Shakuntala Krishna Institute Of Technology KD - 64

Subject : - Computer Network (BCA 5th)

Top – 15 Questions

1. ❖ Explain the components of data communication system with neat diagram.
2. ❖ What is Distributed Processing? Discuss its advantages and disadvantages.
3. ❖ Write short notes on Standards and Organizations in data communication (ISO, IEEE, ITU-T).
4. ❖ Explain different Line Configurations with diagram.
5. ❖ Compare different Network Topologies (Mesh topology,Star topology,Tree (Hierarchical) topology, Bus topology, Ring topology,Cellular topology) with advantages and disadvantages.
6. ❖ What are different Transmission Modes (Simplex, Half Duplex, Full Duplex)? Explain with examples.
7. ❖ Explain the categories of networks (LAN, MAN, WAN, PAN) with examples.
8. ❖ Explain the OSI reference model with diagram and functions of each layer.
9. ❖ Compare the OSI model and TCP/IP model in detail.
10. ❖ Compare various transmission media (Twisted Pair, Coaxial Cable, Optical Fiber, Radio Waves, Microwaves, Satellite).
11. ❖ What is multiplexing? Explain FDM, TDM, and WDM with diagrams.
12. ❖ Differentiate between Circuit Switching, Packet Switching, and Message Switching.
13. ❖ Explain Error Detection and Correction techniques with suitable examples.
14. ❖ Explain the Data Link Control Protocols: Line Discipline, Flow Control, and Error Control.
15. ❖ What is ISDN? Explain its services, subscriber’s access, layers, and historical outline.

Answer No. -1

Data communications

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components:

A data communications system has five components.

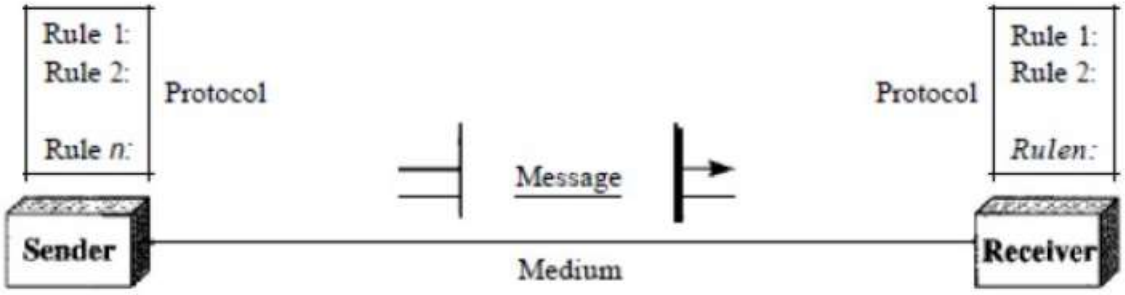
1. **Message-** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. **Sender-** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3**. Receiver-** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. **Transmission medium-** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5**. Protocol-** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.



Answer No. - 2

Distributed Processing

Distributed Processing refers to a model where different parts of a **data processing** task are executed simultaneously across multiple computing resources, usually in a networked environment. This model is employed to improve efficiency, performance, and reliability of data processing tasks. It's particularly beneficial in environments dealing with large-scale data processing and analytics.

"Distributed processing refers to dividing a large computing task into smaller sub-tasks and executing them on multiple computers connected in a network, instead of processing everything on a single computer."

Example: Modern services such as Google, Amazon, or banking systems use distributed processing for scalability and fault tolerance.

Advantages of Distributed Computing

1. Scalability: In distributed computing systems you can add more machines as your requirement.

2. Flexibility: It makes it easy to install, implement and debug new services.

3. Reliability: A system crash on one server does not affect other servers.

4. Fast Calculation Speed: A distributed computer system can have the computing power of multiple computers, making it faster than other systems.

5. Access Remote: Since it can be accessed both locally and remotely.

6. High performance: It compared to centralized computer network clusters, it can provide higher performance and better cost performance.

Disadvantages of Distributed Computing

1. Growing computing power at every data center.

2. Growing storage facility.

3. Under-consumption of the resources in various scattered data centers.

4. Rise in maintenance expenses of data centers.

Answer No. – 3

Standards and Organizations

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards .The purpose is that all data communications equipment manufacturers and users comply with these standards. The primary standards organizations for data communication are:

1. International Standard Organization (ISO) :- ISO is the international organization for standardization on a wide range of subjects. It is comprised mainly of members from the standards committee of various governments

throughout the world. It is even responsible for developing models which provides high level of system compatibility, quality enhancement, improved productivity and reduced costs. The ISO is also responsible for endorsing and coordinating the work of the other standards organizations.

2. International Telecommunications Union-Telecommunication Sector (ITU-T):- ITU-T is one of the four permanent parts of the International Telecommunications Union based in Geneva, Switzerland. It has developed three sets of specifications: the V series for modem interfacing and data transmission over telephone lines, the X series for data transmission over public digital networks, email and directory services; the I and Q series for Integrated Services Digital Network (ISDN) and its extension Broadband ISDN. ITU-T membership consists of government authorities and representatives from many countries and it is the present standards organization for the United Nations.

3. Institute of Electrical and Electronics Engineers (IEEE):- IEEE is an international professional organization founded in United States and is compromised of electronics, computer and communications engineers. It is currently the world's largest professional society with over 200,000 members. It develops communication and information processing

Answer No. – 4

Line Configurations

Line Configuration

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.

There are two possible line configurations.

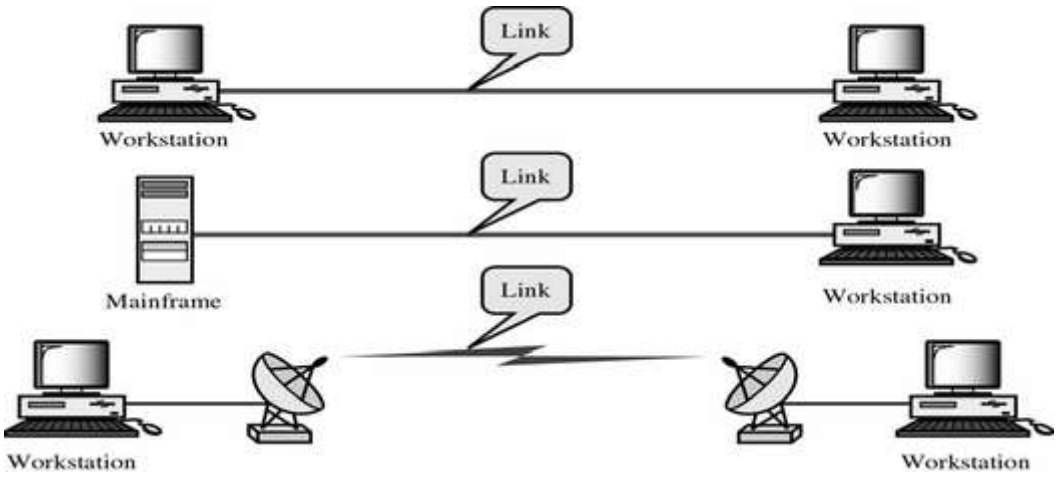
1. Point-to-Point.
2. Multipoint.

Point-to-Point

A **Point to Point Line Configuration** Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control & tvs remote control.

The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Point to point network topology is considered to be one of the easiest and most conventional network topologies. It is also the simplest to establish and understand. To visualize, one can consider point to point network topology as two phones connected end to end for a two way communication

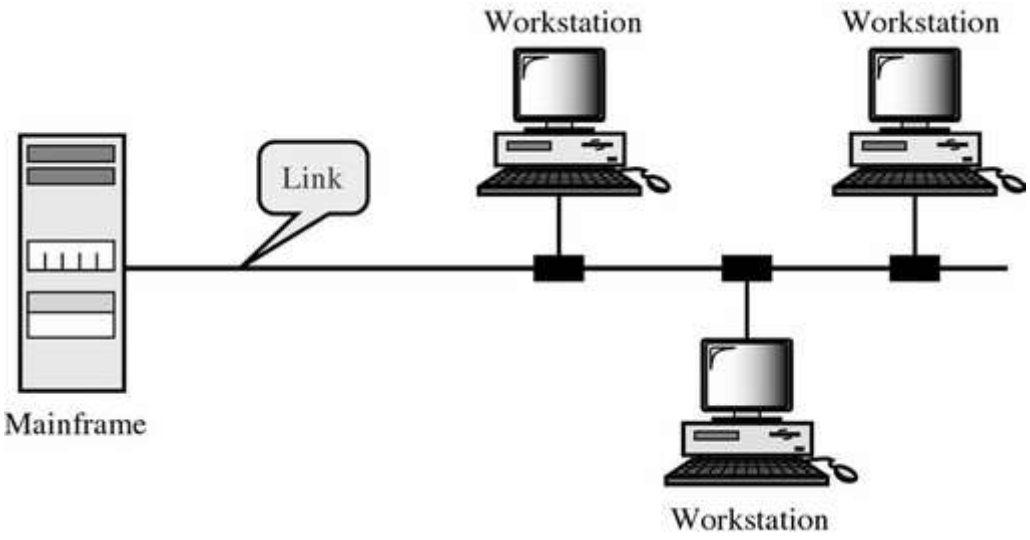


Multipoint Configuration

Multipoint Configuration also known as **Multidrop line configuration** one or more than two specific devices share a single link capacity of the channel is shared.

More than two devices share the Link that is the capacity of the channel is shared now. With shared capacity, there can be two possibilities in a Multipoint Line Config:

- **Spatial Sharing**: If several devices can share the link simultaneously, its called Spatially shared line configuration
- **Temporal (Time) Sharing**: If users must take turns using the link , then its called Temporally shared or Time Shared Line Configuration



Answer No.- 5

Network Topologies

The term "**Topology**" refers to the way in which the end points or stations/computer systems, attached to the networks, are interconnected. We have seen that a topology is essentially a stable geometric arrangement of computers in a network. If you want to select a topology for doing networking. You have attention to the following points.

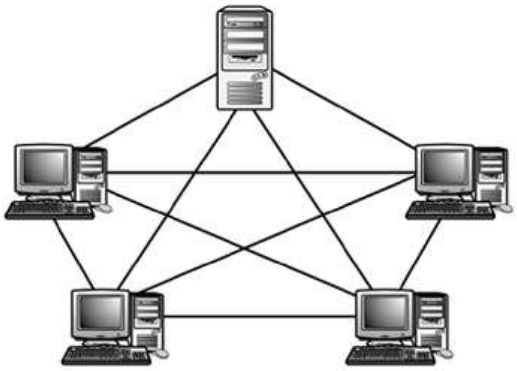
- Application S/W and protocols.
- Types of data communicating devices.
- Geographic scope of the network.
- Cost.
- Reliability.

Depending on the requirement there are different Topologies to construct a network.
(1) Mesh topology.
(2) Star topology.
(3) Tree (Hierarchical) topology.
(4) Bus topology.
(5) Ring topology.
(6) Cellular topology.

- Ring and mesh topologies are felt convenient for peer to peer transmission.
- Star and tree are more convenient for client server.
- Bus topology is equally convenient for either of them.

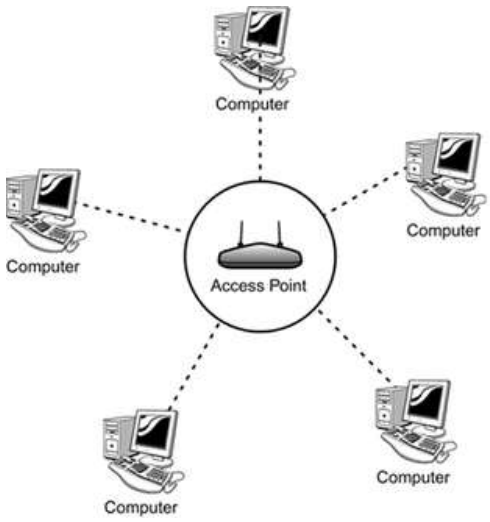
Mesh Topology

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by **Reed's Law**. The number of connections in a full mesh = n(n - 1) / 2



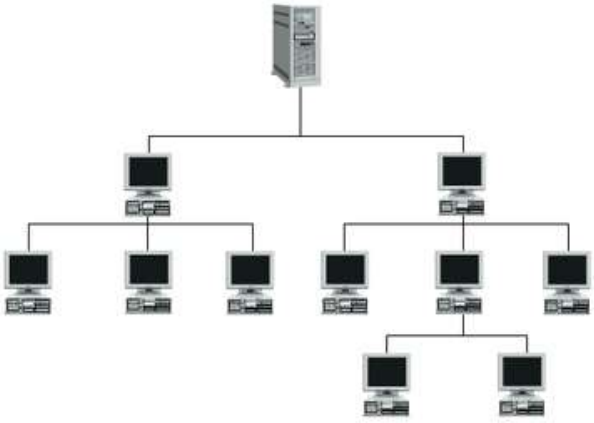
Star Topology

In a star topology, cables run from every computer to a centrally located device called a HUB. Star topology networks require a central point of connection between media segment. These central points are referred to as Hubs.
Hubs are special repeaters that overcome the electromechanical limitations of a media. Each computer on a star network communicates with a central hub that resends the message either to all the computers. (In a broadcast network) or only the destination
computer. (In a switched network).
Ethernet 10 base T is a popular network based on the star topology.



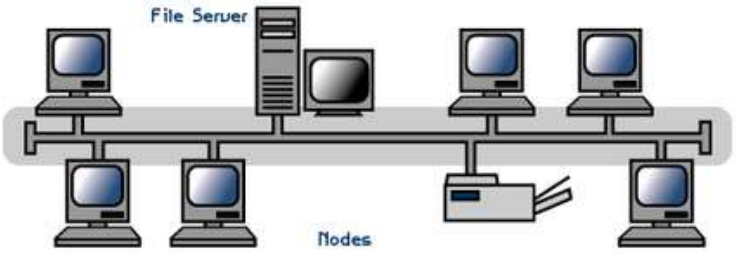
Tree (Hierarchical) topology

It is similar to the star network, but the nodes are connected to the secondary hub that in turn is connected to the central hub.
The central hub is the active hub.
The active hub contains the repeater, which regenerates the bits pattern it receives before sending them out.
The secondary hub can be either active or passive.
A passive hub provides a simple physical connection between the attached devices.



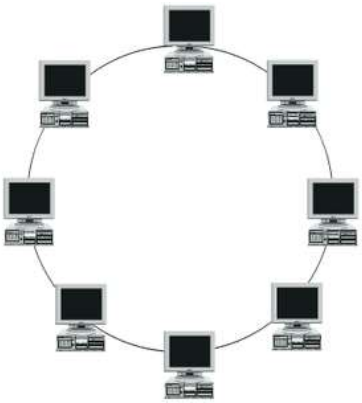
Bus topology

A bus topology connects computers along a single or more cable to connect linearly. A network that uses a bus topology is referred to as a "bus network" which was the original form of Ethernet networks. Ethernet 10Base2 (also known as thinnet) is used for bus topology.



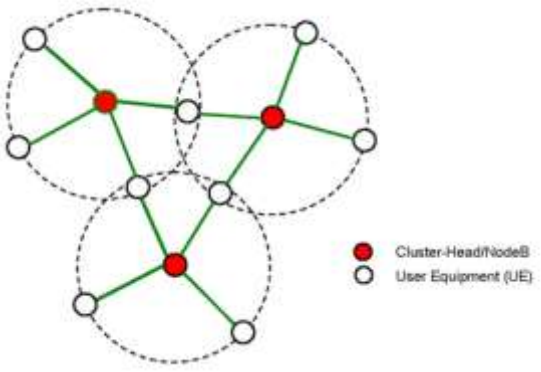
Ring topology

In ring topology, each device has a dedicated point-to-point line configuration only with two devices on either side of it.
A signal is passed along the ring in one direction, from device to device until it reaches its destination.
Each device in the ring has a repeater. When the devices receive the signal intended for the other node, it just regenerates the bits and passes them along.
Ring network passes a token.
A token is a short message with the electronic address of the receiver.
Each network interface card is given a unique electronic address, which is used to identify the computer on the network.



Cellular topology

The cellular topology is applicable only in case of wireless media that does not require cable connection.
In wireless media, each point transmits in a certain geographical area called a cell.
Each cell represents a portion of the total network area.
Devices that are in the cell communicate through a central hub. Hubs in different cells are interconnected. They route data across the network and provide a complete network infrastructure.
The data is transmitted in the cellular digital packet data (CDPD) format.



Advantages:

- Easy to install and connect new devices.
- Requires less cable length compared to other topologies.
- Cost-effective for small networks.

Disadvantages:

- Entire network fails if the backbone cable breaks.
- Performance degrades as more devices are added.
- Troubleshooting is difficult.
- Limited cable length and number of nodes.

Answer No. – 6

Transmission Modes

Transmission Mode

A given transmission on a communications channel between two machines can occur in several different ways. The transmission is characterized by:

- the direction of the exchanges
- the transmission mode: the number of bits sent simultaneously
- synchronization between the transmitter and receiver

Types of Transmission mode

- Simplex
- Half Duplex
- Full Duplex

Simplex

A simplex connection is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer...).

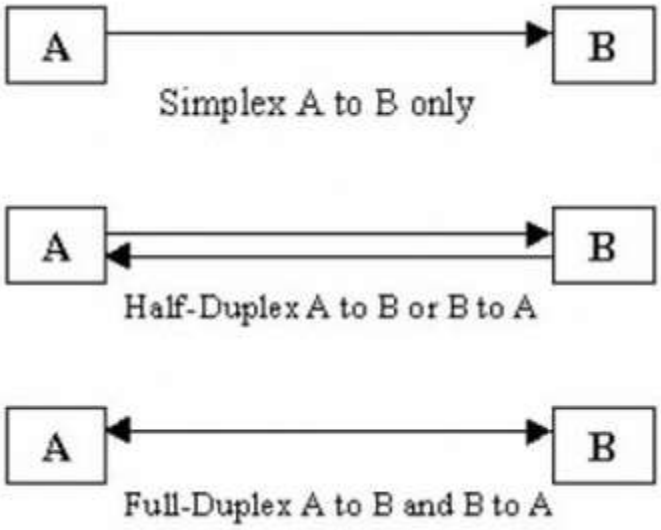
Half Duplex

A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. With this type of connection, each end of

the connection transmits in turn. This type of connection makes it possible to have bidirectional communications using the full capacity of the line.

Full Duplex

A full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission.



Answer No. – 7

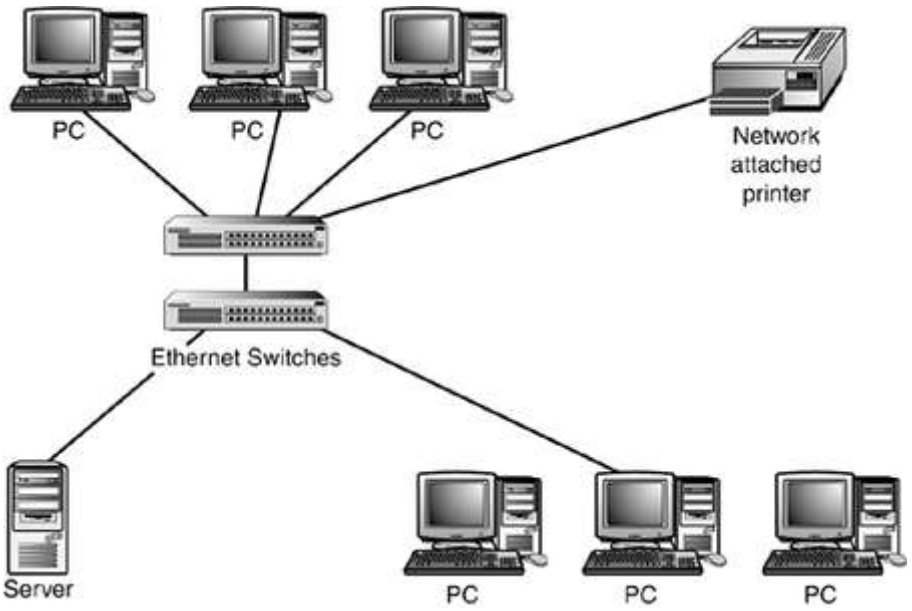
Networks

One way to categorize the different types of computer network designs is by their scope or scale. For historical reasons, the networking industry refers to nearly every type of design as some kind of *area network*. Common examples of area network types are:

- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network

Local Area Network

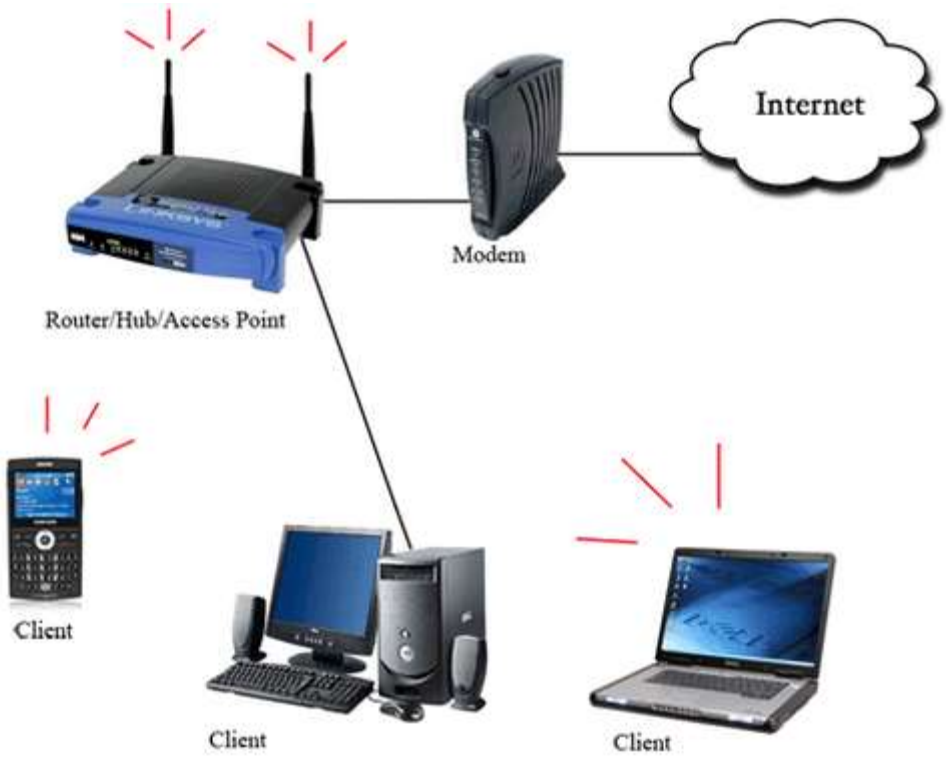
A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet. In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization. They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.



Wireless Local Area Network

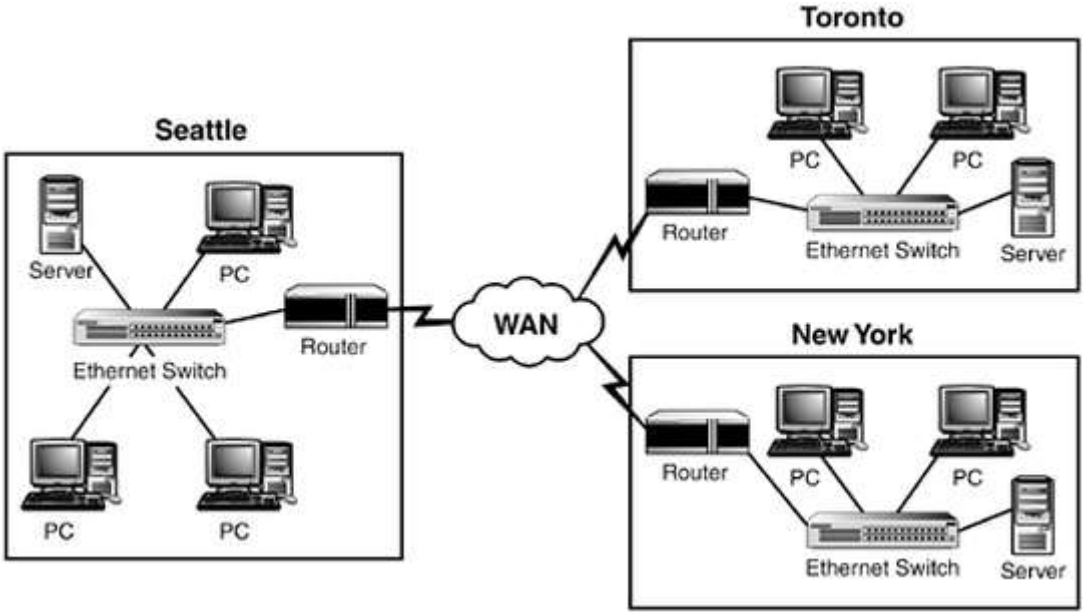
As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.



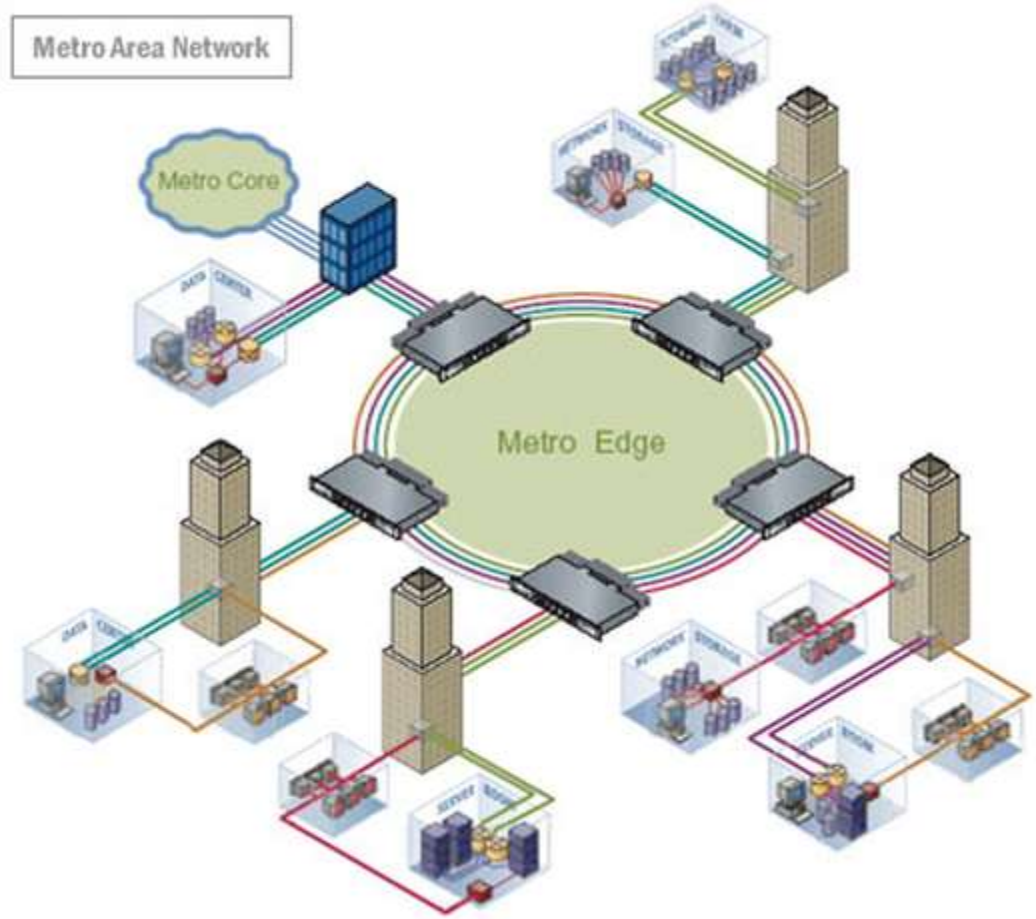
Wide Area Network

A WAN is a network that spans more than one geographical location often connecting separated LANs. WANs are slower than LANs and often require additional and costly hardware such as routers, dedicated leased lines, and complicated implementation procedures.



Metropolitan Area Network

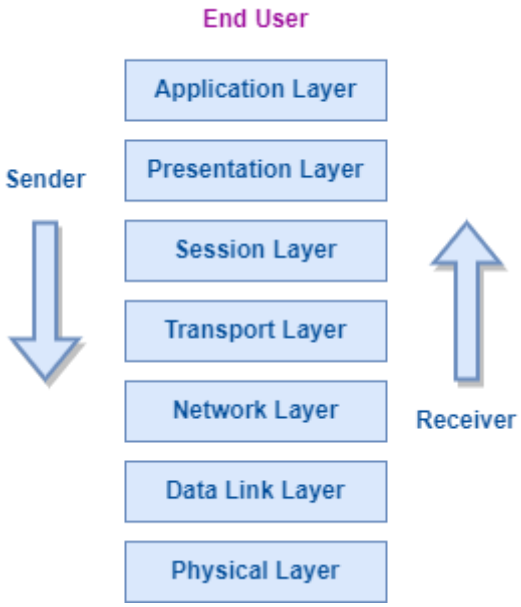
A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned an operated by a single entity such as a government body or large corporation.



Answer No. –8

OSI reference model

The Open Systems Interconnection model (OSI model) is a conceptual model that describes how data is transmitted from one system to another system irrespective of distance and location. It consists of seven-layer architecture. All seven layers contribute to the transmission of data from one system to another system. All the seven layers are shown in the diagram below.



1. Physical Layer - The Physical Layer is the lowest layer of the OSI model. It is responsible for transmitting individual bits from over a medium. It converts the bits into signals. The bit rate or data rate control is done at the physical layer. It is also responsible for how the actual physical devices are connected.

Some of the functionalities of the physical layer are:

- **Physical topology** - It defines the arrangement of the devices in a network.
- **Data rate** - Data rate or the number of bits sent per second is controlled by the physical layer.
- **Transmission mode** - It is the data flow between two devices. It is of three types.

1. Simplex - Data flows in one direction only.
2. Half-duplex - Data flows in both directions but not at the same time.
3. Full-duplex - Data flows in both directions at the same time.

2. Data Link Layer -The data link layer acts as a link between two nodes and transfers data or frames from one node to another node. Frames are created by the data link layer. It is the responsibility of the data link layer to transfer the error-free data from one node to another node.

It is divided into two sub-layers.

1. **Media Access Control (MAC**) - It is responsible for controlling devices' access to a medium.
2. **Logical Link Control (LLC)** - It is responsible for frame synchronization, identification of network layer protocol, and error control.

Some of the functionalities of the data link layer are:

- **Framing -** The data in the form of bits are grouped in packets called frames. Frames are made identifiable to the receiver by attaching special bit patterns as the header or trailer of the frame.
- **Physical Addressing -** The data link layer adds the MAC address (physical address) of the sender and the receiver for the smooth transmission of the data.
- **Flow Control -** Flow control is necessary for saving the data from being corrupted. It is done by maintaining the constant data rate on both sender and receiver ends.
- **Error Control -** This is the function of the data link layer to transfer the non-erroneous data. The erroneous data are traced and retransmitted by the data link layer.
- **Access Control** - The data link layer helps to determine which device has control over a link shared by multiple devices.

3. Network Layer - The Network Layer is responsible for transferring the data from the source to the destination by routing it through the intermediate nodes. Among the different possible paths, it chooses the best possible path to transfer the data from source to destination.

Some of the functionalities of the network layer are:

- **Packetizing** - If the message to be is large to be transmitted, it is split into several fragments and then delivered independently and reassembled at the destination node.
- **Logical Addressing** - The network layer adds the IP address of the source and destination to the header of the frames for its identification among all the devices.
- **Routing** - The best possible path is chosen by the network layer for the transfer of the data from source to destination and this is called routing.

4. Transport Layer - The transport layer creates various smaller units called segments out of the message received from the application layer. It adds source and destination port numbers in the header for the right transfer of the data. The main responsibility of the transport layer is the end-to-end delivery of the message and to ensure flow and error control.

Some of the functionalities of the transport layer are:

- **Segmentation** - The message received from the upper layer is divided into smaller units called segments and is reassembled at the destination by the transport layer.
- **Port Addressing** - The source and destination port numbers are added to the header for the correct handover of the data.
- **Connection Control** - There can be two types of services between two devices

1. Connection-Oriented - In this, the connection is established for the data transmission and is disconnected after the transmission.
2. Connectionless - It is less reliable and faster and doesn't require establishing a connection before data transmission.

- **Error Control** - It checks for erroneous data and retransmits the data on a failed delivery.

5. Session Layer - The main responsibility of the session layer is to establish, maintain and synchronize the communication among the devices. It allows communication either in half-duplex or full-duplex. It synchronizes the communication between the devices to avoid data loss.

Some of the functionalities of the session layer are:

- **Dialog Control** - It allows communication between two systems in half-duplex or full-duplex.
- **Synchronization** - It allows a process to add checkpoints to avoid data loss during a crash.

6. Presentation Layer - The presentation layer establishes context between application layer entities. The main responsibility of the presentation layer is concerning the syntax and semantics of the data exchange between the devices. It transforms data into the form that the application accepts. It is also sometimes called the syntax layer.

Some of the functionalities of the presentation layer are:

- **Translation** - It is the conversion of the data into a commonly acceptable format.
- **Encryption** - Encryption is done to secure the data from unauthorized access. The data is converted into a different code that is not understandable and is decrypted into an understandable form at the receiver's end.
- **Compression** - Compression means compressing the data that is reducing the number of bits that need to be transmitted. It is helpful in the transfer of multimedia messages.

7. Application Layer - This is the closest layer to the end-user. It interacts directly with the software application. It acts as a window for the user and the software applications to access network services. It handles identifying communication partners and determining resource availability.

Some of the functionalities of the application layer are:

- **File transfer and access management** - This allows the user to access the files on a remote computer.
- **Mail services** - It provides access to send or receive email.

Answer No. –9

OSI vs TCP/IP Model

The main difference between OSI and TCP/IP Model is that OSI model has seven layers, while TCP/IP has four and OSI is protocol-independent, whereas TCP/IP is tied to its protocols. Here are some other important differences:

- **Structure**: OSI has 7 well-defined layers with specific functions, offering a clear roadmap for network communication. TCP/IP has a simpler 4-layer structure, combining functionalities for a more practical approach.
- **Purpose**: OSI is a conceptual framework, a blueprint for how networking should work on the other hand, TCP/IP is a working protocol suite, the actual set of rules devices use to communicate on the internet.
- **Implementation**: OSI is not tied to specific protocols, making it adaptable but not directly usable while TCP/IP defines the protocols used on the internet today, making it practical but less flexible for alternative implementations.

Now, let’s move on to understand the OSI model of computer networking in detail.

What is OSI Model?

OSI stands for Open System Interconnection. The OSI Model was developed by (ISO) International Standard organization to help standardize communication between computers.

The original objective behind the OSI model of computer networking was to make communication possible between two different vendors. Because, when the internet was growing at the beginning of the time, different vendors could not communicate with each other and, OSI Model came as the standard model for discussing, teaching, and learning the networking procedures in the field of Information technology.

So, the OSI model was developed, but it was never implemented and remained as just a reference model for study purposes only.

There are 7 layers in OSI Model.

OSI Model Layers

1. **Layer 1 – Physical Layer:** This layer handles data transmission through cables, radio waves, etc.
2. **Layer 2 – Data Link Layer:** This layer makes sure the data transfer between adjacent nodes is error-free.
3. **Layer 3 – Network Layer:** This layer is responsible for routing data packets between different networks.
4. **Layer 4 – Transport Layer:** It makes sure the data is transferred with protocols like TCP and UDP.
5. **Layer 5 – Session Layer:** It manages sessions and connections between network devices.
6. **Layer 6 – Presentation Layer:** This layer handles data formatting, encryption, and compression.
7. **Layer 7 – Application Layer:** This layer supports application services like email and browsing.

These are seven of the OSI Model Layers.

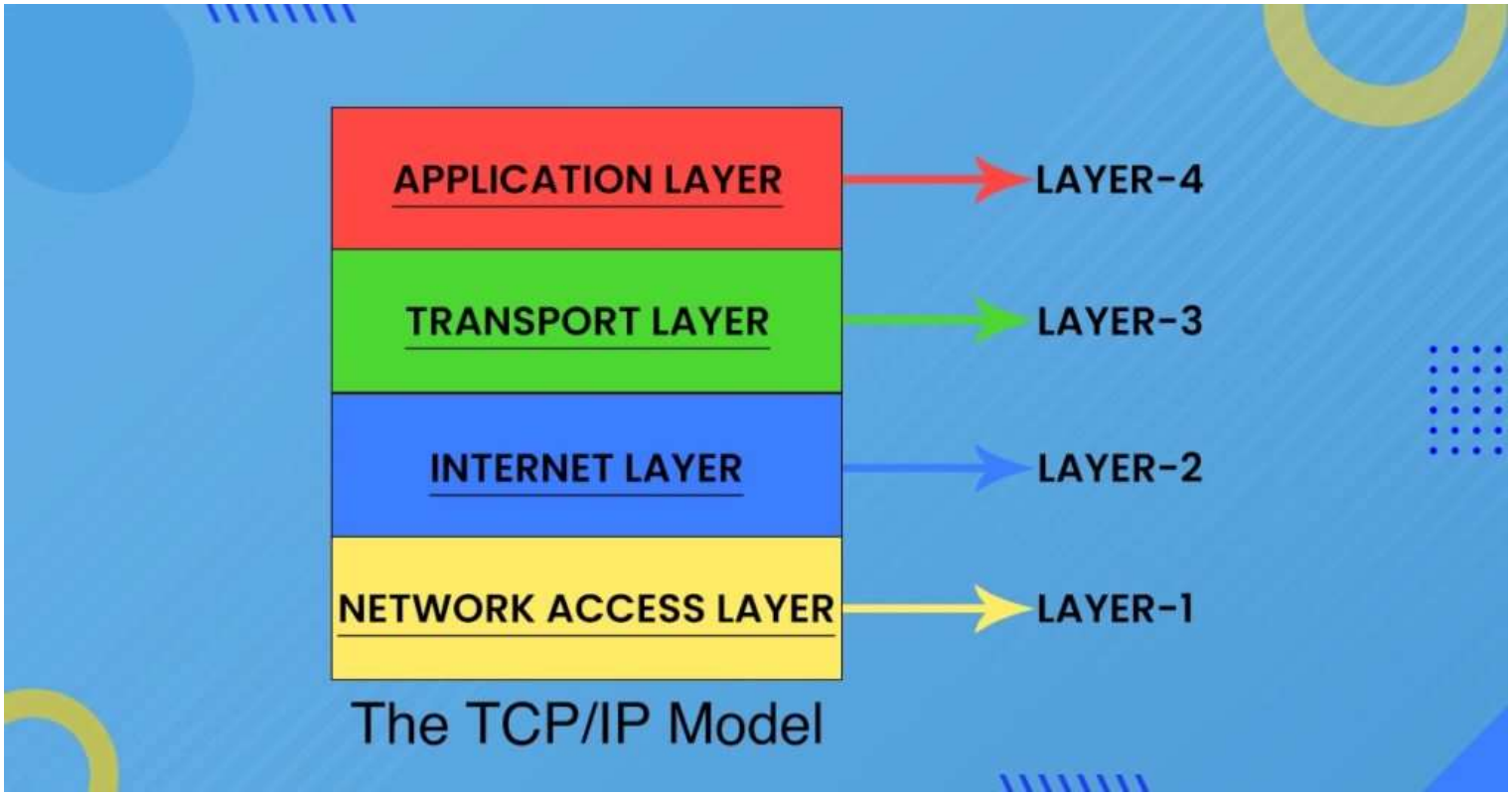
What is TCP/IP Model?

The TCP/IP Model in Computer Network was **designed by the Department of Defense (DOD),** and it is based on standard protocols.

The TCP/IP model is also known as IP Stack, and this model is practically being implemented. This model is a widely adopted model due to its simplicity, and it is also known as the concise version of OSI model.

TCP Layers

As compared to OSI Model, there are 4 TCP layers which are:



- **Layer 1 – Network Interface:** This layer combines the Physical and Data Link layers of the OSI Model for hardware communication.
- **Layer 2 – Internet Layer:** It focuses on addressing and routing via IP.
- **Layer 3 – Transport Layer:** This layer is responsible for reliable data delivery, and it does that with the help of protocols like TCP.
- **Layer 4 – Application Layer:** This layer is a combination of the top three layers of OSI Model and handles user interaction.

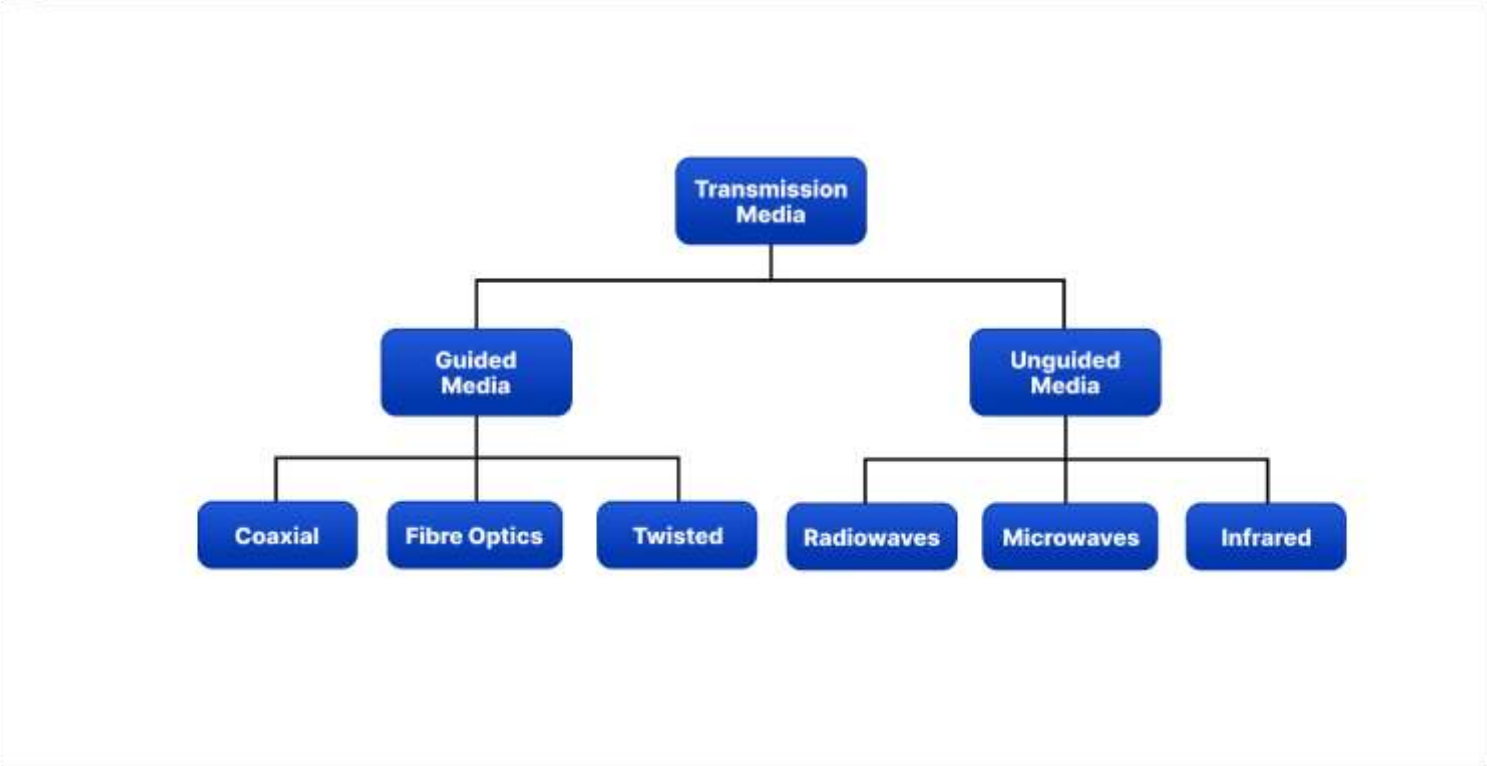
So, there are 7 layers in the OSI Model whereas in TCP/IP, we only have 4 layers.

Answer No. – 10

Transmission Media

Compare various transmission media (Twisted Pair, Coaxial Cable, Optical Fiber, Radio Waves, Microwaves, Satellite).

Types of Transmission Media



Transmission Media can be categorized into two types:

1. Guided Media
2. Unguided Media

Guided Media

Guided media or wires or bounded transmission media are those in which the signals are transmitted through physical wiring connections that indicate the route of the signals. These media are essential for data transfers that are reliable, fast, and safe in computer networks.

1. Twisted Pair Cable

Twisted pair cable represents one of the widely used types of guided media. The pairs of wires are insulated and are twisted together so that the electromagnetic interference and crosstalk are minimized. The twisting greatly boosts signal purity, especially in electrically noisy surroundings. There are two main types:

- **Unshielded Twisted Pair (UTP):** Found in LANs and telephone networks; it is very easy to install and is quite cheap.
- **Shielded Twisted Pair (STP):** A copper braid covering or a foil shield surrounding the insulated wires are the two ways in which the shielded twisted pair offers additional shielding against the interference.

2. Coaxial Cable

A coaxial cable is made up of a central copper conductor, PVC insulation, a metal shield (typically a copper braid covering), and a protective plastic sheath on the outside. This design results in high resistance to EM

interference, thus coaxial cables are extremely common in cable TV, broadband, and other data transmission applications.

3. Optical Fiber Cable

Optical fiber cable or simply fiber optic cable is made of thin glass or plastic fibers through which data is sent in the form of light pulses. The core, which is the light carrier, is protected by the cladding and the other layers which are the protective layers. The principle of offering extremely high bandwidth, low signal loss, and immunity to electromagnetic interference, is the reason why optical fiber cables are placed in long-distance and high-speed data transmission.

4. Stripline

Stripline is a planar type of transmission used for high-frequency and microwave circuits. It consists of a conductive strip in the middle and two ground planes, which are placed on the sides. The space between the ground and the conducting strip is filled with a dielectric material. This configuration ensures that the product is well protected from electromagnetic interference. Printed circuit boards (PCBs) often use this way of routing signals.

5. Microstripline

Microstripline is yet another planar transmission line that finds wide use in microwave and radio frequency circuits. It involves a thin conducting line that is laid on top of the dielectric substrate and a ground plane is located at the opposite side. The main factors that have caused microstriplines to be very popular in the world of communication are the convenience that is gained during the fabrication process as well as the integration of communication devices into the PCBs.

Unguided Media

Unguided media also known as unbound transmission media refers to communication methods that do not use a physical conductor.

1. Radio Waves

Radio waves in computer networks are a form of electromagnetic radiation with longer wavelengths in the electromagnetic spectrum than infrared light. Radio waves are used for wireless communication over many distances, e.g., AM and FM radio broadcasts, TV signals, and cell networks.

2. MicroWaves

Microwaves are electromagnetic waves in the range 1 GHz to 300 GHz. They are applied in high-frequency communication, such as satellite communication and point-to-point microwave links. Applied in radar engineering and some wireless networking.

3. Infrared

Infrared transmission in computer networks uses infrared radiation to transmit information wirelessly. It works in a range of 700 nm to 1 mm. Some prominent applications are remote control, short-range wireless data transfer (e.g., some printers), and infrared data association (IrDA) for device networking.

Answer No. – 11

Multiplexing

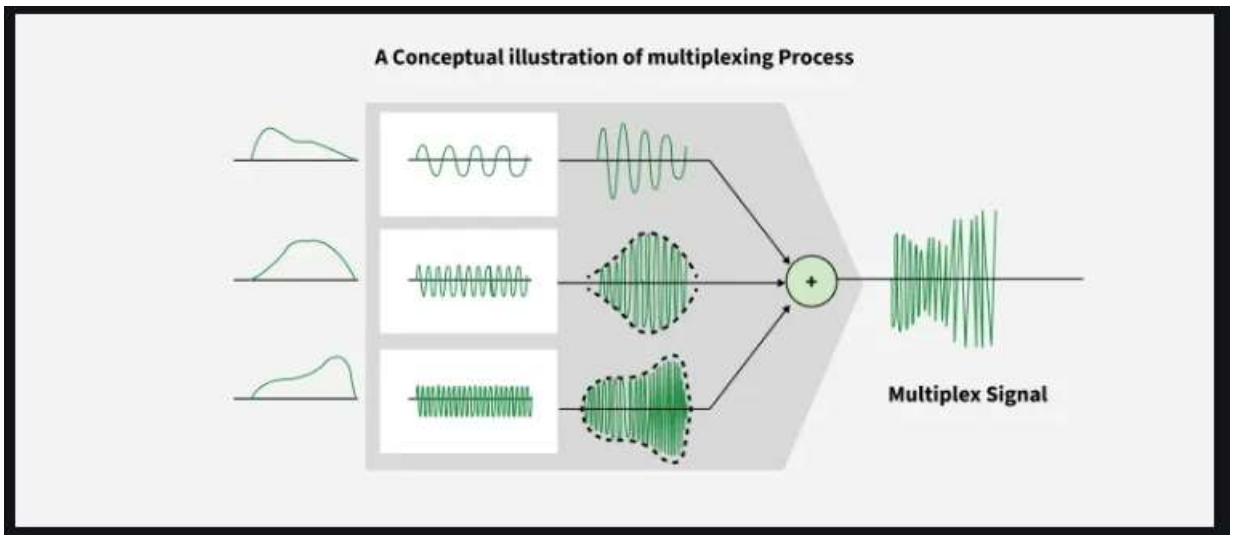
Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. In a multiplexed system, n lines share the bandwidth of one link. The lines direct their transmission streams to a multiplexer (MUX), which combines them into a single stream .

- TDM uses a shared channel to transmit two or more digital or analog signals. It can be used when the transmission media's bit rate exceeds that of the signal to be delivered. Simply divide the available bandwidth into channels, each with a specified bandwidth.
- FDM allows independent signals to use the same transmission channel, such as a cable or optical fiber.
- WDM uses many lasers, each generating a unique color of light, to transfer data over a single fiber optic line.

FDM(Frequency Division Multiplexing)

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies.

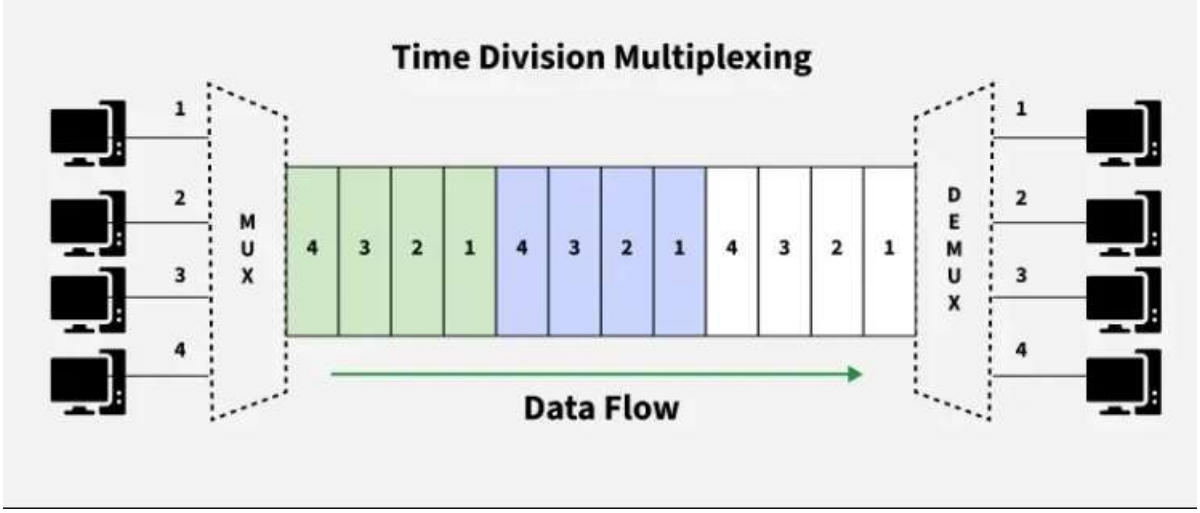
These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel.



TDM(Time Division Multiplexing)

TDM (Time Division Multiplexing) is a multiplexing technology and has low conflict. It works with both digital and analog signals. TDM shares the timeframe of the multiple signals. TDM and synchronous time division multiplexing (sync TDM).

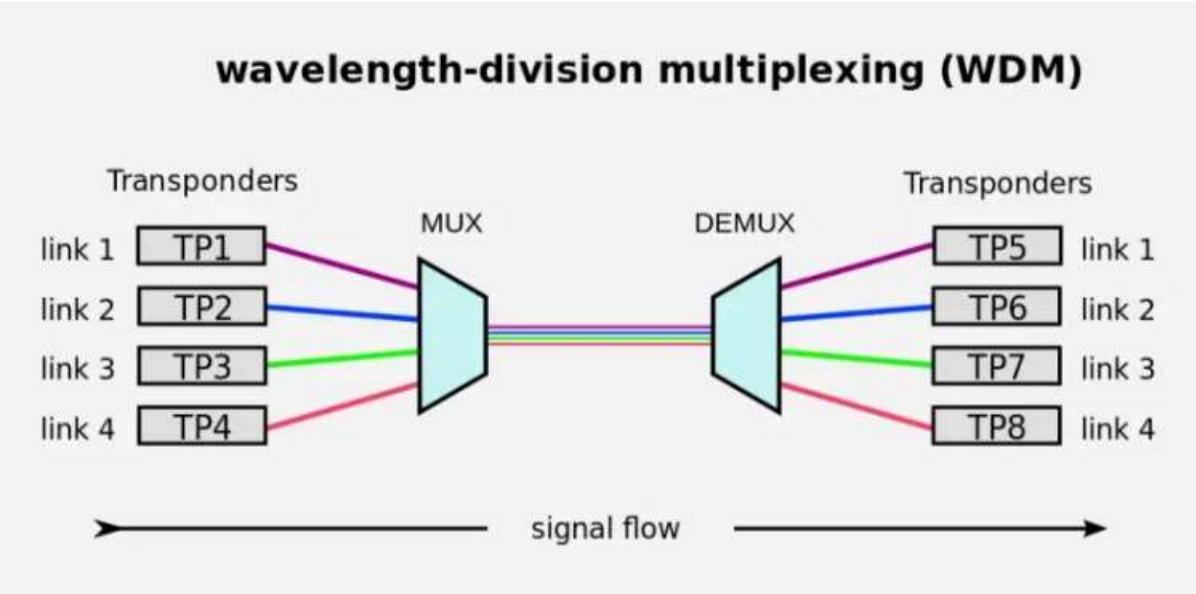
TDM is utilized for long-distance communication networks and can handle high data traffic demands from end users. TDM splits the available time on the channel into discrete time slots, each allocated to a distinct signal or data stream.



WDM(Wavelength Division Multiplexing)

WDM (Wavelength Division Multiplexing) is generally utilized for multiplexing numerous optical carrier signals into a single optical fiber channel. WDM permits communication in both directions via the fiber connection.

Two or more colors of light can flow through a single fiber, and an optical waveguide can transport multiple signals at different wavelengths or frequencies on the optical spectrum.



Answer No. – 12

Circuit Switching, Packet Switching, and Message Switching

Circuit Switching

In this approach, there is a dedicated route between sender and receiver. Before the link is determined in the circuit switching approach, the dedicated route will continue until the connection is eliminated.

Message Switching

Message Switching is an approach in which a message is sent as a whole unit and routed by the intermediate hub at which it is saved and delivered. There is no installation of a dedicated route between the sender and receiver in the message switching approach.

The destination location is added to the message. It supports flexible routing as the message is routed by the intermediate hub based on its data.

Packet Switching

Packet switching is a switching approach in which the message is transmitted in one go, but it is split into the lower item, and they are sent separately. The message divided into lower elements are called packets, and these packets are provided with a specific number to recognize their series at the receiving end.

Data is sent in various units of variable length of structures which are known as packets in a packet-switched network. Each packet includes some data in its headers, including source address, destination address and order number.

Basics	Circuit Switching	Message Switching	Packet Switching
Connection Creation	Connection is created between the source and destination by establishing a dedicated path between source and destination.	Links are created independently one by one between the nodes on the way.	Links are created independently one by one between the nodes on the way.
Queuing	No queue is formed.	Queue is formed.	Queue is formed.
Message and Packets	There is one big entire data stream called a message.	There is one big entire data stream called a message.	The big message is divided into a small number of packets.
Routing	One single dedicated path exists between the source and destination.	Messages follow the independent route to reach a destination.	Packets follow the independent path to hold the destination.
Addressing and sequencing	Messages need not be addressed as there is one dedicated path.	Messages are addressed as independent routes are established.	Packets are addressed, and sequencing is done as all the packets

Basics	Circuit Switching	Message Switching	Packet Switching
			follow the independent route.
Propagation Delay	No	Yes	Yes
Transmission Capacity	Low	Maximum	Maximum
Sequence Order	Message arrives in Sequence.	Message arrives in Sequence.	Packets do not appear in sequence at the destination.
Use Bandwidth	Wastage	Bandwidth is used to its maximum extent.	Bandwidth is used to its maximum extent.

Answer No. – 13

Error Detection Techniques:

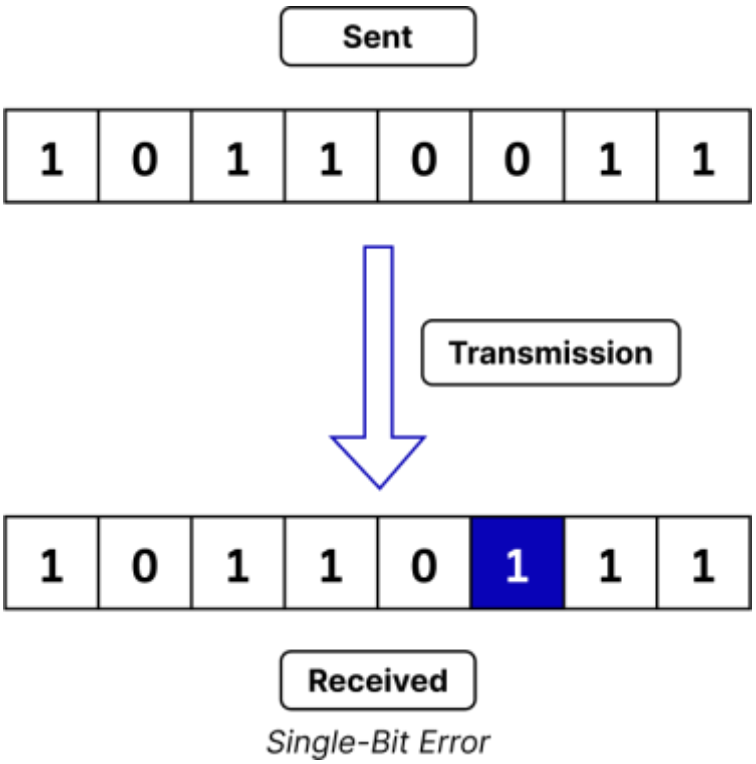
Error correction is the method that is used to figure out and fix errors in data communications or storage that have not been sent again. The procedure is extremely important for the maintenance of data correctness, mostly in places where it is difficult or expensive to send the data again. It also provides the receiver with the capability to find and correct errors that might have occurred during transmission. Turning on error correction makes the systems of digital communication more dependable, which means that the data that are received can be trusted and are accurate.

On the other hand, error detection refers to the methods and techniques used to identify errors that may occur during the transmission or storage of data. The primary goal is to ensure that the data received matches what was originally sent. Error detection identifies the presence of errors, it plays an important role in maintaining data integrity in communication systems

Types of Errors in Computer Networks

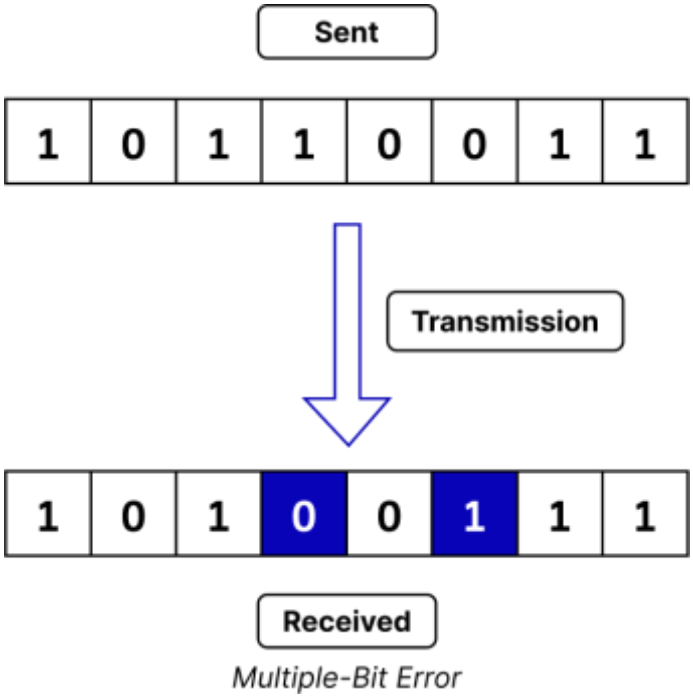
Here are the types of errors in computer networks

1. Single-Bit Error: This type of error occurs when one bit of a transmitted data unit is altered, leading to corrupted data.



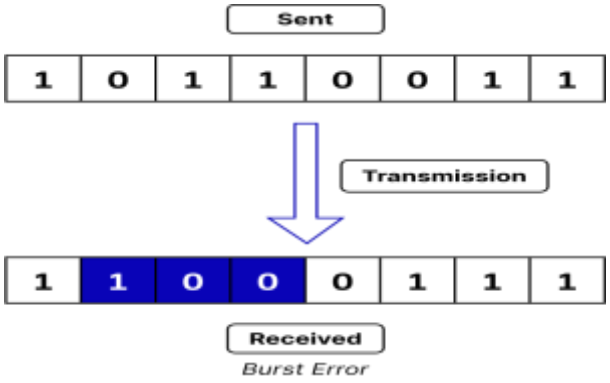
Single-Bit Error

2. Multiple-Bit Error: This type of error occurs when more than one bit is affected. While rarer than single-bit errors, they can occur in high-noise environments.



Multiple-Bit Error

3. Burst Error: This type of error occurs when a sequence of consecutive bits is flipped, resulting in several adjacent bits being incorrect.

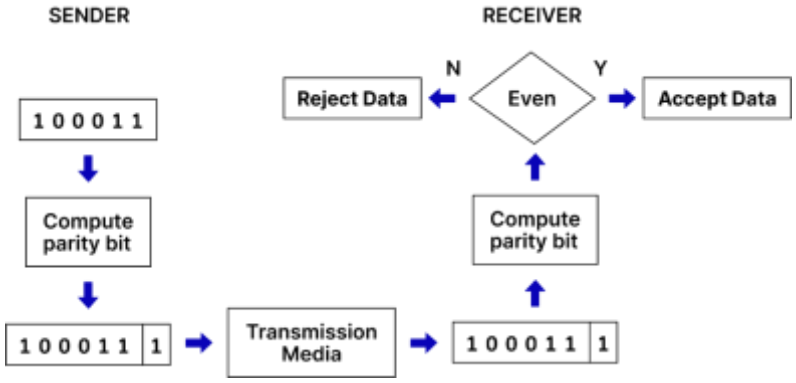


Burst Error

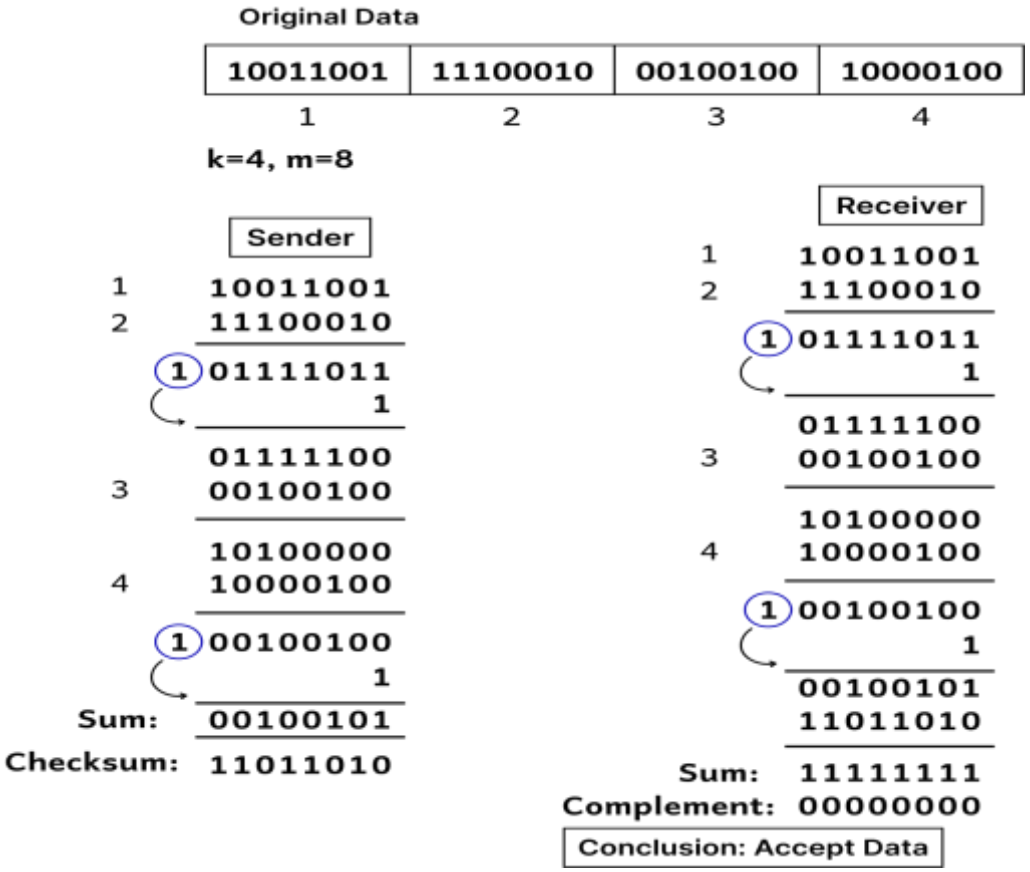
Error Detection Techniques

Error detection techniques are essential in data transmission and storage to ensure data integrity. Here are some common methods:

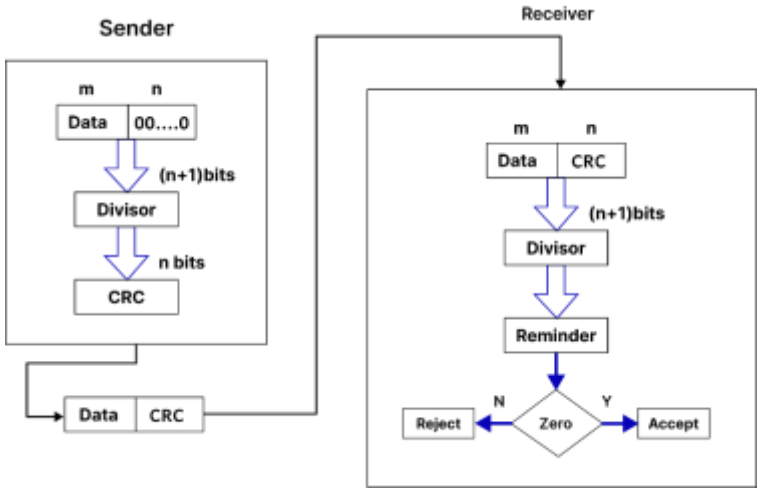
1. Parity Bits: A simple method that adds a single bit to data to ensure the total number of 1s is even (even parity) or odd (odd parity).



2. Checksums: A mathematical sum of data values calculated before transmission and verified at the destination. If the checksum doesn't match, an error is detected.



3. Cyclic Redundancy Check (CRC): A more robust method that uses polynomial division to detect changes to raw data. CRCs are widely used in network communications and file storage.



4. Checksums with Hash Functions: The advanced checksum methods implement hash functions that are of cryptographic nature, such as SHA-256, to be the ultimate guards of data integrity, especially those that are in secure communications.

Types of Error Correction

Here are the types of error correction in computer networks:

1. Backward Error Correction

If the receiver finds an error, they ask the sender to resend the entire data unit.

It's mainly used in cases where the integrity of the data is at stake and retransmission is possible, such as file transfers.

2. Forward Error Correction (FEC)

The receiver without the help of the sender, fixes the errors inside the device by means of error-correcting codes and no retransmission is done. The method is used in real-time communication (such as voice-over IP, video streaming) where retransmission is not possible.

Error Correction Techniques

Following are the error correction techniques of computer networks:

1. Single-bit Error Detection

One extra bit can detect the errors but not correct them.

2. Hamming Code

R.W. Hamming invented it, it detects and corrects single-bit errors by adding redundant bits.

3. Parity Bits

Parity bits are appended to binary data such that the total count of 1s is even or odd.

Even Parity

- When the total count of 1s is even, the parity bit is 0.
- When the total count of 1s is odd, the parity bit is 1.

Odd Parity

- When the total count of 1s is even, the parity bit is 1.
- If the count of 1s is odd, then the parity bit would be 0.

Answer No. – 14

Data Link Control Protocols:-

Data link control protocols coordinate communication over a data link through three main functions: Line Discipline manages which device can transmit to avoid collisions, typically using poll/select or ENQ/ACK methods. Flow Control prevents a fast sender from overwhelming a slow receiver by regulating the data rate, using techniques like stop-and-wait and sliding window protocols. Error Control ensures data integrity by detecting and correcting (retransmitting) corrupted or lost frames, primarily using methods like Automatic Repeat Request (ARQ).

Here's a more detailed explanation of each component:

1. Line Discipline

- **Purpose**:

To coordinate the transmission between devices on a shared data link, especially in half-duplex environments where simultaneous transmission by two devices would cause a collision.

- **Methods**:
  - **ENQ/ACK (Enquiry/Acknowledgement)**: A sender uses an enquiry frame (ENQ) to request permission to send data and waits for an acknowledgment (ACK) from the receiver before starting transmission.
  - **Poll/Select**: A primary station (or controller) controls the communication, either by polling (asking) secondary stations if they have data to send (poll) or by sending data to a specific secondary station (select).

2. Flow Control

- **Purpose**:

To manage the rate of data transmission so that the sender doesn't send data faster than the receiver can process and store it. Receivers have limited buffer space and processing speed, which can lead to data loss if overwhelmed.

- **Methods**:
  - **Stop-and-Wait**: The sender transmits one frame and then waits for an acknowledgment from the receiver before sending the next frame. This is simple but can be inefficient.
  - **Sliding Window**: The sender can transmit multiple frames (a "window" of frames) before requiring an acknowledgment. The window size is agreed upon by the sender and receiver. This improves efficiency and throughput compared to stop-and-wait.

3. Error Control

- **Purpose**:

To detect and correct or retransmit data frames that are lost or corrupted during transmission over the physical medium.

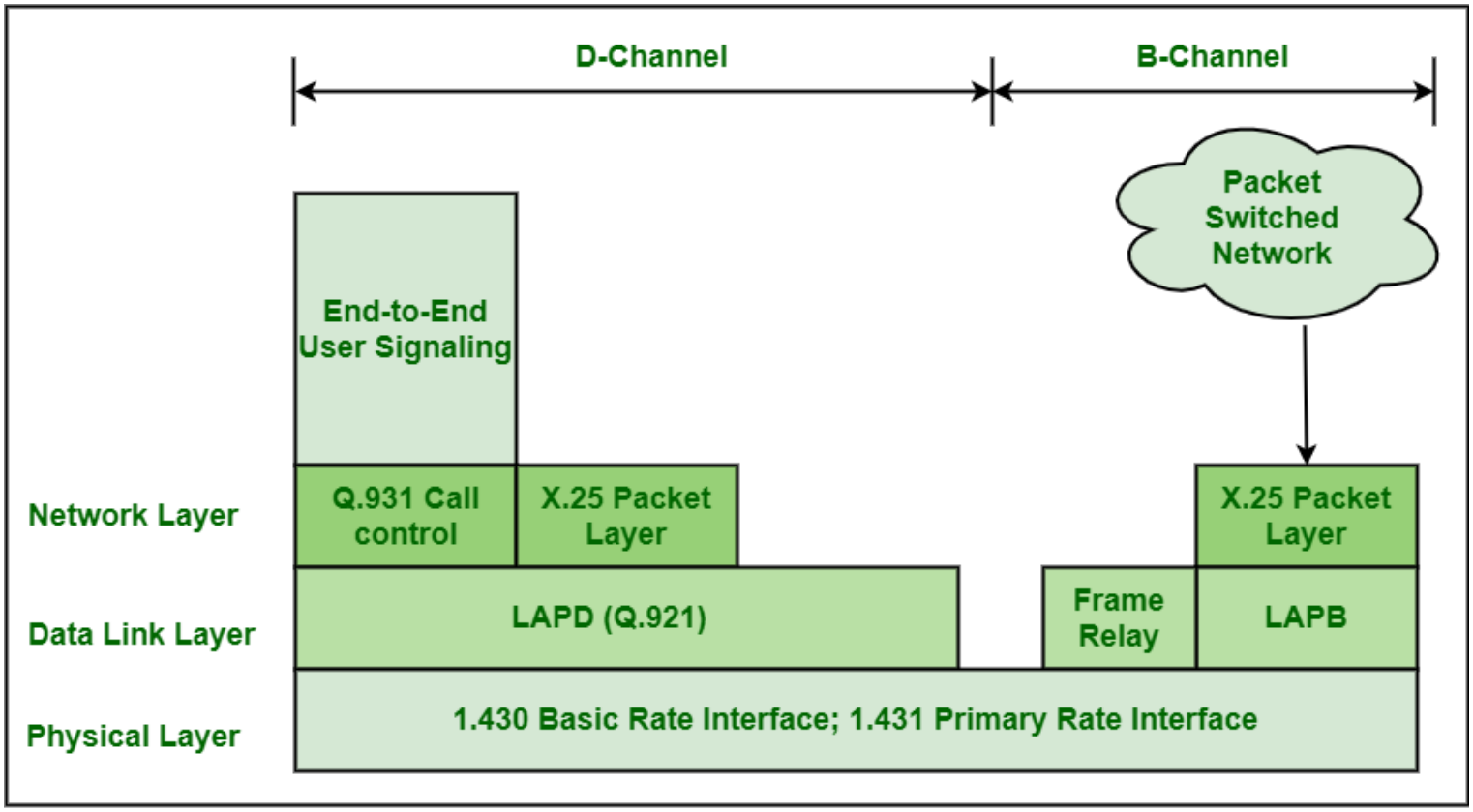
- **Methods**:

- Automatic Repeat Request (ARQ): This is the primary technique used for error control.
    - **Error Detection**: The receiver uses a checksum or cyclic redundancy check (CRC) to detect if a frame has been damaged.
    - **Error Correction/Retransmission**: If an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, or the sender times out without an acknowledgment, indicating the frame was lost. The sender then retransmits the problematic frame.

Answer No. – 15

ISDN:-

It is simply considered as general-purpose digital network that is being capable of highly and fully supporting wide range of services like voice, data, text, and image with the help of very small set of standard multipurpose user-network interfaces. It is also useful in providing very useful framework for development and establishment of future telecommunications networks and services. Previously, it is known as Integrated Digital Network (IDN) which is basically standardization digital technique for switching and transmission. ISDN also supports two types of switching operations i.e., circuit-switched operations and packet-switched operations. ISDN protocol architecture takes care of both of these switching operations. Circuit Switching is provided at the very nominal bit rate of 64 kbps whereas packet switching is provided for wide range of bit rates up to 64 kbps.



ISDN Protocol Architecture

Types of Channels : ISDN generally contains three types of channels i.e., B-channel (Bearer channel), D-channel (Data Channel), and H-channel (Hybrid Channel).

1. **B-Channel :** B-channel usually has 64 kbps data rate. This channel is required for voice, data, or other low data rate information. For higher data rates, two B-channel will get combined to give total of 128 kbps data rates.
2. **D-Channel :** D-channel usually has 16 to 64 kbps data rate. This channel is required for signaling or packet-switched data. D-channel does not even carry data. It is simply required for carrying all of the controlling signals as establishing call, ringing, call interrupt, etc. It is common channel signaling that carries control signals for all of the using out-band signaling. Using this channel subscribes generally provide security to B connection. It is also required to carry data or information as videotext, tele-text, emergency services alarms, etc. in case of no signaling.
3. **H-Channel :** H-channel generally has kbps, 1536 kbps, or 1920 kbps data rate. This channel is required for video, video-conferencing, high-speed data/audio, etc.

Types of Layers : ISDN usually contains two different layering mechanisms out of which one is for B/H Channels and other one for D Channel. For D-channel, ISDN contains three-layered protocol architecture. On the other hand, for B-channel, ISDN contains only one protocol layer i.e. physical layer and rest of upper layers are dependent on the application.

1. **Physical Layer :** At this layer, B and D channels are same and uses either BRI or PRI Interface. It defines various primary aspects such as mechanical and electrical specifications of interface R, S, T, and U, Encoding, or power supply, etc. It is also based in X.21 for interfacing with public circuit switching network through an 8-pin connector.
2. **Data Link Layer :** At this layer, B or D Channel generally uses LAPB or LAPD. B and D channels use different data link protocols i.e. LAPB For B channel and LAPD for D channel.
3. **Network Layer :** At this channel, B-channel has different options in connecting to circuit either circuit-switched, packet-switched, frame relay, or ATM networks.