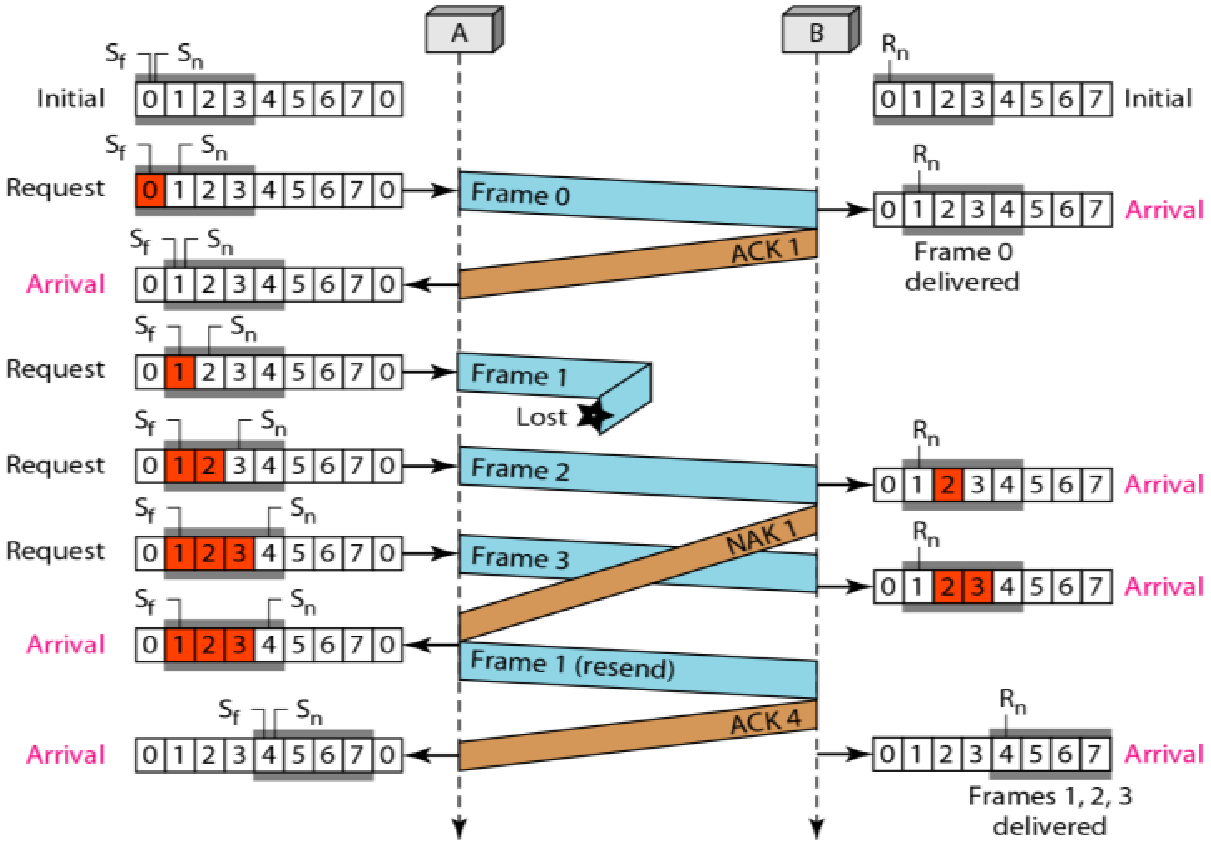


Fig 2.14 Selective Repeat ARQ



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

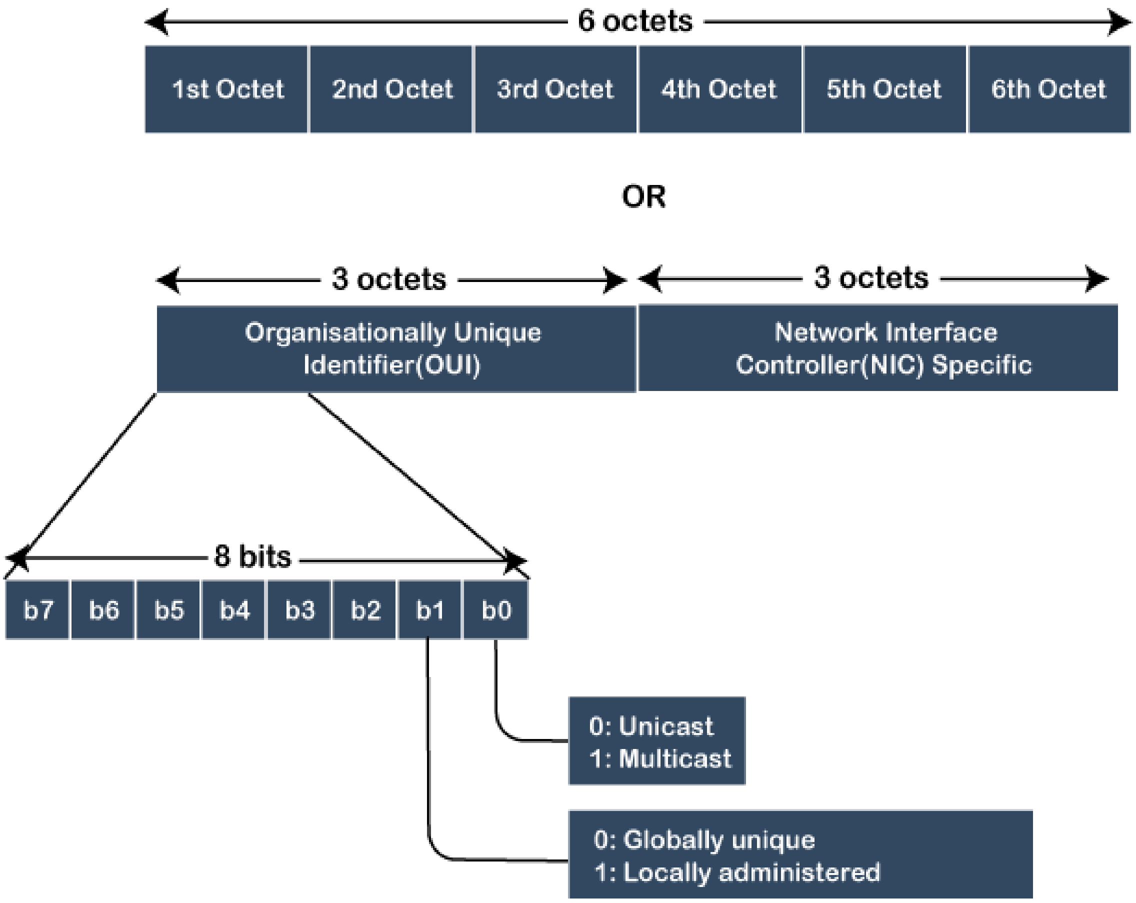
The sender in this case, sends only packet for which NACK is received.

In Selective Repeat ARQ, the size of In the sender and receiver window must be at most one-half of 2m.

- **9. MAC Addressing**
- A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network.
- Primarily specified as a unique identifier during device manufacturing, the MAC address is often found on a device's network interface card (NIC).
- To communicate or transfer data from one computer to another, we need an address.
- A MAC address is a 48 or 64-bit address associated with a network adapter.
- MAC addresses are linked to the hardware of the network adapters, hence they are also known as the "hardware address" or "physical address."
- MAC addresses uniquely identify the adapter on the LAN.
- MAC addresses are expressed in hexadecimal notation. For example, "01-23-45-67-89-AB" in a 48-bit address or "01-23-45-67-89-AB-CD-EF" in a 64-bit address. Sometimes, colons (:) are used instead of dashes (-).

- MAC addresses are often considered permanent, but in some conditions, they can be changed.
  Types of MAC addresses

1. Unicast MAC address. A unicast address is attached to a specific NIC on the local network. Therefore, this address is only used when a frame is sent from a single transmitting device to a single destination device.
2. Multicast MAC address. A source device can transmit a data frame to multiple devices by using a multicast A multicast group IP address is assigned to devices belonging to the multicast group.
3. Broadcast MAC address. This address represents every device on a given network. The purpose of a broadcast domain is to enable a source device to send data to every device on the network by using the broadcast address as the destination's MAC address.
   Format of MAC address

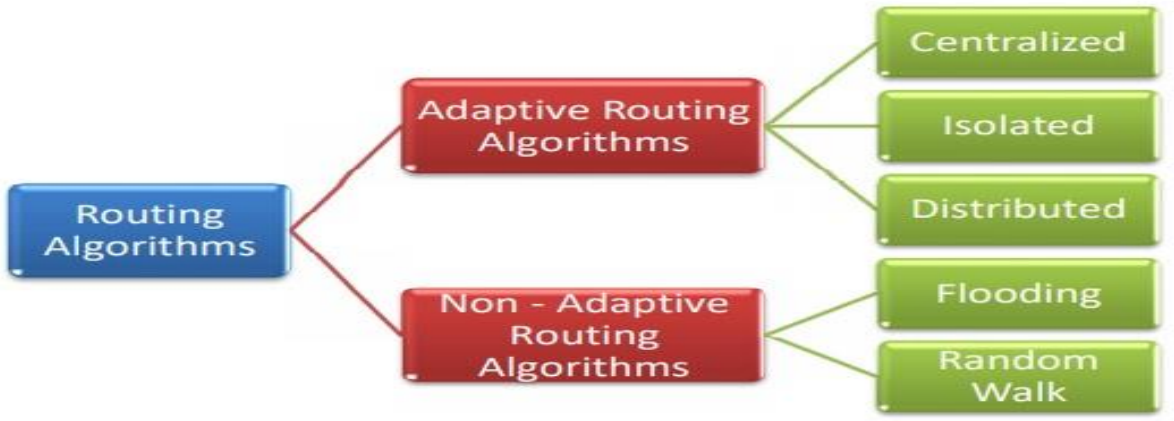


10. Routing Protocols

- Routing is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.
- A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. They help in directing Internet traffic efficiently.
- After a data packet leaves its source, it can choose among the many different paths to reach its destination.

- Routing algorithm mathematically computes the best path, i.e. “least – cost path” that the packet can be routed through.

Classification of a Routing algorithm



An adaptive routing algorithm is also known as **dynamic routing algorithm.**

This algorithm makes the routing decisions based on the topology and network traffic.

The main parameters related to this algorithm are hop count, distance and estimated transit time.

An adaptive routing algorithm can be classified into three parts:

- **Centralized algorithm:** It is also known as global routing algorithm as it computes the least-cost path between source and destination by using complete and global knowledge about the network. This algorithm takes the connectivity between the nodes and link cost as input, and this information is obtained before actually performing any calculation. **Link state algorithm** is referred to as a centralized algorithm since it is aware of the cost of each link in the network.

- **Isolation algorithm:** It is an algorithm that obtains the routing information by using local information rather than gathering information from other nodes.
- **Distributed algorithm:** It is also known as decentralized algorithm as it computes the least-cost path between source and destination in an iterative and distributed manner. In the decentralized algorithm, no node has the knowledge about the cost of all the network links. In the beginning, a node contains the information only about its own directly attached links and through an iterative process of calculation computes the least-cost path to the destination. A Distance vector algorithm is a decentralized algorithm as it never knows the complete path from source to the destination, instead it knows the direction through which the packet is to be forwarded along with the least cost path.

Non Adaptive routing algorithm is also known as a **static routing algorithm**. When booting up the network, the routing information stores to the routers. Non Adaptive routing algorithms do not take the routing decision based on the network topology or network traffic.

The Non-Adaptive Routing algorithm is of two types:

- **Flooding:** In case of flooding, every incoming packet is sent to all the outgoing links except the one from it has been reached. The disadvantage of flooding is that node may contain several copies of a particular packet.

- **Random walks:** In case of random walks, a packet sent by the node to one of its neighbors randomly. An advantage of using random walks is that it uses the alternative routes very efficiently.

Optimality Principle

A general statement is made about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle(Bellman,1975).

Statement of the optimality principle :

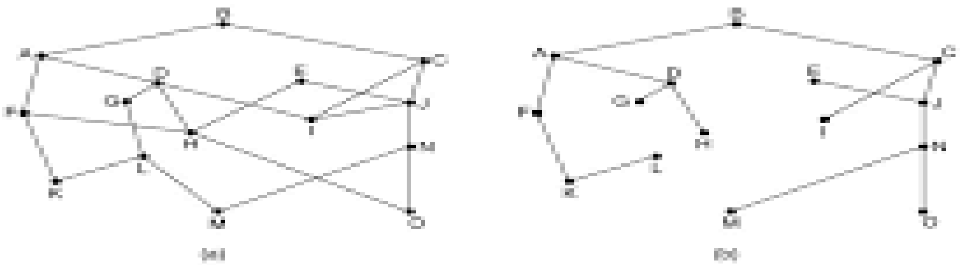
- It states that if the router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route. Call the route from I to J *r1* and the rest of the route *r2*. it could be concatenated with *r1* to improve the route from I to K, contradicting our statement that *r1r2* is optimal only if a route better than r2 existed from J to K.

Sink Tree for routers :

- We can see that the set of optimal routes from all sources to a given destination from a tree rooted at the destination as a directed consequence of the optimality principle. This tree is called a **sink tree**

The Optimality Principle

(a) A subnet. (b) A sink tree for router B.



Examples of Routing algorithms

- ❖ shortest path routing Algorithm
- ❖ distance vector routing Algorithm
- ❖ Link State Routing Algorithm
- ❖ Flooding Algorithm Algorithm

shortest path routing Algorithm

- Consider that a network comprises of N vertices (nodes or network devices) that are connected by M edges (transmission lines).
- Each edge is associated with a weight, representing the physical distance or the transmission delay of the transmission line.
- The target of shortest path algorithms is to find a route between any pair of vertices along the edges, so the sum of weights of edges is minimum.

- If the edges are of equal weights, the shortest path algorithm aims to find a route having minimum number of hops.

  Example : Dijkstra's Algorithm

  Input − A graph representing the network; and a source node, s

  Output − A shortest path tree, spt[], with s as the root node.

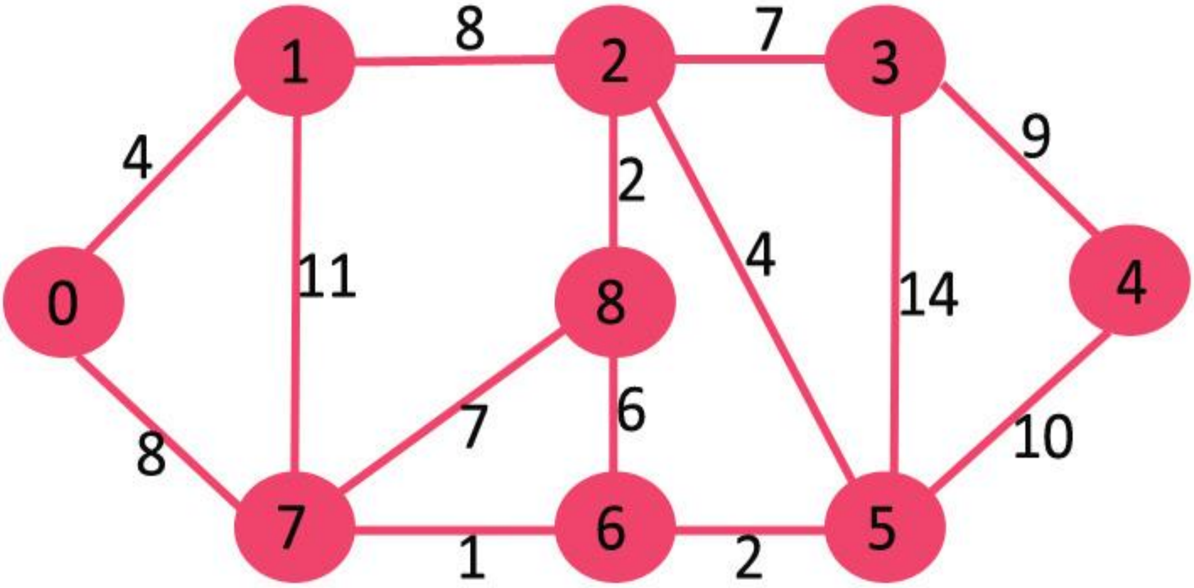
  Initializations :

- An array of distances **dist[]** of size **|V|** (number of nodes), where **dist[s] = 0** and **dist[u]** = ∞ (infinite), where u represents a node in the graph except s.
- An array, **Q**, containing all nodes in the graph. When the algorithm runs into completion, **Q** will become empty.
- An empty set, **S**, to which the visited nodes will be added. When the algorithm runs into completion, **S** will contain all the nodes in the graph.
- Repeat while **Q** is not empty −
  - Remove from **Q**, the node, **u** having the smallest **dist[u]** and which is not in **S**. In the first run, dist[s] is removed.
  - Add **u** to **S**, marking u as visited.
  - For each node **v** which is adjacent to **u**, update **dist[v]** as −
    - If **(dist[u] + weight of edge u-v)** < **dist[v]**, Then

– Update **dist[v] = dist[u] + weight of edge u-v**

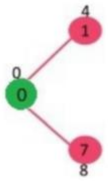
The array **dist[]** contains the shortest path from **s** to every other node.

Input: src = 0, the graph is shown below.

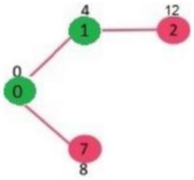


Output: 0 4 12 19 21 11 9 8 14

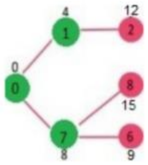
Step 1:



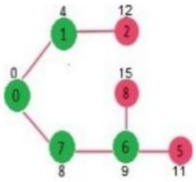
Step 2:



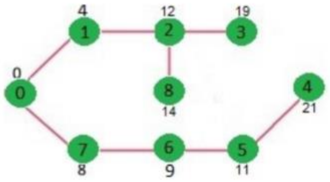
Step 3:



Step 4:



Step 5:



Output: *0 4 12 19 21 11 9 8 14*

Distance vector routing Algorithm

A router transmits its distance vector to each of its neighbors in a routing packet.

Each router receives and saves the most recently received distance vector from each of its neighbors.

A router recalculates its distance vector when:

- It receives a distance vector from a neighbor containing different information than before.
- It discovers that a link to a neighbor has gone down.

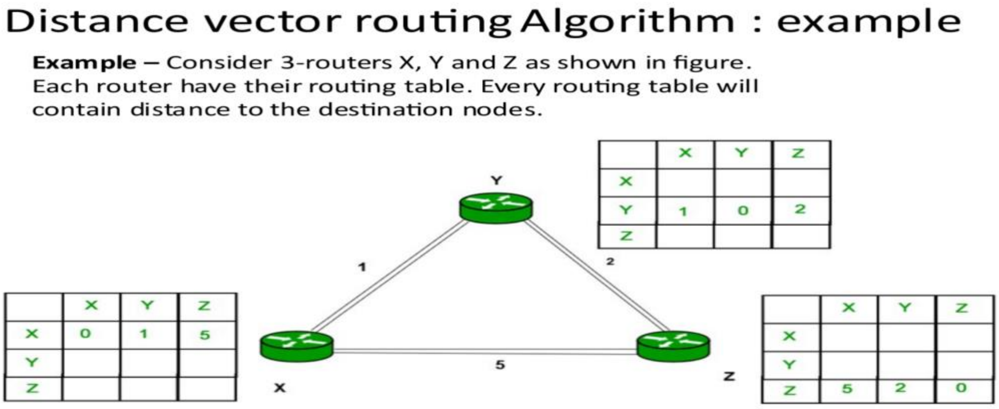
Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

Node x also maintains its neighbors' distance vectors

For each neighbor v, x maintains Dv = [Dv(y): y ∈ N



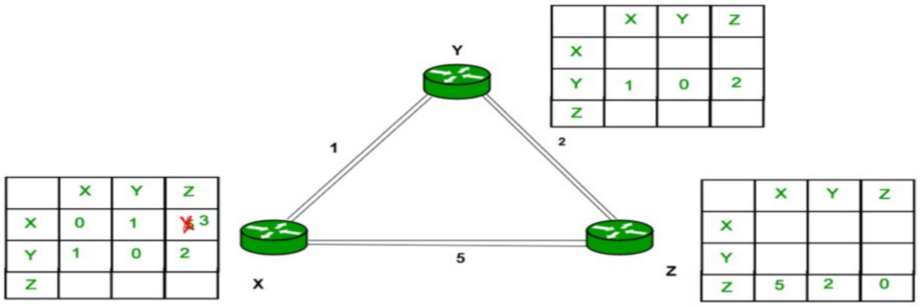
Distance vector routing Algorithm : example

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.

	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	5
Y			
Z			

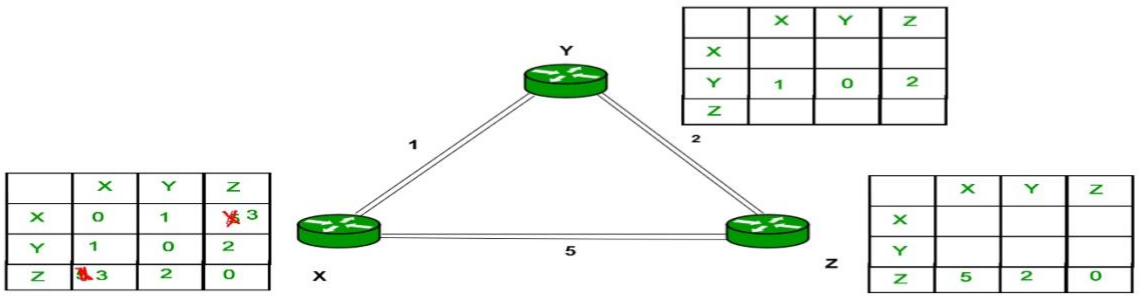
	X	Y	Z
X			
Y			
Z	5	2	0



	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

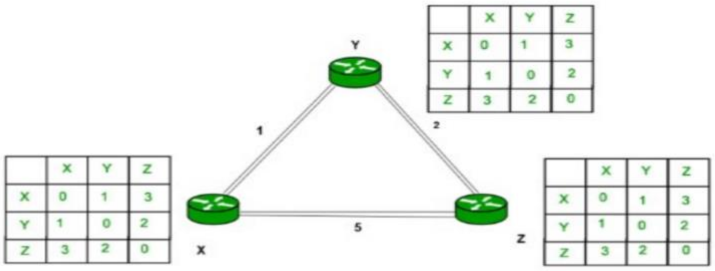
	X	Y	Z
X			
Y			
Z	5	2	0



	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z	~~5~~ 3	2	0

	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Advantages of Distance Vector routing

It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.