Computer Network

Lecture taken by
Dharmendra Kumar
(Associate Professor)
United College of Engineering and Research, Prayagraj

Syllabus

Syllabus

Unit-1:

Introductory Concepts: Goals and applications of networks, Categories of networks, Organization of the Internet, ISP, Network structure and architecture (layering principles, services, protocols and standards), The OSI reference model, TCP/IP protocol suite, Network devices and components.

Physical Layer: Network topology design, Types of connections, Transmission media, Signal transmission and encoding, Network performance and transmission impairments, Switching techniques and multiplexing.

Syllabus

Unit-2:

Data Link Layer: Framing, Error Detection and Correction, Flow control (Elementary Data Link Protocols, Sliding Window protocols). Medium Access Control and Local Area Networks: Channel allocation, Multiple access protocols, LAN standards, Link layer switches & bridges (learning bridge and spanning tree algorithms)

Unit-3:

Network Layer: Point-to-point networks, Logical addressing, Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP), Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion control algorithms, IPv6.

Syllabus

Unit-4:

Transport Layer: Process-to-process delivery, Transport layer protocols (UDP and TCP), Multiplexing, Connection management, Flow control and retransmission, Window management, TCP Congestion control, Quality of service.

Unit-5:

Application Layer: Domain Name System, World Wide Web and Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login, Network management, Data compression, Cryptography – basic concepts.

Books

1. Behrouz Forouzan, “Data Communication and Networking”, McGraw Hill

2. Andrew Tanenbaum “Computer Networks”, Prentice Hall.

3. William Stallings, “Data and Computer Communication”, Pearson.

4. Kurose and Ross, “Computer Networking-A Top-Down Approach”, Pearson.

Course Outcome (CO's)

CO1	Explain basic concepts, OSI reference model, services and role of each layer of OSI model and TCP/IP, networks devices and transmission media, Analog and digital data transmission
CO2	Apply channel allocation, framing, error and flow control techniques.
CO3	Describe the functions of Network Layer i.e. Logical addressing, subnetting & Routing Mechanism.
CO4	Explain the different Transport Layer function i.e. Port addressing, Connection Management, Error control and Flow control mechanism.
CO5	Explain the different protocols used at application layer i.e.

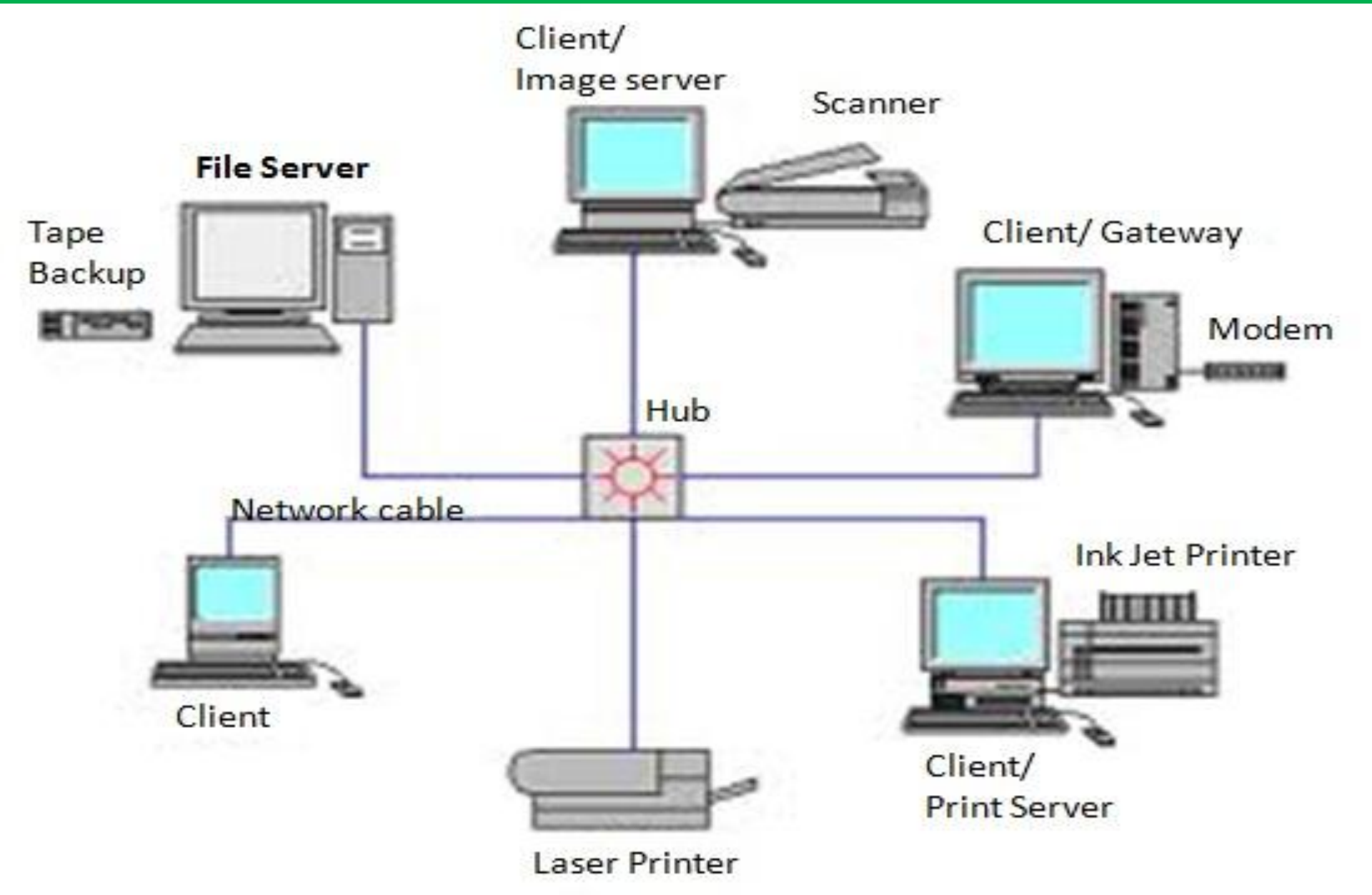
Unit-1

Computer Network

- A computer network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

- “Computer network’’ to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

Computer Network



Computer Network

- Networks come in many sizes, shapes and forms. They are usually connected together to make larger networks.
- Internet being the most well-known example of a network of networks.

Uses of Computer Network

1. Business Applications

- Information sharing: To distribute information throughout the company
- Resource sharing: Sharing physical resources such as printers, and tape backup systems
- Client-Server model: It is widely used and forms the basis of much network usage.
- E-mail: Employees generally use for a great deal of daily communication.
- Voice over IP (VoIP): Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called IP telephony or Voice over IP (VoIP) when Internet technology is used.
- Desktop sharing: Remote workers see and interact with a graphical computer screen
- E-commerce: Doing business electronically, especially with customers and suppliers. It has grown rapidly in recent years.

Uses of Computer Network

2. Home Applications

- Person-to-Person communication
- Electronic commerce
- Entertainment (game playing)

3. Mobile Users

- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- M-commerce
- NFC (Near Field Communication)

4. Social Issues

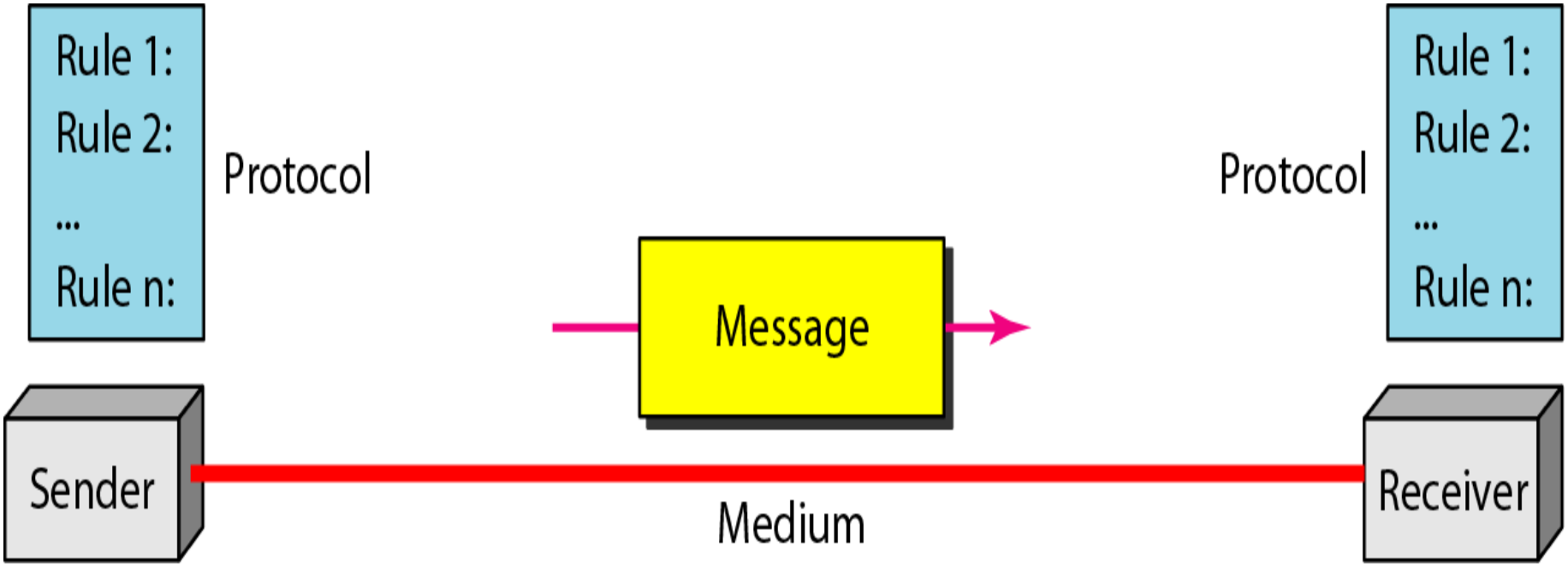
Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals.

Data Communication System

A data communication 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. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Communication System



Data Representation

- Text
- Numbers
- Images
- Audio
- Video

Effectiveness of a Data Communication System

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.

Effectiveness of a Data Communication System

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.

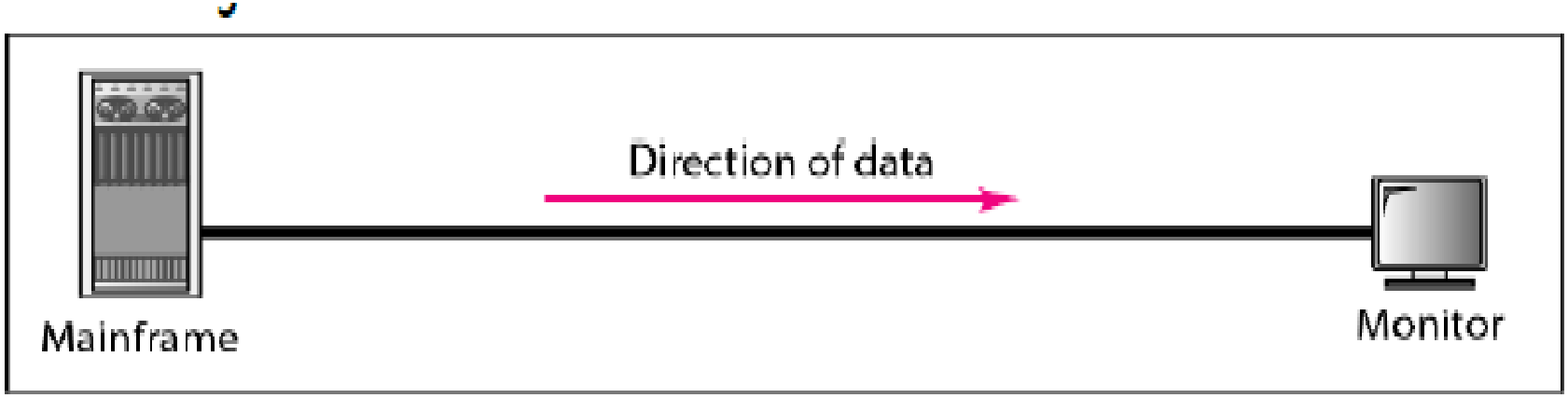
4. Jitter: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30 ms delay and others with 40 ms delay, then an uneven quality in the video is the result.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

Simplex Communication

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.



Keyboards and traditional monitors are examples of simplex devices.

Data Flow

Half-Duplex Communication

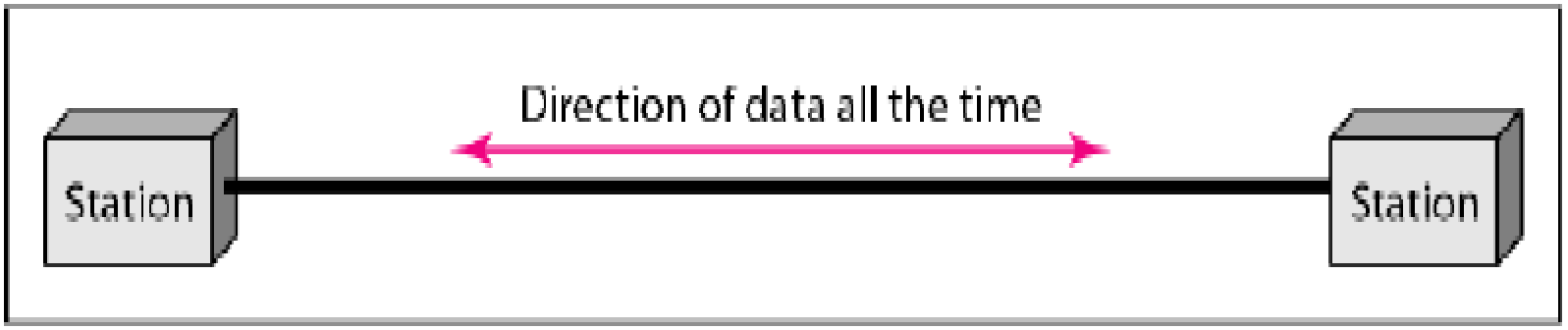
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice-versa.

Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Data Flow

Full-Duplex Communication

In full-duplex, both stations can transmit and receive simultaneously. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.



Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

- Performance can be measured in many ways, including transit time and response time.
  - Transit time is the amount of time required for a message to travel from one device to another.
  - Response time is the elapsed time between an inquiry and a response.
- The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay.
- However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Network Criteria

Reliability: In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

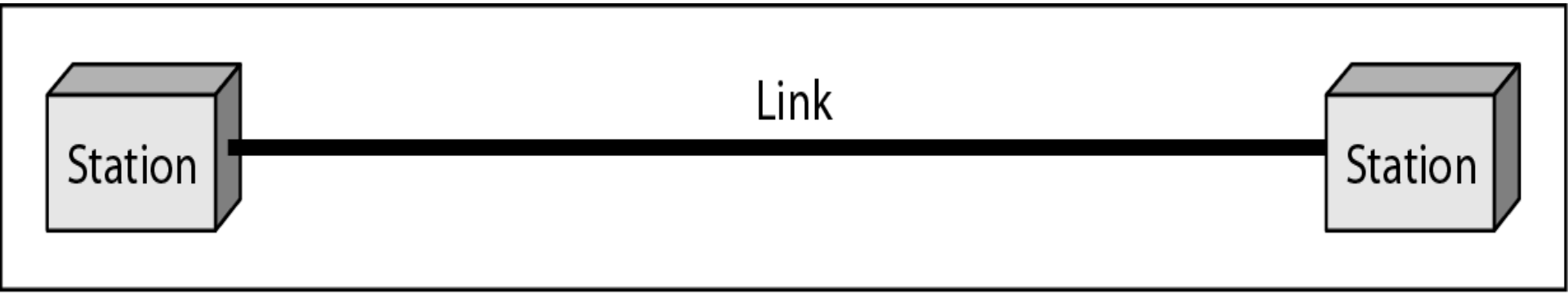
Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point Connection

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections 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.

When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

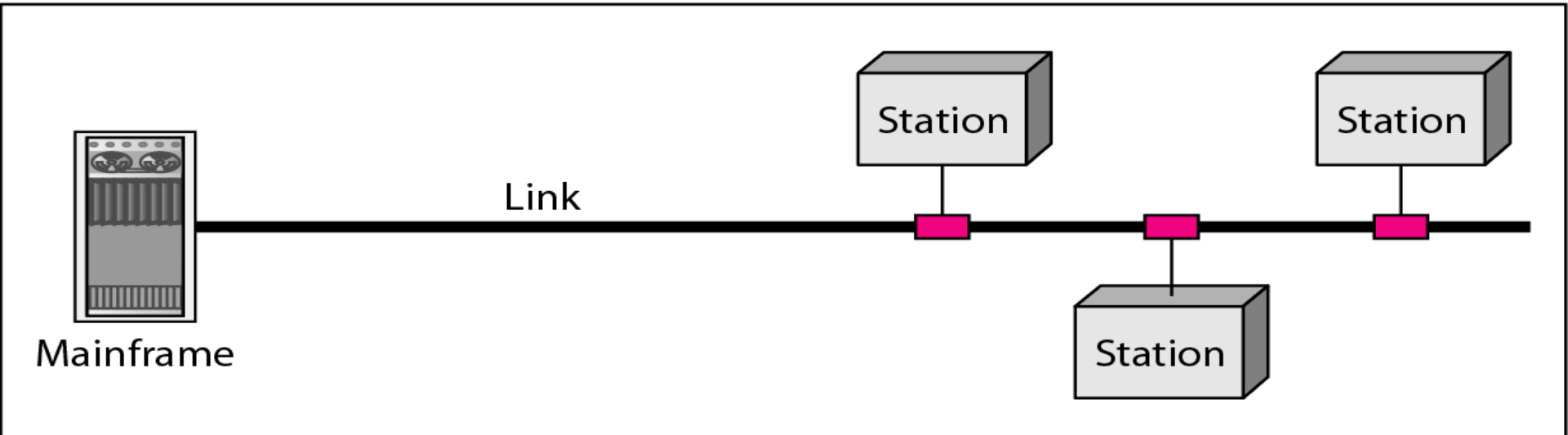


Type of Connection

Multipoint Connection

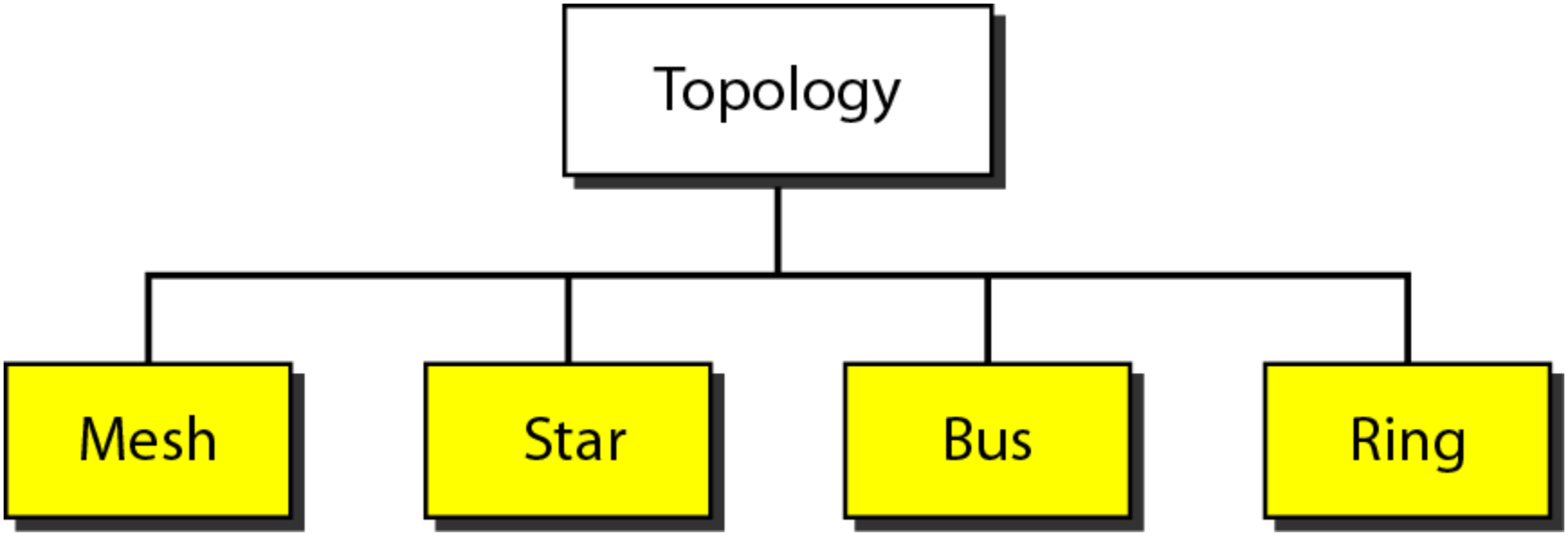
A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link.

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



Network Topology

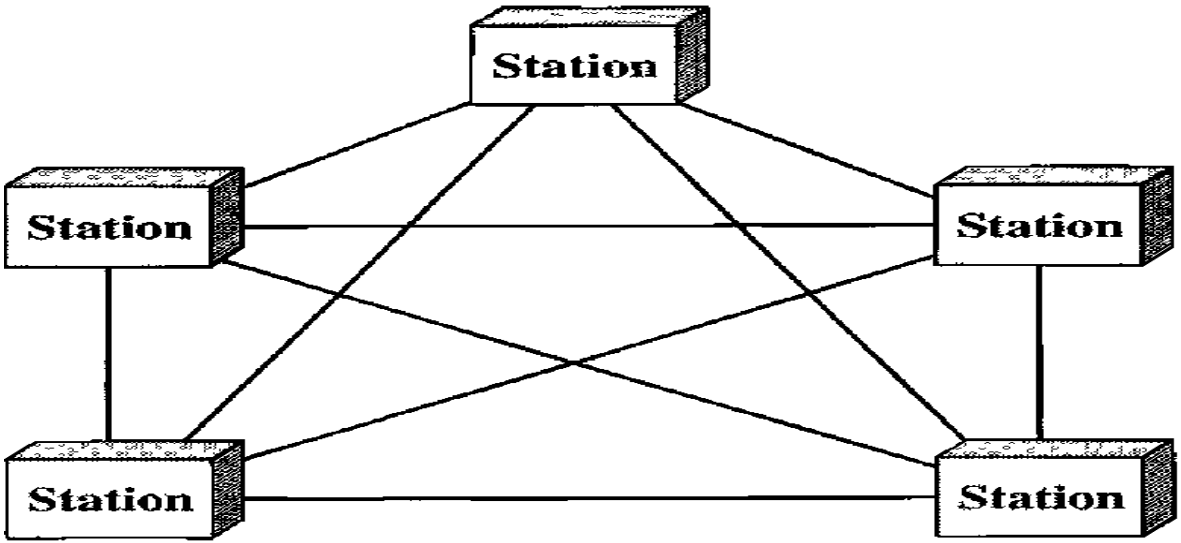
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are four basic topologies possible: mesh, star, bus, and ring.



Mesh Topology

Mesh Topology:

- In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.
- The number of **physical links** in a fully connected mesh network with **n** nodes = **n(n-1)/2.**



Mesh Topology

Advantages of a mesh topology

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

4. Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Mesh Topology

Disadvantages of a mesh topology

1. Since every device must be connected to every other device, therefore installation and reconnection are difficult.

2. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

3. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

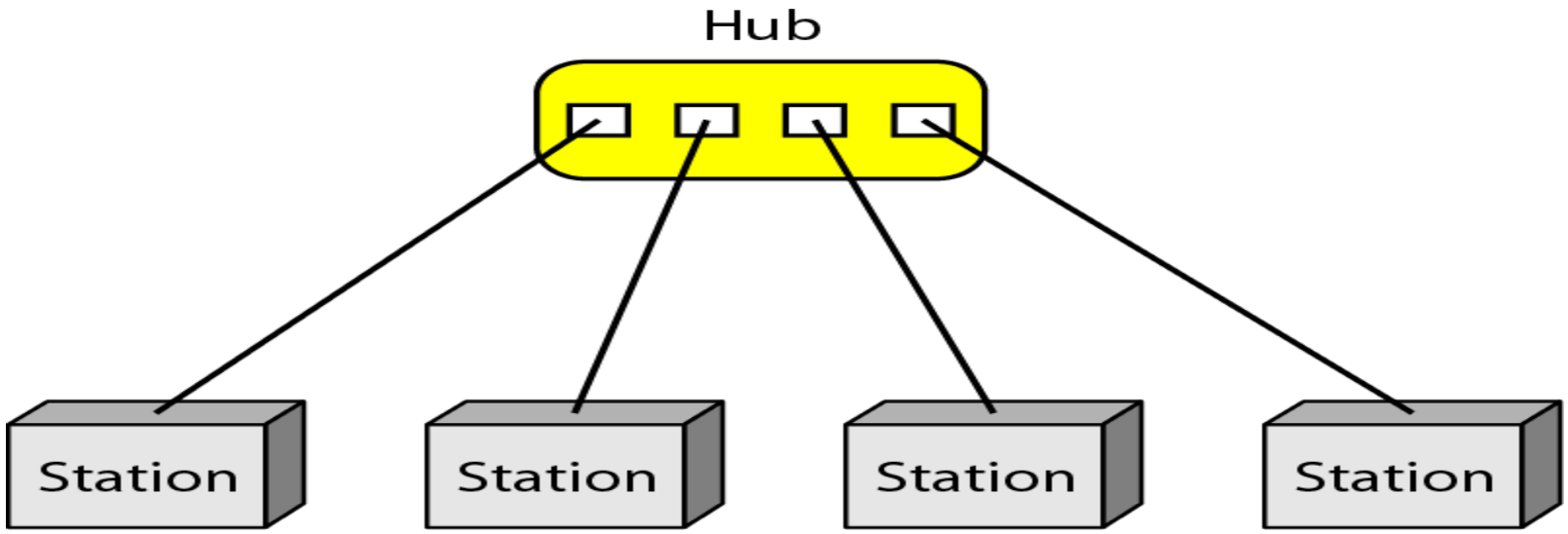
Mesh Topology

Uses of mesh topology

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Star Topology

Advantages of Star topology

1. A star topology is less expensive than a mesh topology.
2. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
3. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Star Topology

Disadvantages of Star topology

A disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

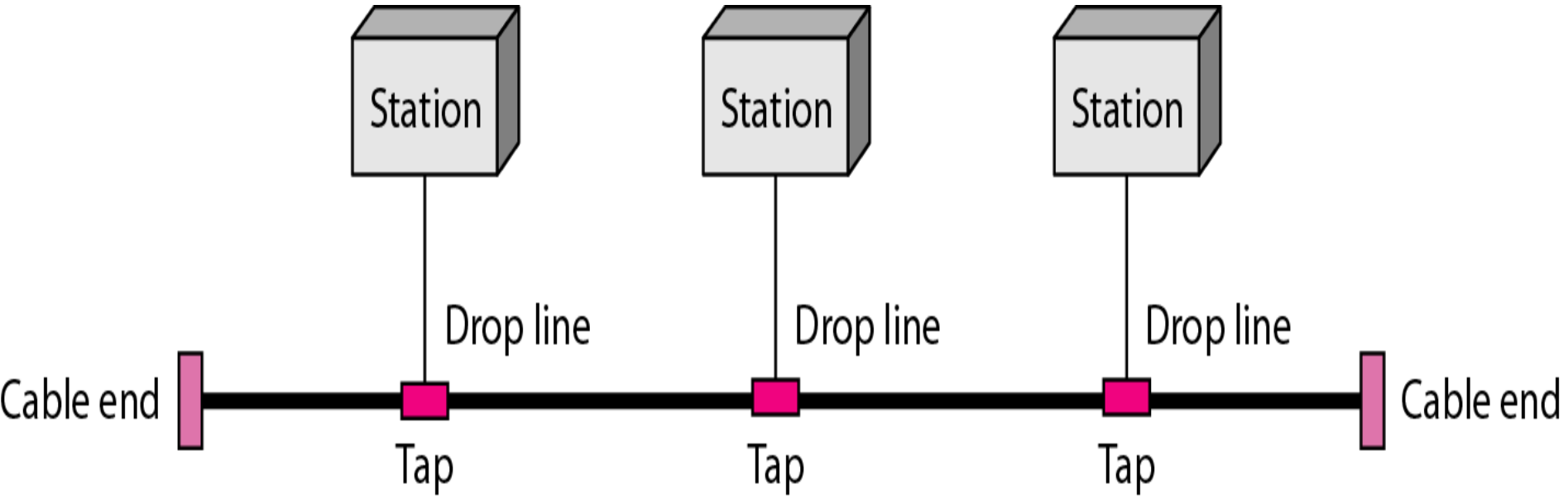
Uses:

The star topology is used in local-area networks (LANs).

High-speed LANs often use a star topology with a central hub.

Bus Topology

Bus topology uses multipoint connection link. One long cable acts as a backbone to link all the devices in a network.



Bus Topology

- Nodes(systems) are connected to the backbone cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther.
- For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Bus Topology

Advantages of bus topology

- **Ease of installation**

Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- **A bus topology uses less cabling than mesh or star topologies.**

In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Bus Topology

Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

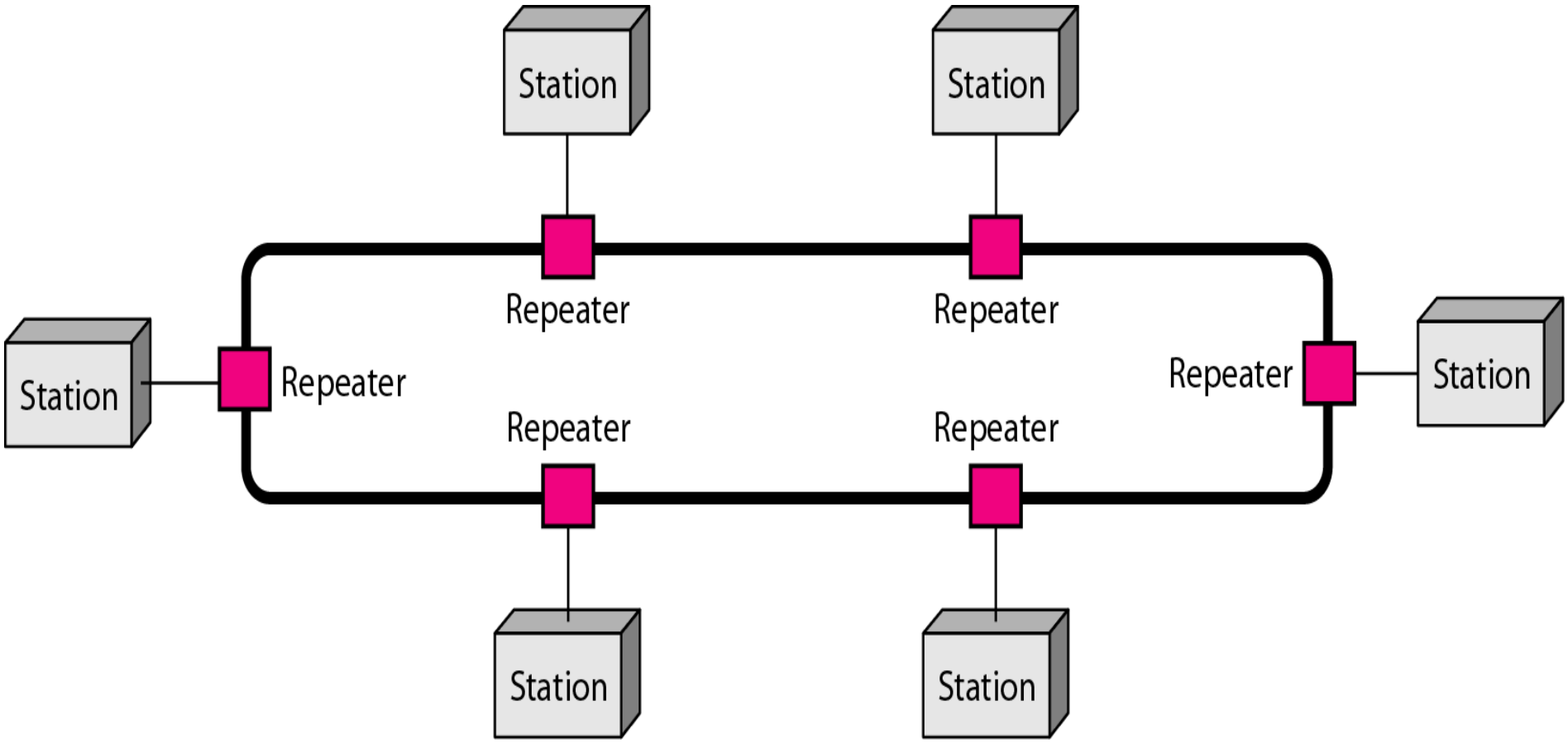
Bus Topology

Uses of bus topology

- Bus topology was the one of the first topologies used in the design of early local area networks.

- Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology



Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the 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 incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Ring Topology

Advantages of ring topology

- **A ring topology is relatively easy to install and reconfigure.**

Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.

- **Fault isolation is simplified.**

Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Ring Topology

Disadvantages of ring topology

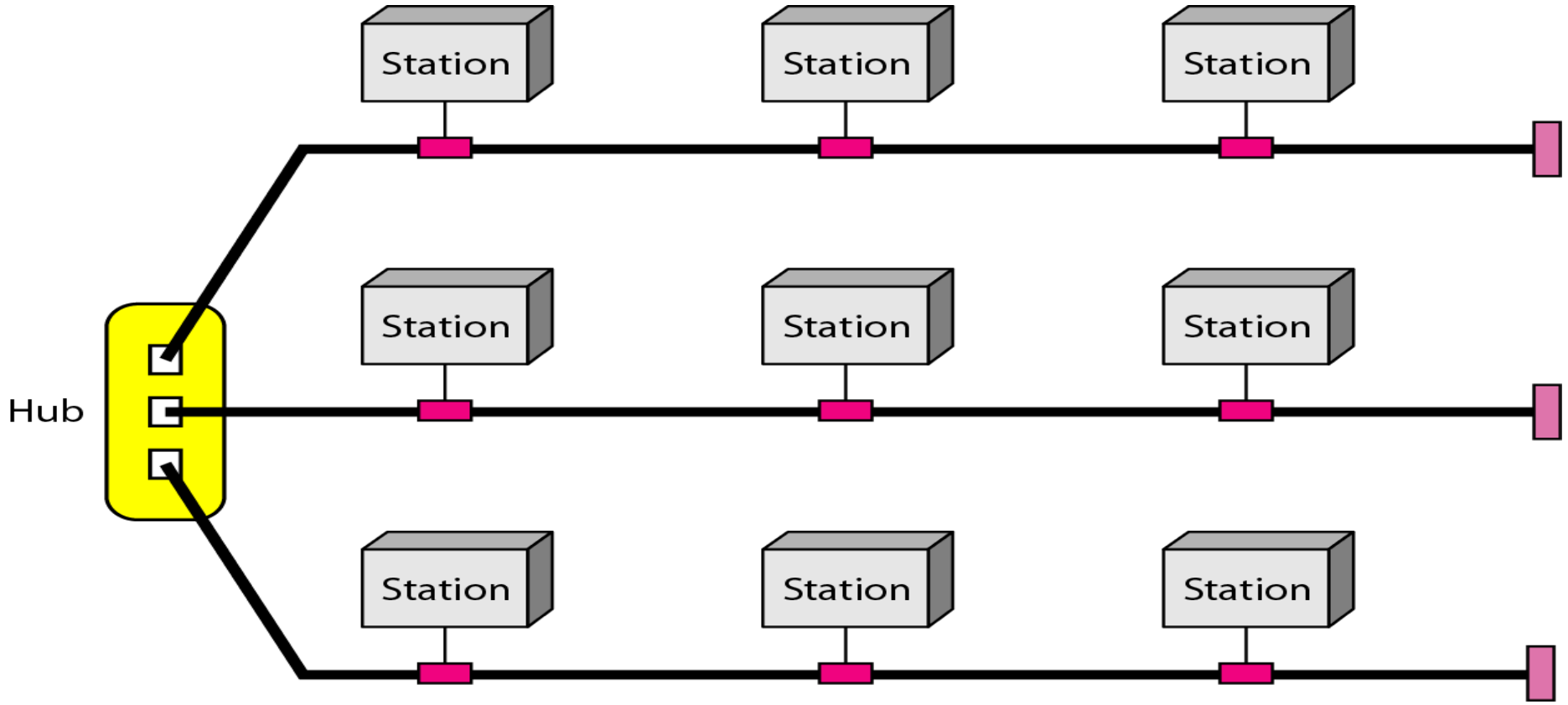
- Unidirectional traffic can be a disadvantage.
- In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Uses of ring topology

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure:-



Categories of Networks

Networks are classified based upon the size, the area it covers and its physical architecture. The three primary network categories are **LAN, WAN and MAN**. Each network differs in their characteristics such as distance, transmission speed, cables and cost.

Local Area Network(LAN)

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company.
- Currently, LAN size is limited to a few kilometers.

Local Area Network(LAN)

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company.
- Currently, LAN size is limited to a few kilometers.
- LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software(e.g., an application program), or data.

Local Area Network(LAN)

- The most common LAN topologies are **bus, ring,** and **star.**
- Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.
- Wireless LANs are the newest evolution in LAN technology.

Wide Area Network(WAN)

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

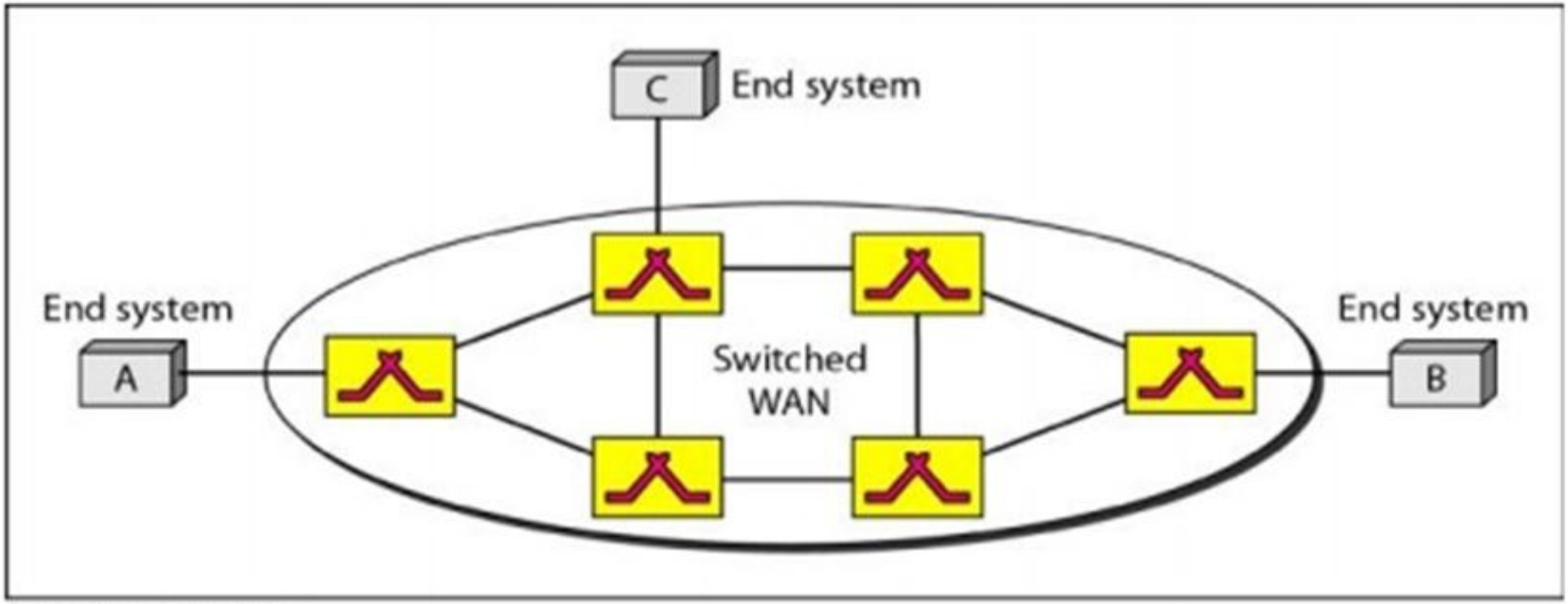
A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.

Wide Area Network(WAN)

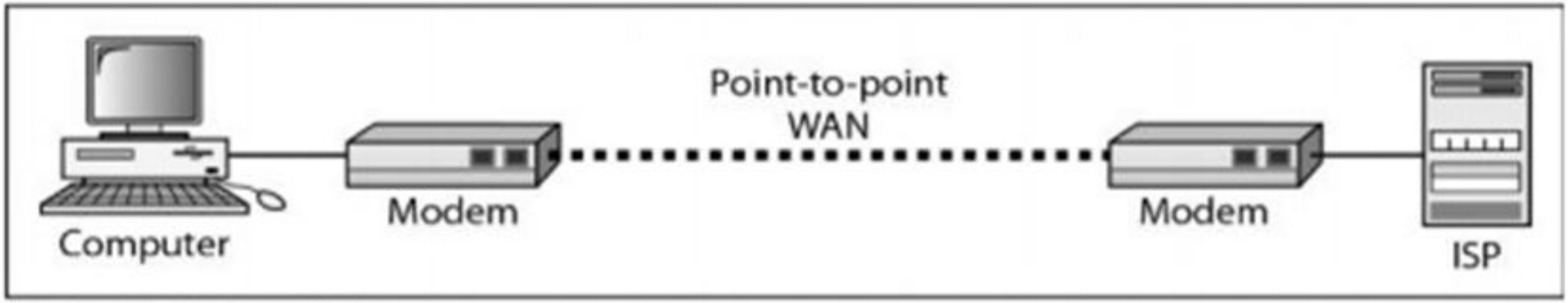
We normally refer to the first as a switched WAN and to the second as a point-to-point WAN.

- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

Wide Area Network(WAN)



a. Switched WAN



b. Point-to-point WAN

Wide Area Network(WAN)

- An early example of a switched WAN is X.25, a network designed to provide connectivity between end users.
- X.25 is being gradually replaced by a high-speed, more efficient network called Frame Relay.
- A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.
- Another example of WANs is the wireless WAN that is becoming more and more popular.

Metropolitan Area Networks(MAN)

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.
- A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.
- Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

Interconnection of Networks: Internetwork

An internetwork can be defined as two or more computer networks (typically Local Area Networks LAN) which are connected together, using Network Routers.

It is also called internet.

Each network in an Internetwork has its own Network Address, which is different from other networks in the Internetwork. Network Address is used to identify the networks inside an Internetwork.

Internetwork allows different users at different geographical locations of an organization to share data, resources and to communicate. Modern businesses cannot even function without Internetwork. Internet, Intranet and Extranet are different types of internetwork.

Internet, Intranet and Extranet

Internet:

Internet is a worldwide, publicly accessible computer network of interconnected computer networks (internetwork) that transmit data using the standard Internet Protocol (IP). Largest Internetwork in the world is Internet.

Internet, Intranet and Extranet

Intranet:

- An intranet is a private network that is contained within an enterprise.
- Typical intranet for a business organization consists of many interlinked local area networks (LAN) and use any Wide Area Network (WAN) technology for network connectivity.
- The main purpose of an intranet is to share company information and computing resources among employees.
- Intranet is a private Internetwork, which is usually created and maintained by a private organization.
- The content available inside Intranet are intended only for the members of that organization (usually employees of a company).

Internet, Intranet and Extranet

Extranet:

- An extranet can be viewed as part of a company's intranet that is extended to users outside the company like suppliers, vendors, partners, customers, or other business associates.
- Extranet is required for normal day-to-day business activities. For example, placing purchase order to registered vendors, billing & invoices, payments related activities, joint venture related activities, product brochures for partners, discounted price lists for partners etc.

Network Models

OSI Model

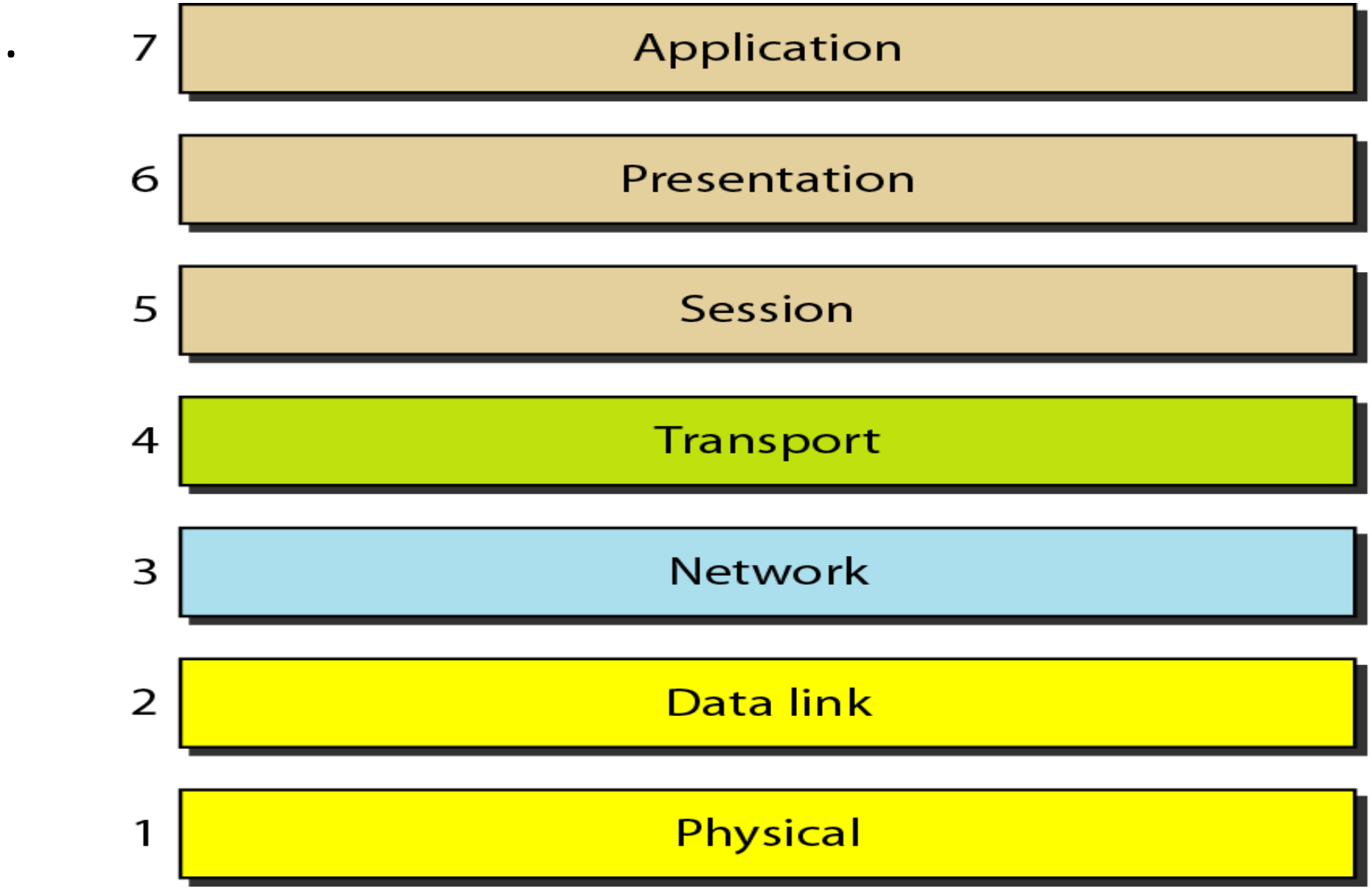
- Its full form is Open Systems Interconnection model.
- It was developed by International Standards Organization (ISO) organization in 1970.
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

OSI Model

- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.

- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

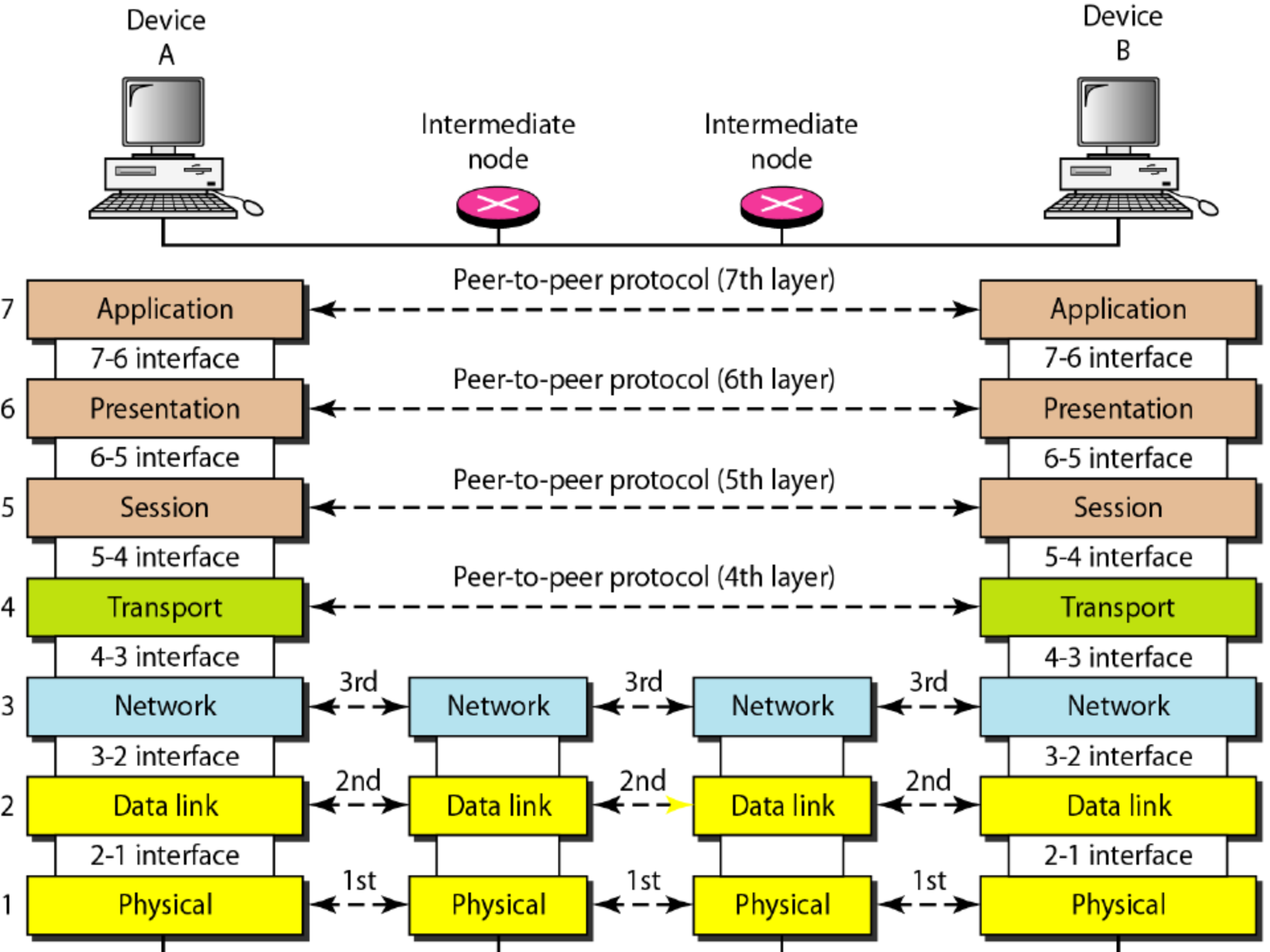
OSI Model


7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical

OSI Model

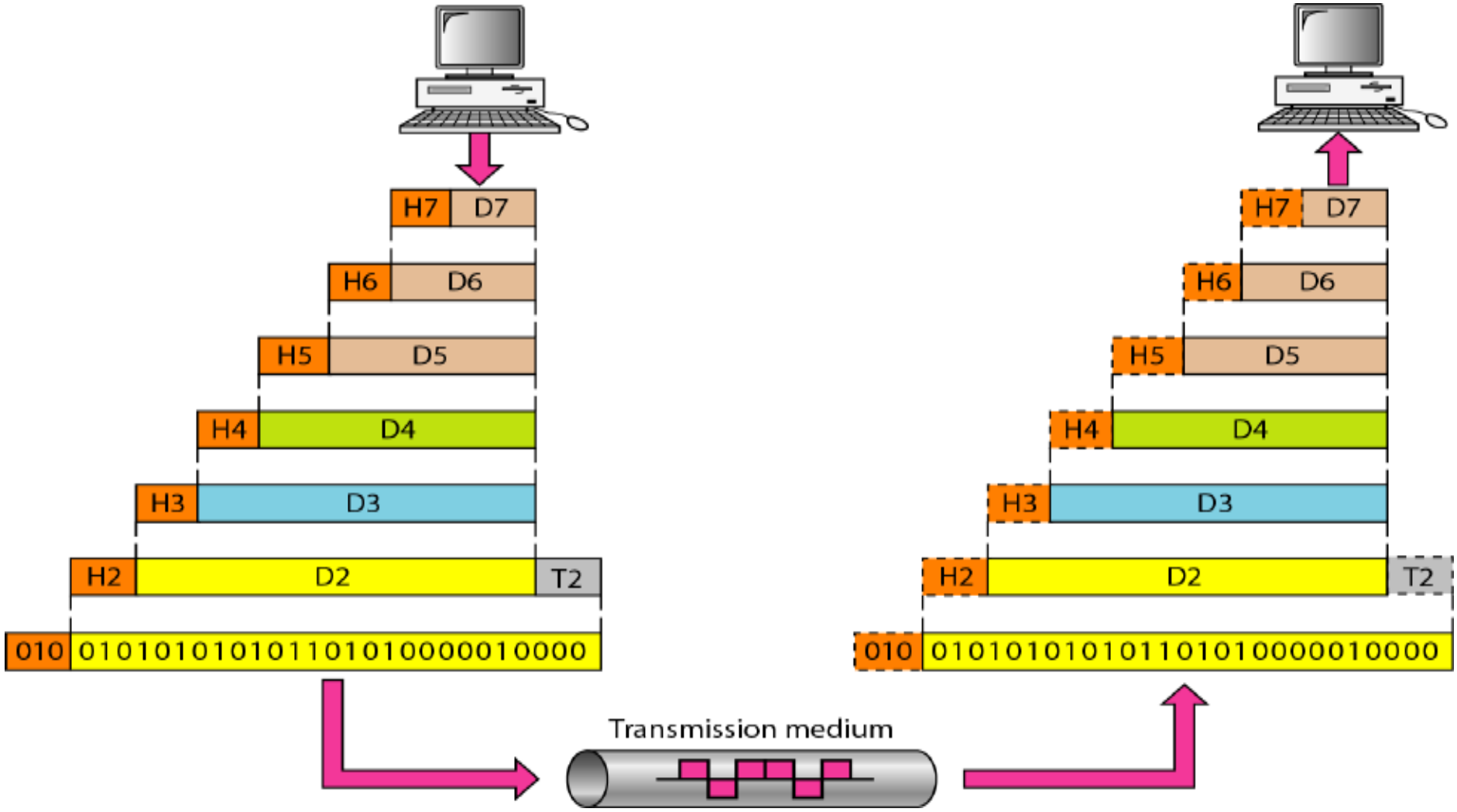
Layered Architecture

Following figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
2nd
1st

OSI Model

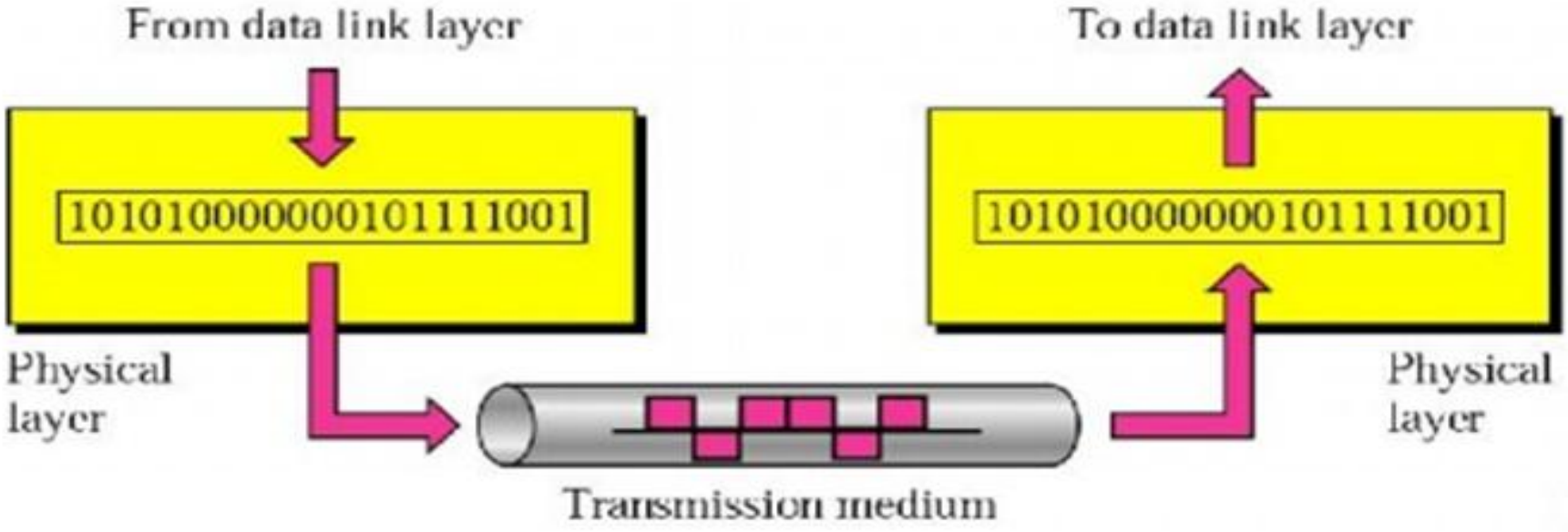
An exchange of messages using OSI model is shown in the following figure:-



Functions of Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.

Note: The physical layer is responsible for movements of individual bits from one hop (node) to the next.



Functions of Physical Layer

The physical layer is also concerned with the following:

- Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

Functions of Physical Layer

- Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer.
- Synchronization of bits: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.
- Line configuration: The physical layer is concerned with the connection of devices to the media; it may be point-to-point configuration or multi-point.

Functions of Physical Layer

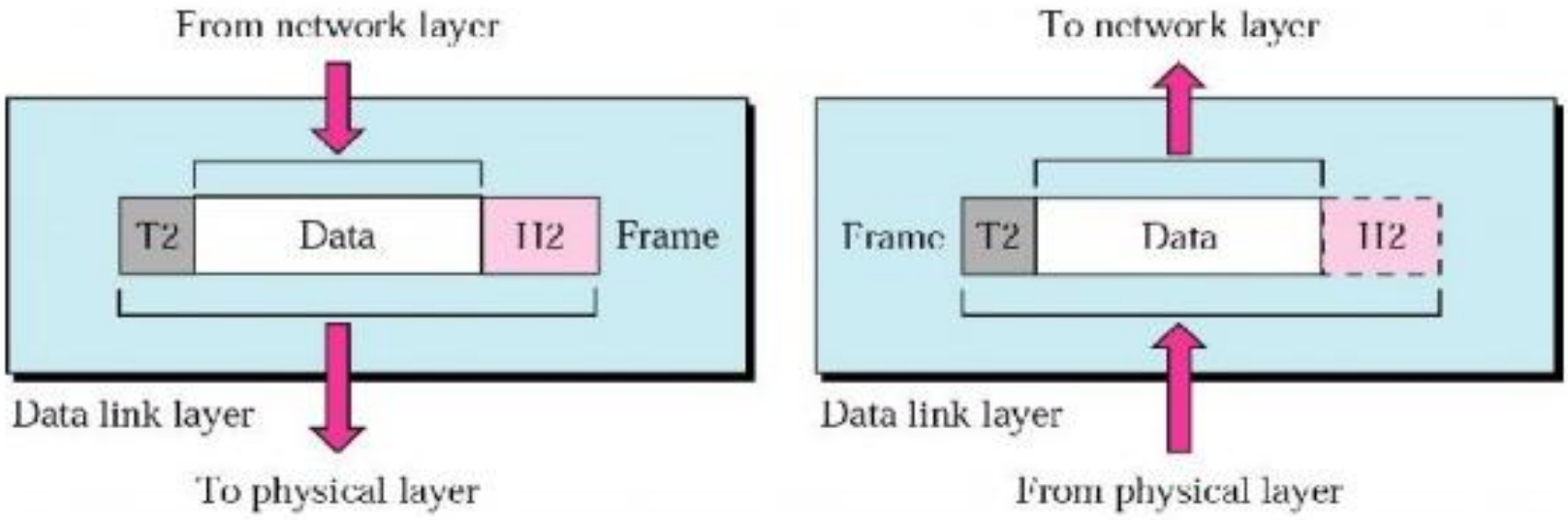
- Physical topology: The physical topology defines how devices are connected to make a network. Ex. Mesh, Star, Ring, Bus, or a hybrid topology.

- Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

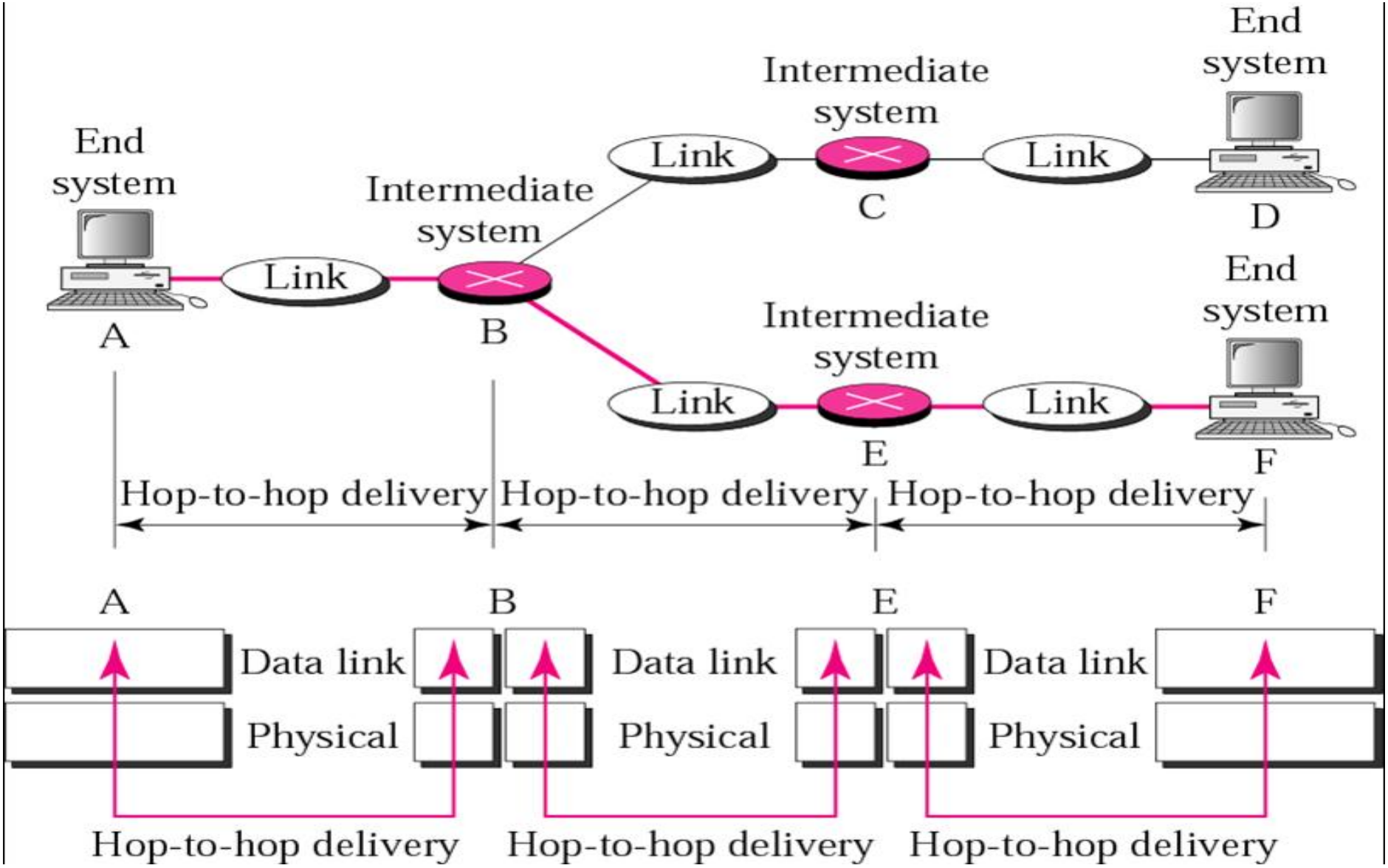
Functions of Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Note: The data link layer is responsible for moving frames from one hop (node) to the next.



Functions of Data Link Layer



Functions of Data Link Layer

Other responsibilities of the data link layer include the following:

1. Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

2. Physical addressing: If frames are to be distributed to different systems on the network , the data link layer adds a header to the frame to define the sender and/or receiver of the frame.

3. Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Functions of Data Link Layer

4. Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.

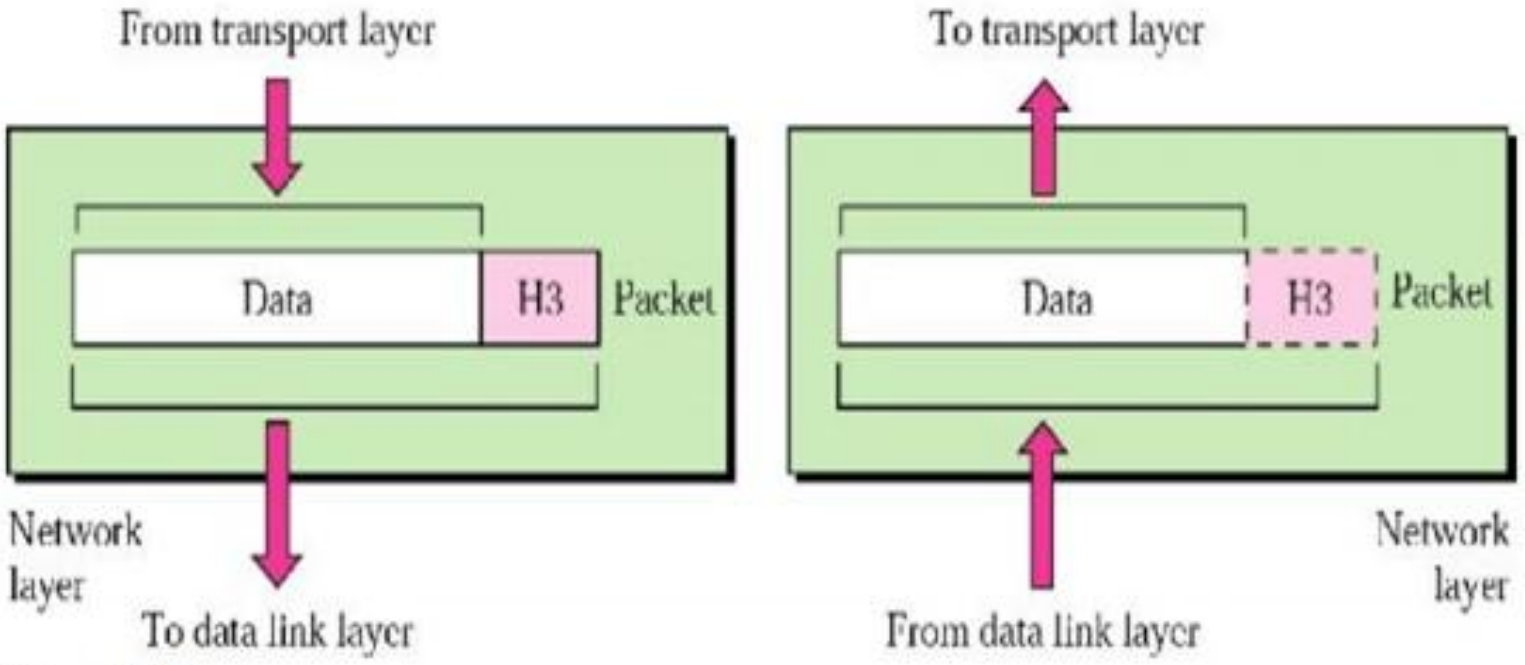
5. Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Functions of Network Layer

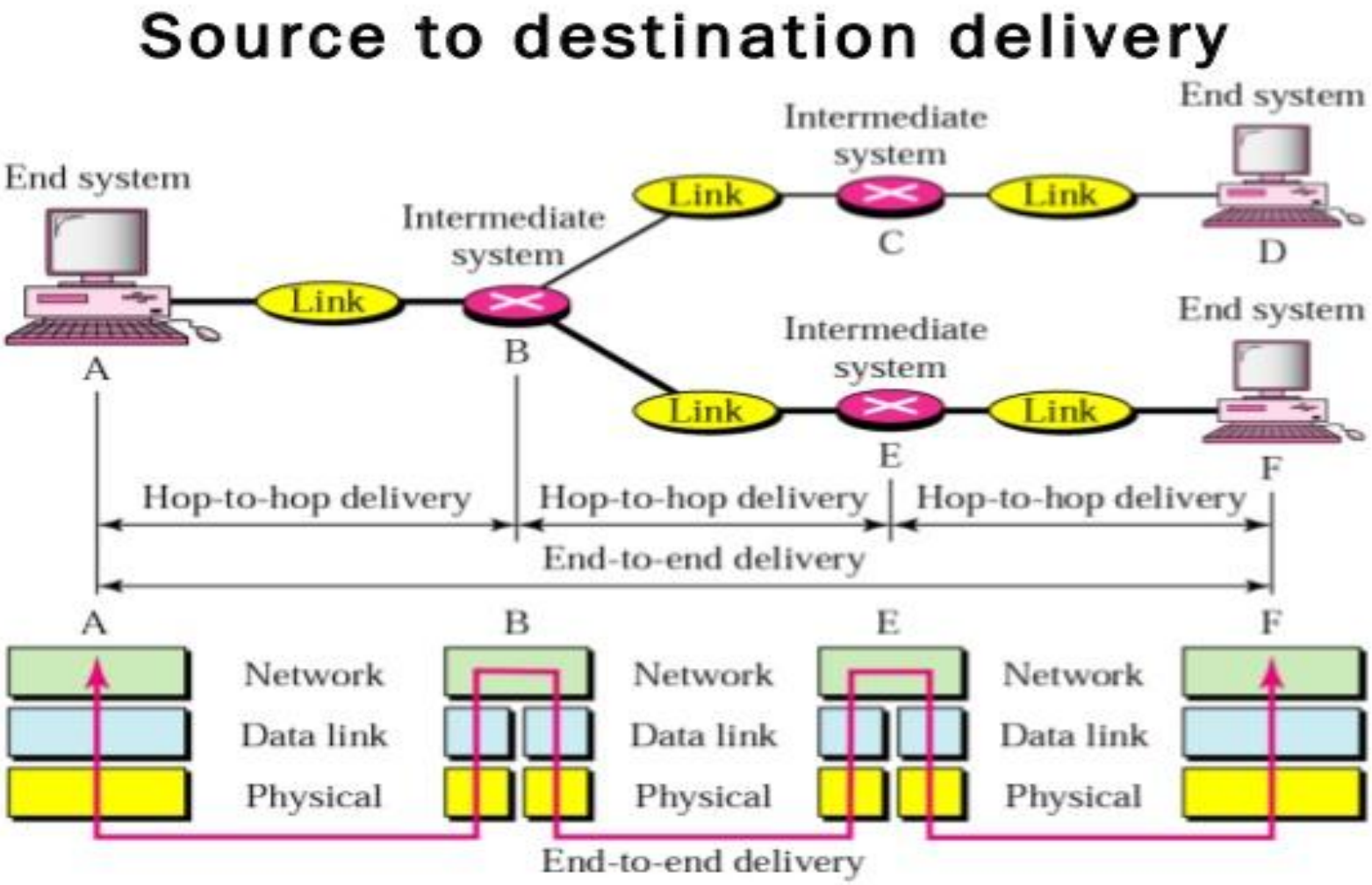
- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.
- If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Functions of Network Layer

Note: The network layer is responsible for the delivery of individual packets from the source host to the destination host.



Functions of Network Layer



Functions of Network Layer

Other responsibilities of the network layer include the following:

- Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

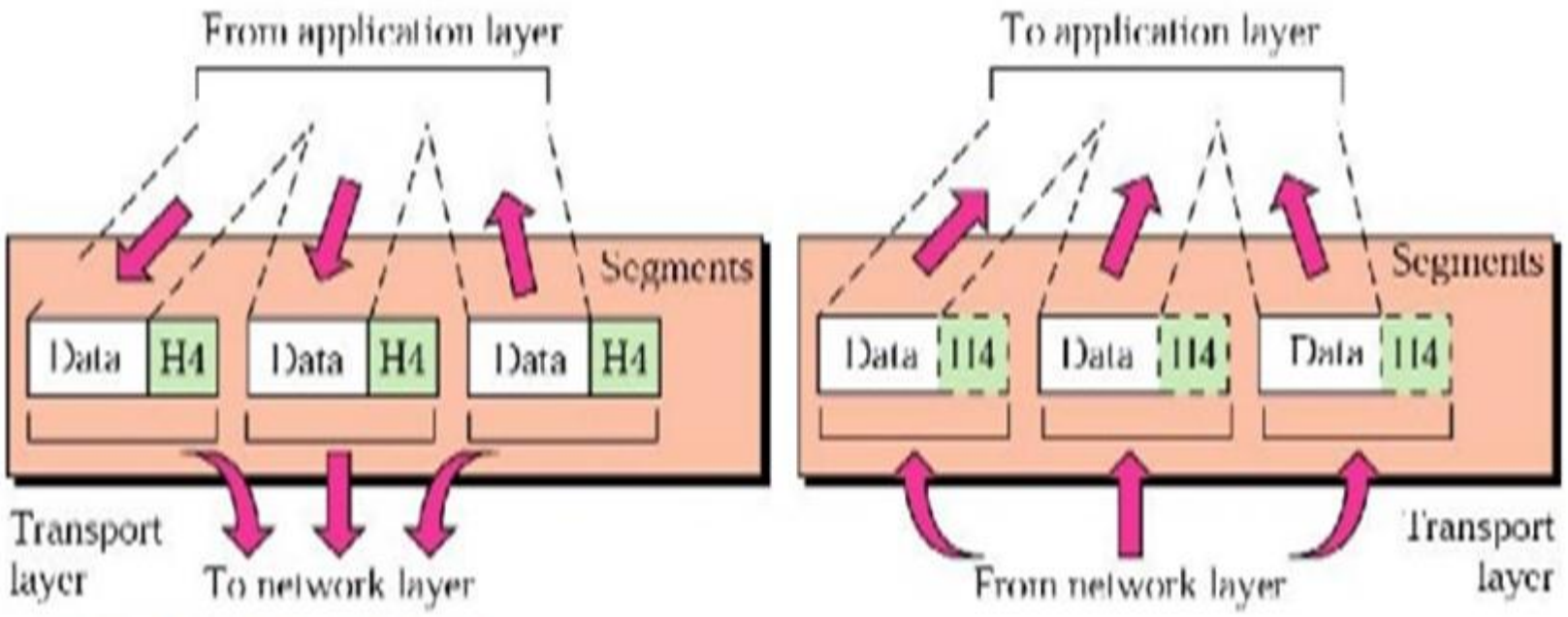
- Routing. When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

Functions of Transport Layer

- The transport layer is responsible for process-to-process delivery of the entire message.
- A process is an application program running on a host.
- Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Functions of Transport Layer

Following figure shows the relationship of the transport layer to the network and session layers.



Note: The transport layer is responsible for the delivery of a message from one process to another.

Functions of Transport Layer

Other responsibilities of the transport layer include the following:

a. Service-point addressing: Source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).

b. Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Functions of Transport Layer

c. Connection control: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

d. Flow control: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

Functions of Transport Layer

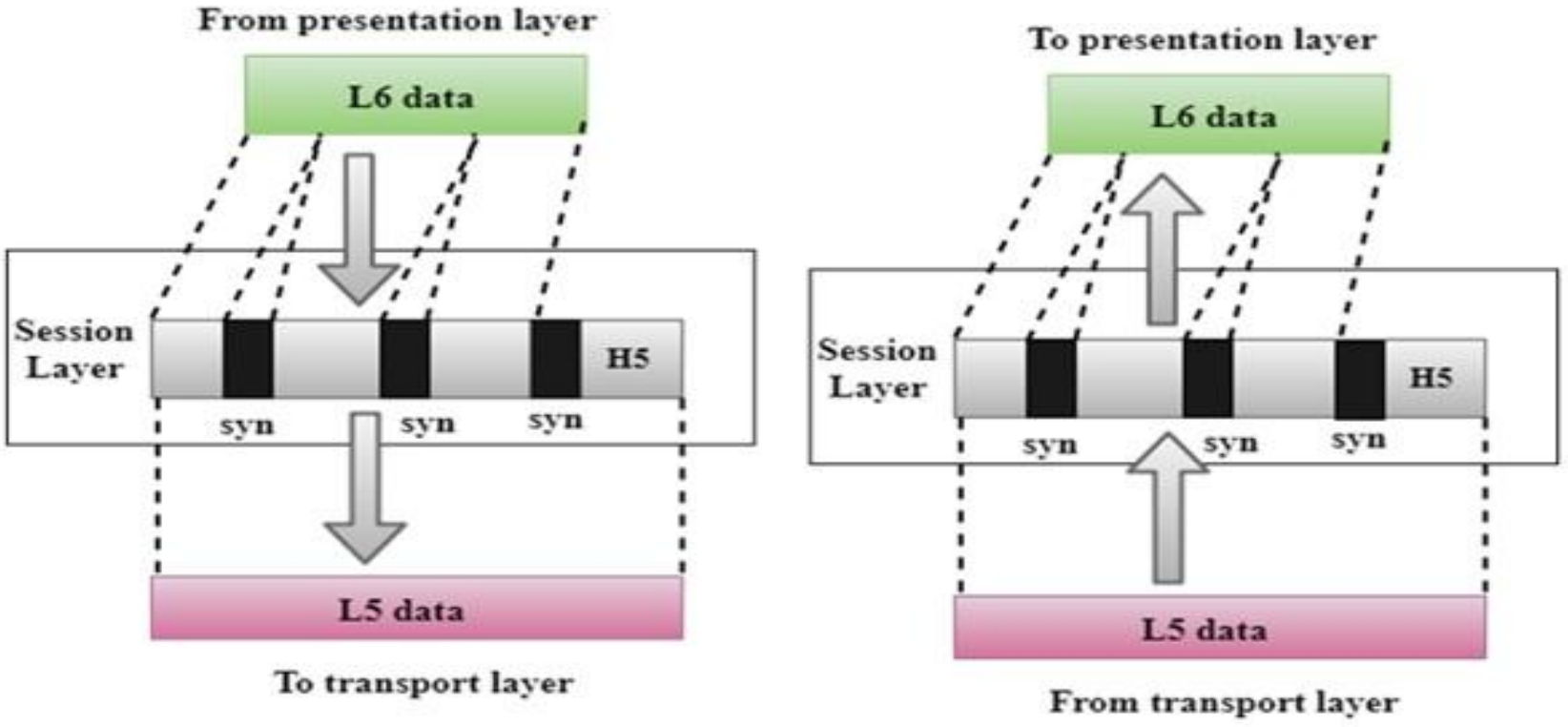
e. Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Functions of Transport Layer

Functions of Session Layer

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

Note: The session layer is responsible for dialog control and synchronization.



Functions of Session Layer

Specific responsibilities of the session layer include the following:

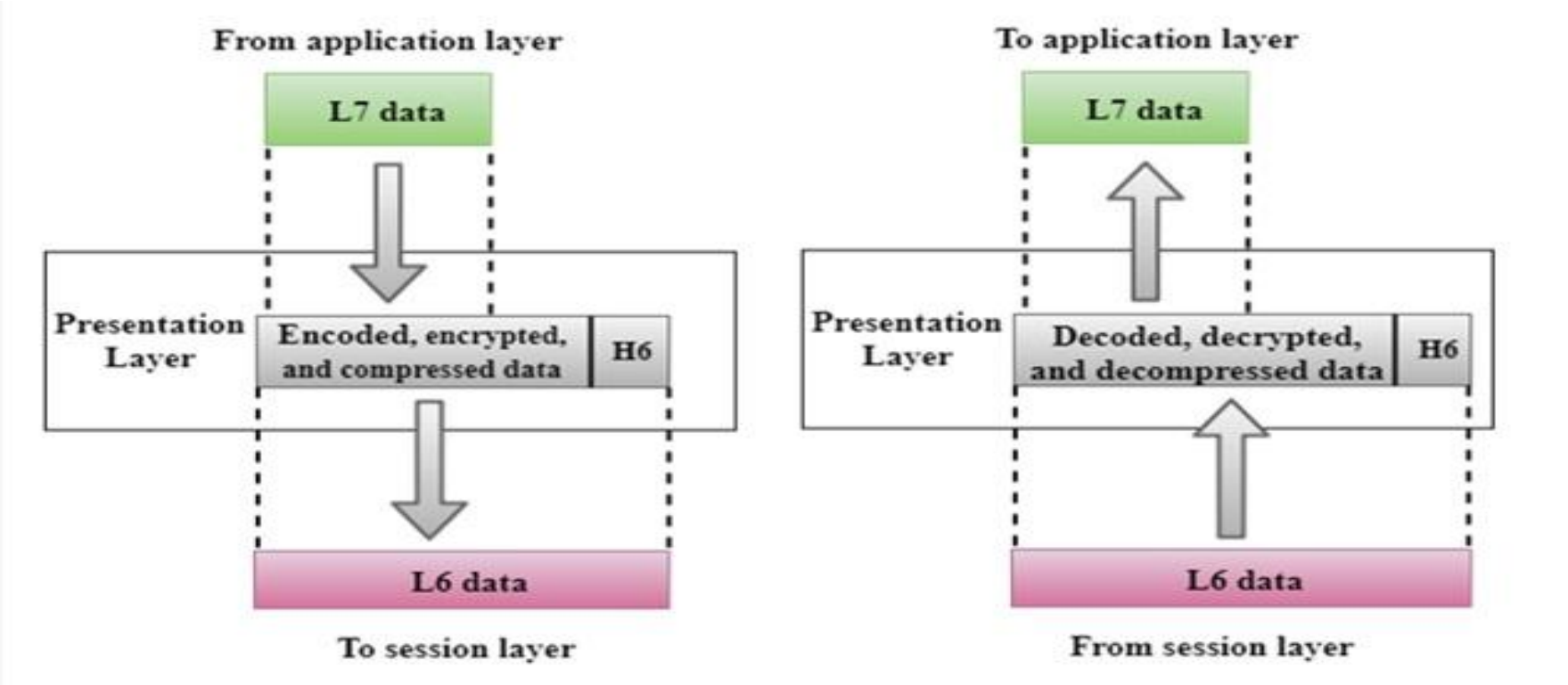
a. Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex or full-duplex.

b. Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Functions of Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Note: The presentation layer is responsible for translation, compression, and encryption.



Functions of Presentation Layer

Specific responsibilities of the presentation layer include the following:

a. Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Functions of Presentation Layer

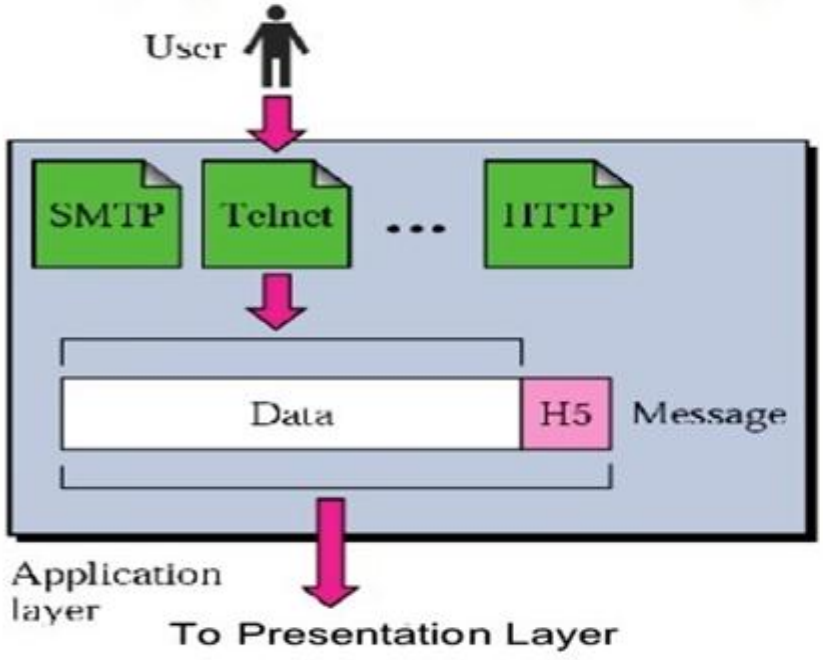
b. Encryption. A system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

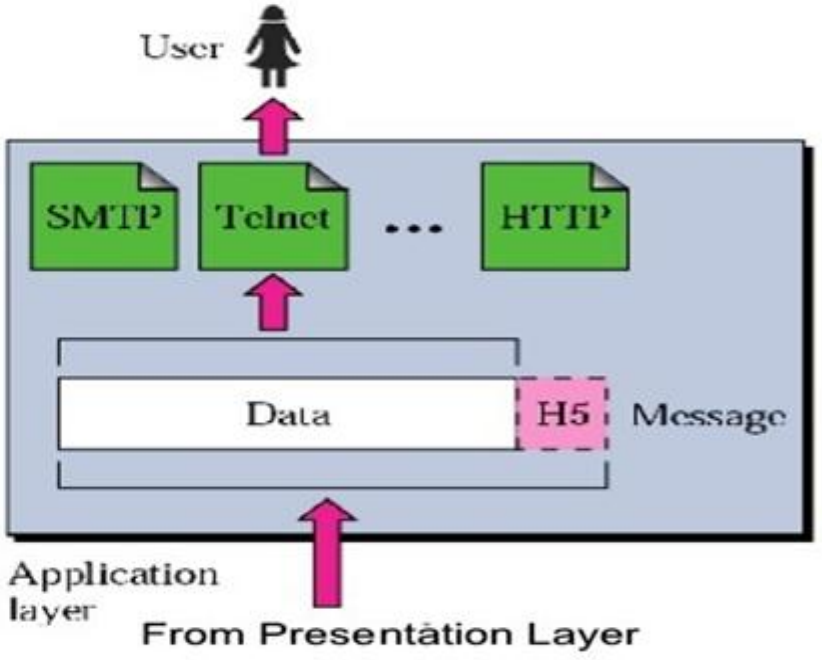
c. Compression. Data compression reduces the number of bits contained in the information. It is very important in the transmission of multimedia such as text, audio, and video.

Functions of Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Note: The application layer is responsible for providing services to the user.





Functions of Application Layer

Specific services provided by the application layer include the following:

a. Network virtual terminal. It is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host.

b. File transfer, access, and management. This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Functions of Application Layer

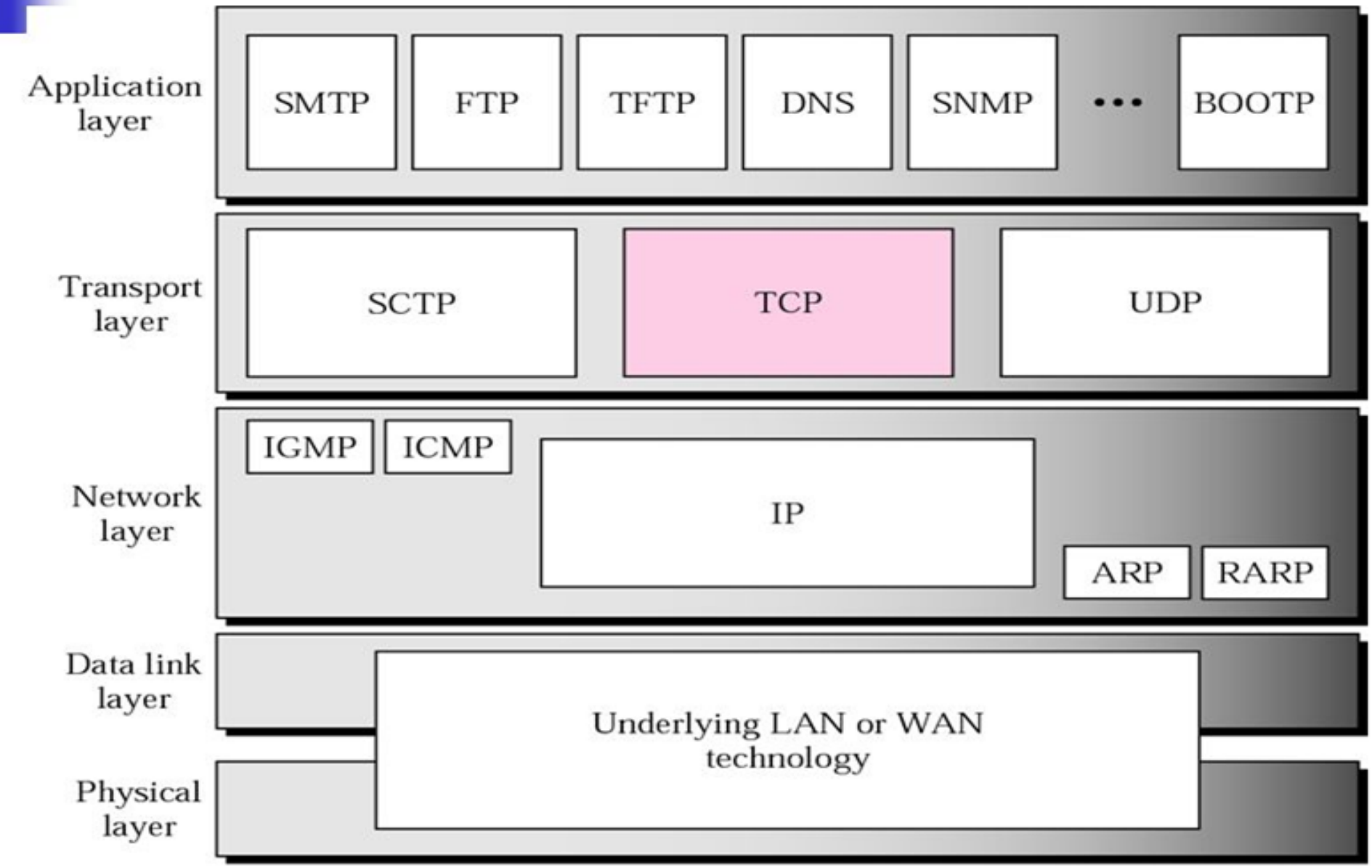
c. Mail services. This application provides the basis for e-mail forwarding and storage.

d. Directory services. This application provides distributed database sources and access for global information about various objects and services.

TCP/IP Protocol Suite

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the transport layer.

TCP/IP Protocol Suite



TCP/IP Protocol Suite

1. Physical and Data Link Layers:

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2. Network Layer:

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

a. Internetworking Protocol (IP)

The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol a best-effort delivery service. The term **best effort** means that IP provides no error checking or tracking.

TCP/IP Protocol Suite

b. Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

c. Reverse Address Resolution Protocol

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

TCP/IP Protocol Suite

d. Internet Control Message Protocol

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

e. Internet Group Message Protocol

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. Transport Layer:

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

TCP/IP Protocol Suite

a. User Datagram Protocol

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

b. Transmission Control Protocol

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

c. Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

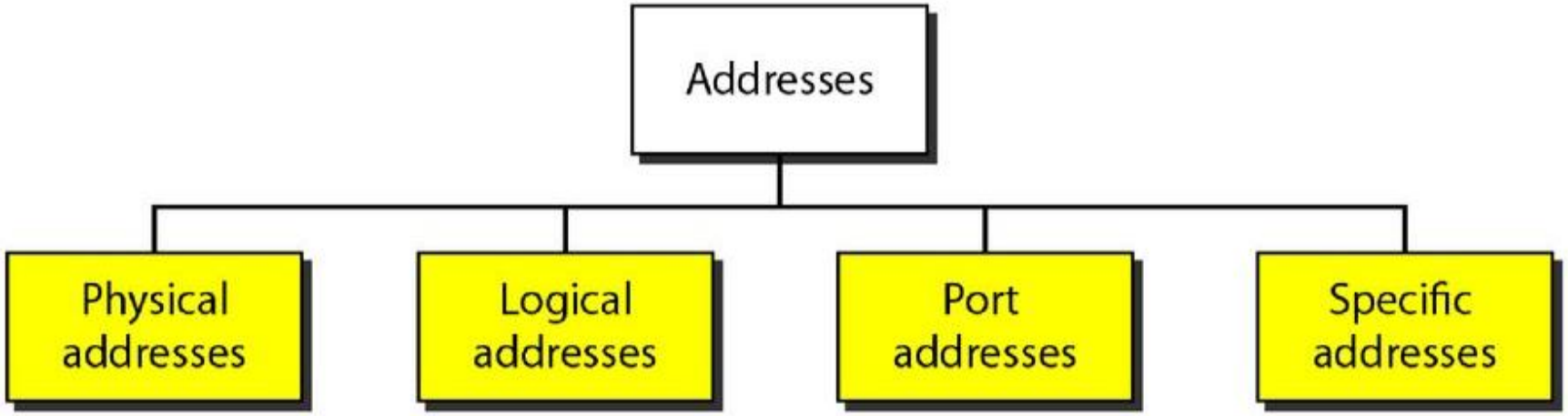
TCP/IP Protocol Suite

4. Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer such as FTP, Telnet, SMTP, DNS, SNMP.

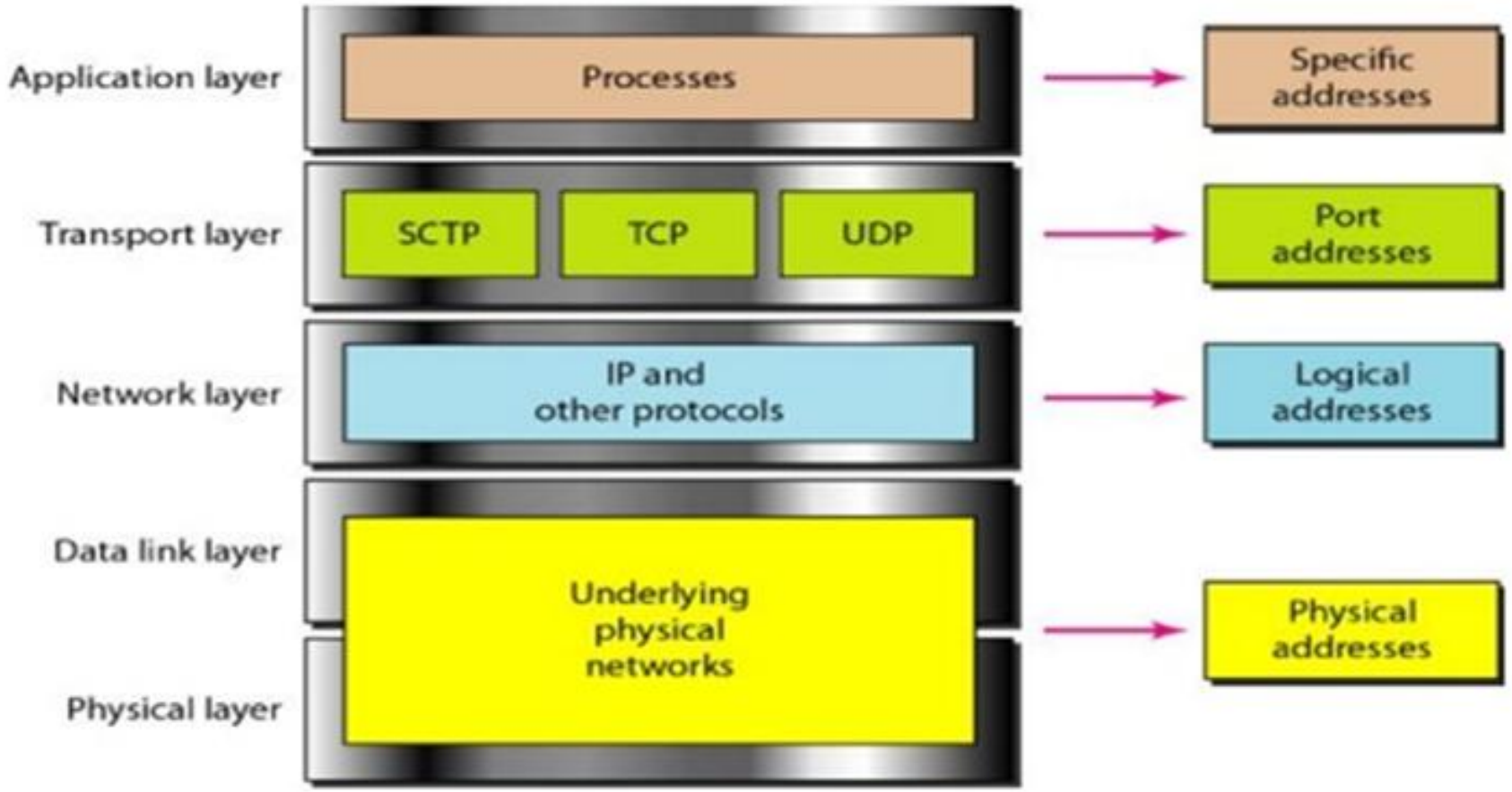
ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses.



ADDRESSING

Each address is related to a specific layer in the TCP/IP architecture.



Computer Network Components

Some important network components are NIC, switch, cable, hub, router, and modem.

NIC

- NIC stands for network interface card.
- NIC is a hardware component used to connect a computer with another computer onto a network
- It can support a transfer rate of 10, 100 to 1000 Mb/s.
- The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

There are two types of NIC:

(1) Wired NIC (2) Wireless NIC

Wired NIC: The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC: The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

Computer Network Components

Hub

- A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

- The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

Computer Network Components

Switch

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

Computer Network Components

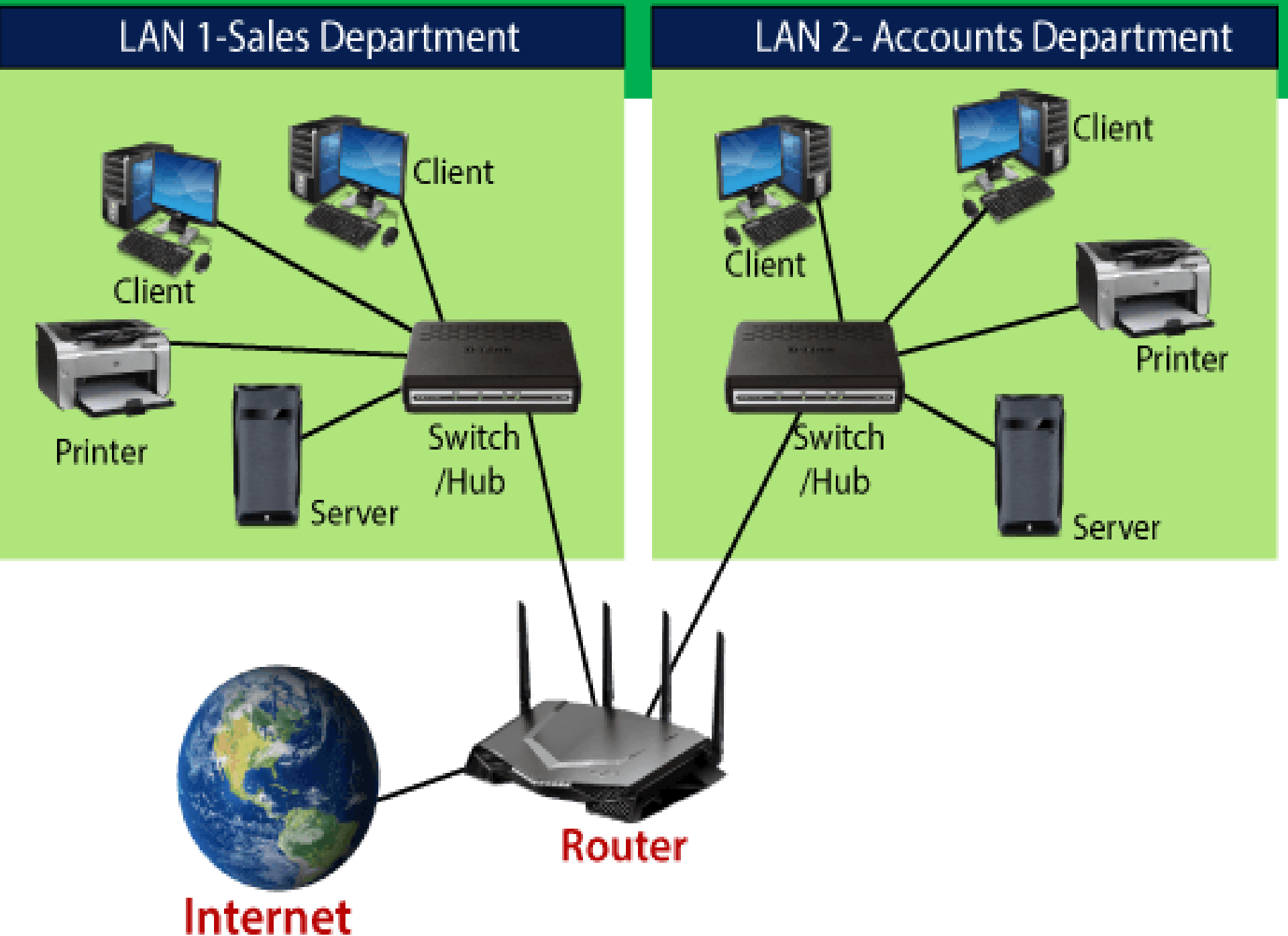
Router

A router is a hardware device which is used to connect a LAN with an internet connection. It is used to receive, analyze and forward the incoming packets to another network.

A router works in a Layer 3 (Network layer) of the OSI Reference model.

A router forwards the packet based on the information available in the routing table.

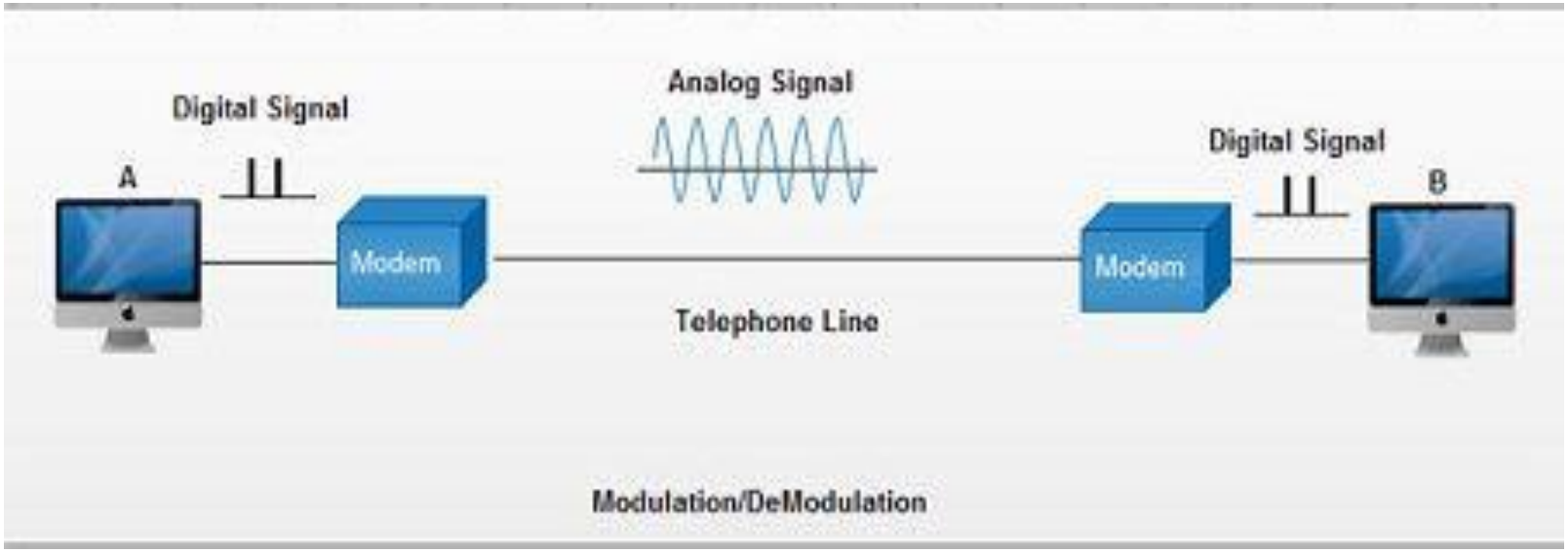
It determines the best path from the available paths for the transmission of the packet.


LAN 1-Sales Department
Client
Client
Printer
Server
Switch
/Hub
LAN 2- Accounts Department
Client
Client
Printer
Switch
/Hub
Server
Router
Internet

Computer Network Components

Modem

- A modem is a hardware device that allows the computer to connect to the internet over the existing telephone line.
- A modem is not integrated with the motherboard.
- It stands for Modulator/Demodulator. It converts the digital data into an analog signal over the telephone lines.

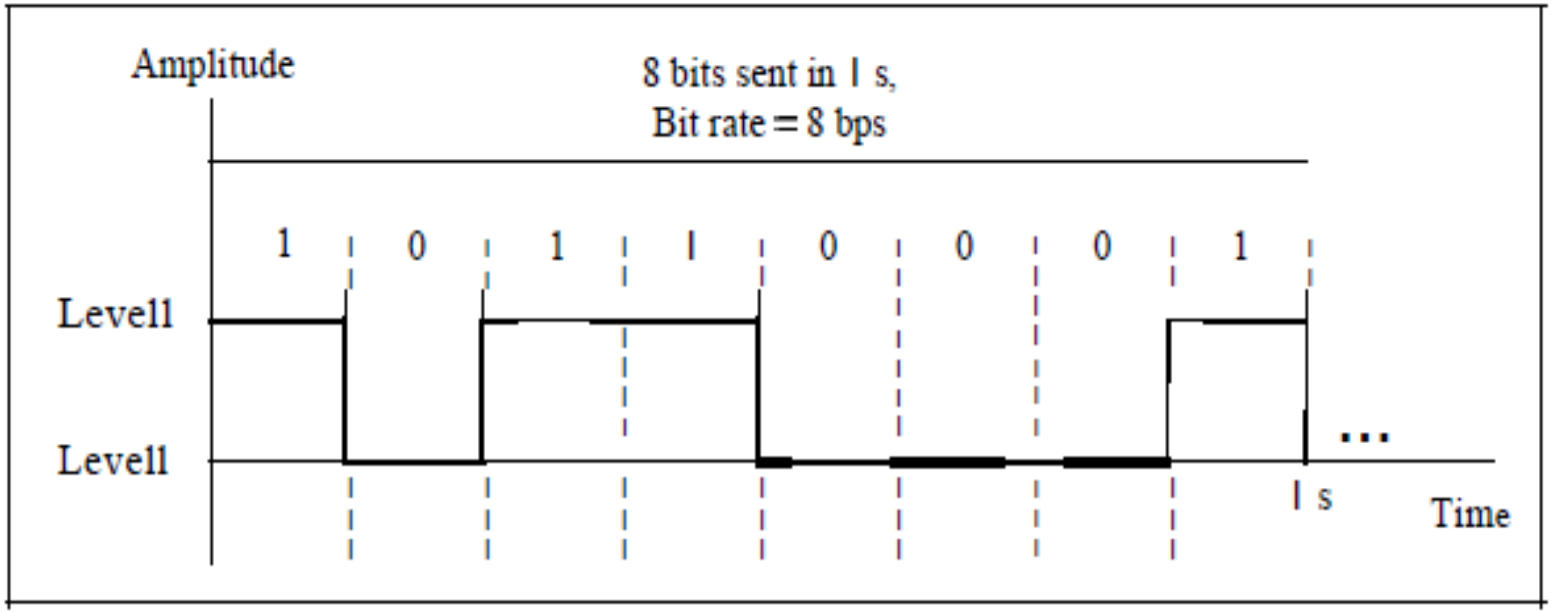


Physical Layer

Digital Signal

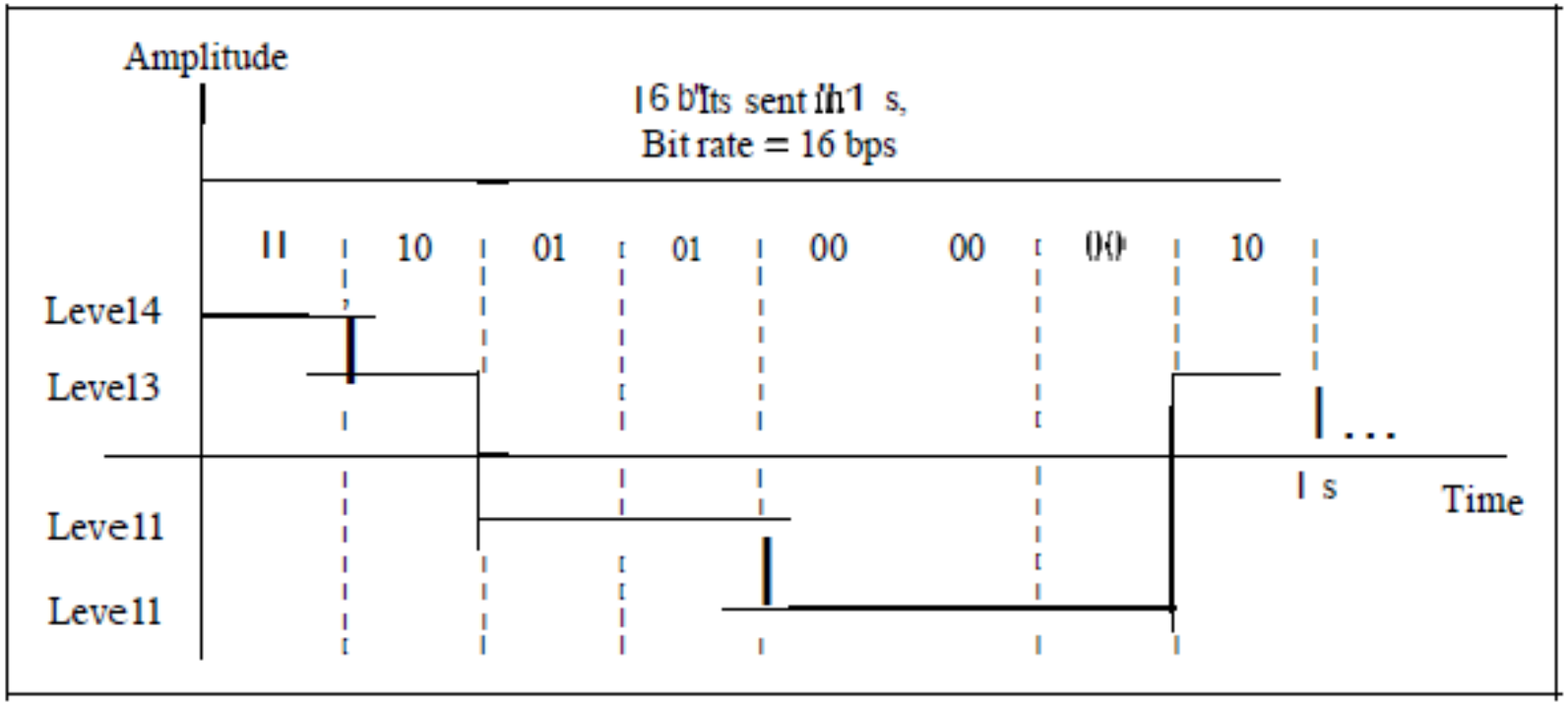
In addition to being represented by an analog signal, information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage.

A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level. Following figure shows two signals, one with two levels and the other with four.



a. A digital signal with two levels

Digital Signal



b. A digital signal with four levels

Note: If a signal has L levels, each level needs $\log_2 L$ bits.

Digital Signal

Example: A digital signal has eight levels. How many bits are needed per level?

Solution: Here, number of levels, L = 8.

Therefore, number of bits per level = $\log_2 L = \log_2 8 = 3$

Example: A digital signal has nine levels. How many bits are needed per level?

Solution: Here, number of levels, L = 9.

Therefore, number of bits per level = $\log_2 L = \log_2 9 = 3.17$ bits

However, this answer is not realistic. The number of bits sent per level needs to be an integer as well as a power of 2. For this example, 4 bits can represent one level.

Digital Signal

Bit rate

The bit rate is the number of bits sent in 1 second. It is expressed in bits per second (bps).

Bit length

The bit length is the distance one bit occupies on the transmission medium.

Bit length =propagation speed x bit duration

Digital Signal

Baud rate

It is the rate at which a signal level changes over a given period of time.

Baud rate = Bit rate / bits per signal level

When binary bits are transmitted as an electrical signal with two levels 0 and 1, the bit rate and baud rate are the same.

Example:

Consider bit rate is 8 bps and number of signal levels is 4. find baud rate.

Solution: Number of bits required per signal level = 2

Therefore, Baud rate = 8/2 = 4 bauds

TRANSMISSION IMPAIRMENT

- Signals travel through transmission media, which are not perfect.
- The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received.
- Three causes of impairment are attenuation, distortion, and noise.

Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

Attenuation

Decibel

The decibel (dB) measures the relative strengths of two signals or one signal at two different points.

Note: The decibel is negative if a signal is attenuated and positive if a signal is amplified.

$$\mathrm{dB} = 10 \log_{10} \frac{P_2}{P_1}$$

Variables P_1 and P_2 are the powers of a signal at points 1 and 2, respectively.

Attenuation

Example: Suppose a signal travels through a transmission medium and its power is reduced to one-half. Find its attenuation.

Solution:

Clearly $P_2 = P_1/2$,

Therefore ,

$$\text{Attenuation(dB)} = 10 \log_{10} (P_2/P_1) = 10 \log_{10} (1/2)$$

$$= 10*(-0.3) = -3 \text{ dB}$$

Example: A signal travels through an amplifier, and its power is increased 10 times. Find its attenuation.

Solution:

Clearly $P_2 = 10P_1$,

Therefore ,

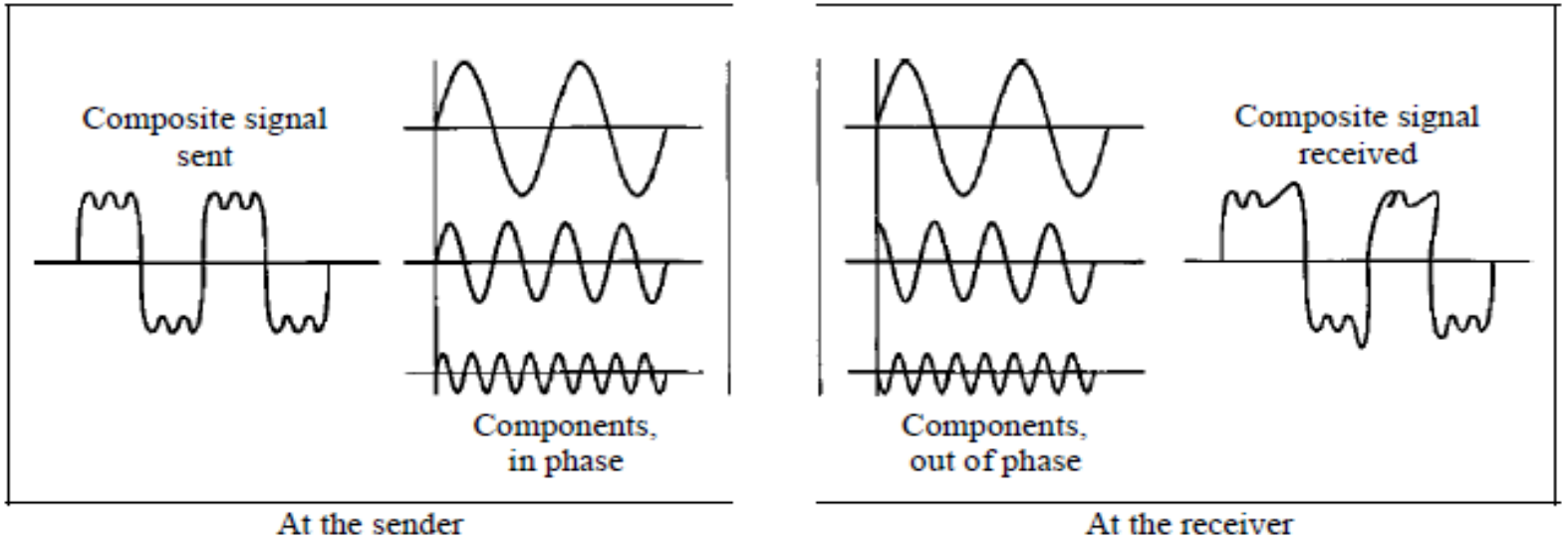
$$\text{Attenuation(dB)} = 10 \log_{10} (P_2/P_1)$$

$$= 10* \log_{10}(10)$$

$$= 10 \text{ dB}$$

Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed (see the next section) through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender. The shape of the composite signal is therefore not the same. Following figure shows the effect of distortion on a composite signal.



Noise

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.

Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

Noise

Signal-to-Noise Ratio(SNR)

The signal-to-noise ratio is defined as

$$\textbf{SNR} = \frac{\textbf{average signal power}}{\textbf{average noise power}}$$

Note: A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

Because SNR is the ratio of two powers, it is often described in decibel units, SNR(dB), defined as

$$\textbf{SNR(dB)} = 10 \log_{10} \textbf{SNR}$$

Example :

The power of a signal is 10 mW and the power of the noise is 1 μW; what are the values of SNR and SNR(dB)?

Example : Find SNR and SNR(dB) for noiseless channel.

Noiseless Channel: Nyquist Bit Rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate.

$$\textbf{Bit Rate} = 2 \times B \times 10 \log_2 L$$

In this formula, **B** is the bandwidth of the channel, **L** is the number of signal levels used to represent data, and **Bit Rate** is the bit rate in bits per second.

Note: Increasing the levels of a signal may reduce the reliability of the system.

Example: Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. Find the maximum bit rate.

Solution: Bit Rate = $2 \times 3000 \times \log_2 2 = 6000$ bps

Noise

Example: We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Solution:

We can use the Nyquist formula as shown:

$$265{,}000 = 2 \times 20{,}000 \times \log_2 L$$

$$\log_2 L = 6.625$$

Therefore, $L = 2^{6.625} = 98.7$ levels

Since this result is not a power of 2, we need to either increase the number of levels or reduce the bit rate. If we have 128 levels, the bit rate is 280 kbps. If we have 64 levels, the bit rate is 240 kbps.

Noisy Channel: Shannon Capacity

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

$$\mathbf{C = B \times \log_2 (1 + SNR)}$$

In this formula, **B** is the bandwidth of the channel, **SNR** is the signal-to-noise ratio, and **C** is the capacity of the channel in bits per second.

Note: We cannot achieve a data rate higher than the capacity of the channel.

Noisy Channel: Shannon Capacity

Example: A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communications. The signal-to-noise ratio is usually 3162. Compute the capacity of this channel.

Solution:

$$C = B \log_2 (1 + SNR) = 3000 \log_2 (1 + 3162) = 3000 \log_2 3163$$

$$= 3000 \times 11.62 = 34{,}860 \text{ bps}$$

Note: This means that the highest bit rate for a telephone line is 34.860 kbps. If we want to send data faster than this, we can either increase the bandwidth of the line or improve the signal-to-noise ratio.

Noisy Channel: Shannon Capacity

Example: The signal-to-noise ratio is often given in decibels. Assume that SNR(dB) = 36 and the channel bandwidth is 2 MHz. Compute the theoretical channel capacity.

Solution:

We know that, $SNR(dB) = 10 \log_{10} SNR$

Therefore, $36 = 10 \log_{10} SNR$

$SNR = 10^{3.6} = 3981$

Now, Channel capacity $C = B^* \log_2(1+SNR)$

$= 2 * 10^6 \log_2(1+3981)$

$= 24$ Mbps (approx.)

Note: For practical purposes, when the SNR is very high, we can assume that SNR + 1 is almost the same as SNR. In these cases, the theoretical channel capacity can be simplified to

C = B X SNR(dB)/3

Noisy Channel: Shannon Capacity

Example: We have a channel with a 1-MHz bandwidth. The SNR for this channel is 63. What are the appropriate bit rate and signal level?

Solution:

First, we use the Shannon formula to find the upper limit.

$C = B * \log_2 (1 + SNR) = 10^6 * \log_2 (1 + 63) = 10^6 * \log_2 64 = 6$ Mbps

The Shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps, for example. Then we use the Nyquist formula to find the number of signal levels.

$$\text{Bit rate} = 2 * B * \log_2 L$$

$$4 \times 10^6 = 2 \times 10^6 \times \log_2 L$$

Therefore, $L = 4$

Noisy Channel: Shannon Capacity

Example: If a binary signal is sent over a 3 kHz channel whose signal to noise ratio is 20dB. What is the maximum achievable data rate ?

Solution:

$$SNR(dB) = 10 * \log_{10} SNR$$

$$20 = 10 * \log_{10} SNR$$

$$SNR = 100$$

For maximum achievable data rate

$$C = B * \log_2 (1 + SNR) = 3000 * \log_2 (1 + 100) = 3000 * \log_2 101$$

$$= 3000 * 6.658 = 19.974 \text{ kbps}$$

$$\text{Nyquist Bit rate} = 2*B*\log_2 L = 2*3000*\log_2 2$$

$$= 6000 \text{ kbps}$$

The bottleneck is therefore the Nyquist limit giving a maximum channel capacity of **6** kbps.

PERFORMANCE

Bandwidth

One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second.

Bandwidth in Hertz

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

PERFORMANCE

Throughput

- The throughput is a measure of how fast we can actually send data through a network.
- For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.
- Imagine a highway designed to transmit 1000 cars per minute from one point to another. However, if there is congestion on the road, this figure may be reduced to 100 cars per minute. The bandwidth is 1000 cars per minute; the throughput is 100 cars per minute.

Note: The bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

PERFORMANCE

Example :

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution:

We can calculate the throughput as

$$\text{Throughput} = \frac{12{,}000 \times 10{,}000}{60} = 2 \text{ Mbps}$$

The throughput is almost one-fifth of the bandwidth in this case.

PERFORMANCE

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

Latency is made of four components: propagation time, transmission time, queuing time and processing time.

$$\text{Latency} = \text{propagation time} + \text{transmission time} + \text{queuing time} + \text{processing time}$$

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination.

$$\text{Propagation time} = \frac{\text{Distance}}{\text{Propagation speed}}$$

PERFORMANCE

Example:

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4 x 10^8 m/s in cable.

Solution:

We can calculate the propagation time as

$$\text{Propagation time} = \frac{12000 \text{ x } 1000}{2.4 \text{ x } 108} = 50 \text{ ms}$$

Transmission time

The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

$$\text{Transmission time} = \frac{\text{Message size}}{\text{Bandwidth}}$$

PERFORMANCE

Example:

What are the propagation time and the transmission time for a 2.5-kbyte message (an e-mail) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution:

We can calculate the propagation and transmission time as

$$\text{Propagation time} = \frac{12000 \times 1000}{2.4 \times 108} = 50 \text{ ms}$$

$$\text{Transmission time} = \frac{2.5 \times 1000 \times 8}{10^9} = 0.020 \text{ ms}$$

PERFORMANCE

Queuing Time

It is the time needed for each intermediate or end device to hold the message before it can be processed.

- The queuing time is not a fixed factor; it changes with the load imposed on the network.
- When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues the arrived messages and processes them one by one. If there are many messages, each message will have to wait.

Processing time

It is the time taken by intermediate or end devices to process the arrived message.

PERFORMANCE

Bandwidth-delay product

The bandwidth-delay product defines the number of bits that can fill the link.

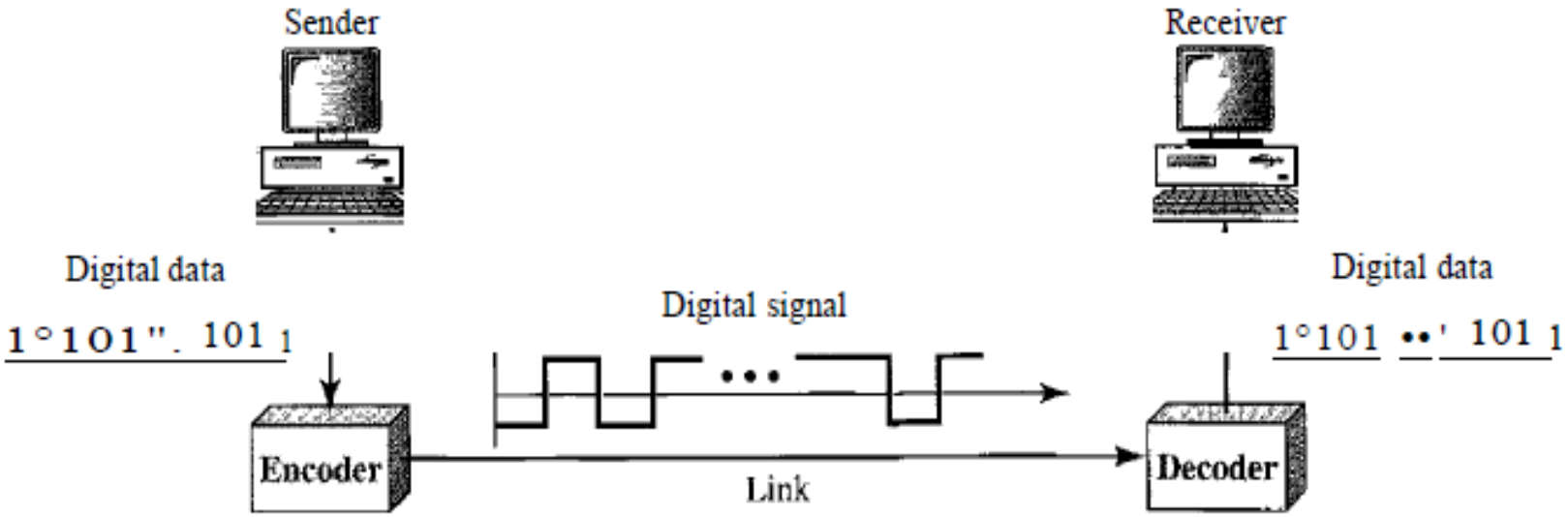
Bandwidth-delay product = Bandwidth * Propagation time

Encoding Schemes

Line Coding Schemes:

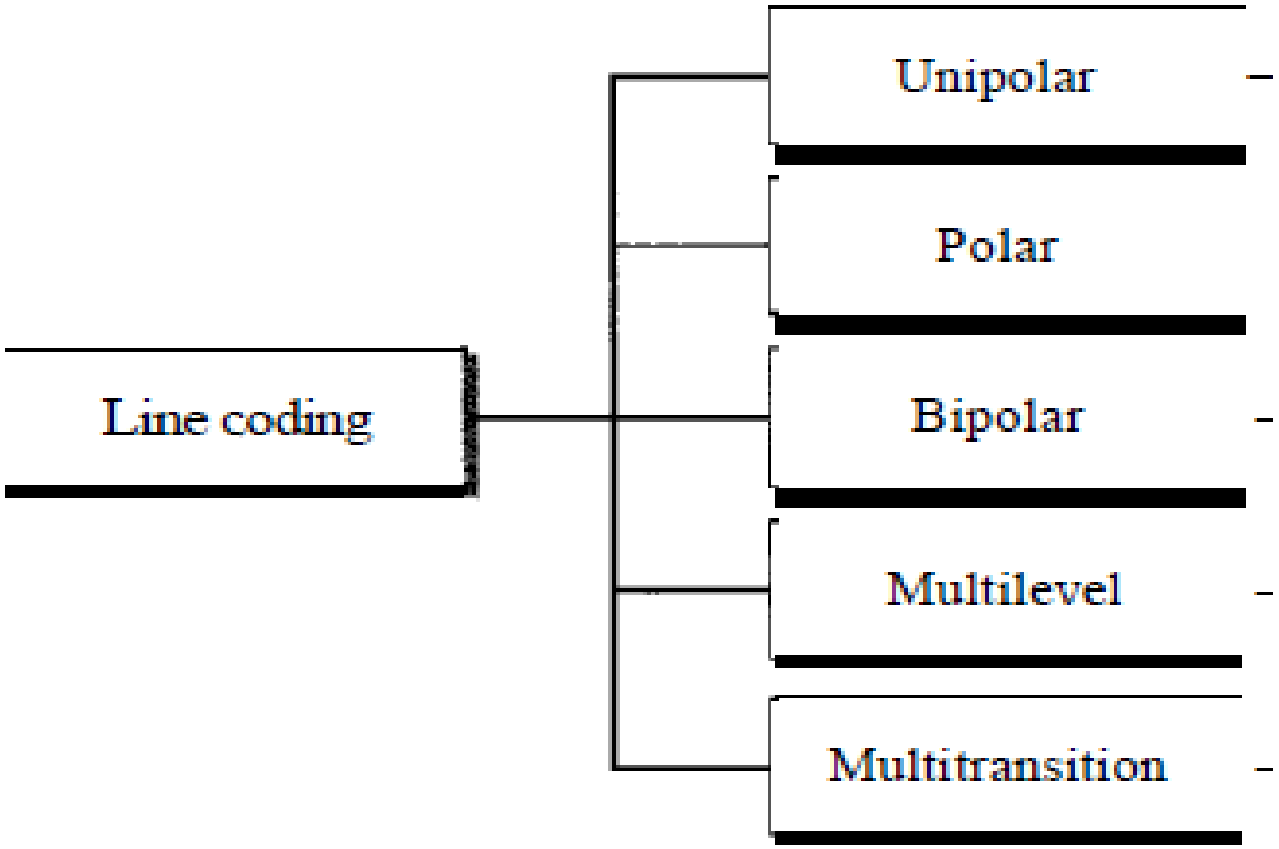
Line coding is the process of converting digital data to digital signals. We assume that data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits.

Line coding converts a sequence of bits to a digital signal. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal. Following figure shows the process.



Encoding Schemes

We can roughly divide line coding schemes into five broad categories, as the following:-

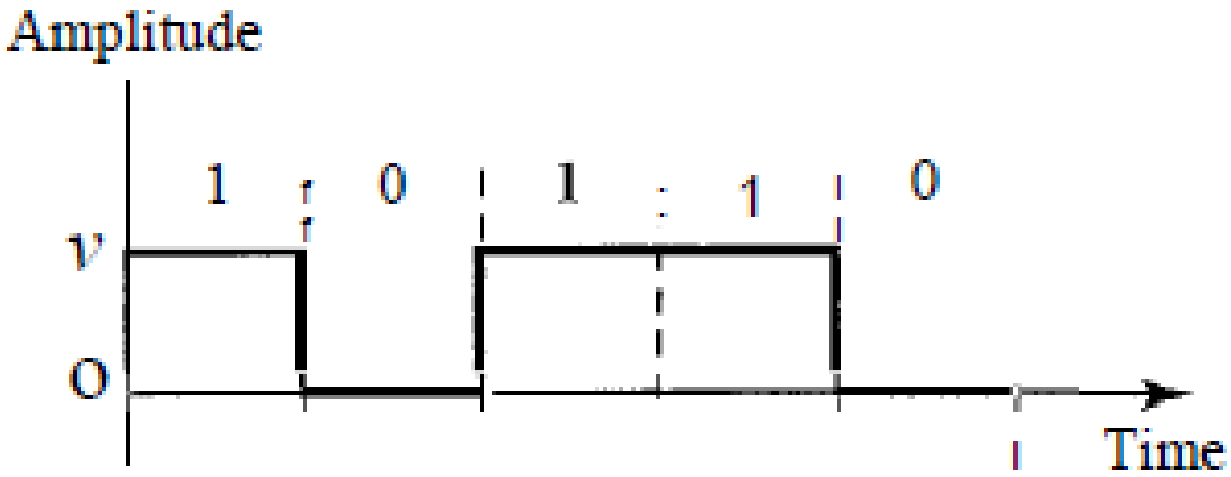


Encoding Schemes

Unipolar Scheme:

In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below.

NRZ (Non-Return-to-Zero): Traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit 1 and the zero voltage defines bit 0. It is called NRZ because the signal does not return to zero at the middle of the bit. Following figure shows a unipolar NRZ scheme.



Encoding Schemes

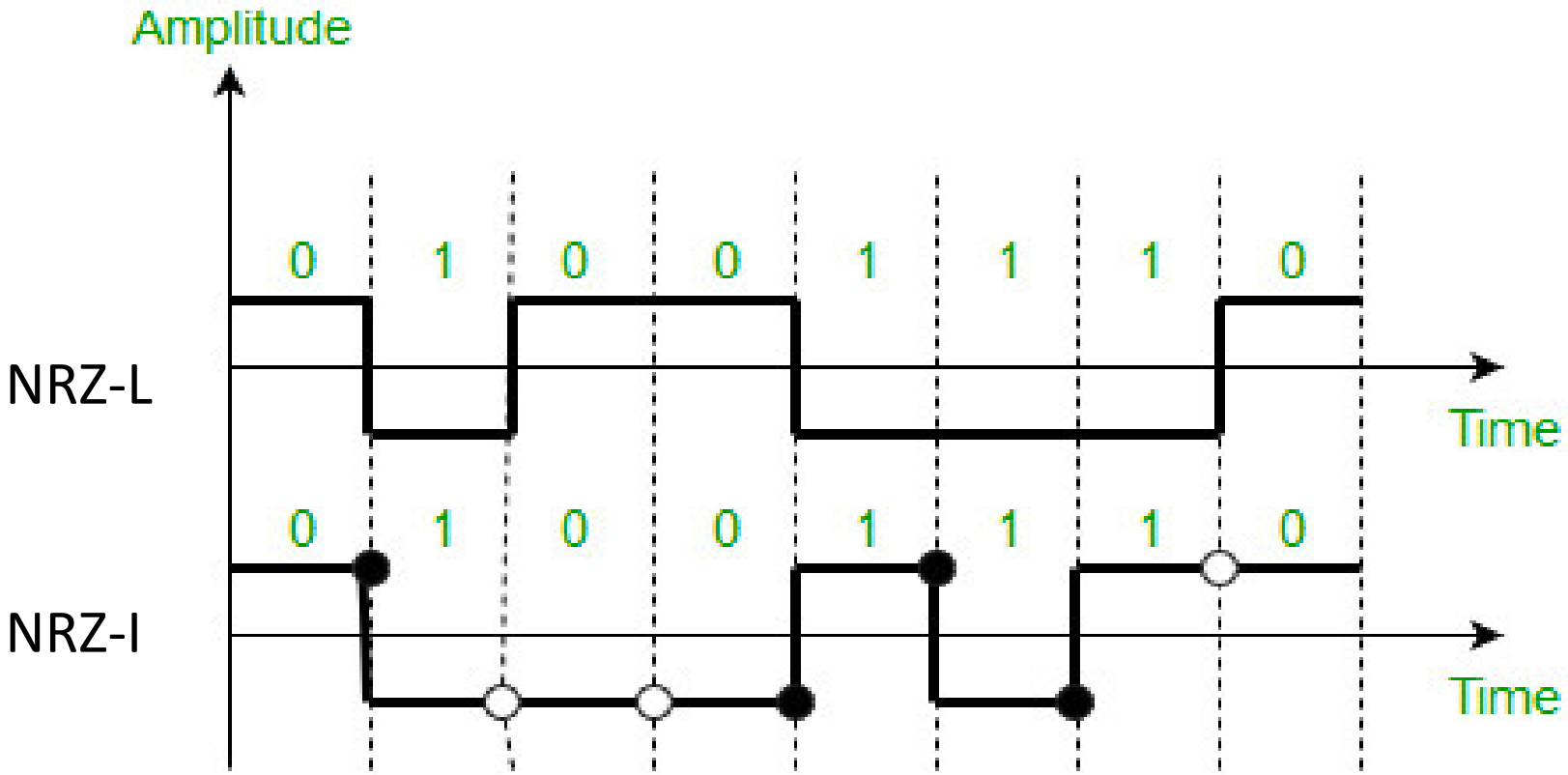
Polar Schemes:

In polar schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.

Non-Return-to-Zero (NRZ):

- In polar NRZ encoding, we use two levels of voltage amplitude. There are two versions of polar NRZ: NRZ-L and NRZ-I.
- In the first variation, NRZ-L (NRZ-Level), the level of the voltage determines the value of the bit.
- In the second variation, NRZ-I (NRZ-Invert), the change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1.

Encoding Schemes

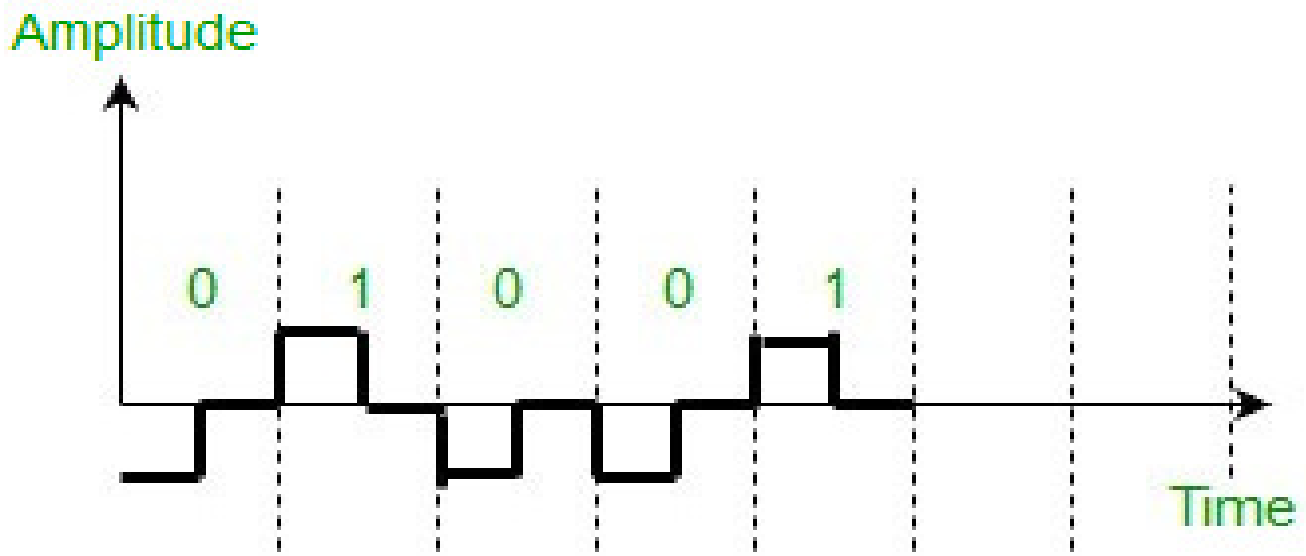


Note: In NRZ-L the level of the voltage determines the value of the bit. In NRZ-I the inversion or the lack of inversion determines the value of the bit.

Encoding Schemes

Return to Zero (RZ):

Return-to-zero (RZ) scheme uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit. It remains there until the beginning of the next bit.



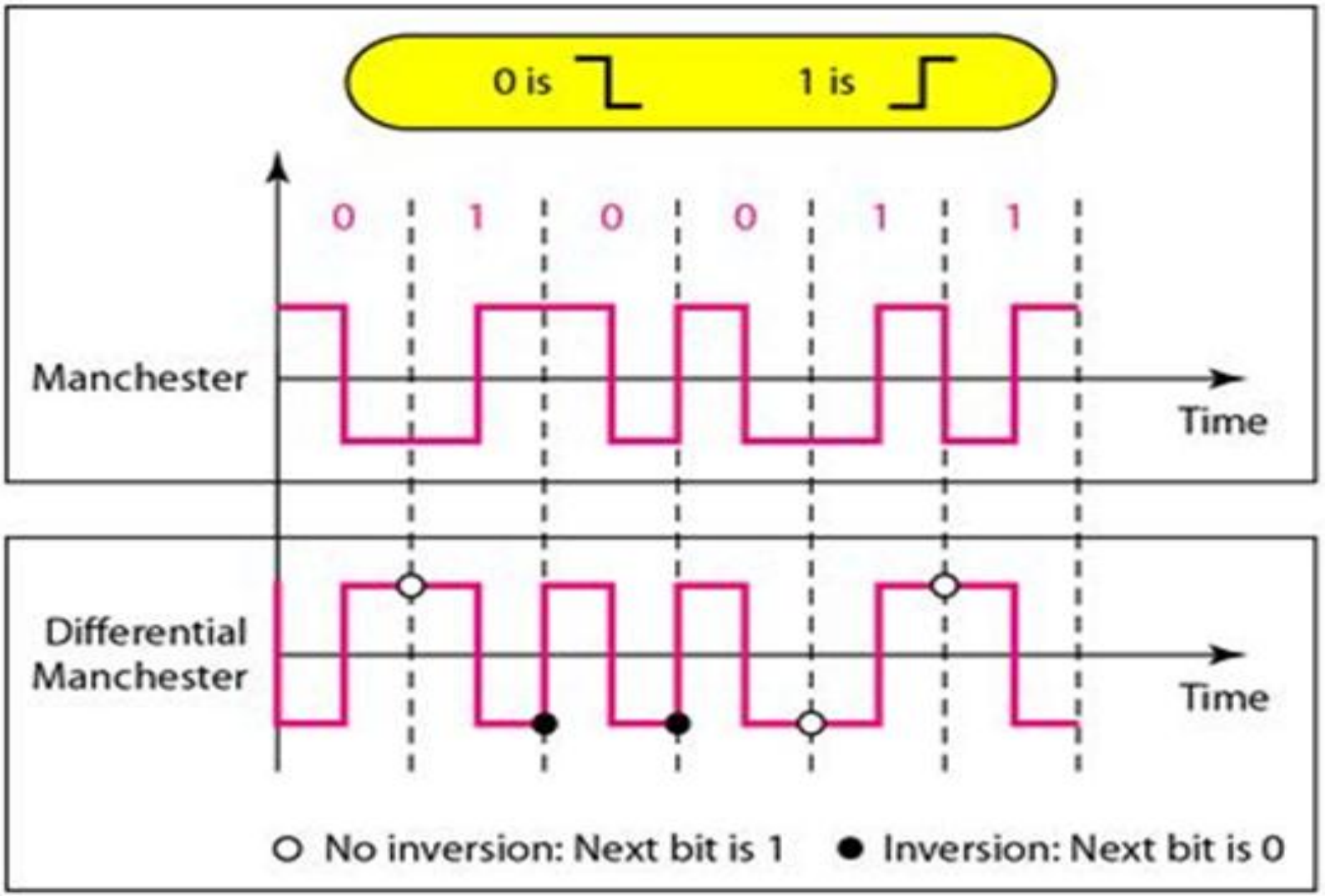
Encoding Schemes

Biphase: Manchester and Differential Manchester:

- The idea of RZ and the idea of NRZ-L are combined into the Manchester scheme. In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half.

- Differential Manchester, on the other hand, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none.

Encoding Schemes



Encoding Schemes

Bipolar Schemes:

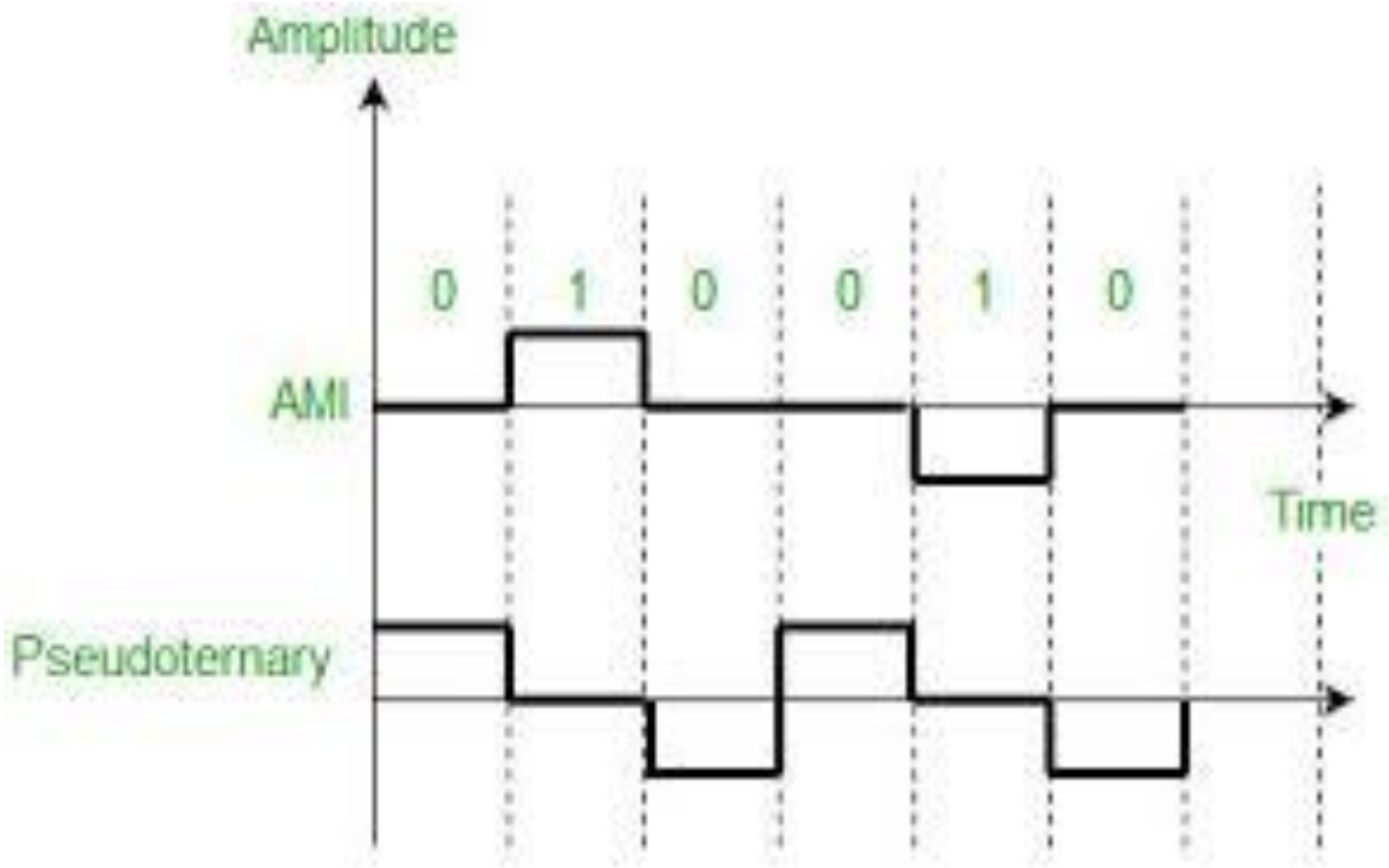
In bipolar encoding (sometimes called multilevel binary), there are three voltage levels: positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.

AMI and Pseudoternary:

There are two variations of bipolar encoding: AMI and pseudoternary.

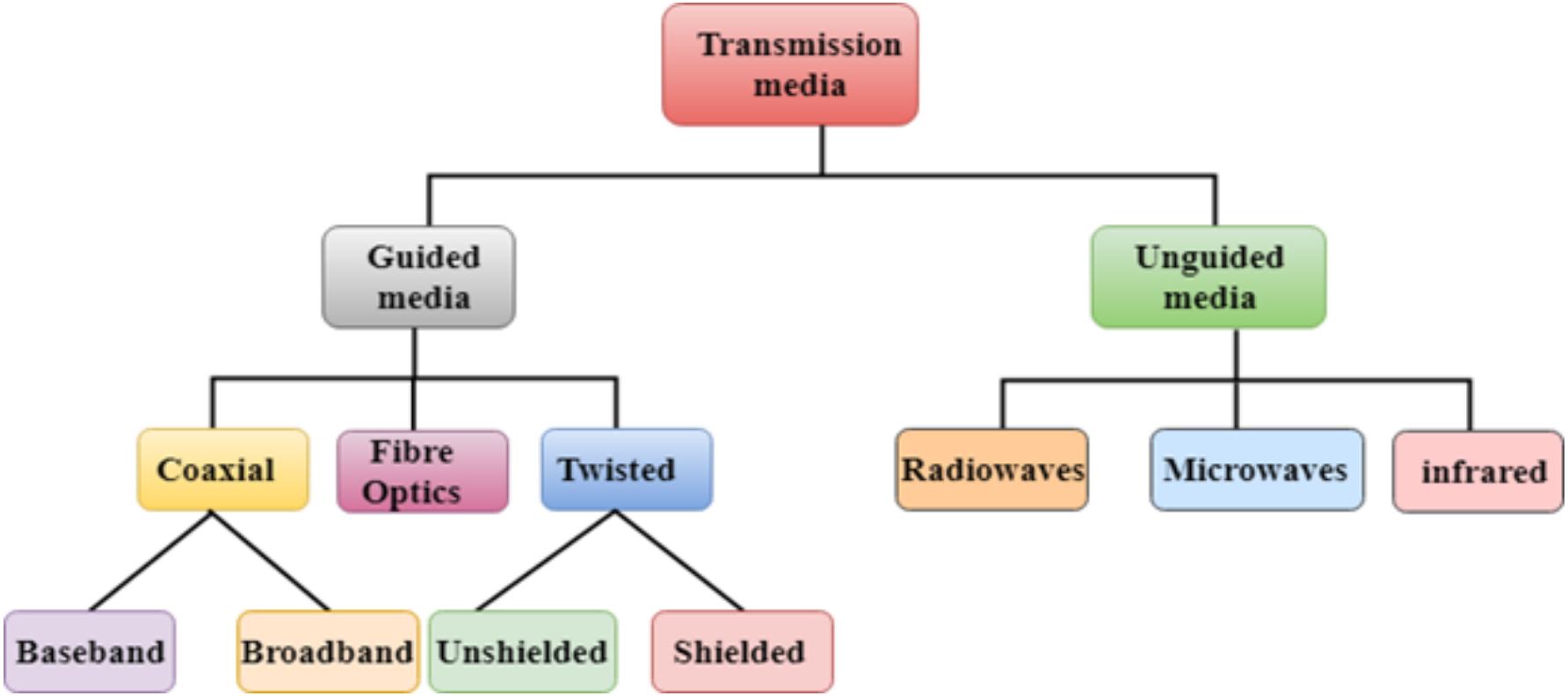
- A common bipolar encoding scheme is called bipolar alternate mark inversion (AMI). In the term alternate mark inversion, the word mark comes from telegraphy and means 1. So AMI means alternate 1 inversion. A neutral zero voltage represents binary 0. Binary 1's are represented by alternating positive and negative voltages.
- A variation of AMI encoding is called pseudoternary in which the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negative voltages.

Encoding Schemes



Transmission Media

- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.



GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

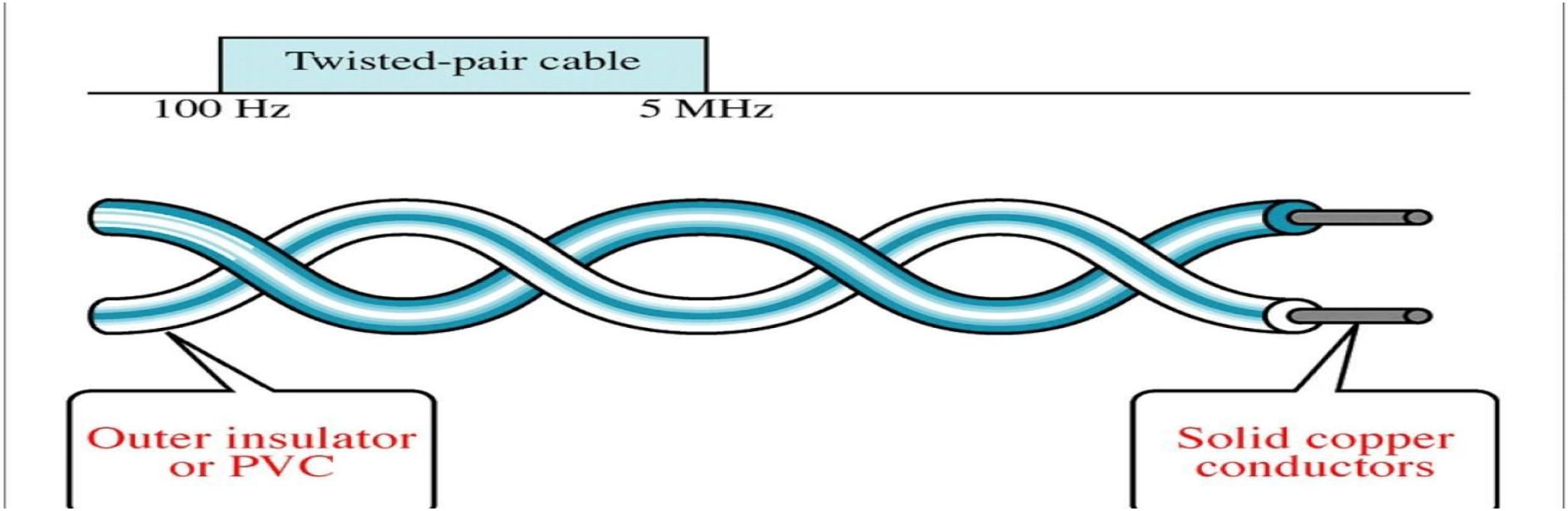
GUIDED MEDIA

Twisted-Pair Cable

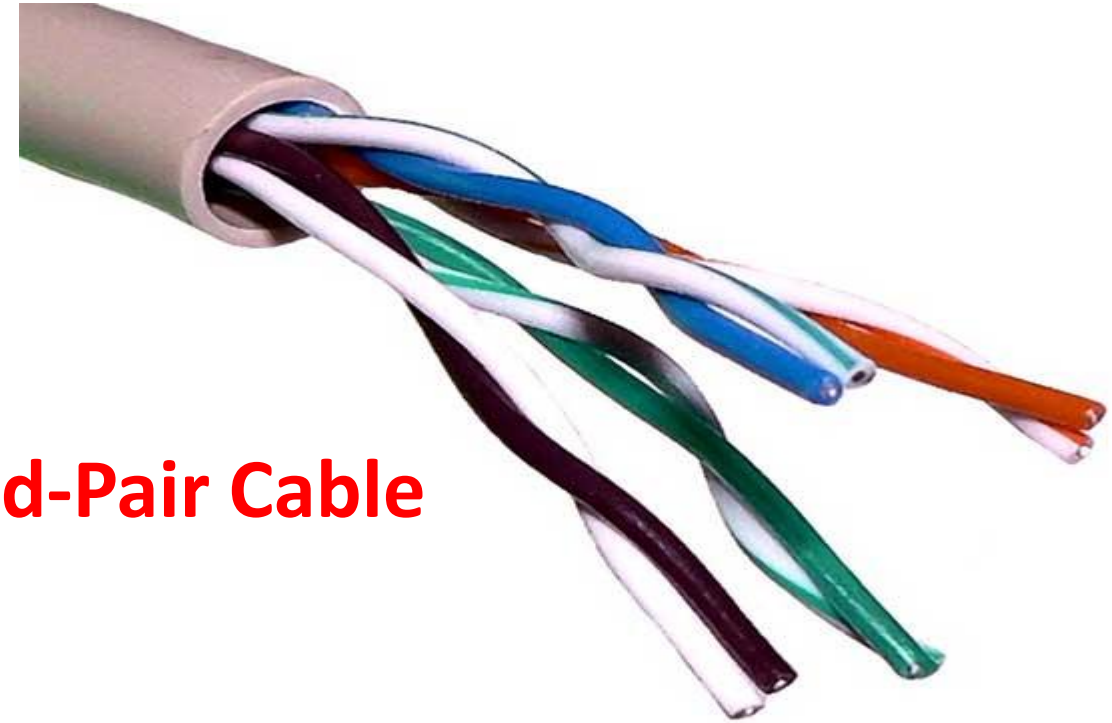
A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference.

The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.

The receiver uses the difference between the two.



GUIDED MEDIA



Twisted-Pair Cable

GUIDED MEDIA

There are two types of twisted pair cables:

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (UTP) Cable

Unshielded Twisted Pair (UTP) Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).

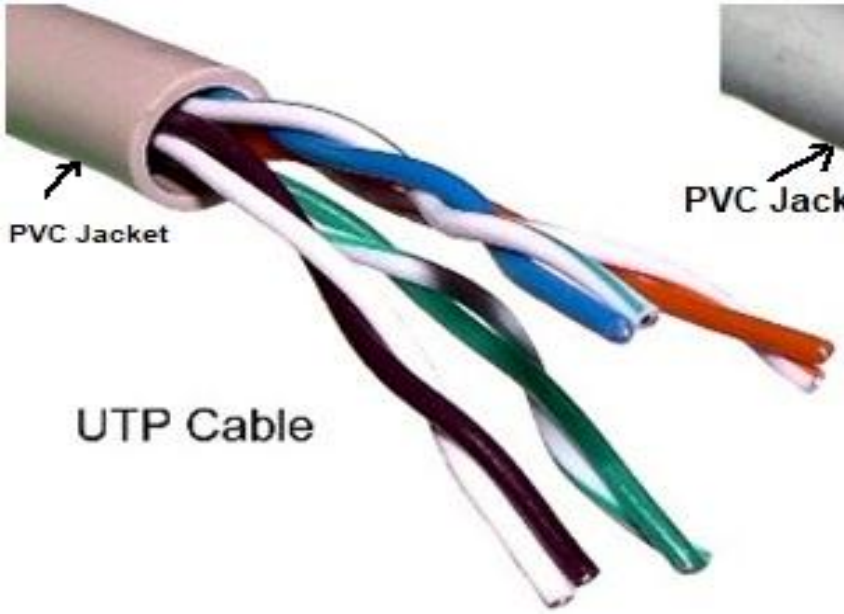
The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

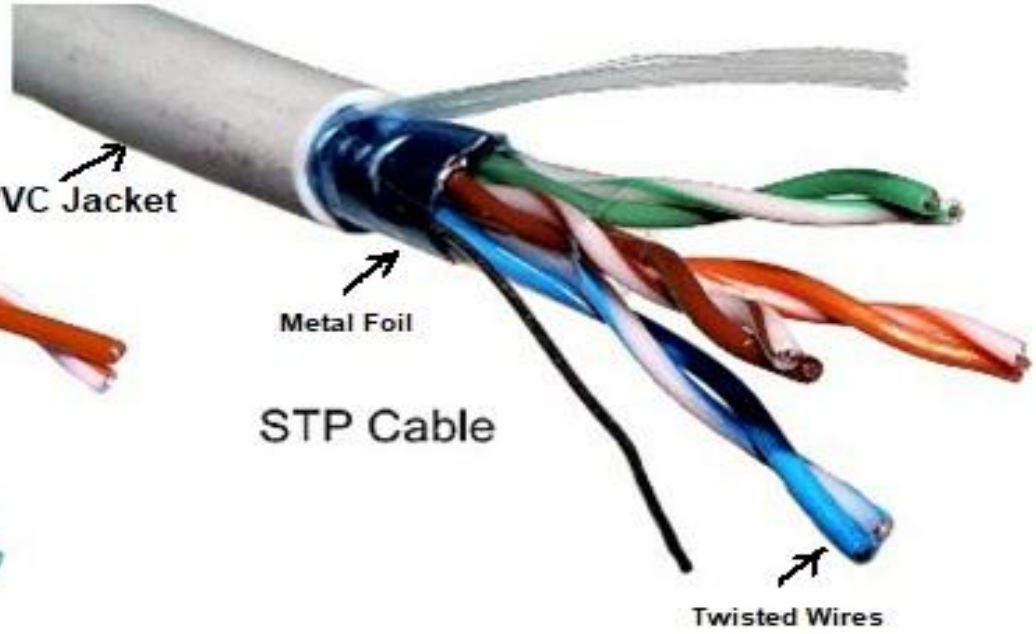
In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

Shielded Twisted Pair (STP) Cable

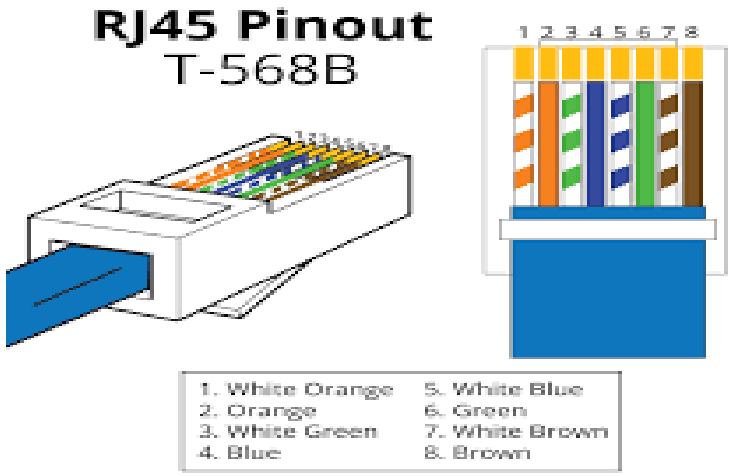
STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.

GUIDED MEDIA





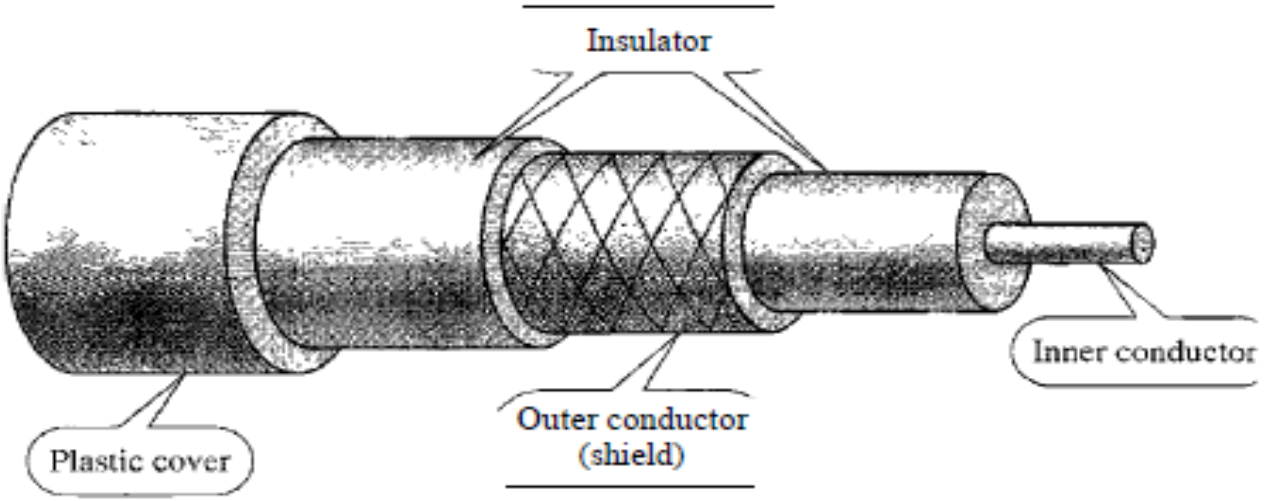
RJ45 connector



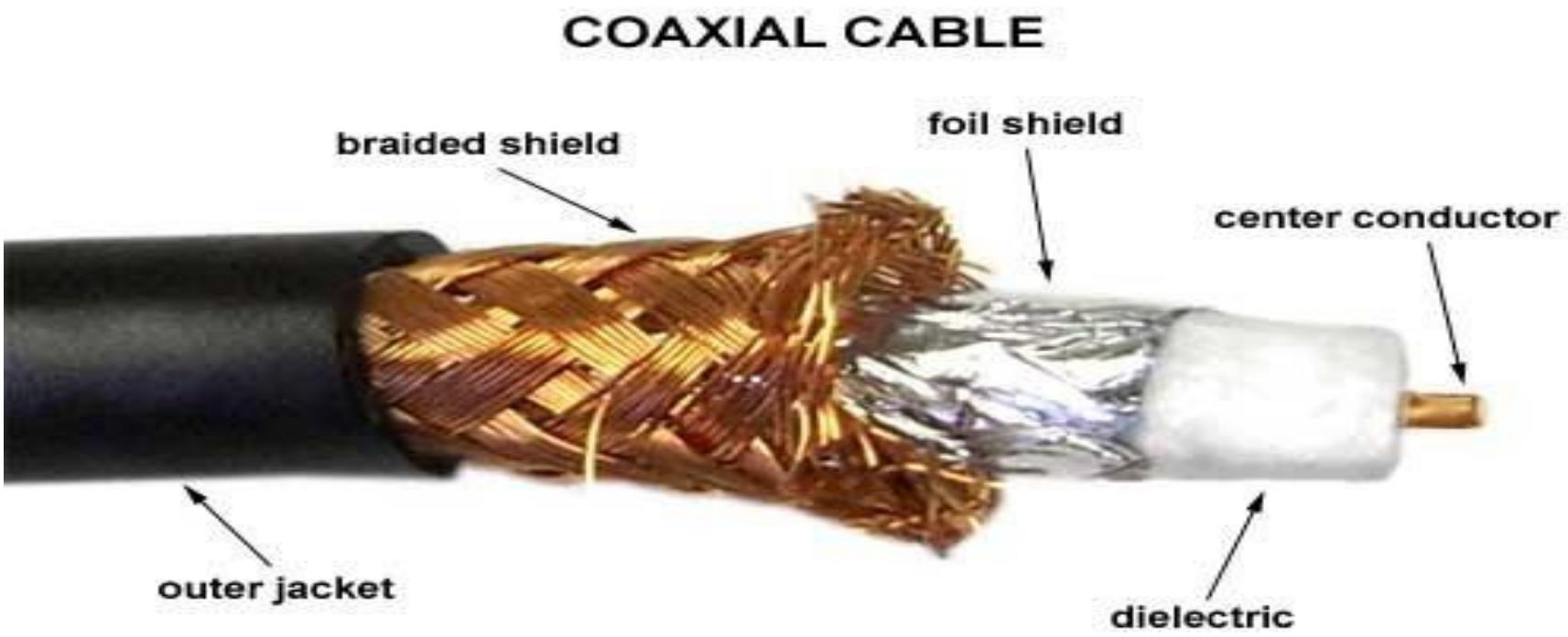
Guided Media

Coaxial Cable

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable Instead of having two wires. Coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Guided Media



Guided Media

Coaxial Cable Standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

Category	Use
RG-59	Cable TV
RG-58	Thin Ethernet
RG-11	Thick Ethernet

Guided Media

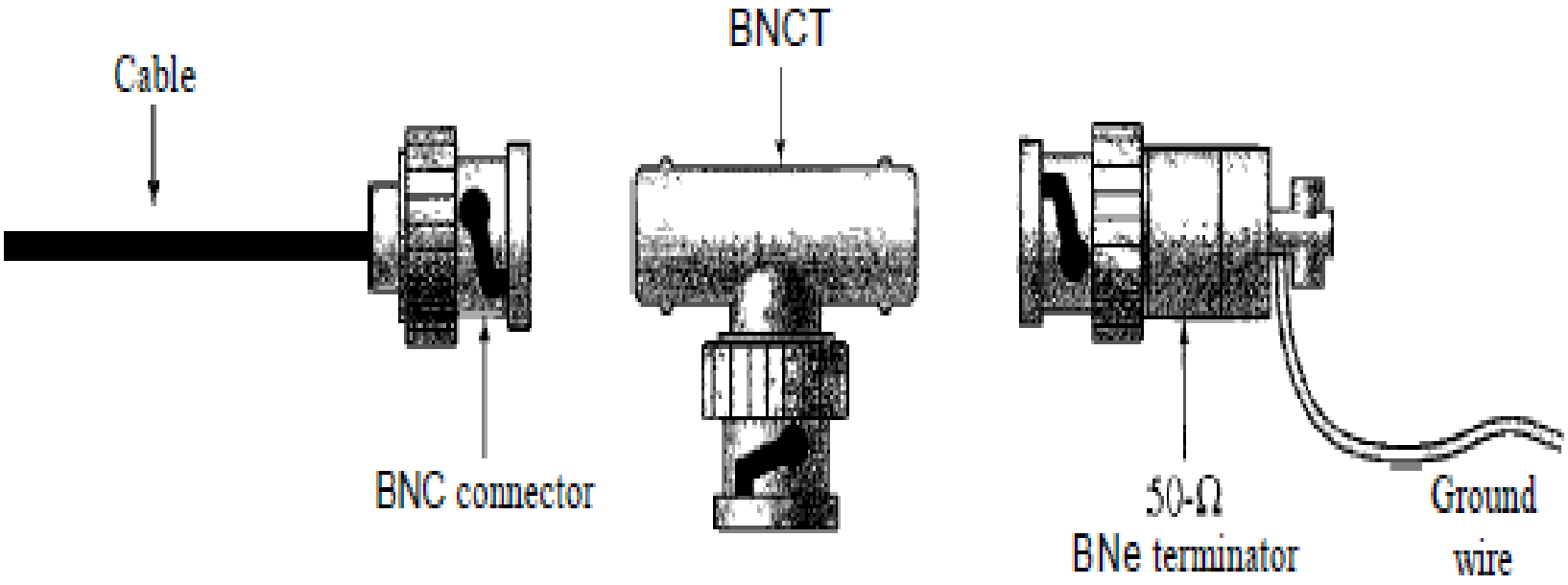
Coaxial Cable Connectors

The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. Three popular types of these connectors are the BNC connector, the BNC-T connector, and the BNC terminator.

- The BNC connector is used to connect the end of the cable to a device, such as a TV set.
- The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device.
- The BNC terminator is used at the end of the cable to prevent the reflection of the signal.

Guided Media

Coaxial Cable Connectors

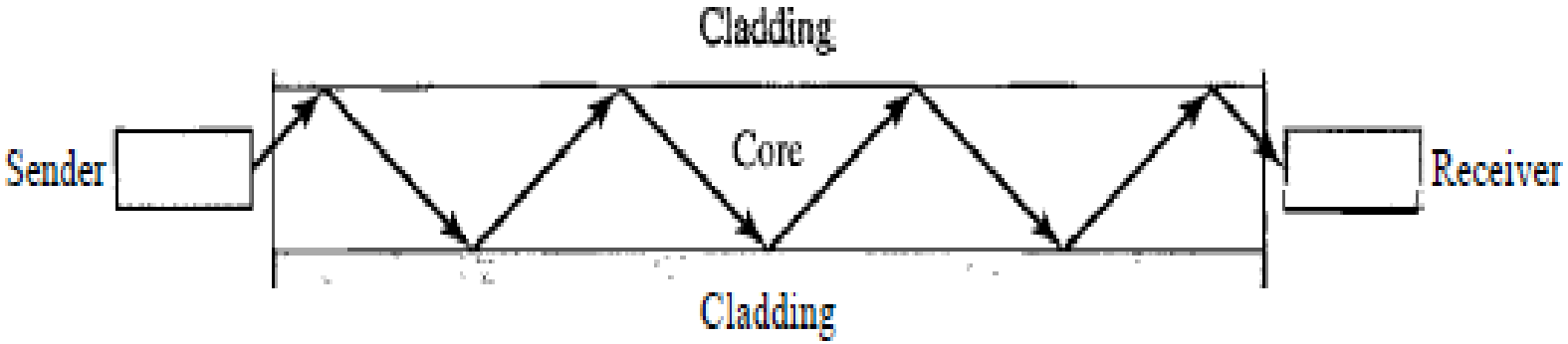


Guided Media

Fiber-Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

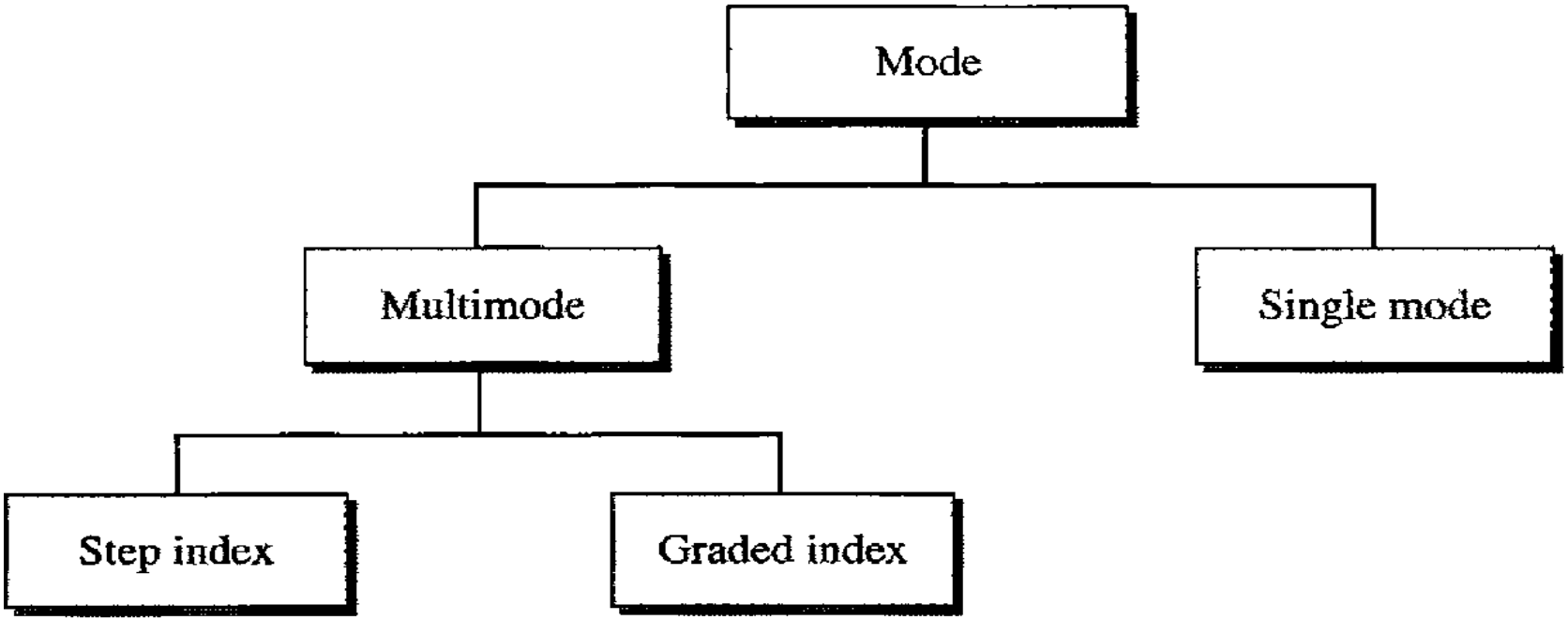
Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



Guided Media

Propagation Modes

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.



Guided Media

Multimode

In this mode, multiple beams from a light source move through the core in different paths.

In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

A graded-index fiber is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

Guided Media

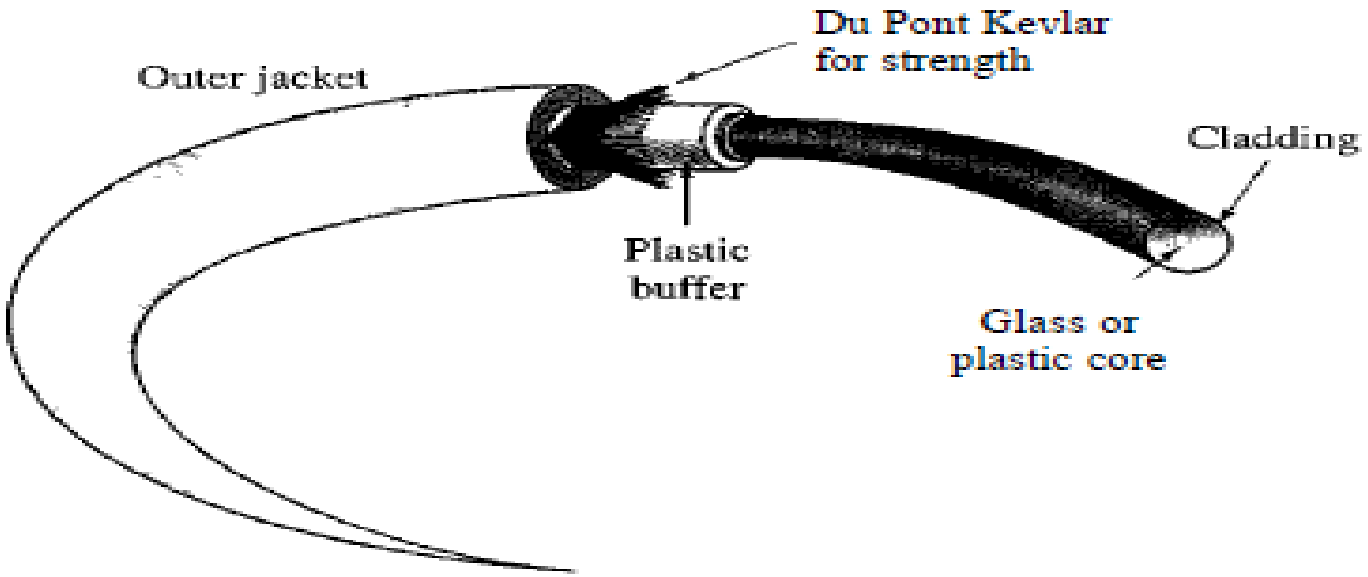
Single-Mode

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

Guided Media

Cable Composition

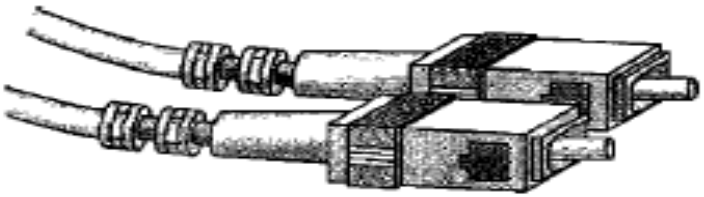
Following figure shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.



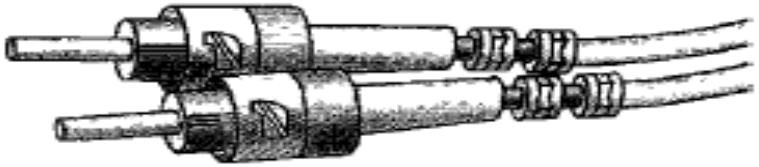
Guided Media

Fiber-Optic Cable Connectors

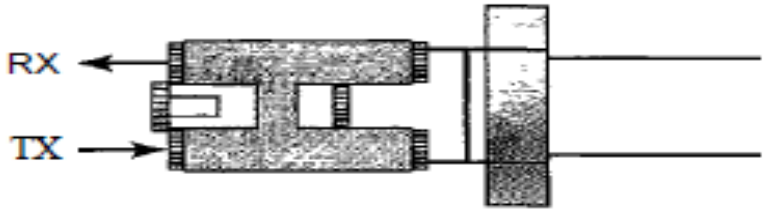
There are three types of connectors for fiber-optic cables, as shown in figure:



SC connector



ST connector



MT-RJ connector

The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. MT-RJ is a connector that is the same size as RJ45.

Guided Media

Advantages of Optical Fiber

Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

- **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable.
- **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.
- **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper.
- **Light weight.** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping.** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Guided Media

Disadvantages of Optical Fiber

There are some disadvantages in the use of optical fiber.

- **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, then the use of optical fiber cannot be justified.

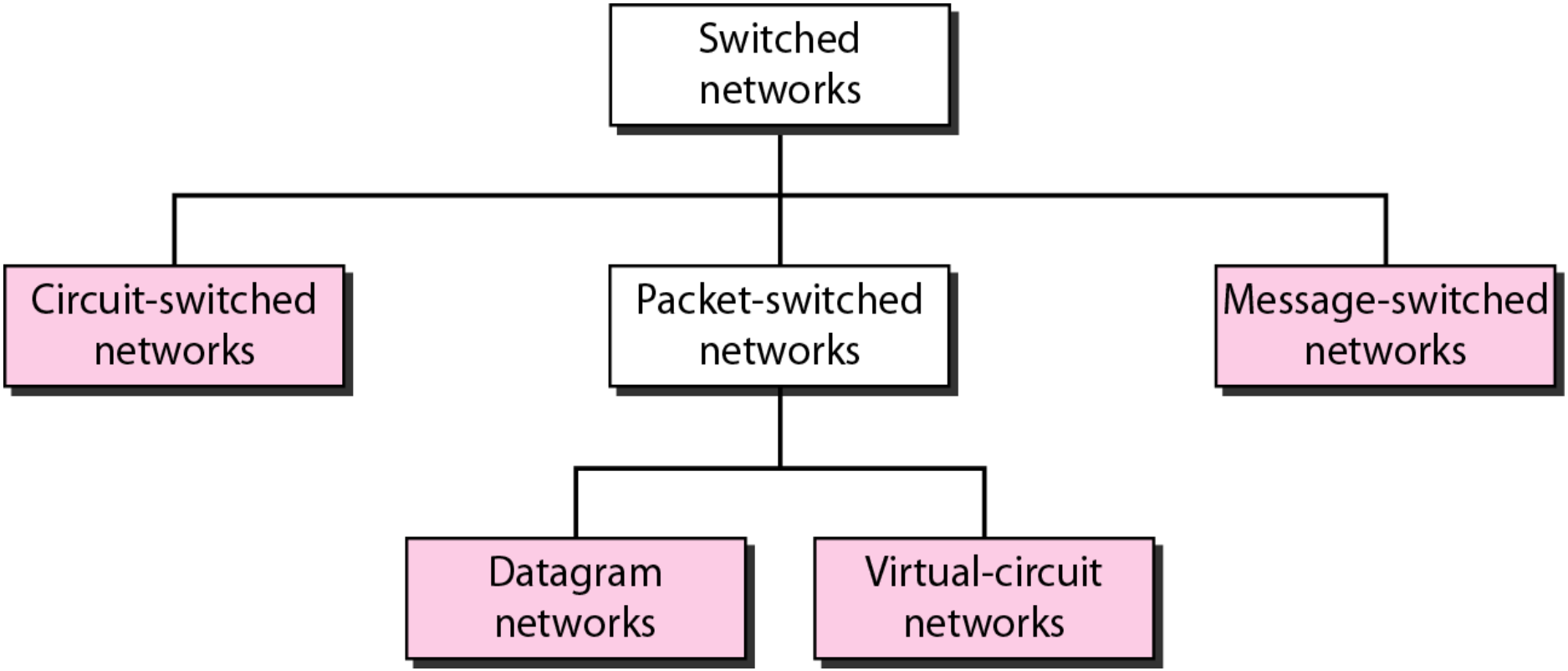
Switching

- The technique of transferring the information from one computer network to another network is known as switching.
- Switching in a computer network is achieved by using **switches**. A **switch** is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.

Switching

Switching techniques are classified in to the following three types:-

- Circuit Switching
- Packet Switching
- Message Switching

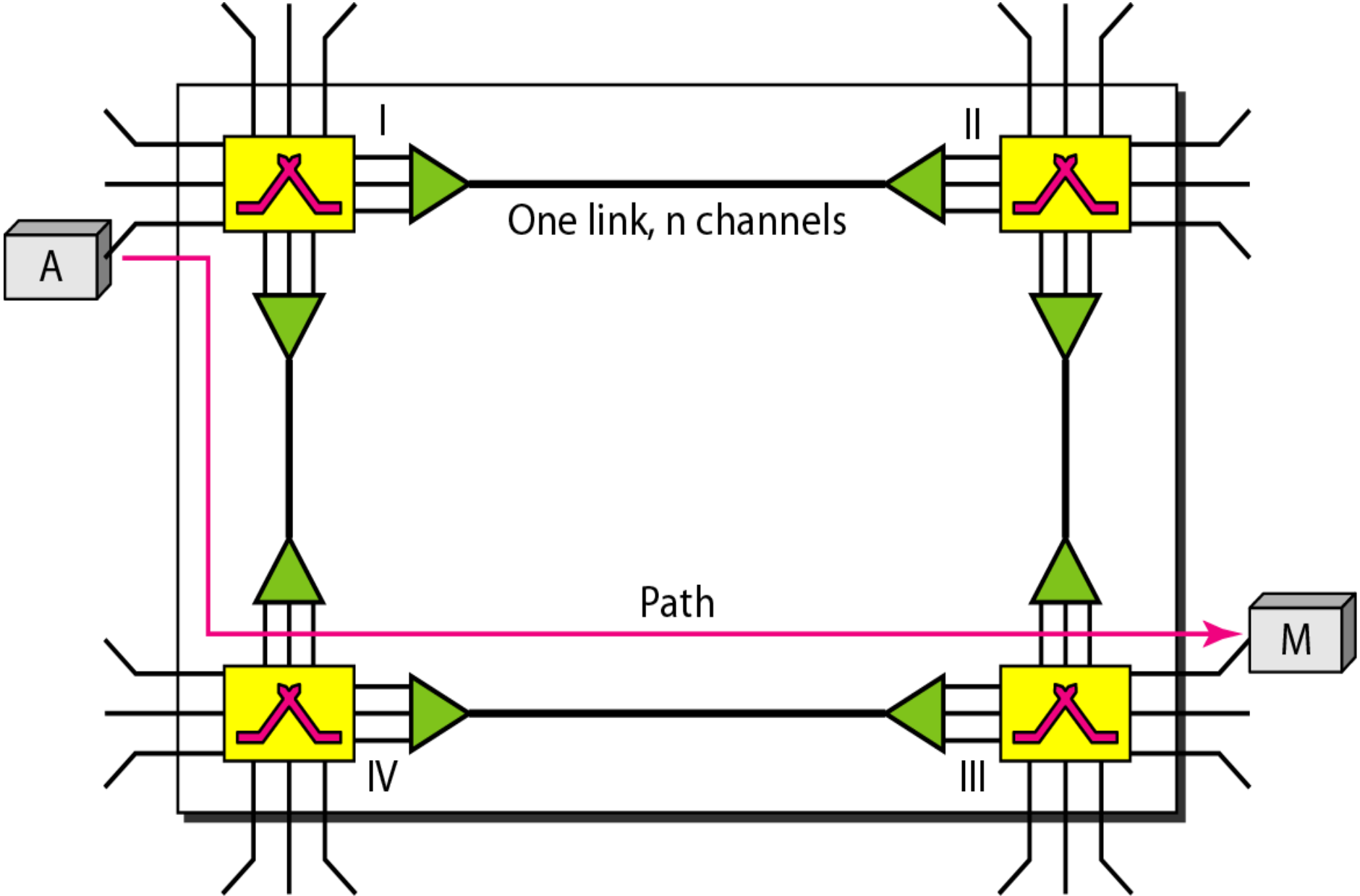


Switching

Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Switching



Switching

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established.

Connection setup means creating dedicated channels between the switches.

For example, in Figure, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

Switching

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency

Circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Delay

The delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

Note: Switching at the physical layer in the traditional telephone network uses the circuit-switching approach.

Switching

Packet Switching

The packet switching is a switching technique in which the message is divided into smaller pieces, and they are sent individually. The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.

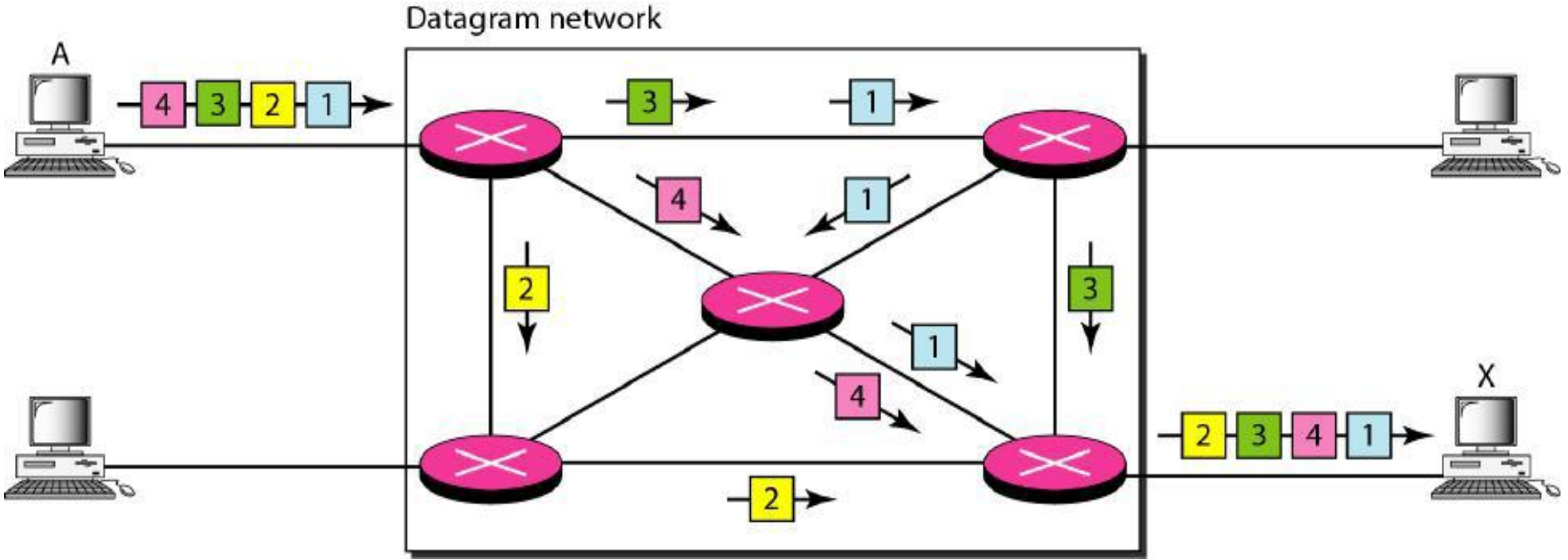
There are two types of packet switching.

1. Datagram Switching
2. Virtual Circuit Switching

Switching

Datagram Switching

- In a datagram network, each packet is treated independently of all others.
- Packets in this approach are referred to as datagrams.
- Datagram switching is normally done at the network layer.
- Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.



Switching

A switch in a datagram network uses a routing table that is based on the destination address. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

Note: Switching in the Internet is done by using the datagram packet switching at the network layer.

Switching

Virtual Circuit Switching

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3. As in a datagram network, data are packetized and each packet carries an address in the header.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

Switching

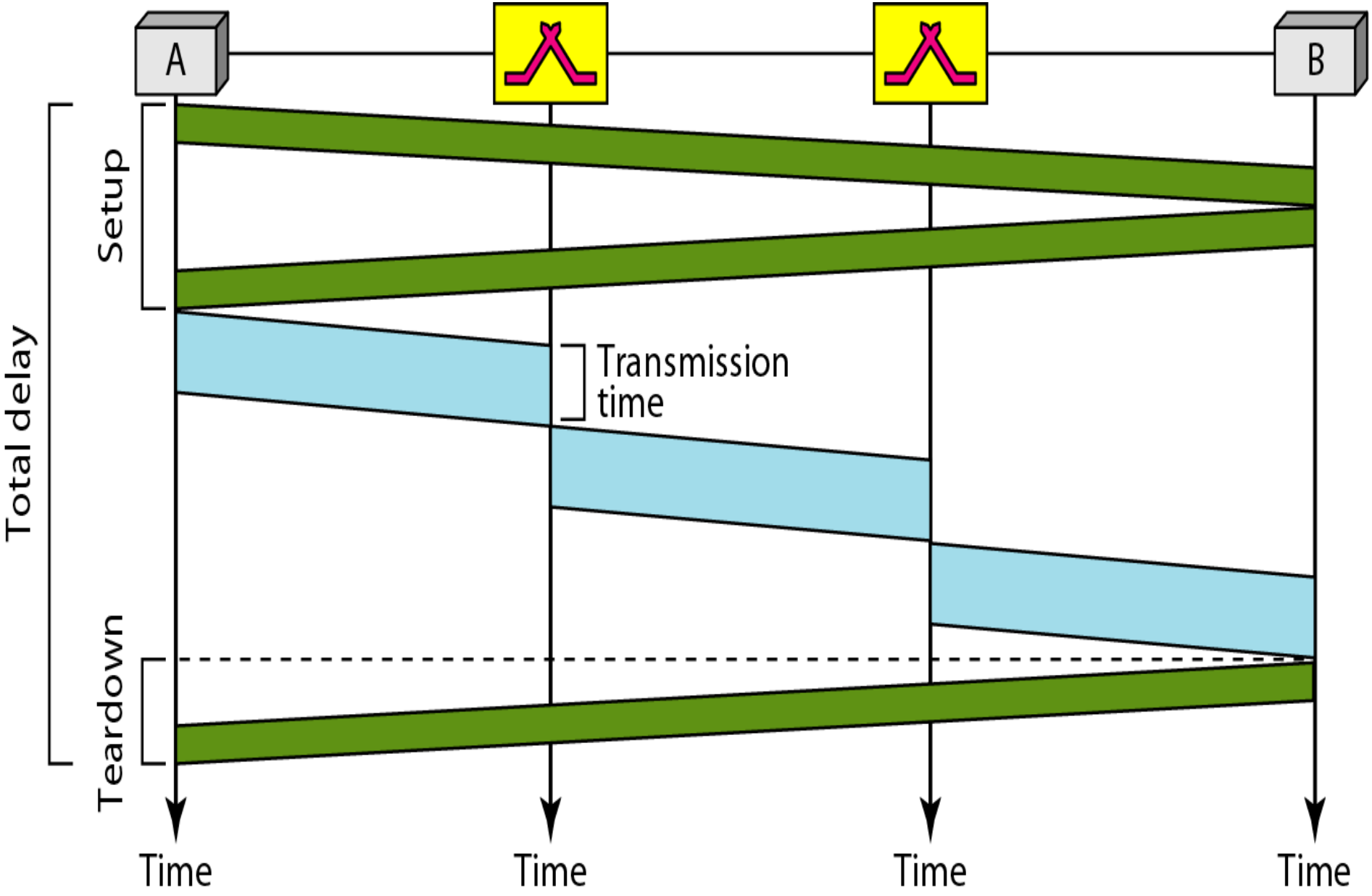
Efficiency

In virtual-circuit switching, all packets belonging to the same source and destination travel the same path; but the packets may arrive at the destination with different delays if resource allocation is on demand.

Delay

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Figure shows the delay for a packet traveling through two switches in a virtual-circuit network.

Switching

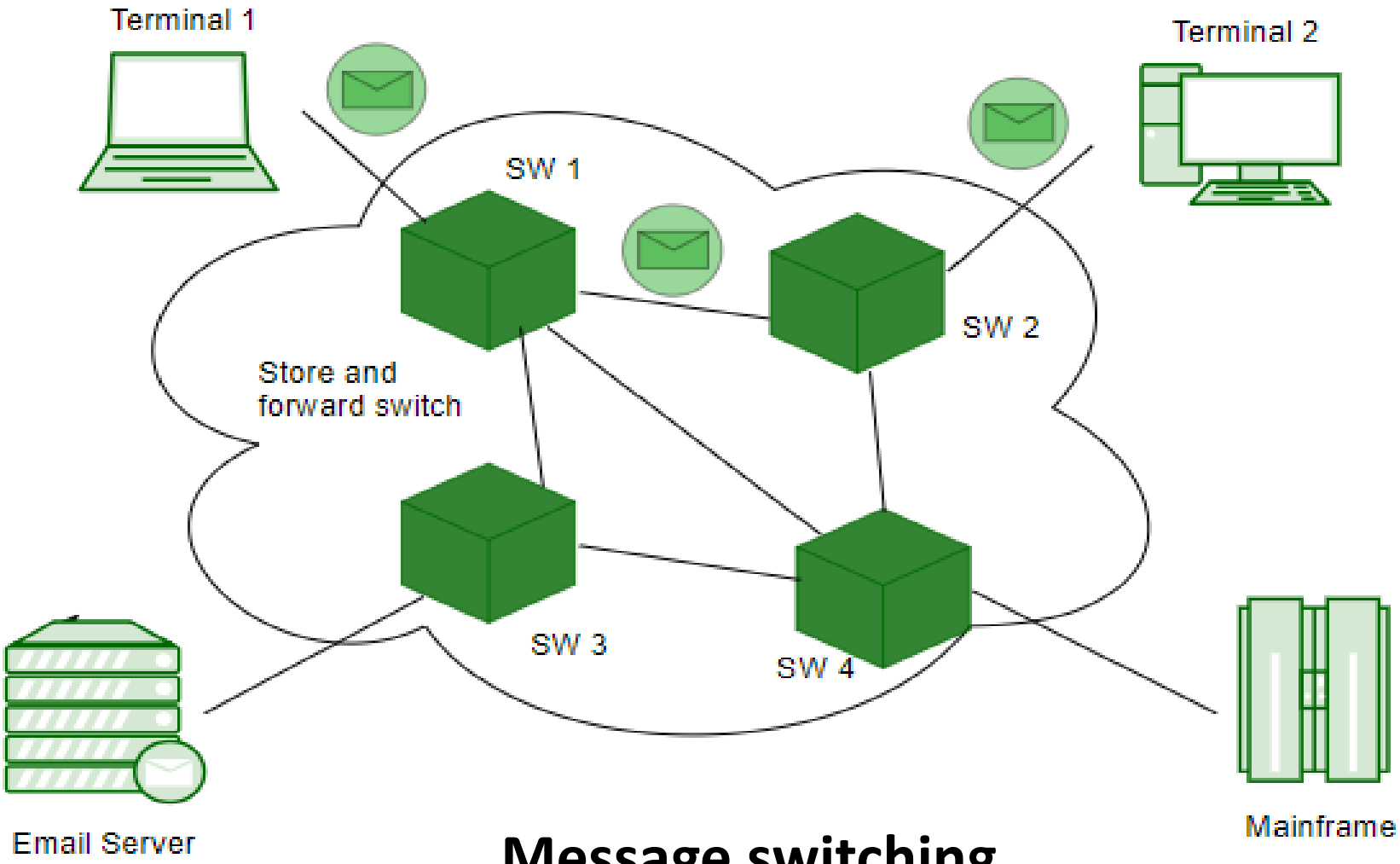

A
B
Setup
Total delay
Transmission time
Teardown
Time
Time
Time
Time

Switching

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

Switching



Message switching

Switching

Advantages

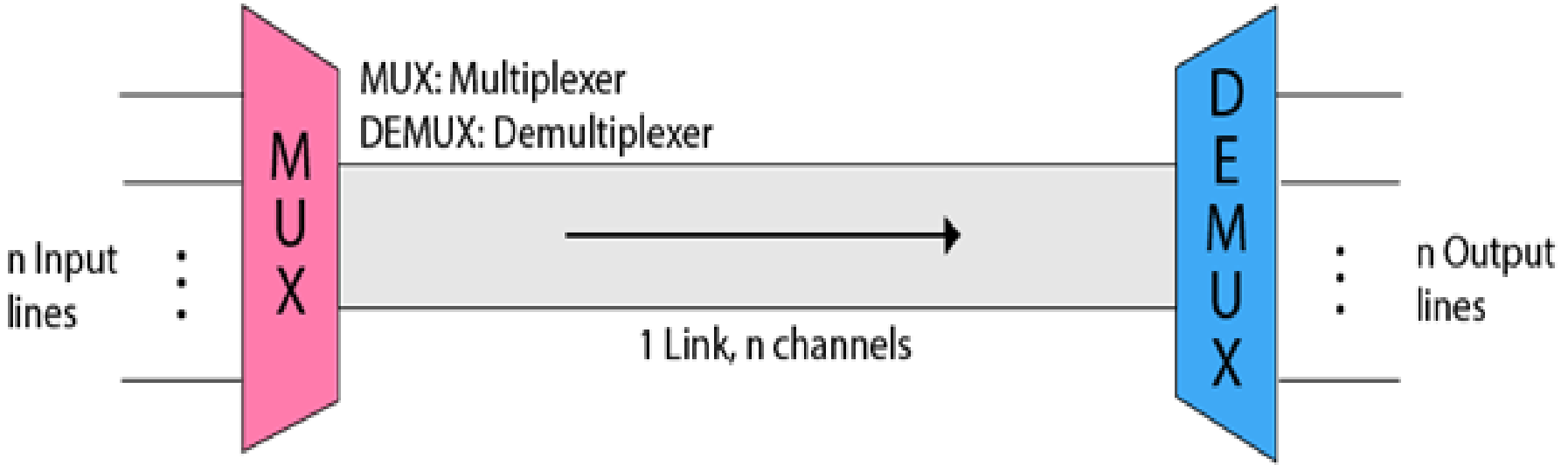
- Sharing of communication channels ensures better bandwidth usage.
- It reduces network congestion due to store and forward method. Any switching node can store the messages till the network is available.
- Broadcasting messages requires much less bandwidth than circuit switching.
- Messages of unlimited sizes can be sent.
- It does not have to deal with out of order packets or lost packets as in packet switching.

Disadvantages

- In order to store many messages of unlimited sizes, each intermediate switching node requires large storage capacity.
- Store and forward method introduces delay at each switching node. This renders it unsuitable for real time applications.

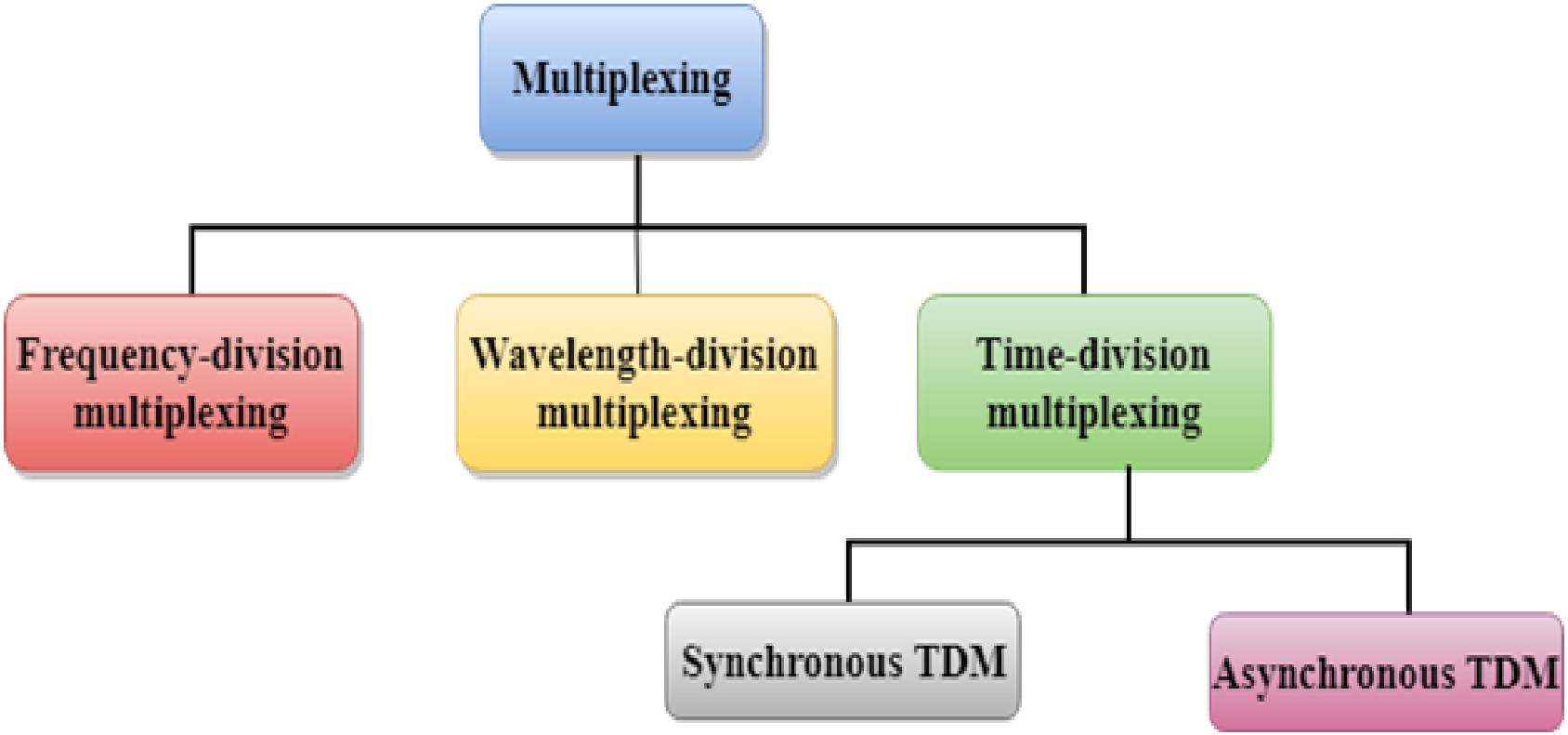
Multiplexing

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
- Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.
- Demultiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.



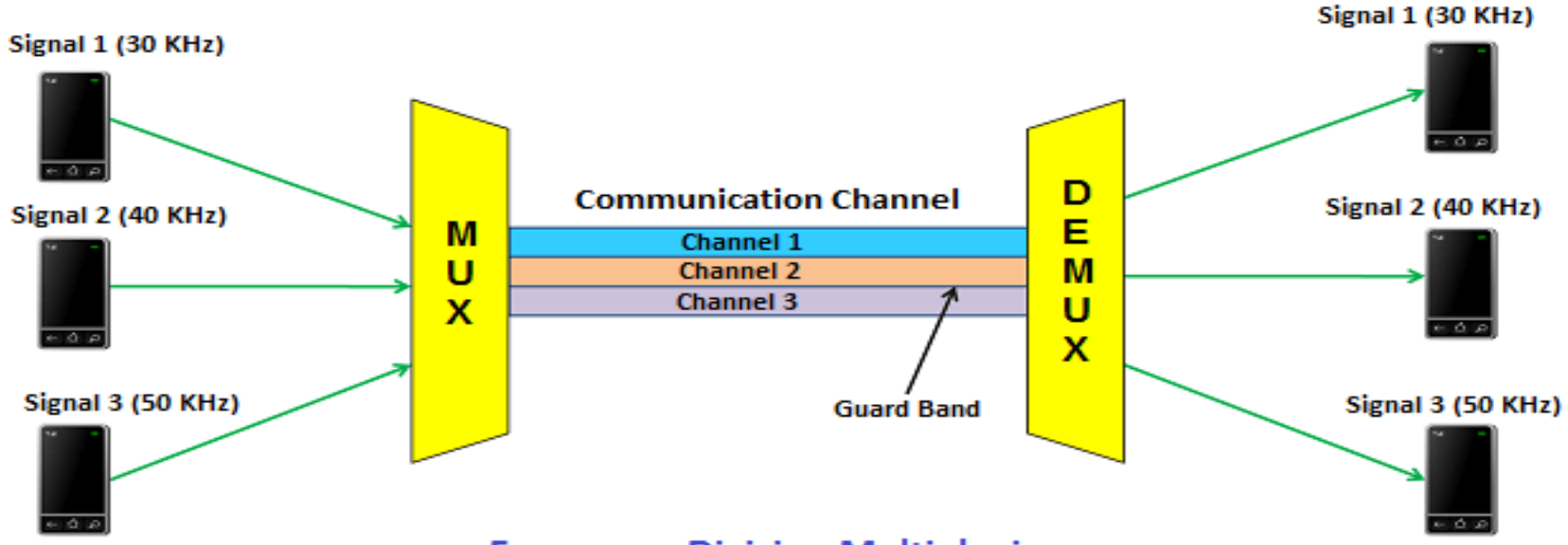
Multiplexing

There are three basic multiplexing techniques: frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals.



Frequency-division Multiplexing (FDM)

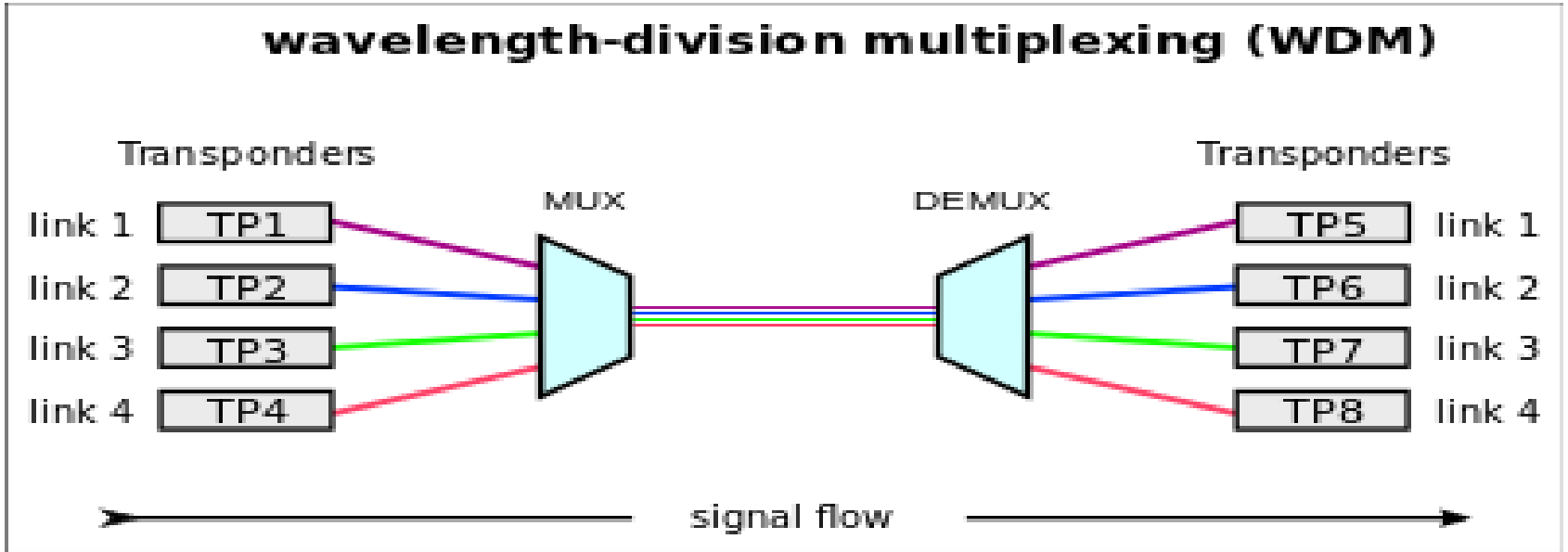
- Frequency Division Multiplexing is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.
- Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- FDM is mainly used in radio broadcasts and TV networks.



Frequency Division Multiplexing

Wavelength Division Multiplexing (WDM)

- Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fiber optic cable.
- WDM is used on fiber optics to increase the capacity of a single fiber.
- It is used to utilize the high data rate capability of fiber optic cable.
- It is an analog multiplexing technique.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- One application of WDM is the SONET network in which multiple optical fiber lines are multiplexed and demultiplexed.



Time Division Multiplexing (TDM)

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In Time Division Multiplexing technique, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.

Time Division Multiplexing (TDM)

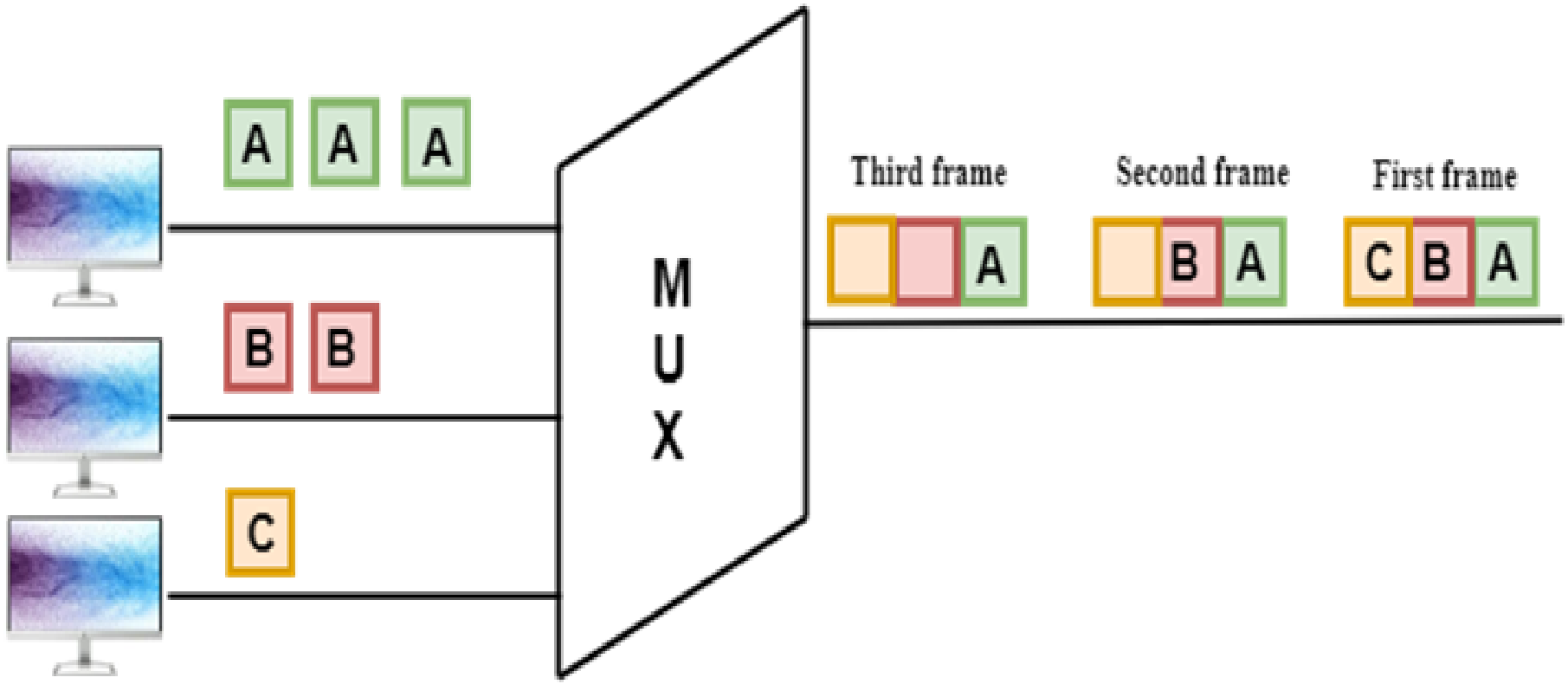
There are two types of TDM:

1. **Synchronous TDM**
2. **Asynchronous TDM**

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is pre-assigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.

Time Division Multiplexing (TDM)



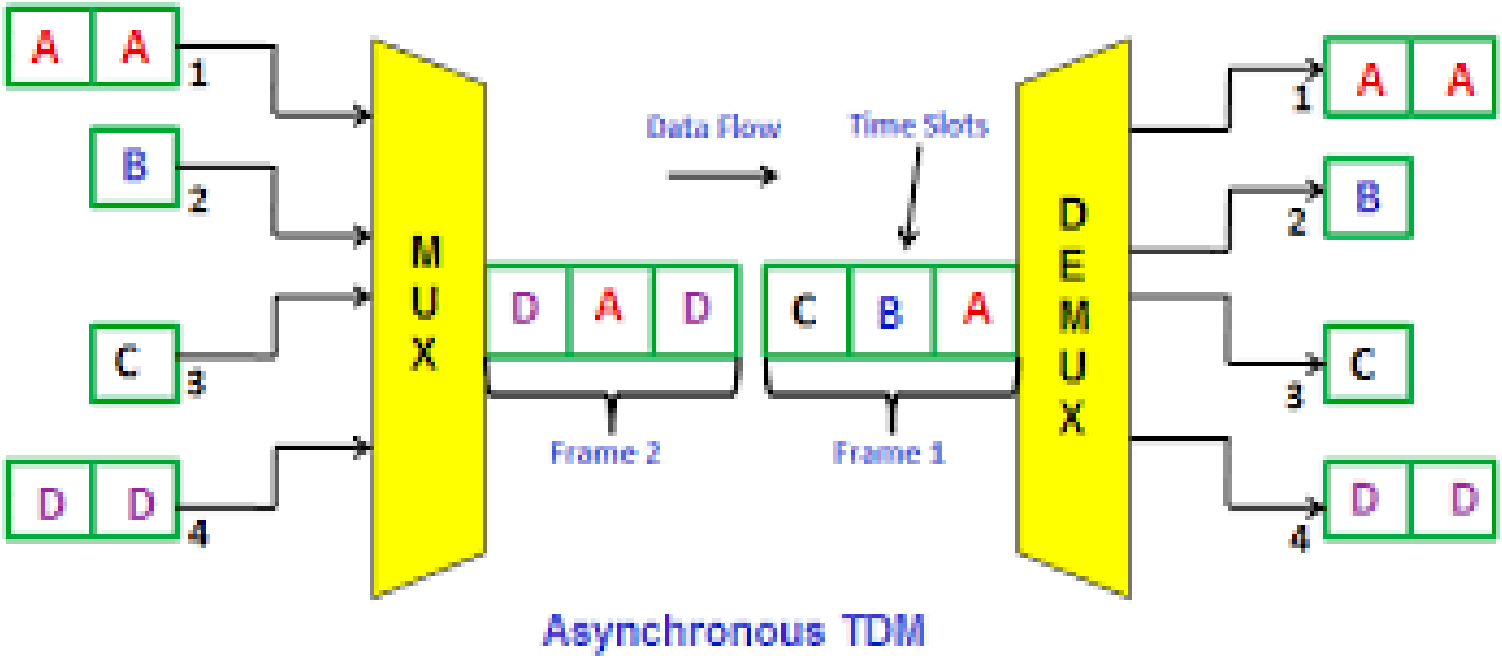
Multiplexing

Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

Multiplexing

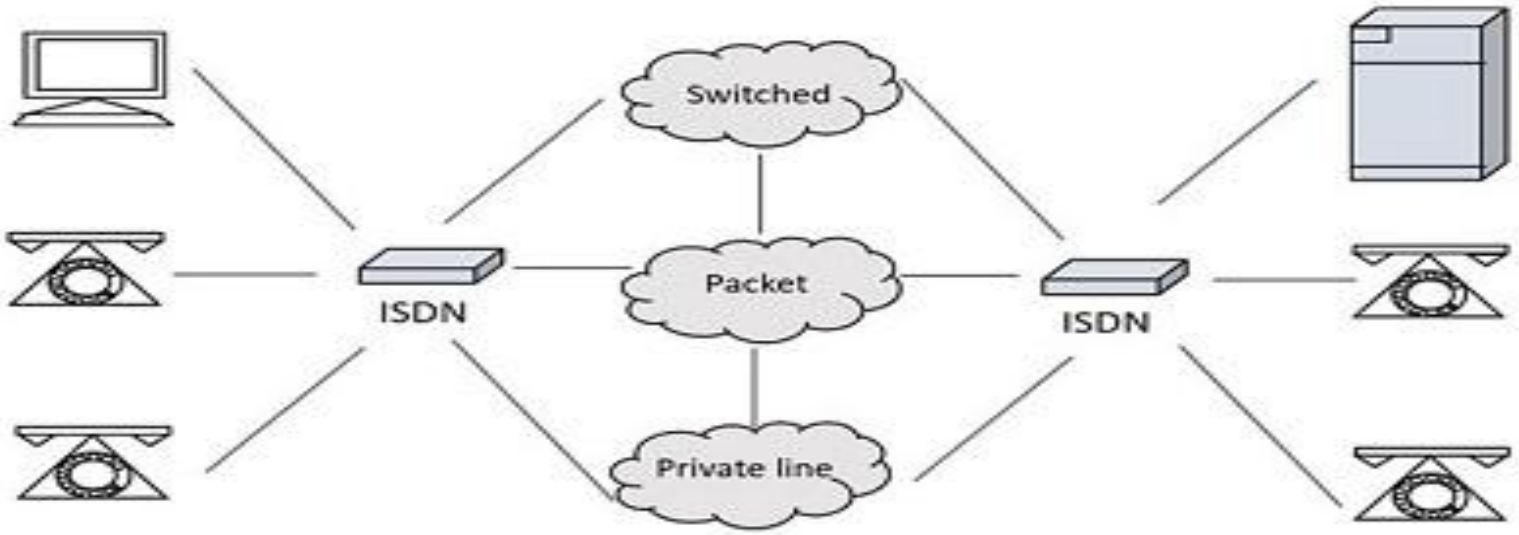
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (m<n).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.



Asynchronous TDM

ISDN

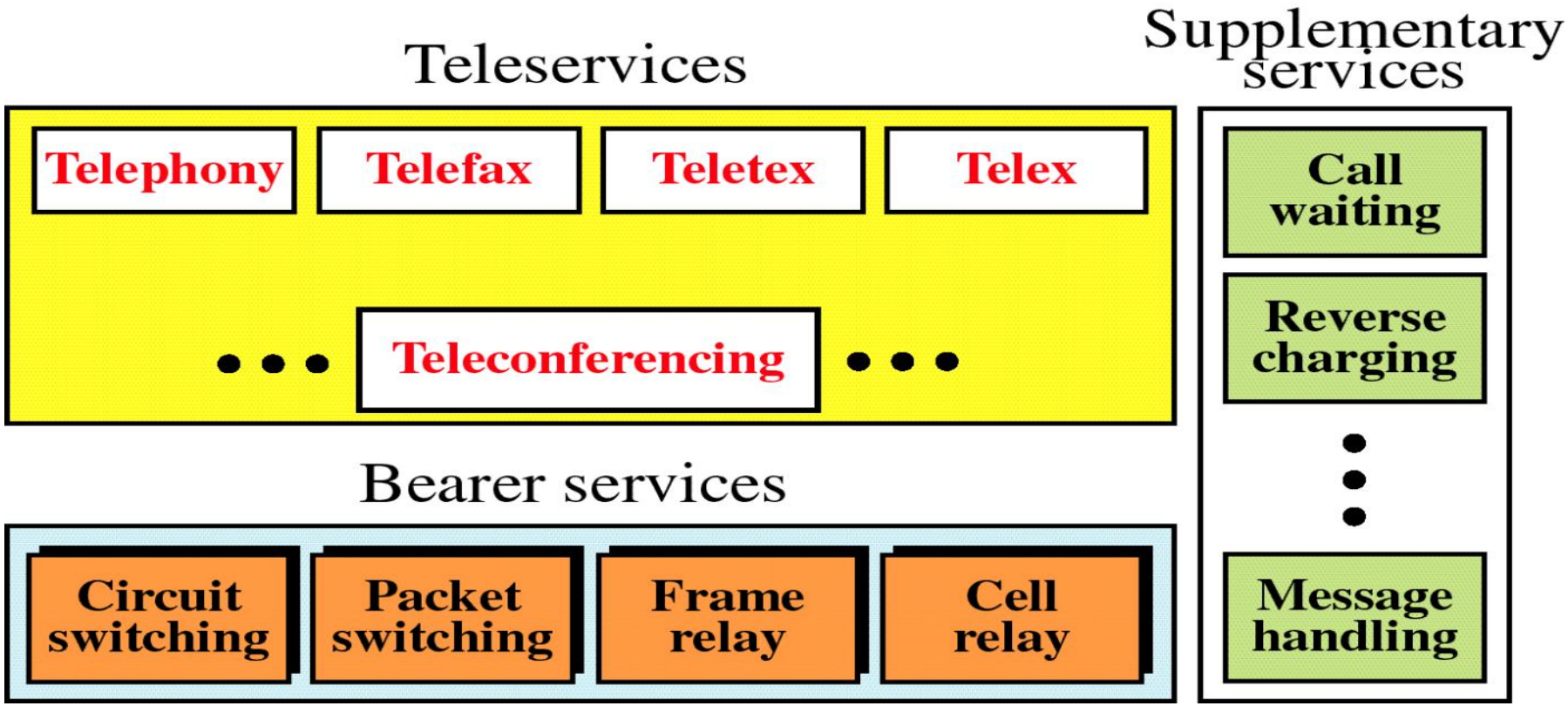
- Its full form is Integrated Services Digital Network.
- ISDN is a telephone network based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency.
- This is a circuit switched telephone network system, which also provides access to Packet switched networks.
- The model of a practical ISDN is as shown below:-



ISDN

ISDN Services

The purpose of the ISDN is to provide fully integrated digital services to users. These services fall into three categories: bearer services, teleservices and supplementary services.



ISDN

Bearer Services

These services provide the means to transfer information between users without the network manipulating the content of that information. The network does not need to process the information and therefore does not change the content. Bearer services belong to the first three layers of the OSI model. They can be provided using circuit-switched, packet-switched, frame-switched or cell switched networks.

Teleservices

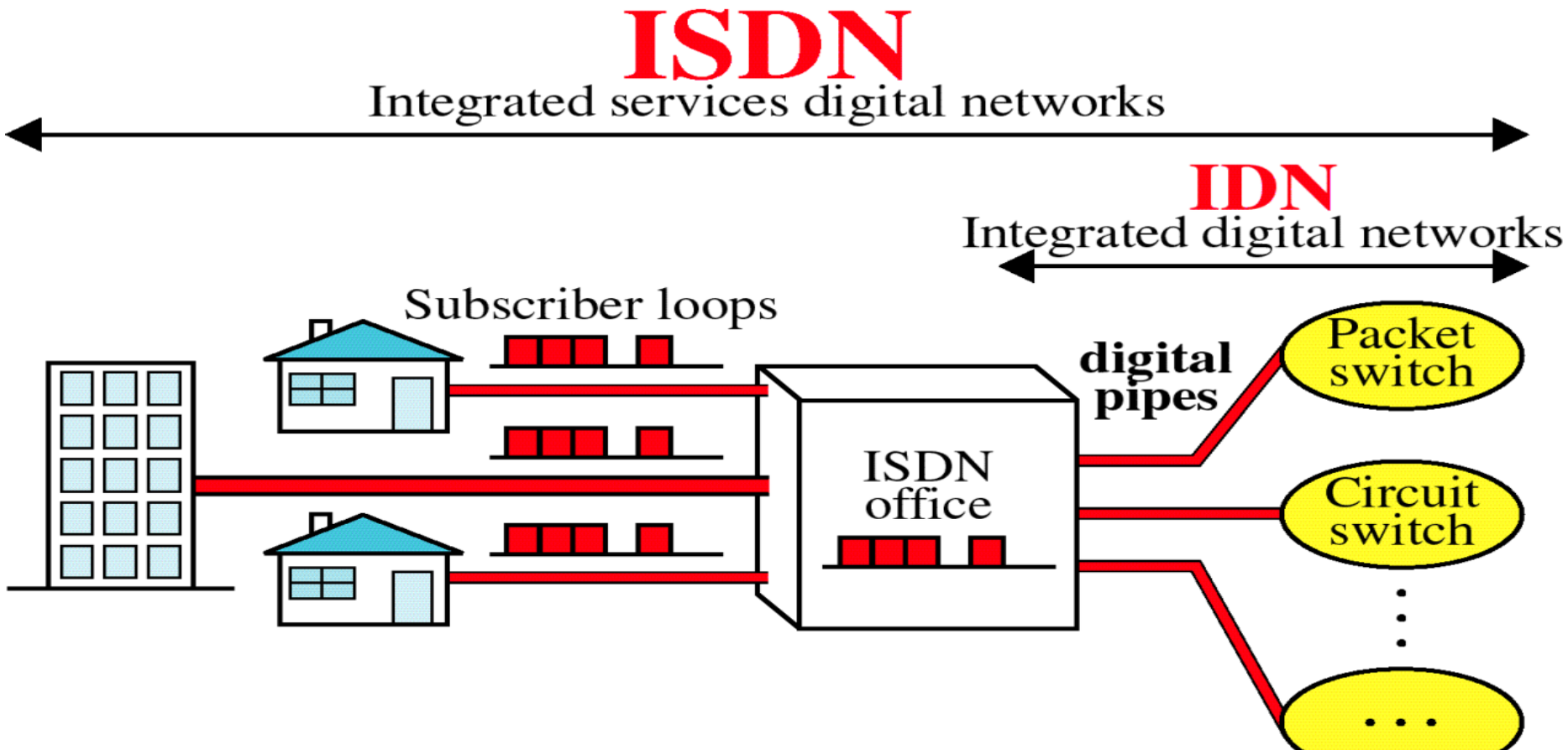
In teleservicing, the network may change or process the contents of the data. These services correspond to layers 4-7 of the OSI model. Teleservices include telephony, teletex, telefax, videotex, telex and teleconferencing.

Supplementary Services

Supplementary services are those services that provide additional functionality to the bearer services and teleservices. These services are reverse charging, call waiting and message handling.

ISDN

Following figure gives a conceptual view of the connection between users and an ISDN control office.



ISDN

- Each user is linked to the central office through a digital pipe.
- Digital pipes between user and ISDN office are organized into multiple channels of different sizes. ISDN standard defines three channel types, each with different transmission rate: bearer channel, data channel and hybrid channels.

B-Channel (Bearer Channel): Bearer channel is defined at a rate of 64 kbps. It is the basic user channel and can carry any type of digital information in full duple mode as long as the required information rate does not exceed 64 kbps.

D channel (Data Channel): Data channel can be either 16 or 64 kbps, depending on the needs of user. The primary function of D channel is to carry control signal for the B channel.

H channel (Hybrid Channel): Hybrid channels are available with data rates of 384 Kbps, 1536 Kbps or 1920 Kbps. These rates suit H channels for high data rate applications such as video, teleconferencing and so on.

ISDN

User Interfaces

Digital subscriber loops are of two types:

(1) Basic rate interface (BRI)

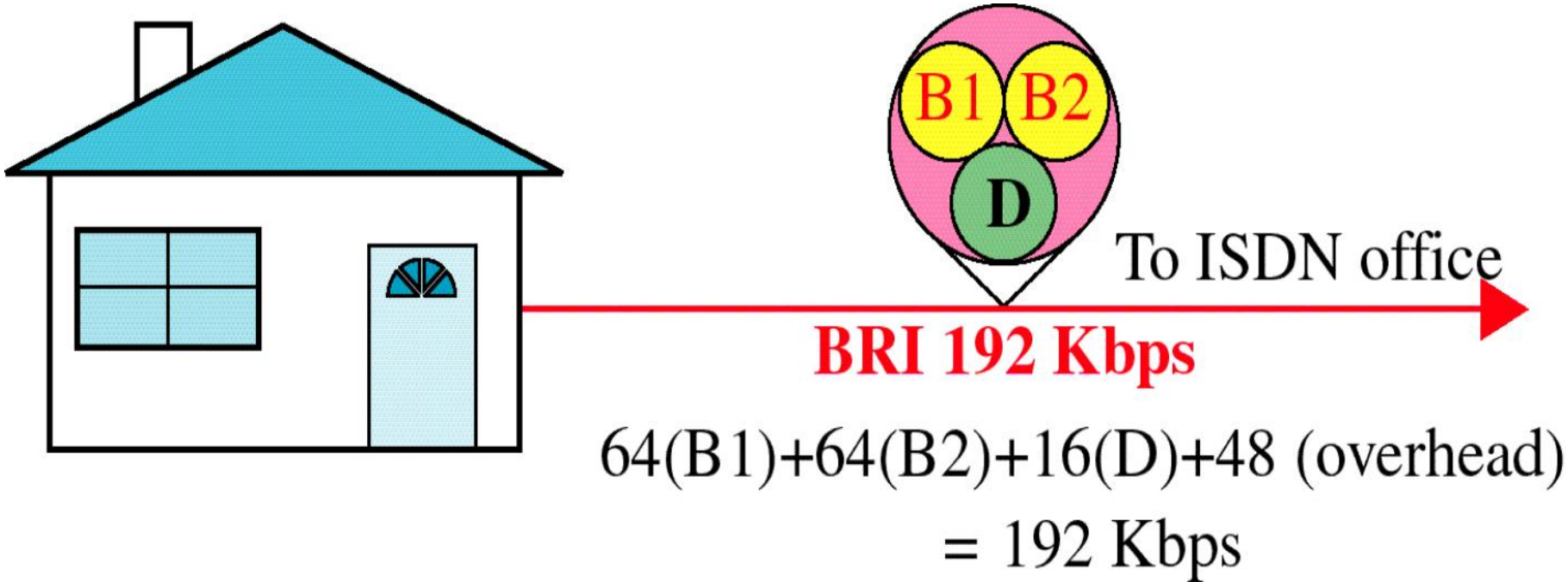
(2) Primary rate interface (PRI)

Each type is suited to a different level of customer needs. Both include one D channel and some number of either B or H channels.

ISDN

Basic rate interface

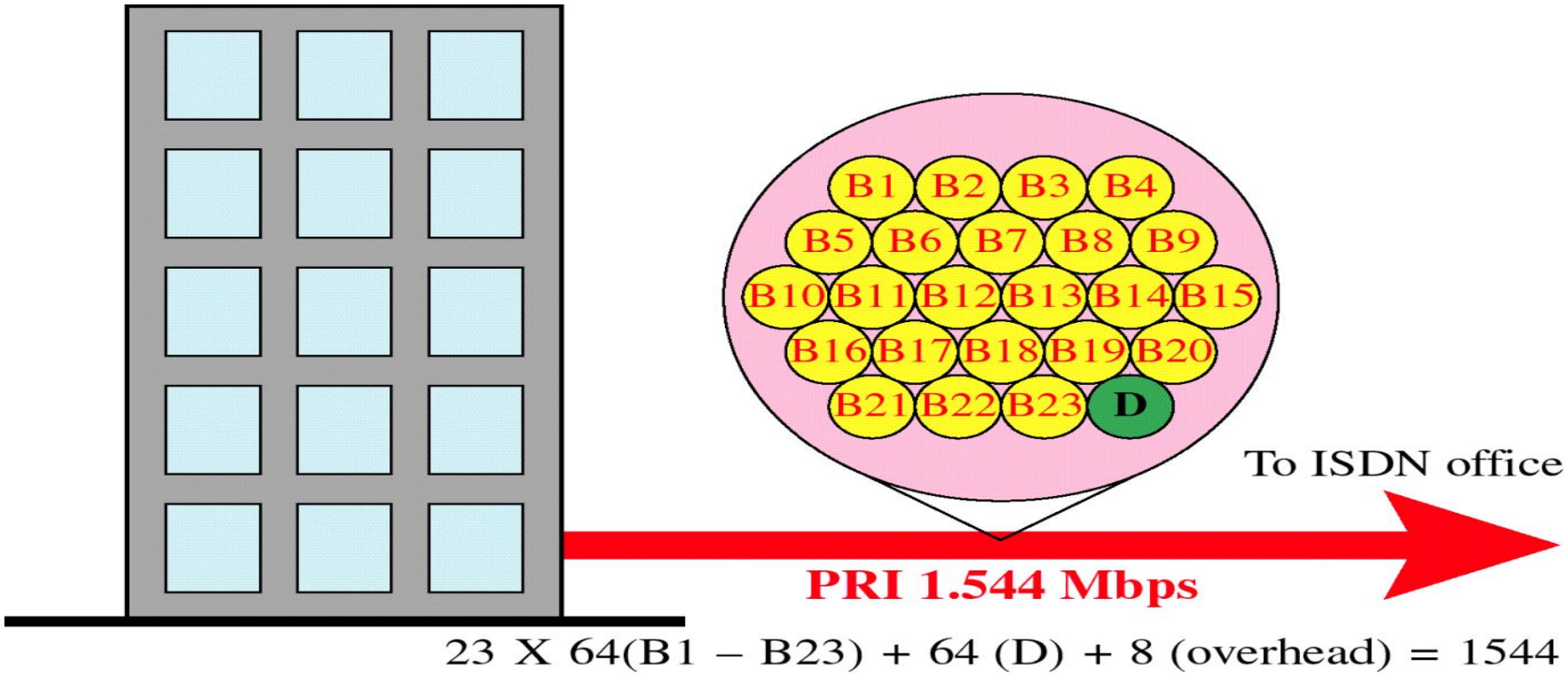
- The basic rate interface specifies a digital pipe consisting of two B channels and one 16 Kbps D channel.
- Two B channel of 64 Kbps each, plus one D channel of 16 Kbps, equal 144 Kbps. In addition, the BRI service itself requires 48 Kbps of operating overhead. Therefore, BRI requires a digital pipe of 192 Kbps.
- BRI is designed to meet the needs of residential and small-office customers.



ISDN

Primary rate interface

- The primary rate interface specifies a digital pipe with 23 B channels and one 64 Kbps D channel.
- Twenty three B channels of 64 Kbps each plus one D channel of 64 Kbps equals 1.536 Mbps. In addition, the PRI service itself uses 8 Kbps of overhead. Therefore, PRI requires a digital pipe of 1.544 Mbps.



ISDN

Broadband ISDN

- When ISDN was originally designed, data rates of 64 Kbps to 1.544 Mbps were sufficient to handle all existing transmission needs. But after sometimes, this rate is insufficient.
- To provide for the needs of next generation of technology, B-ISDN has been developed. The original ISDN is now known as narrow ISDN(N-ISDN). B-ISDN provides subscribers to the network with data rates in the range of 600 Mbps.

AKTU Examination Questions

1. What are header and trailers and how do they get added and removed?
2. What is the difference between network layer delivery and the transport layer delivery?
3. Define topology and explain the advantage and disadvantage of Bus, Star and Ring topologies.
4. What is OSI Model? Explain the functions, protocols and services of each layer?
5. Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with four signal levels. What is the maximum bit rate?

AKTU Examination Questions

6. Encode the data-stream 10011010 using the following encoding scheme:
   i. Unipolar
   ii. Bipolar NRZ-L
   iii. Bipolar NRZ-I
   iv. RZ
   v. Manchestor
   vi. Differential Manchestor
   vii. AMI
7. Write four differences between circuit switching and packet switching.
8. Sketch Manchester and differential Manchester encoding for the following bit stream: 1011110001001011101

AKTU Examination Questions

9. What are the services of Transport Layer?
10. What are the major advantages of using optical fiber over twisted pair cable?
11. What do you mean by network architecture? What should be their design issues? Explain briefly.
12. Discuss different types of transmission media with their advantages and disadvantages.
13. Differentiate OSI and TCP/IP reference model. Which one is more popular and why?

AKTU Examination Questions

14. Suppose a signal travels through a transmission medium then find:
    i. The attenuation (loss of power) if the power is reduced to one half.
    ii. The amplification (gain of power) if the power is Increased 10 times.
15. What do you mean by transmission impairment? Explain different types of transmission impairment.
16. What are the applications of Computer Networks?
17. List the advantages and disadvantages of ring topology.
18. If a binary signal is sent over a 3KHZ channel. Whose signal to noise ratio is 20db. What is the maximum achievable data rate?

AKTU Examination Questions

19. Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies.
20. Discuss the different physical layer transmission media.
21. Write about user access in ISDN.
22. List the advantages and disadvantages of star topology.
23. Explain functionalities of every layer in OSI reference model with neat block diagram.