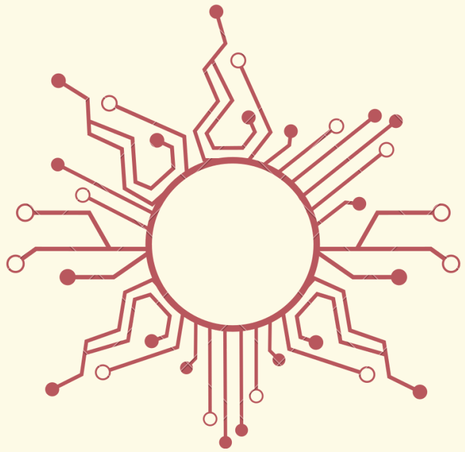
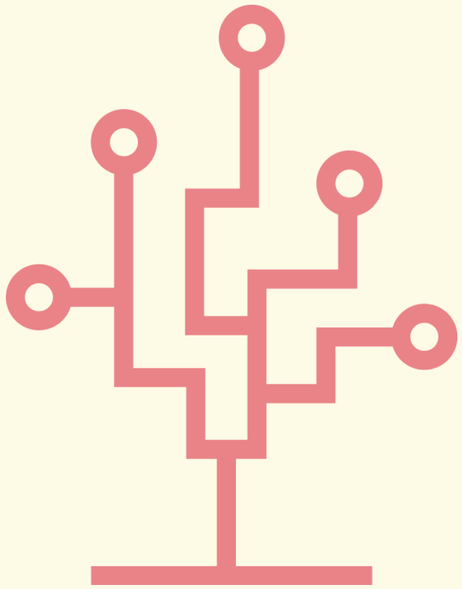


Computer Networks



A computer network is a system of interconnected computers and peripheral devices.

For example, it may connect computers, printers, scanners and cameras.

The connecting media could be a copper wire, optical fiber, microwave, or satellite.

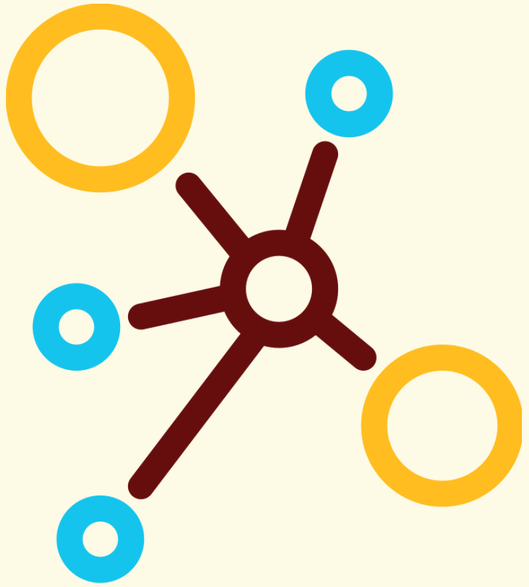
NETWORKING ELEMENTS

At least two computers

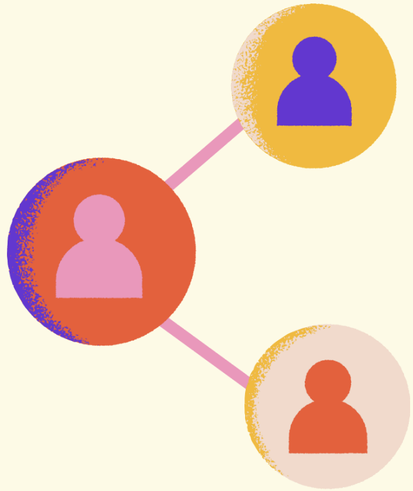
Transmission medium either wired or wireless

Protocols or rules that govern the communication

Network software such as Network Operating System



NETWORK CRITERIA



Performance

Reliability

Security

Network Topology

GOALS OF COMPUTER NETWORK

1. Resource Sharing
2. High Reliability
3. Inter Process Communication
4. Flexible Access
5. Security
6. Performace
7. Scalability

TYPES_OF_NETWORK

Personal Area Network — **PAN**

Local Area Network — **LAN**

Metropolitan Area Network — **MAN**

Wide Area Network — **WAN**

Wireless Area Network — **WLAN**

Personal Area Network

- A Personal Area Network (PAN) is a type of computer network that is used for communication among devices in a small area, typically within a range of 10 meters or less.
- PANs can be created using various technologies such as Bluetooth, ZigBee, and Infrared.
- PANs are used for a variety of purposes such as file sharing and printing. They are also used for connecting different devices such as keyboards and mouse.
- PANs have many advantages such as: Convenience, low cost, easy to set up, security

Local Area Network

- LAN is a type of computer network that connects computers and devices in a small geographic area such as a home, office, or building. , typically within a range of 10 meters or less.
- LANs are typically built using Ethernet technology, which involves connecting each device to a switch or router using an Ethernet cable.
- LANs are designed to allow users to share resources such as printers, files, and internet access, as well as communicate with each other.
- LANs have many advantages such as: High-speed communication, easy to manage, enhanced security and cost-effective

Metropolitan Area Network

- MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP.
- Devices used for transmission of data through MAN are Modem and Wire/Cable.
- Examples of a MAN are part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network.
- PANs have many advantages such as: Provides high-speed connectivity over a large geographical area, used as an ISP for multiple customers, high data transfer rates

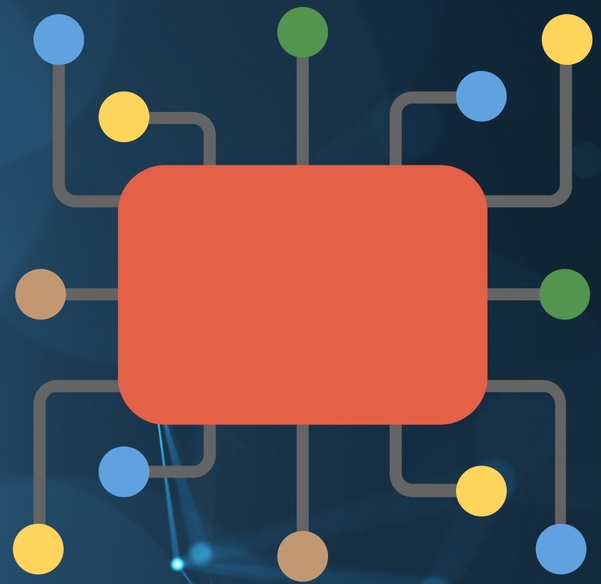
Wide Area Network

- WAN or Wide Area Network is a computer network that extends over a large geographical area. WAN has a range of above 50 km.
- A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves. Communication medium used for WAN is PSTN or Satellite Link.
- Example are asynchronous transfer mode (ATM) network and a dial-up line connecting computer to the Internet.
- PANs have many advantages such as: covers large geographical areas and can connect remote locations, connectivity to the internet, supports multiple users and applications simultaneously.

Wireless Area Network

- WLAN is a wireless computer network that links two or more devices using wireless communication to form a LAN within a limited area such as a home, school or office building.
- WLAN transmits information over radio waves. Data is sent in packets. The packets contain layers with labels and instructions with the unique MAC addresses assigned to endpoints, enable routing to intended locations.
- PANs have many advantages such as: requires no cables to connect the devices, can also connect small electronic gadgets and no limit of devices

NETWORK STRUCTURE AND ARCHITECTURE



CONTENTS

COMPUTER NETWORKS

Computer networks are essential for modern communication and information sharing. They enable users to share resources, communicate, access information from anywhere, scale up or down as needed, and implement security measures to protect data and other resources.

It is an integral part of modern-day communication and information sharing. They allow computers and other devices to connect and communicate with each other, enabling people to share information and resources across large distances quickly and easily.

Importance of computer networks are

- Resource sharing
- Communication
- Accessibility
- Scalability
- Security

NETWORK STRUCTURES

Network structure refers to the way in which computers and other devices are interconnected. There are two main types of network structure: physical and logical.

Physical network structure: The physical network structure refers to the actual physical connections between devices. There are three main types of physical network structures:

Bus: In a bus network, all devices are connected to a single cable or backbone. Data is transmitted to all devices on the network.

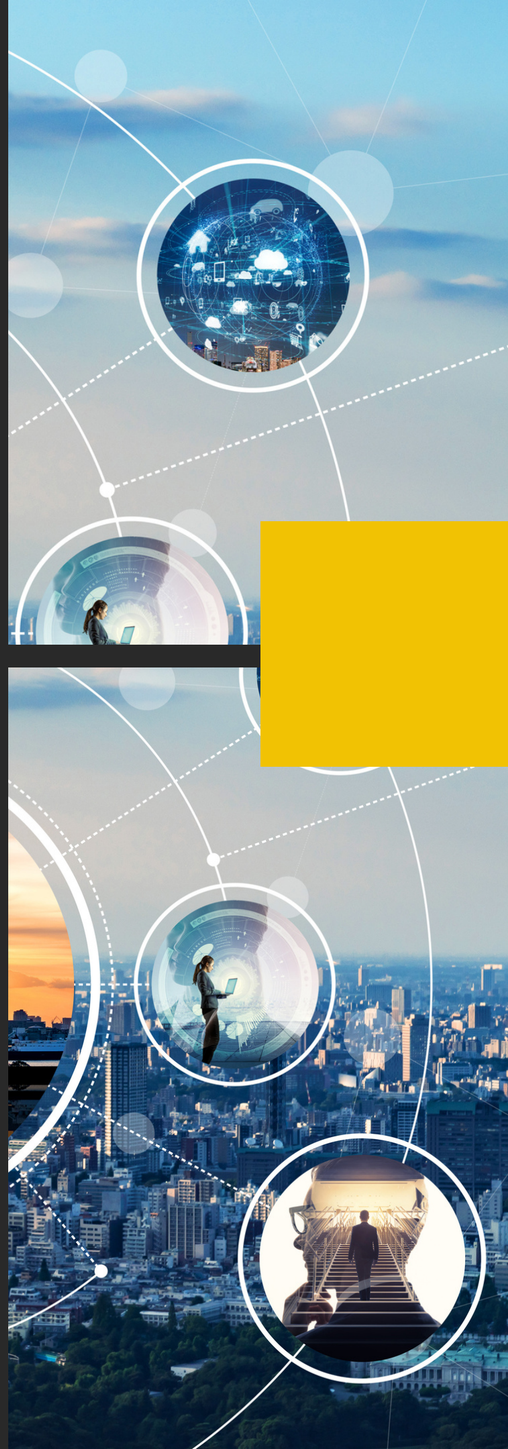
Ring: In a ring network, devices are connected in a circular fashion, and data travels around the ring in one direction.

Star: In a star network, all devices are connected to a central hub or switch, which acts as a central point of communication. Data is transmitted from the sending device to the hub.

Logical network structure: The logical network structure refers to the way in which devices are organized and connected in a network. There are two main types of logical network structures:

Peer-to-peer: In a peer-to-peer network, all devices have equal status and can act as both clients and servers.

Client-server: In a client-server network, there is a central server that provides resources and services to clients.



NETWORK TOPOLOGIES

Network topology refers to the physical or logical arrangement of nodes and links in a network. There are different types of network topologies, including bus, ring, star, mesh, and hybrid.

Bus topology:
In a bus topology, all devices are connected to a common cable or bus. Data is transmitted on the bus, and all devices receive the data simultaneously.

Ring topology:
In a ring topology, all devices are connected to a ring, and data is transmitted in one direction around the ring.

Star topology:
In a star topology, all devices are connected to a central hub or switch, and data is transmitted through the hub or switch.

Mesh topology:
In a mesh topology, all devices are connected to each other in a network of interconnected nodes. Data is transmitted through multiple paths, which can provide redundancy and fault tolerance.

Hybrid topology:
A hybrid topology is a combination of two or more different topologies, such as a star-bus or ring-mesh.

SOME EXAMPLES OF NETWORK TOPOLOGIES

Bus Topology: A local area network (LAN) in a school or small office may use a bus topology. All computers are connected to a single cable, which serves as the backbone for data transmission.

Ring Topology: A token ring network is an example of a ring topology. IBM Token Ring is one of the most popular examples of this topology.

Star Topology: A company's network that has a central switch or router, with individual computers or devices connected to it, is an example of a star topology.

Mesh Topology: A wireless mesh network that connects different access points to provide seamless wireless coverage is an example of a mesh topology.

Hybrid Topology: A large company that uses a combination of a star topology for its local area network and a mesh topology for its wide area network is an example of a hybrid topology.

In general, different types of network topologies are used in different scenarios based on the specific needs and requirements of the organization.

NETWORK ARCHITECTURE

Network architecture refers to the overall design and structure of a computer network. There are three main types of network architectures: peer-to-peer, client-server, and distributed.

- Peer-to-peer architecture: In a peer-to-peer architecture, all devices have equal status and can act as both clients and servers. Devices communicate directly with each other, without the need for a central server or hub. This type of architecture is commonly used in small networks, such as home networks.

- Client-server architecture: In a client-server architecture, there is a central server that provides resources and services to clients. Clients request resources from the server, and the server provides them with the requested resources. This type of architecture is commonly used in large networks, such as corporate networks.

- Distributed architecture: In a distributed architecture, the network resources and services are distributed across multiple servers and nodes, which work together to provide the required services. This type of architecture is commonly used in large networks, such as the internet.

DIFFERENT LAYERS OF THE OSI MODEL AND TCP/IP MODEL

Both the OSI and TCP/IP models define a set of protocols and services that are required for communication between devices on a network. Here's a brief overview of the layers in each model:

Physical Layer: The physical layer is the lowest layer in the OSI model and TCP/IP model. It deals with the physical transmission of data over the network, such as signals, cables, and connectors.

Data Link Layer: The data link layer is responsible for the reliable transmission of data between two devices on the same physical network.

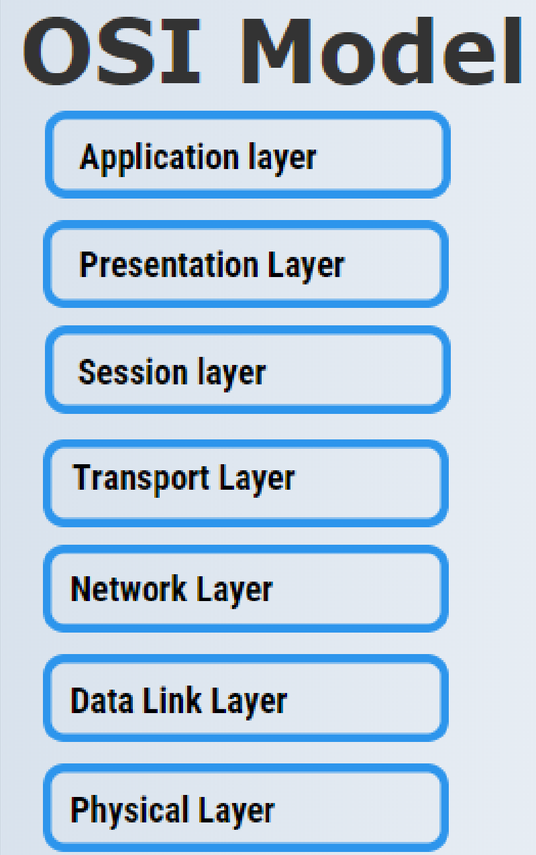
Network Layer: The network layer is responsible for the routing of data between different networks. It determines the best path for data to travel from the source to the destination.

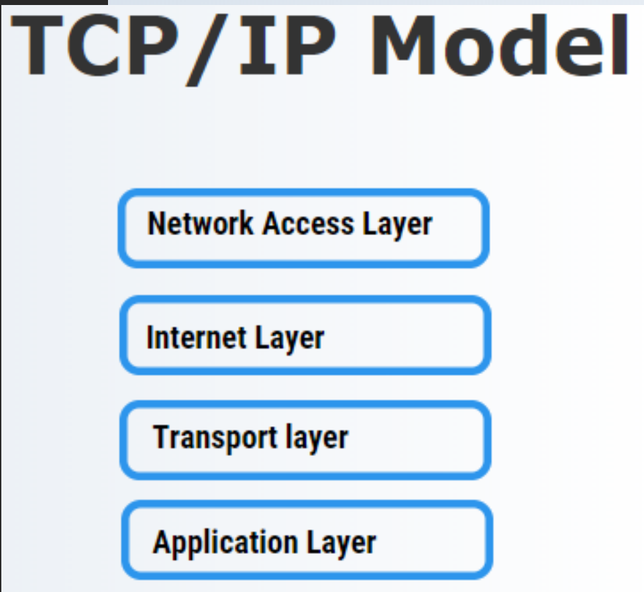
Transport Layer: The transport layer provides reliable, end-to-end data delivery between applications running on different devices. It segments large data packets into smaller, manageable packets .

Session Layer: The session layer is responsible for establishing, maintaining, and terminating sessions between applications running on different devices.

Presentation Layer: The presentation layer is responsible for formatting and presenting data in a way that is understandable by the applications. .

Application Layer: The application layer provides a user interface for accessing network services. It includes applications such as web browsers, email clients, and file transfer utilities.





IMPORTANCE OF NETWORK STRUCTURE AND ARCHITECTURE IN COMPUTER NETWORKS

The importance of network structure and architecture in computer networks cannot be overstated. Proper network structure and architecture are critical for the successful operation of computer networks. A well-designed network structure ensures that devices are efficiently connected, which can lead to better performance, increased reliability, and improved security.

Different network architectures, such as peer-to-peer, client-server, and distributed architectures, have different advantages and disadvantages. Selecting the appropriate architecture for a particular network can have a significant impact on its performance and efficiency.

Similarly, network topology plays a crucial role in determining the efficiency and reliability of a network. The choice of topology depends on various factors, such as the number of devices, the distance between devices, and the amount of traffic on the network.

A well-designed network structure and architecture can improve network performance, enhance security, and reduce the likelihood of network failures. Therefore, it's crucial to pay close attention to network structure and architecture during the design and implementation of computer networks.

SOME EXAMPLES OF PROTOCOLS THAT OPERATE AT EACH LAYER OF THE OSI MODEL:

- Physical Layer: Ethernet, RS-232, USB, Wi-Fi, Bluetooth, Fiber Channel.
- Data Link Layer: Ethernet, Token Ring, HDLC, PPP, SLIP.
- Network Layer: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).
- Transport Layer: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SCTP (Stream Control Transmission Protocol).
- Session Layer: NetBIOS, SAP (Service Advertising Protocol), NFS (Network File System).
- Presentation Layer: SSL/TLS (Secure Sockets Layer/Transport Layer Security), MIME (Multipurpose Internet Mail Extensions), ASCII (American Standard Code for Information Interchange), EBCDIC (Extended Binary Coded Decimal Interchange Code).
- Application Layer: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), DNS (Domain Name System). lectures.

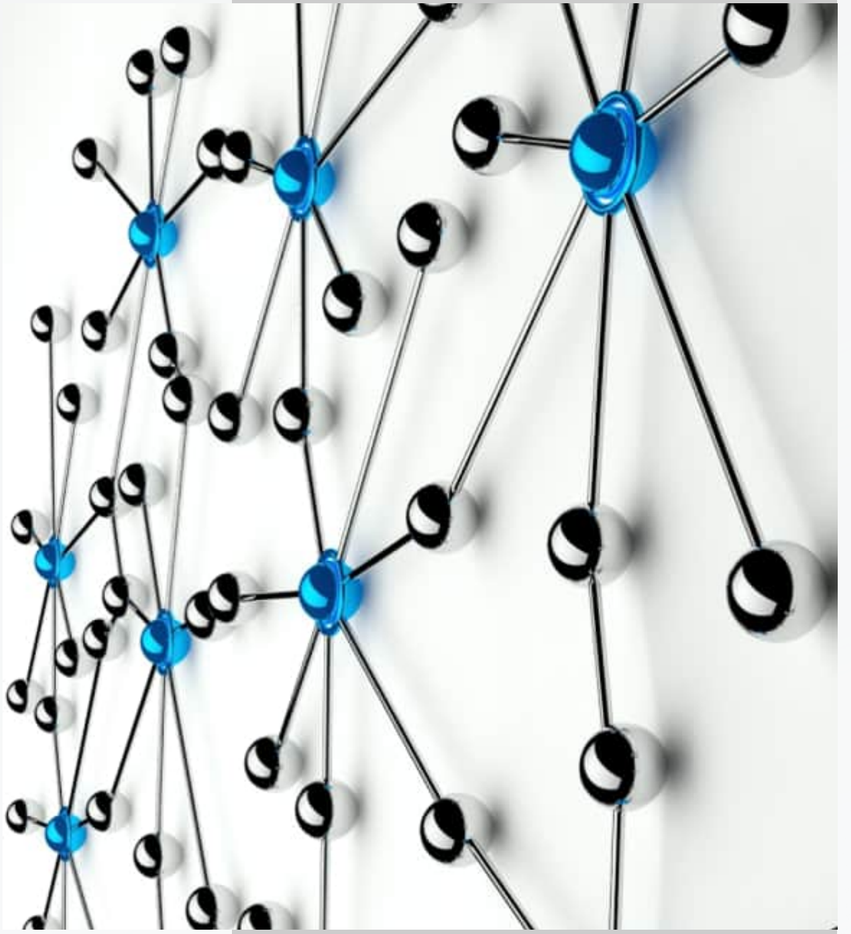
THE OSI REFERENCE MODEL

CONTENT

NETWORK

A network is a combination of hardware and software that sends data from one location to another.

The hardware consists of the physical equipment that carries signals from one point of the network to another.



LAYERING

We have a sender, a receiver, and a carrier that transports the letter.
There is a hierarchy of tasks.

Sender

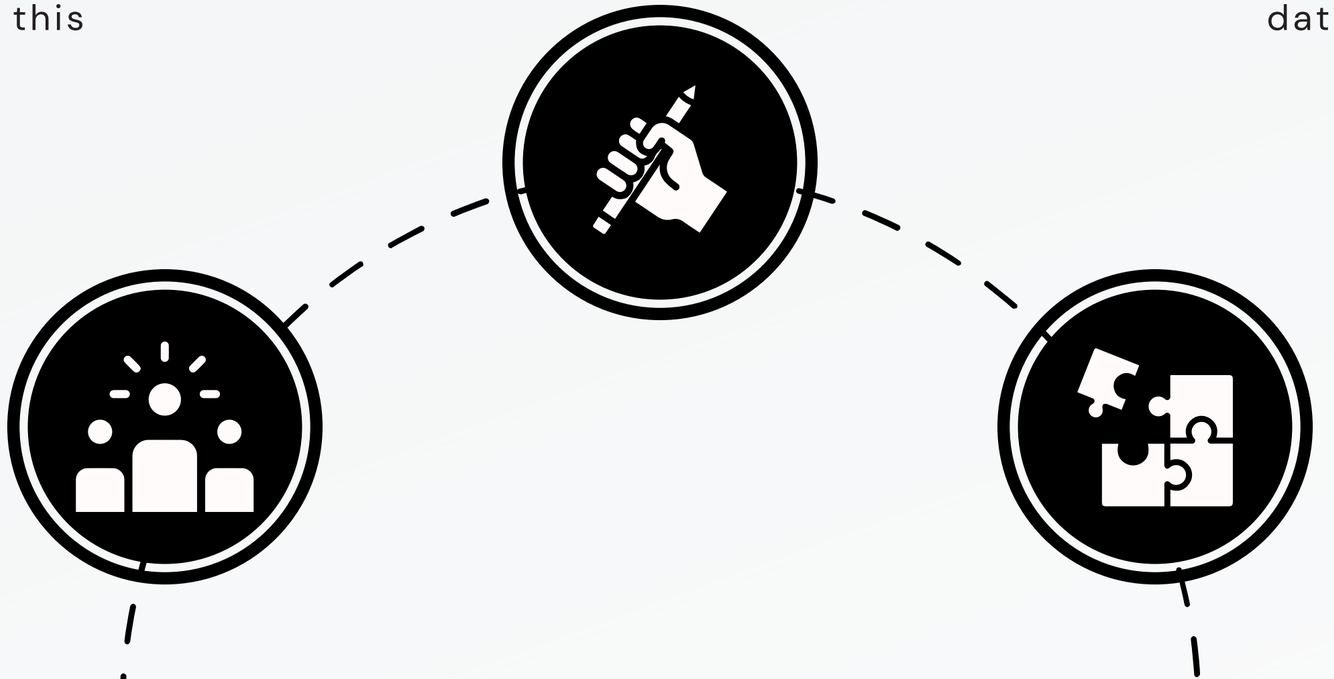
A sender is the originator of a message on a particular occasion; receivers are their audience on this occasion.

Carrier

The transmission is not restricted to one channel and may use several channels simultaneously. The choice of the right channel affects successful communication.

Receiver

A receiver is a computer or any such device which is capable of receiving data from the network



HIERARCHY

- Computer networks are comprised of or contain a large number of pieces of hardware and software.
- Each and every layer has some particular task or function. In programming, this concept is very common. The networks are organized and arranged as different layers or levels simply to reduce and minimize complexity of design of network software.
- The layers generally reduce complexity of communication between networks
- It increases network lifetime.

SERVICES

- Each layer at the sending site uses the services of the layer immediately below it.
- The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.
- The TCPIIP protocol suite became the dominant commercial architecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

THE OSI MODEL

- OSI stands for Open Systems Interconnection.
- It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
- The OSI model is important because it helps network designers and administrators understand how different protocols and technologies work together to provide network communication.
- It also helps in troubleshooting network issues by isolating problems to specific layers.
- This model allows complete interoperability between otherwise incompatible systems.

ARCHITECTURE

01

To translate, encrypt, and compress data

02

APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATA LINK

PHYSICAL

04

To allow access to network resources

To establish, manage, and terminate sessions

To provide reliable process-to process message delivery and error recovery

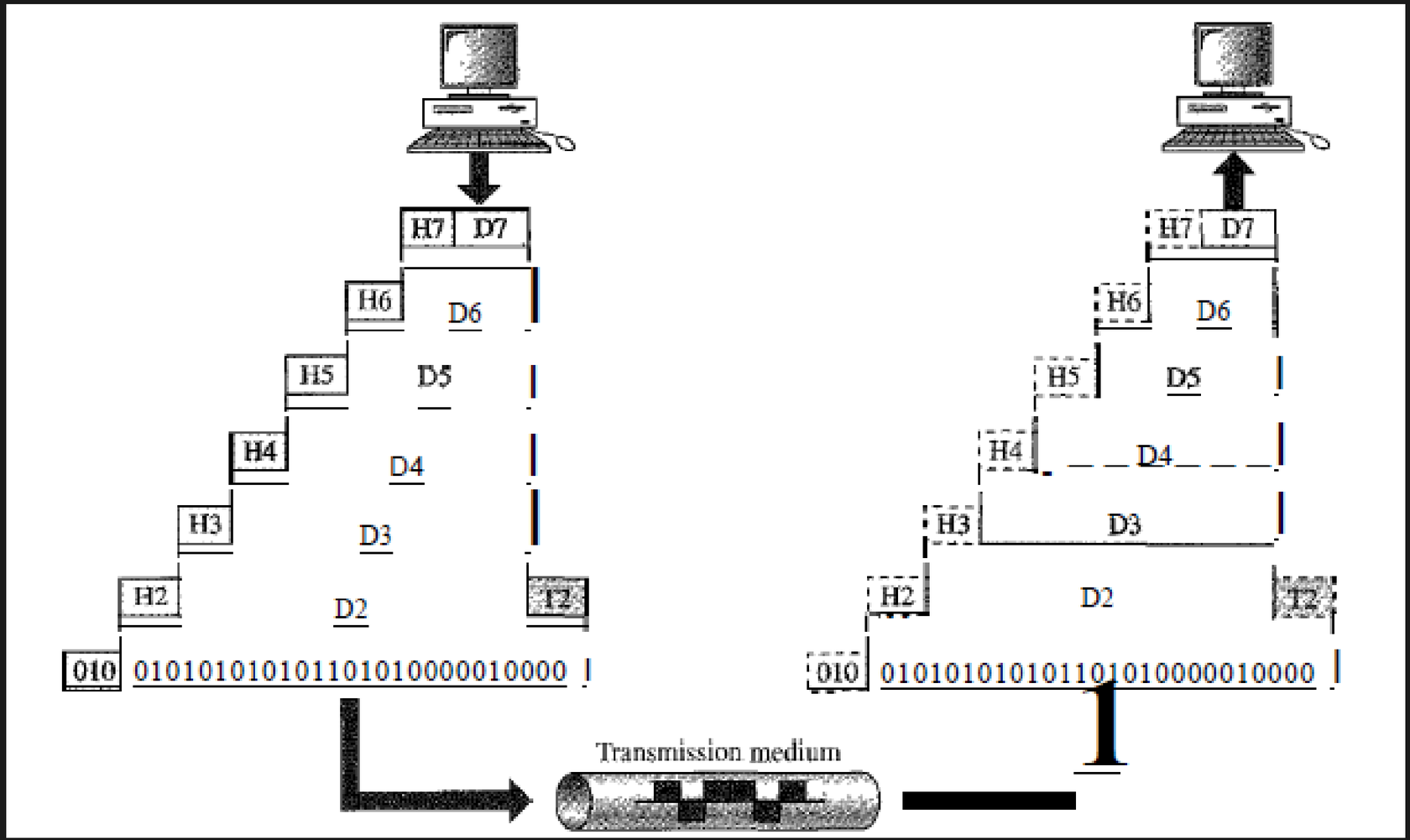
To move packets from source to destination; to provide internetworking

To organize bits into frames; to provide hop-to-hop delivery

To transmit bits over a medium; to provide mechanical and electrical specifications

AN EXCHANGE USING THE OSI MODEL

- The process starts at the application layer, then moves from layer to layer in descending order.
- At each layer, a header or trailer, can be added to the data unit.
- When the formatted data unit passes through layer 1, it is changed into an electromagnetic signal and transported along a physical link.
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form.
- The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it are removed.



PEER-TO-PEER PROCESSES

Within a single machine, each layer calls upon the services of the layer just below it.

Between machines, layer x on one machine communicates with layer x on another machine.

The processes on each machine that communicate at a given layer are called peer-to-peer processes.

INTERFACING BETWEEN LAYERS

The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.

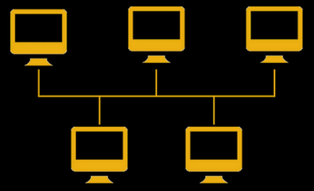
Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network.

As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

ENCAPSULATION

The data portion of a packet at level N – 1 carries the whole packet (data and header and maybe trailer) from level N.
Level N – 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N – 1, the whole packet coming from level N is treated as one integral unit.

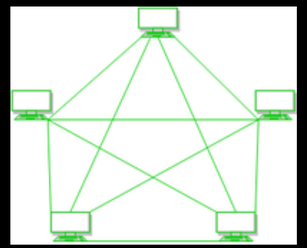
NETWORK TOPOLOGY DESIGN - DELAY ANALYSIS

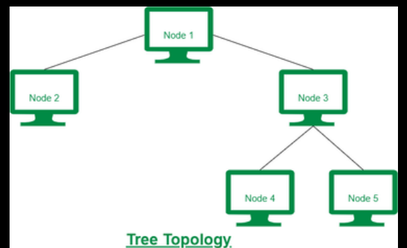


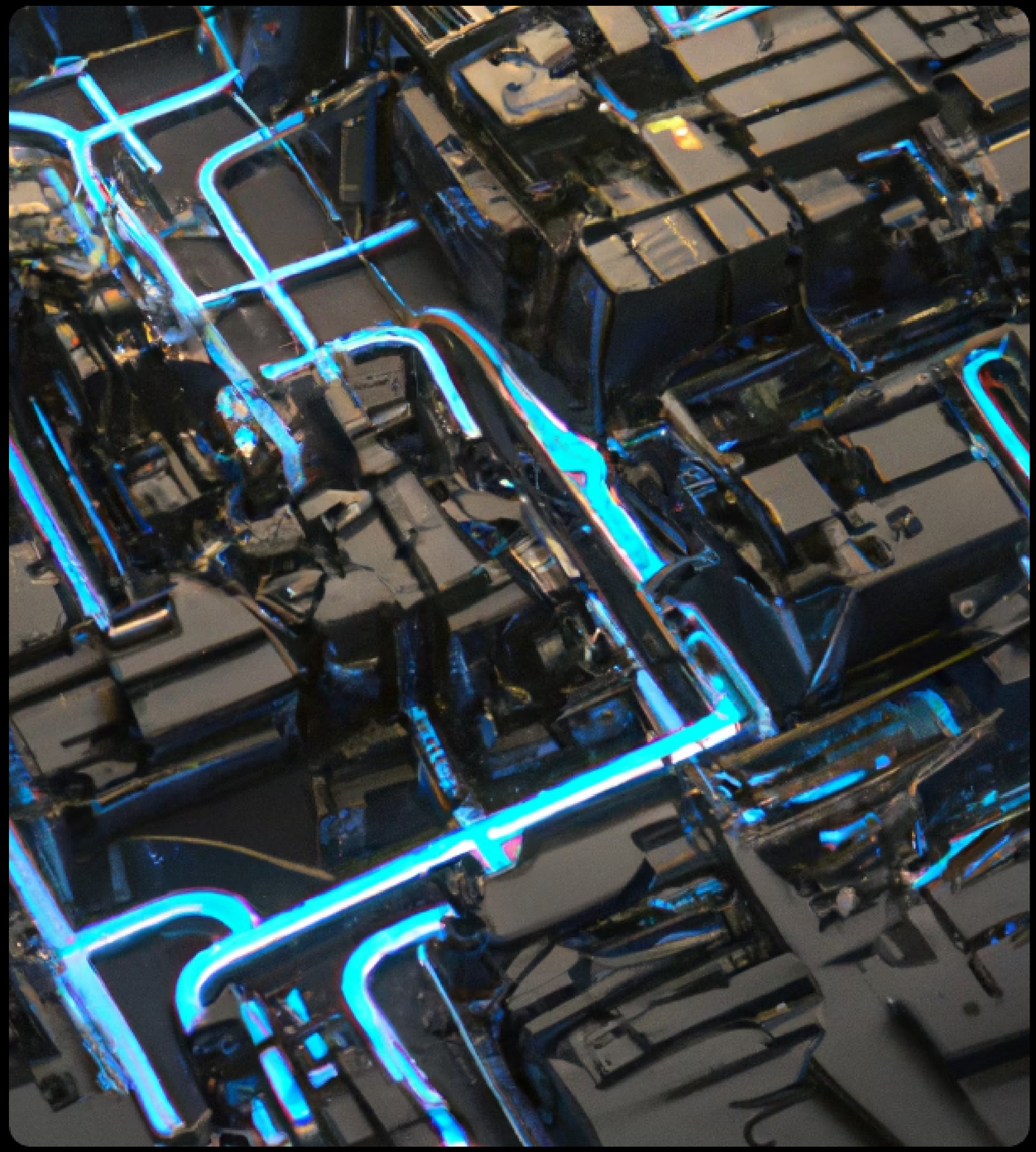
Introduction to Network Topology Design

Network topology refers to the physical or logical layout of a network. It defines how devices are connected and how data is transmitted between them. The design of a network topology plays an important role in determining the performance, reliability, and security of a network.

There are several types of network topology designs, including bus, star, ring, mesh, tree, and hybrid topologies. Each type has its own advantages and disadvantages, and the choice of topology depends on the specific requirements of the network.







Bus Topology Design

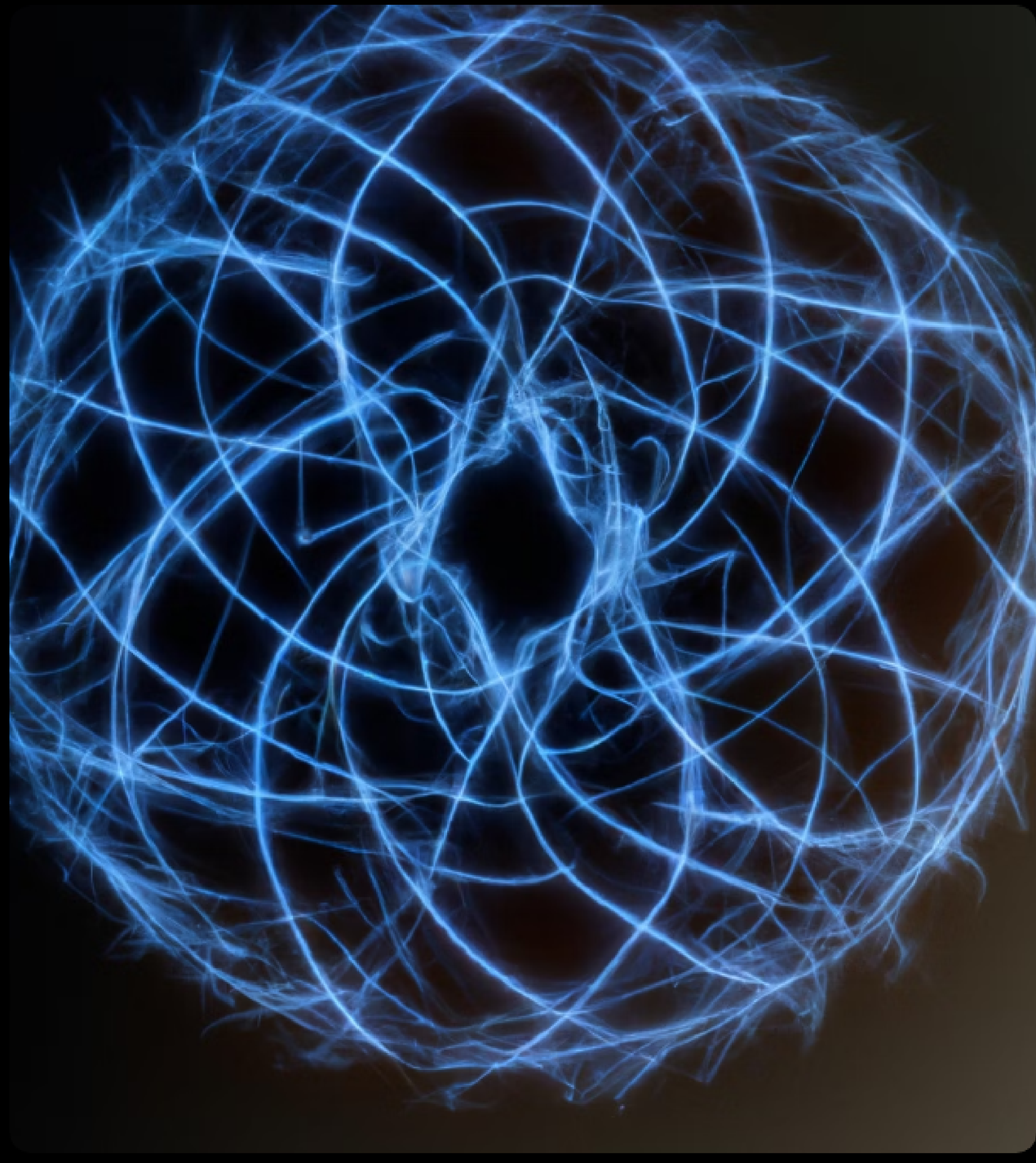
A bus topology design connects all devices to a single cable called a backbone. Data is transmitted along the backbone, and each device receives the data and filters out the data meant for it. The advantage of this design is that it is simple and inexpensive to implement.

However, a disadvantage of the bus topology is that if the backbone fails, the entire network is affected. Additionally, as more devices are added to the network, the bandwidth available to each device decreases.

Star Topology Design

In a star topology design, all devices connect to a central hub or switch. Data is transmitted between devices through the hub or switch. This design provides high performance and is easy to troubleshoot.

However, a disadvantage of the star topology is that if the hub or switch fails, the entire network is affected. Additionally, this design requires more cabling than a bus topology.

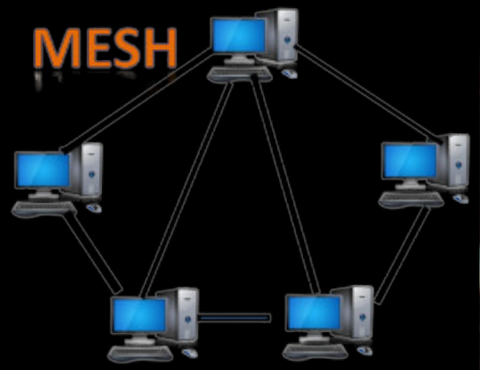


Ring Topology Design

A ring topology design connects devices in a circular loop. Data is transmitted around the ring, and each device receives the data and passes it on to the next device until it reaches its destination. This design provides high performance and is fault-tolerant.

However, a disadvantage of the ring topology is that if one device fails, the entire network is affected. Additionally, adding or removing devices can be difficult and may require the entire network to be shut down.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. 3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.



Mesh Topology Design

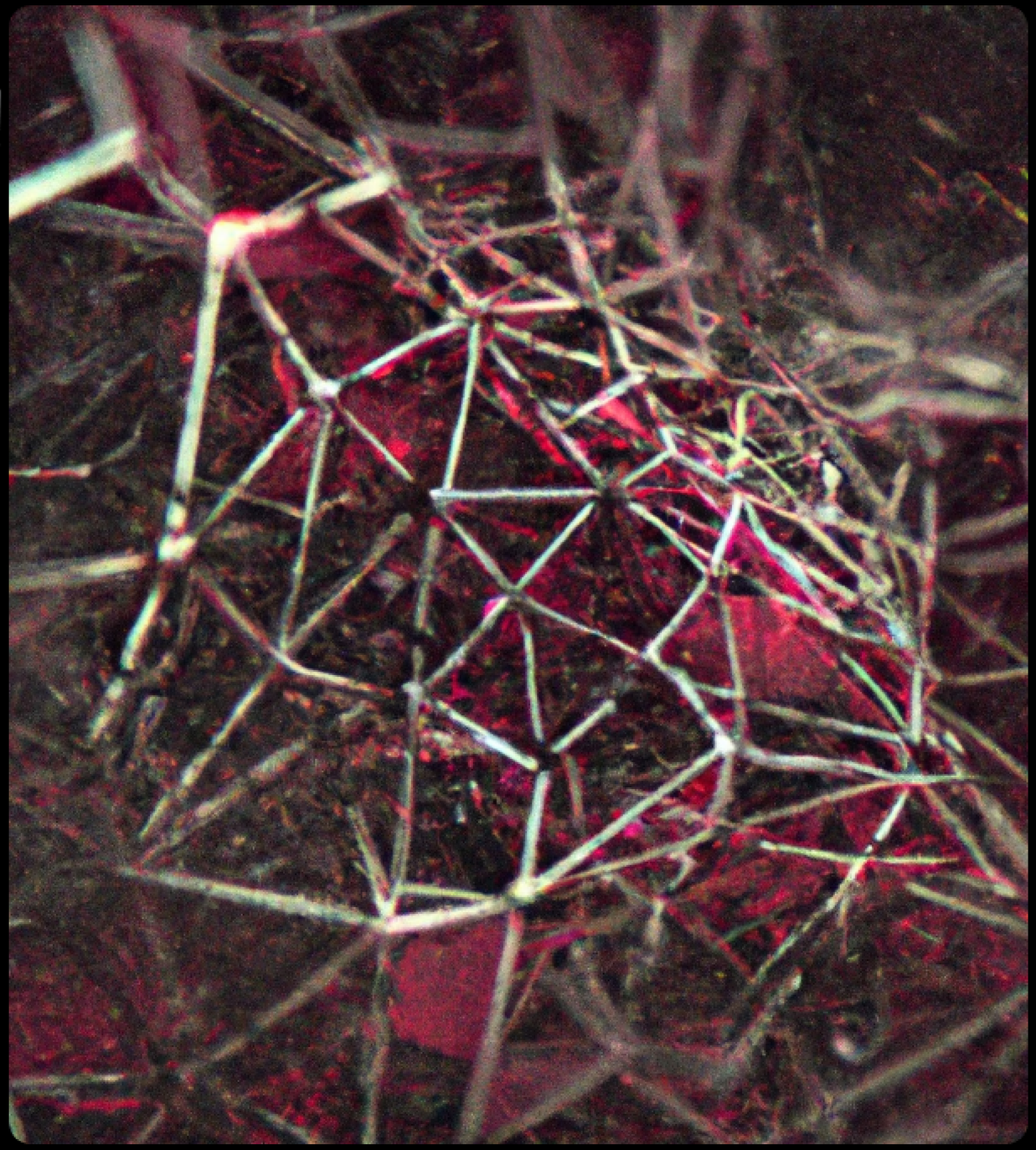
In a mesh topology design, every device is connected to every other device. This provides redundancy and fault-tolerance, as data can be rerouted if one path fails. This design is also highly scalable and can support a large number of devices.

However, a disadvantage of the mesh topology is that it requires a lot of cabling and can be expensive to implement. Additionally, the complexity of the design makes it difficult to troubleshoot.

Number of cables = (n*(n-1))/2

Types:

1. **Routing**
2. **Flooding**



Tree Topology Design

A tree topology design combines multiple star topologies into a hierarchical structure. Devices connect to a central hub, which in turn connects to other hubs. This design provides scalability and fault-tolerance.

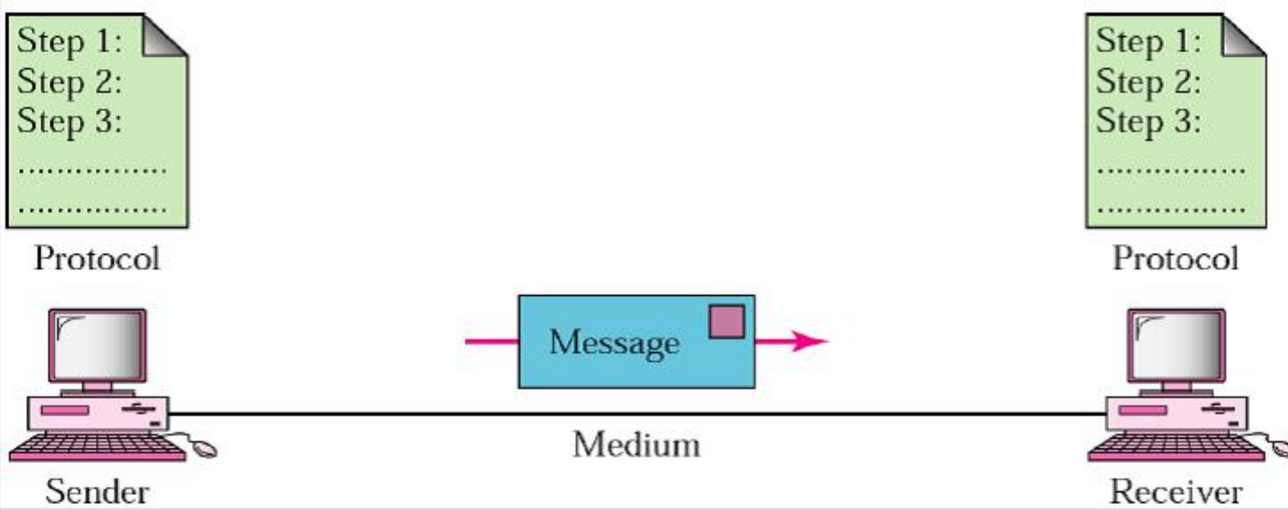
However, a disadvantage of the tree topology is that if the central hub fails, the entire network is affected. Additionally, adding or removing devices can be difficult and may require the entire network to be shut down.

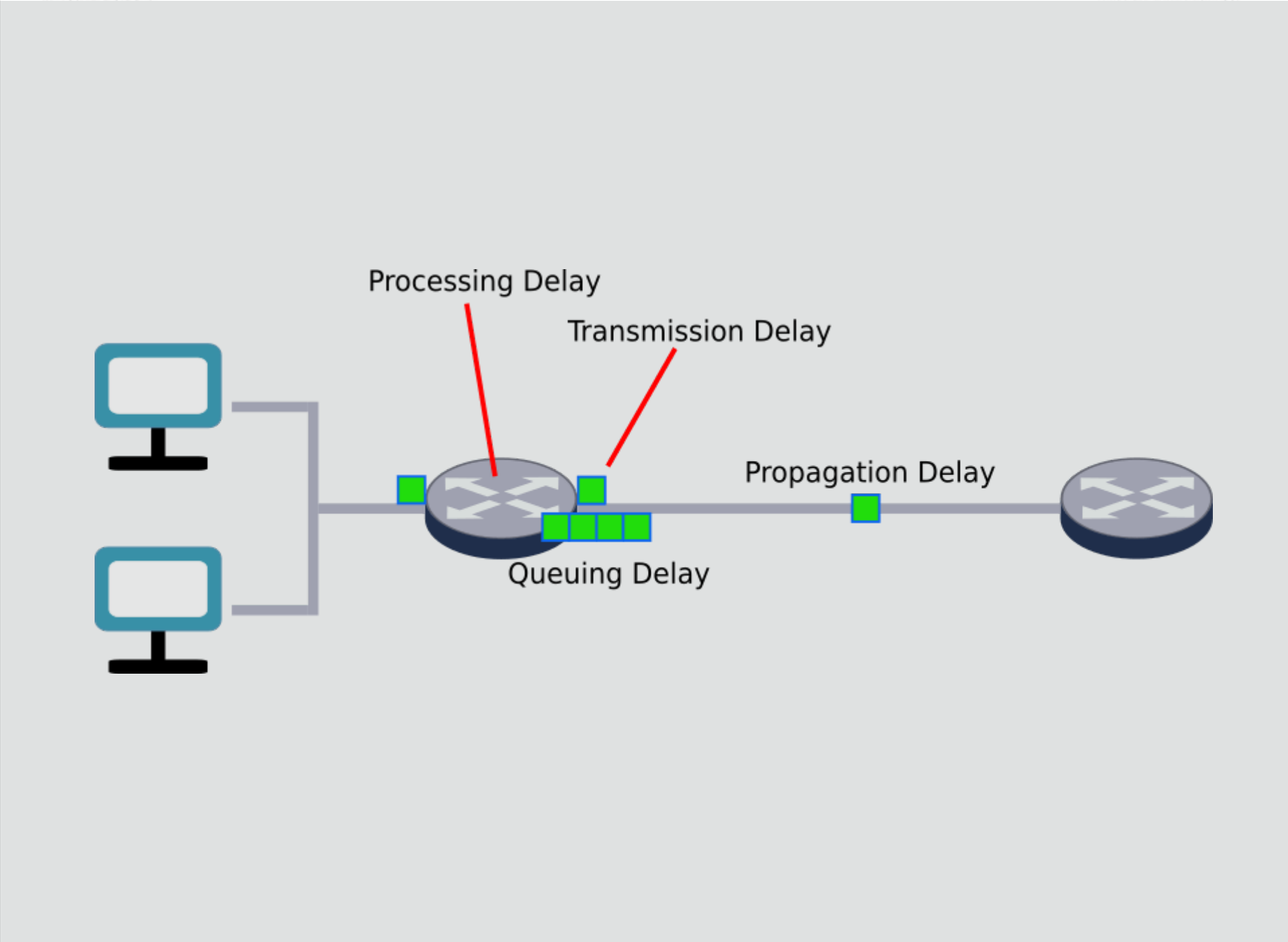
Delay Analysis in Network Topology Design

Delay analysis is the process of measuring and analyzing the time it takes for data to travel from one point to another in a network. There are different types of delay analysis, including propagation delay, transmission delay, queuing delay, and processing delay.

Propagation delay is the time it takes for a signal to travel from one point to another in a network. Transmission delay is the time it takes for data to be transmitted over a network. Queuing delay is the time it takes for data to wait in a queue before being transmitted. Processing delay is the time it takes for a device to process data before transmitting it.

Total Delay =TD + PD + QD + PD



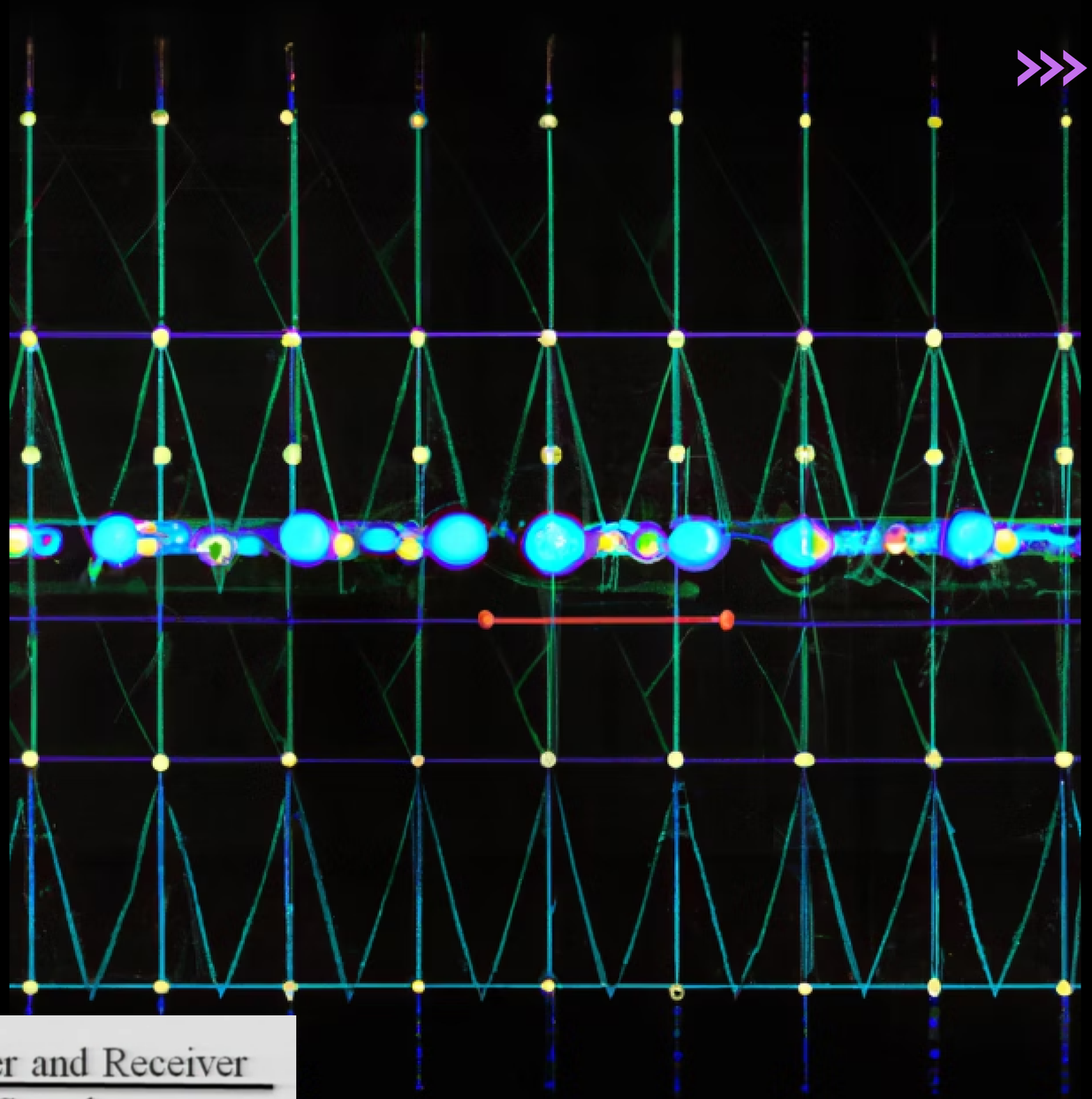


TRAVEL time

Propagation Delay in Network Topology Design

Propagation delay is the time it takes for a signal to travel from one point to another in a network. It is affected by the distance between the devices and the speed of light.

Propagation delay can be minimized by using shorter cables, reducing the number of intermediate devices, and using faster transmission media.

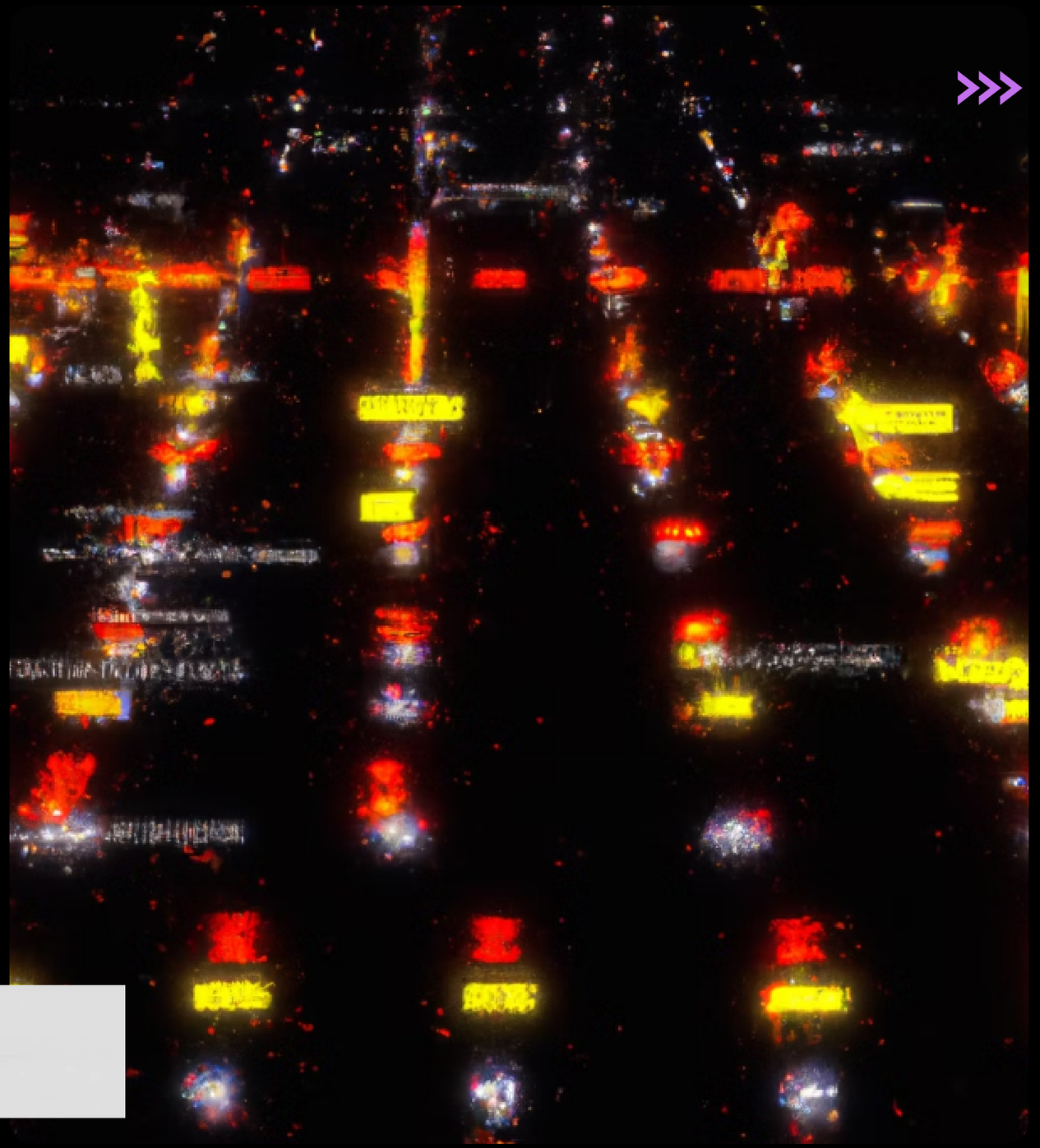


- Propagation delay $\rightarrow \frac{\text{Distance between Sender and Receiver}}{\text{Transmission Speed}}$

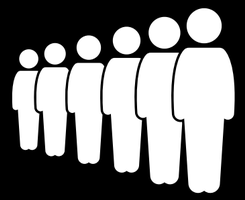
Transmission Delay in Network Topology Design

Transmission delay is the time it takes for data to be transmitted over a network. It is affected by the bandwidth of the transmission medium and the size of the data being transmitted.

Transmission delay can be minimized by using higher bandwidth transmission media, compressing data before transmission, and reducing the size of the data being transmitted.



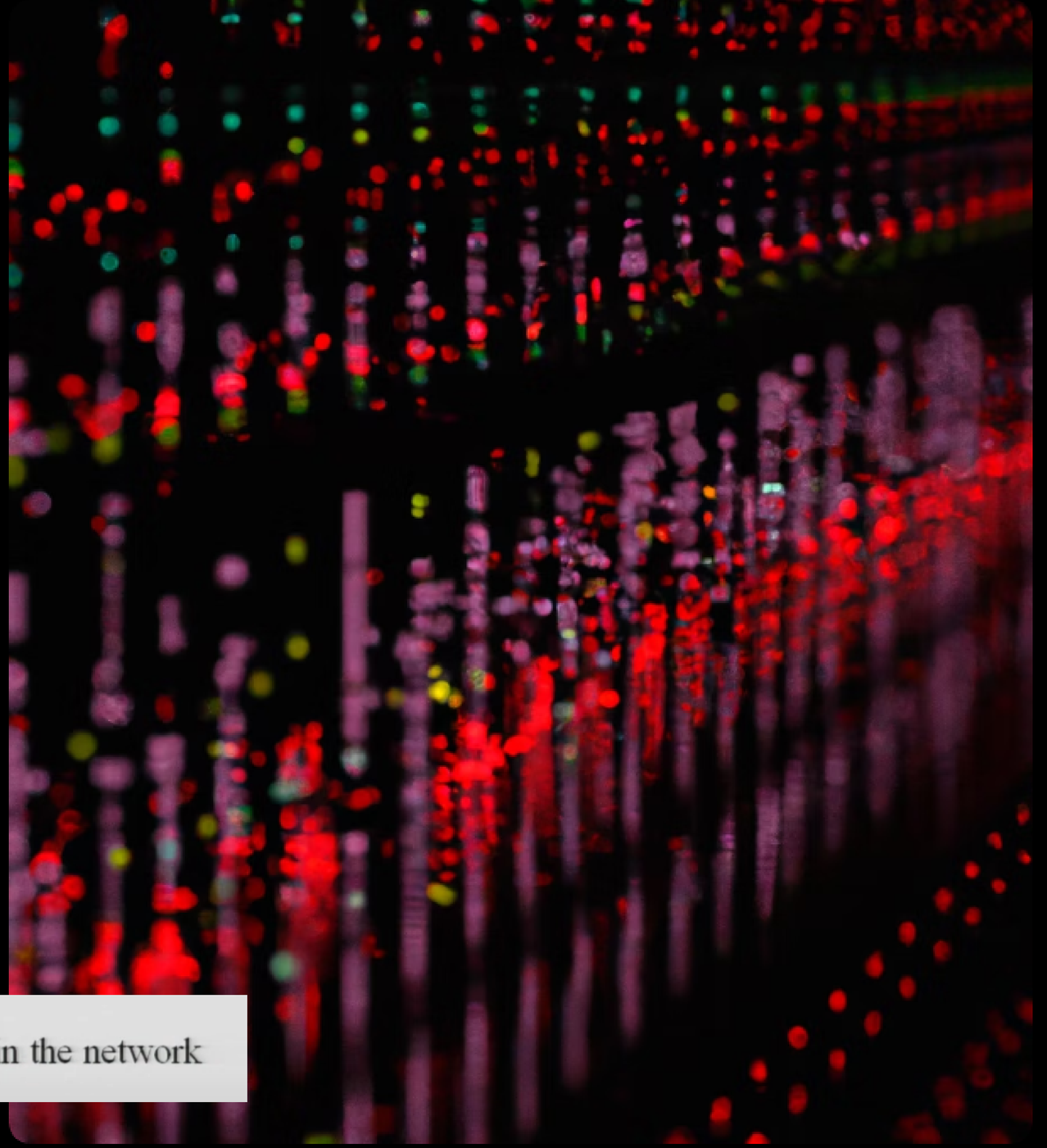
- Transmission delay → $\frac{\text{Length of Data packet}}{\text{Bandwidth}}$



Queuing Delay in Network Topology Design

Queuing delay is the time it takes for data to wait in a queue before being transmitted. It is affected by the amount of traffic on the network and the priority of the data being transmitted.

Queuing delay can be minimized by prioritizing critical data, reducing the amount of traffic on the network, and increasing the capacity of the network.

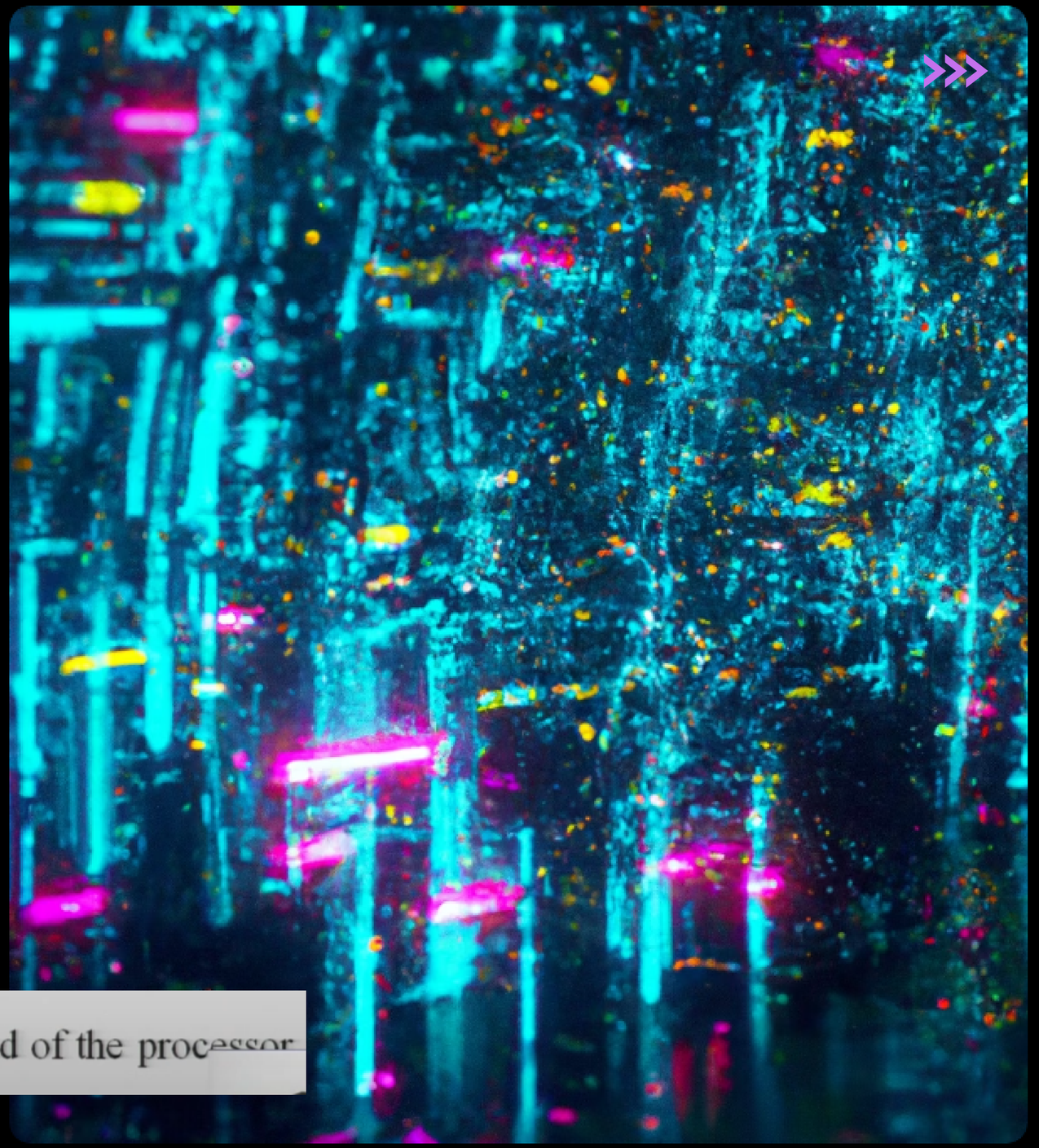


- Queuing delay → Depends on the congestion in the network

Processing Delay in Network Topology Design

Processing delay is the time it takes for a device to process data before transmitting it. It is affected by the processing power of the device and the complexity of the data being processed.

Processing delay can be minimized by using devices with higher processing power, optimizing the data being transmitted for the device, and reducing the complexity of the data being processed.



- Processing delay → Depends on the speed of the processor

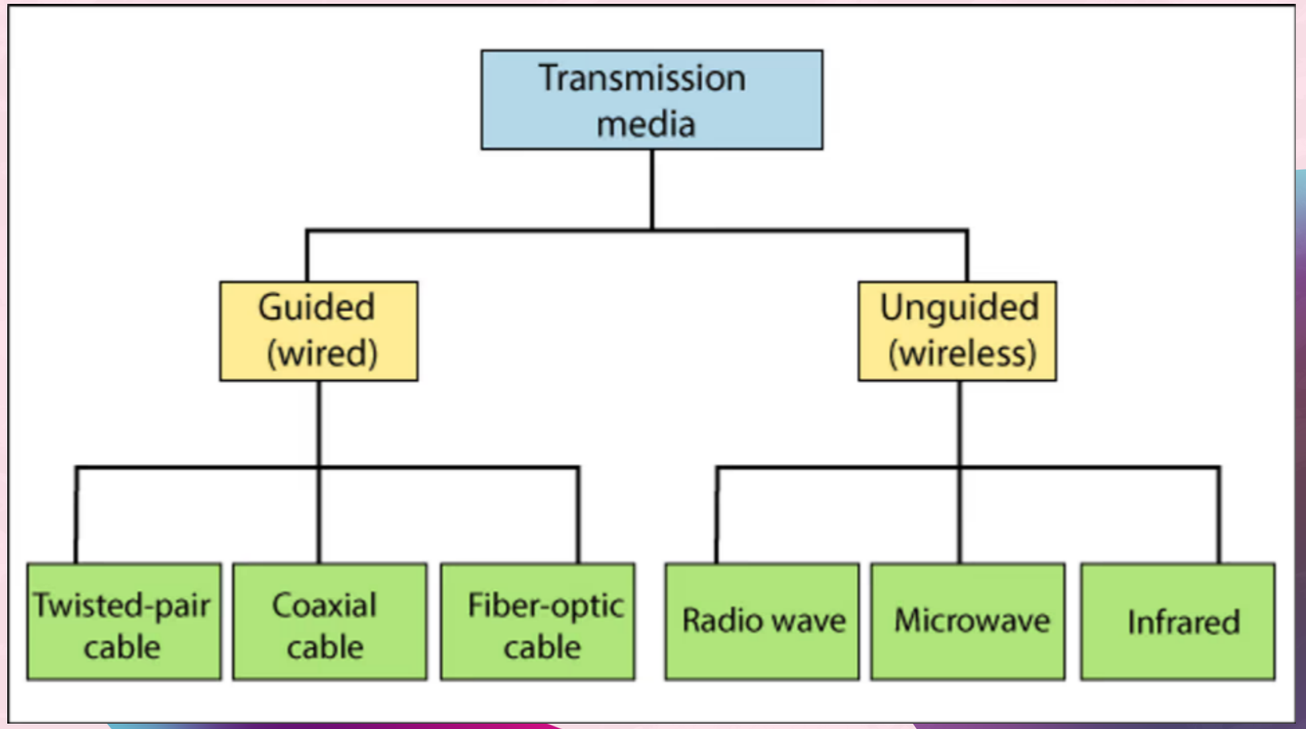
Physical Layer Transmission Media

For Live PPT, click the Title!

Transmission media can be guided, such as copper wires or fiber optic cables, or unguided, such as radio waves or infrared signals.

TRANSMISSION MEDIA IN PHYSICAL LAYER

Transmission Media is a means of establishing a communication medium to send and receive information through electromagnetic signal waves. Transmission media is a physical path between the sender and the receiver in data communication. The physical layer in the OSI model of computer networks is responsible for transmitting raw bits over the communication channel. It operates with various physical elements, therefore, it is placed beneath the physical layer while being worked on by physical elements from the physical layer. The Local Area Network (LAN), which contains both the transmitter and the receiver, is the network that operates via the transmission medium. The electrical or optical signals are transmitted through either copper or fibre-based transmission media.



The physical layer of a computer network is responsible for transmitting raw bits over a communication channel.

There are two main types of transmission media in computer networks. These are guided and unguided media. While guided media requires a physical medium, unguided media requires air for communication.

TYPES OF TRANSMISSION MEDIA

Guided Media (Wired Media)

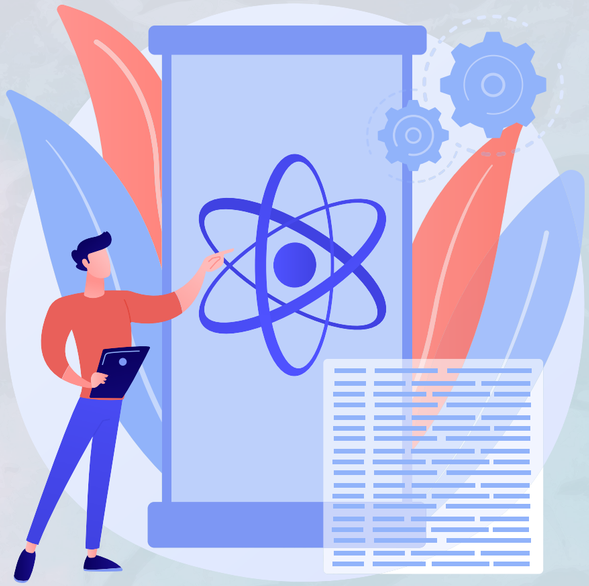
In guided media, the transmission signal properties are controlled and focused in a fixed constricted channel, which can be implemented with the help of physiologically connected contacts. One of the most prominent aspects of Guided Media is its fast transmission velocity.

Advantages of Guided Media

- The cost of guided media is very low (inexpensive) and easily available.
- This is very Flexible and Lightweight.
- Very easy to set up and install.

Disadvantages of Guided Media

- Bandwidth is very low in guided media.
- Susceptible to interference and noise- (Noise is an electrical disturbance that can degrade communication).
- High maintenance and installation costs.



GUIDED MEDIA TYPES

Various types of guided media are based on the connecting material used for creating the network are:

1. Coaxial Cable: Coaxial cable is a type of guided media comprising a copper core surrounded by insulation, a braided metal shield, and an outer jacket. It is commonly used for cable television and high-speed Internet connections.

Advantages of coaxial cable:

- Can transmit data over longer distances than twisted pair cable
- Better resistance to electromagnetic interference
- Can support higher bandwidths than twisted pair cable

Disadvantages of coaxial cable:

- More expensive than twisted pair of cable
- Difficult to install
- Limited flexibility

2

TWISTED PAIR CABLE

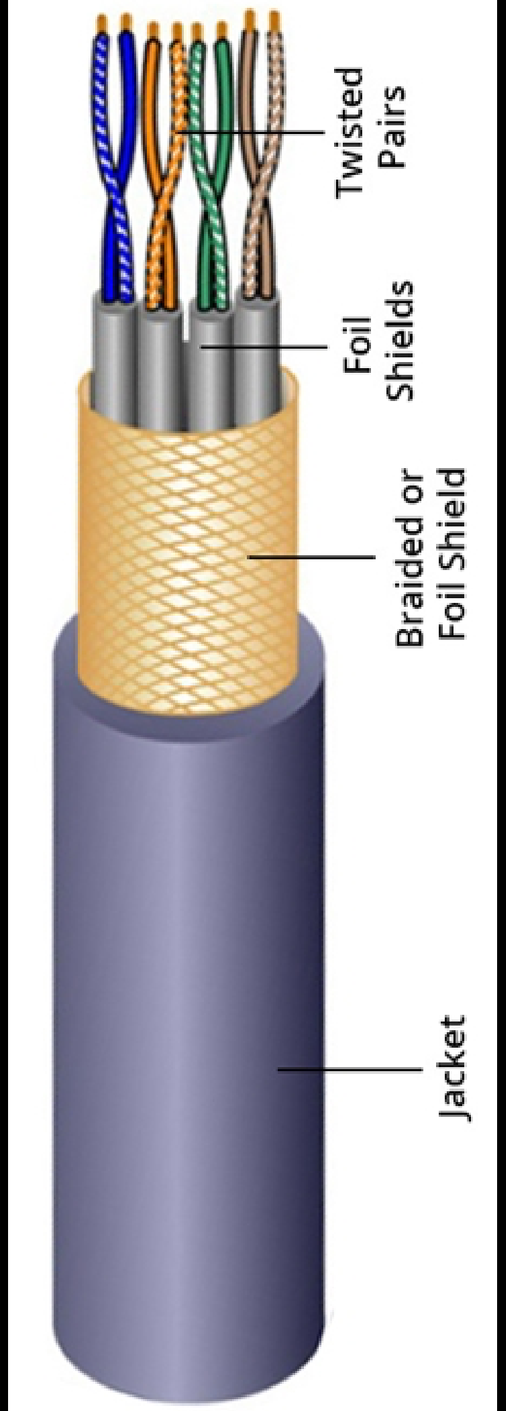
Twisted pair cable is the most commonly used type of guided media. It consists of two insulated copper wires twisted together to reduce electromagnetic interference. There are two types of twisted pair cable: unshielded twisted pair (UTP) and shielded twisted pair (STP).

Advantages of twisted pair cable:

- Inexpensive
- Easy to install
- Flexible and can be used for different applications
- Can transmit data over long distances

Disadvantages of twisted pair cable:

- Susceptible to electromagnetic interference
- Limited bandwidth
- Not suitable for high-speed data transmission



3

FIBER OPTIC CABLE

Optical Fibre Cables are glass-based cables that transmit light signals. The reflection concepts are employed for light signal transmission over cables. It is recognized for allowing bulkier data to be delivered with more bandwidth and reduced electromagnetic interference during transmission.

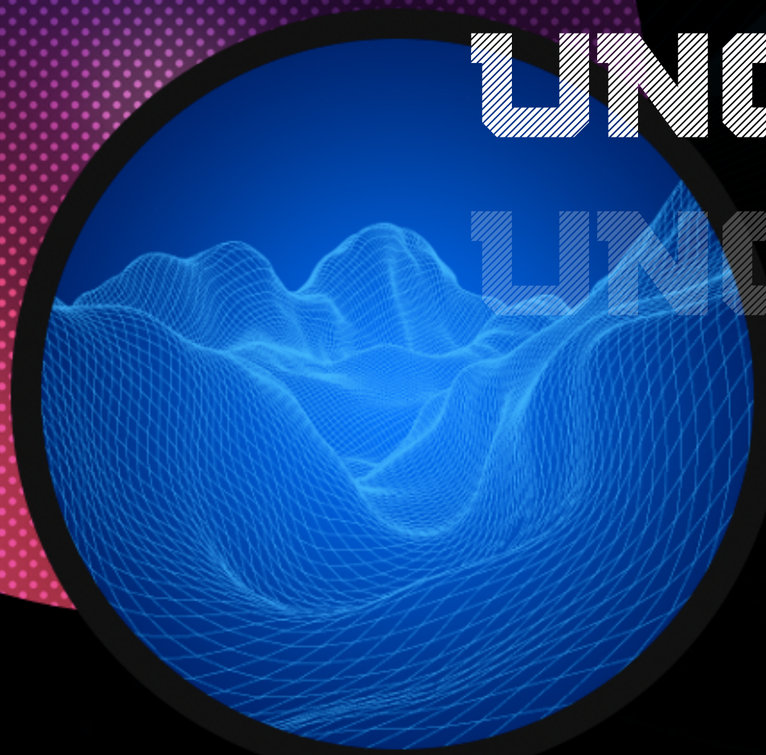
Advantages of fiber optic cable:

- Can transmit data over longer distances than other types of guided media
- High bandwidth
- Immune to electromagnetic interference

Disadvantages of fiber optic cable:

- Expensive
- Requires specialized equipment for installation and maintenance
- Fragile and can be easily damaged

$-\hat{\mathbf{z}} = |1\rangle$



UNGUIDED MEDIA

UNGUIDED MEDIA
UNGUIDED MEDIA

UNGUIDED

Unguided media is also referred to as Wireless or Unbounded transmission media. It can be described as a wireless transmission medium without a physical link to the network's nodes or servers. In comparison to guided media, electromagnetic signal waves are less secure because they are transmitted in the air over a wider geographic area.

Advantages of Unguided Media

- Used for large-distance transmission.
- Highly convenient for users.
- Maintenance and installation cost is less compared to guided media.

Disadvantages of Unguided Media

- Less secure.
- Unavailability of bandwidth.

UNGUIDED MEDIA TYPES

Unguided media can be classified into three types based on the signals used for the transmission.The types of unguided media include:

1. Radio Waves: Radio waves are electromagnetic waves that are used for communication in wireless networks. They are commonly used for mobile phones, wireless LANs, and Bluetooth devices.

Advantages of radio waves:

- Easy to install and use
- Can transmit data over long distances
- Can penetrate walls and other obstacles

Disadvantages of radio waves:

- Susceptible to interference from other wireless devices
- Limited bandwidth
- Limited security

2

MICRO WAVES

Microwaves are high-frequency radio waves that are commonly used for point-to-point communication. They are used for satellite communication, microwave ovens, and cellular networks.

Advantages of microwaves:

- Can transmit data over long distances
- Can support high bandwidths
- Immune to electromagnetic interference

Disadvantages of microwaves:

- Limited range
- Susceptible to interference from weather conditions
- Expensive to install and maintain

3

INFRARED WAVES

Infrared waves are electromagnetic waves that are used for short-range communication. They are commonly used for remote controls, wireless keyboards, and computer mice.

Advantages of infrared waves:

- Easy to install and use
- Low cost
- Immune to electromagnetic interference

Disadvantages of infrared waves:

- Limited range
- Requires line-of-sight communication
- Can be blocked by obstacles

CONCLUSION

- In conclusion, The selection of transmission media in computer networks depends on several factors, such as the cost, distance, bandwidth requirements, and the nature of the application.
- Each type of transmission media has its own advantages and disadvantages, and network designers must weigh these factors when selecting a transmission media for a particular application.
- Guided media offers better security, reliability, and higher bandwidth, but it is generally more expensive and difficult to install than unguided media. Unguided media provides easy installation, lower cost, and can transmit data over long distances, but it is susceptible to interference and has limited bandwidth and range.
- Ultimately, the selection of guided or unguided media depends on the specific requirements of the network and the trade-offs between the advantages and disadvantages of each media type.

01

Switching Methods

What is Switching

Switching is the mechanism in computer networks.that helps indeciding the bestroute for data transmission if there are multiple paths available in a large network.

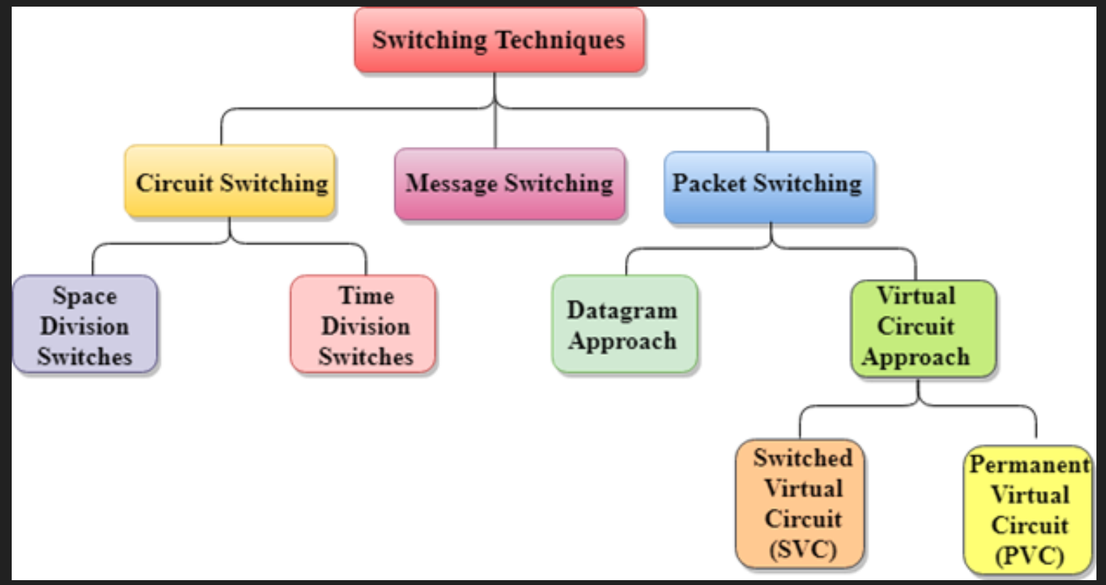
A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch

In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example).

Types of Switching Techniques

Traditionally, three methods of switching have been important:
1.Circuit switching
2.Packet switching
3.Message switching.

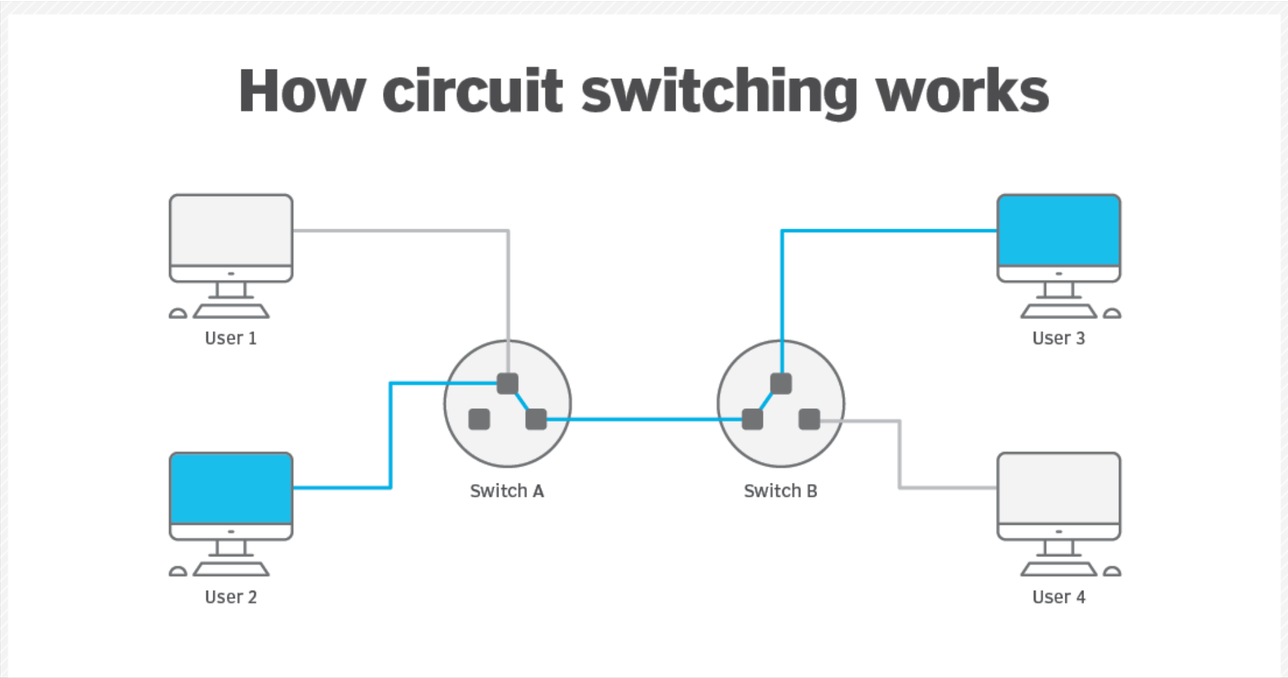
The first two are commonly used today. The third has been phased out in general communications but still has networking applications.



04

Circuit Switching

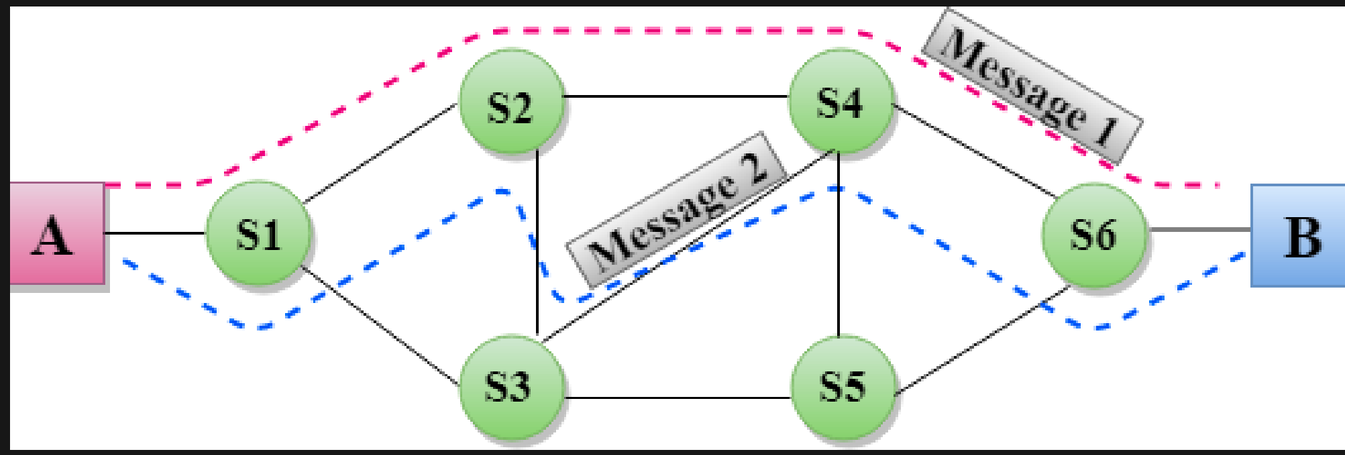
- When a dedicated path or circuit is created between the sender and receiver to communicate, this type of switching technique is called circuit switching.
- A connection is established before the transfer of the data.
- An example of such a circuit is a telephone network. A virtual circuit is established between the caller and the callee before the user can make a call.



05

Message Switching

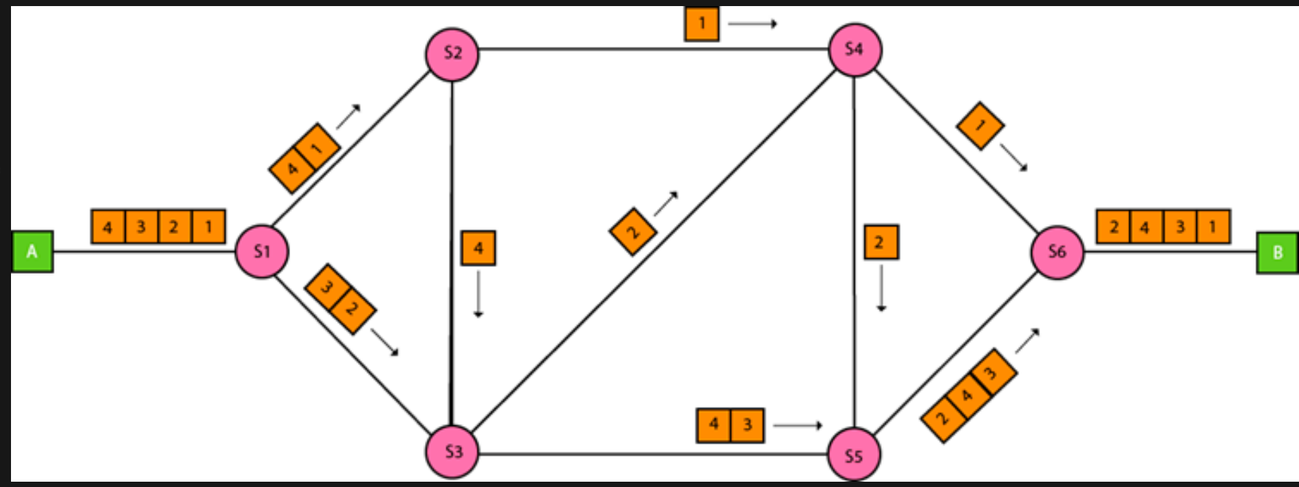
- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**



06

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it 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.



- Packets will travel across the network, taking the shortest path as possible.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.
- If any packet is missing or corrupted, then the message will be sent to resend the message.

Approaches of Packet Switching

DATAGRAM PACKET SWITCHING

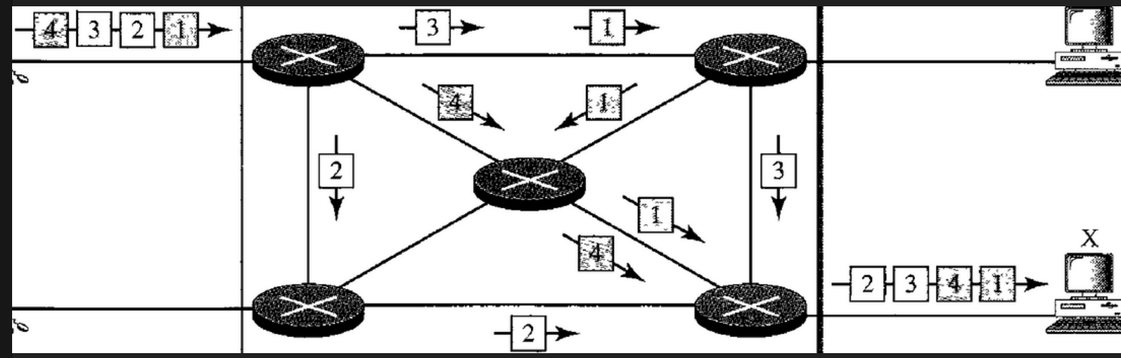
In a datagram network, each packet is treated independently of all others

VIRTUAL CIRCUIT SWITCHING

It is a cross between a circuit-switched network and a datagram network

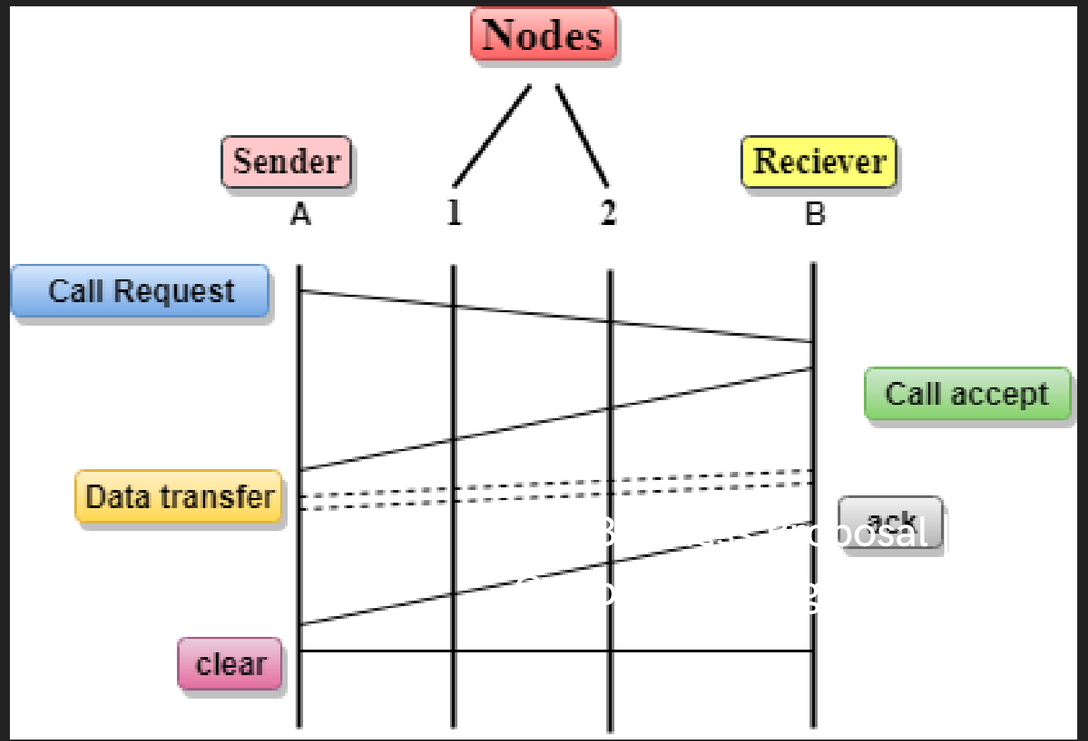
Datagram Packet Switching

- In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams.
- Datagram switching is normally done at the network layer.
- As in a datagram network, data are packetised and each packet carries an address in the header.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.



VIRTUAL-CIRCUIT NETWORKS

- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a datagram network, data are packetised and each packet carries an address in the header.
- As in a circuit-switched network, all packets follow the same path established during the connection.
- 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. But this may change in the future.

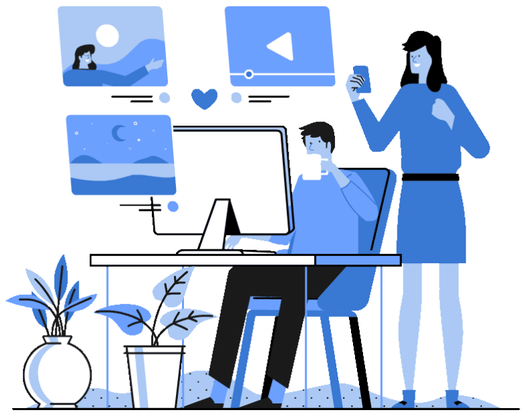


Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

COMPUTER NETWORKS

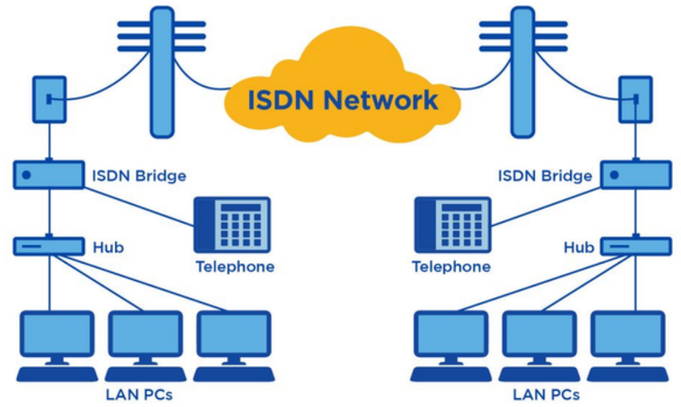
ISDN



- What is ISDN ?
- ISDN Components
- ISDN reference points
- ISDN encapsulation
- Telecommuter/Remote User
- Telecommuter / Remote Office
- ISDN Service
- Dail on Demand Routing
- ISDN Protocols
- Advantages and Disadvantages of ISDN

ISDN & Its features

- ISDN is a set of standards which define and end to end Digital network
- It uses existing telephone wiring
- It is an alternative to using leased lines
- It can transport many types of Network traffic such as voice, data, video, text, graphics etc.
- Faster data transfer rate than modems
- Faster call setups than modems



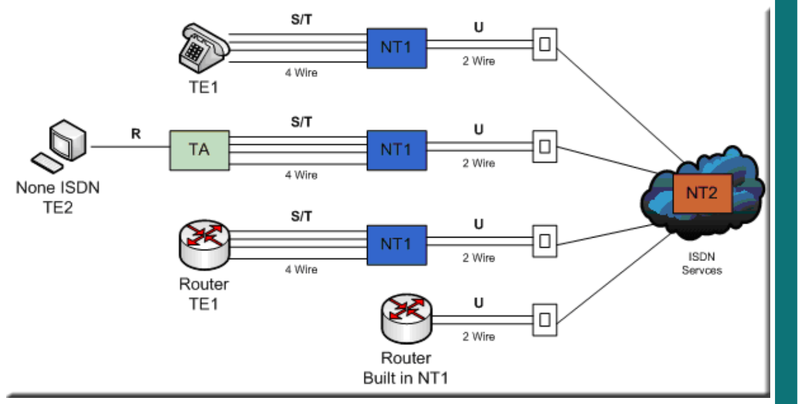
ISDN components

- **Network termination type 1 (NT1)**

Network termination devices that connect the four wire subscriber wiring to the conventional two wire local loop.

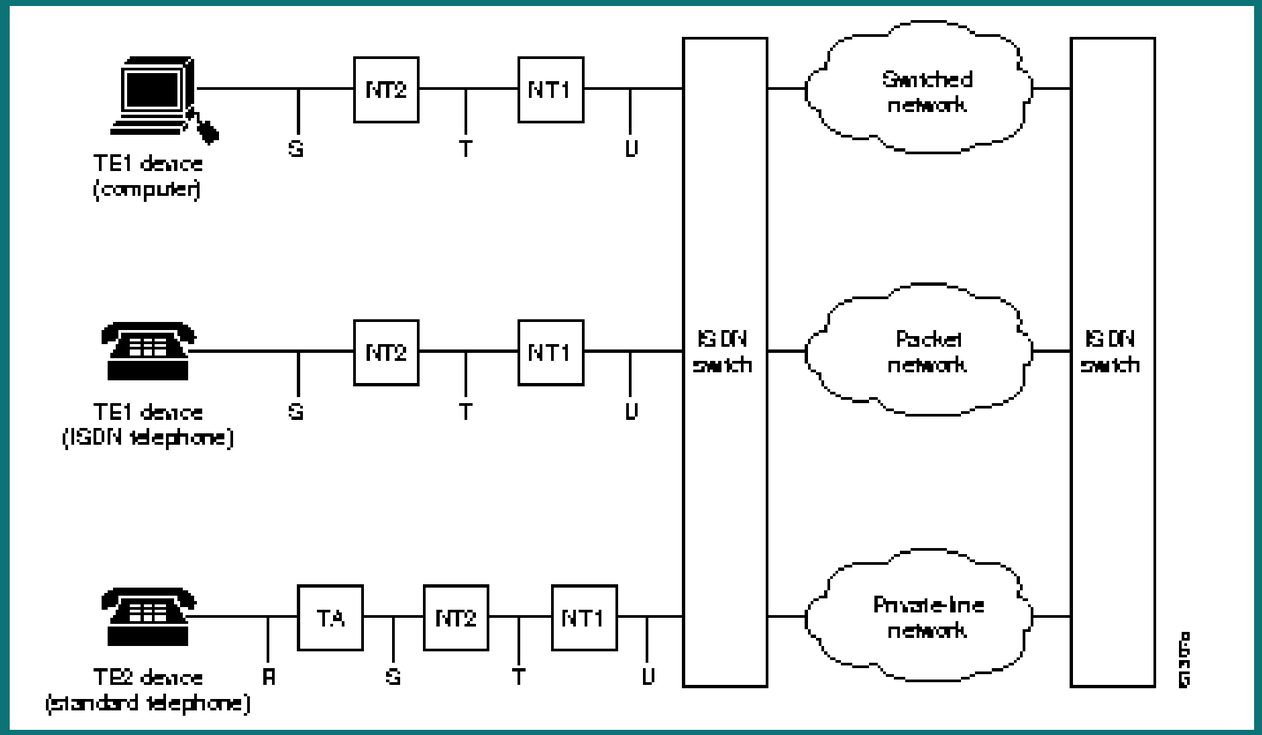
- **Network termination type 2 (NT2)**

Provides multiple ISDN interfaces on an ISDN line. The NT2 maybe as simple as bridging device connected to an NT1 unit.



ISDN reference points

- The ISDN reference points define the communication protocols between the different ISDN functional devices.
- The importance of reference points is that different protocols may be used at each reference point.



ISDN encapsulation

- HDLC

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes.

- PPP

In computer networking, Point-to-Point Protocol (PPP) is a data link layer (layer 2) communication protocol between two routers directly without any host or any other networking in between.

- LAPB

LAPB is a bit-oriented protocol derived from HDLC that ensures that frames are error free and in the correct sequence.
LAPB is used to manage communication and packet framing between data terminal equipment (DTE) and the data circuit-terminating equipment (DCE) devices in the X.25 protocol stack.

Telecommuter/Remote User

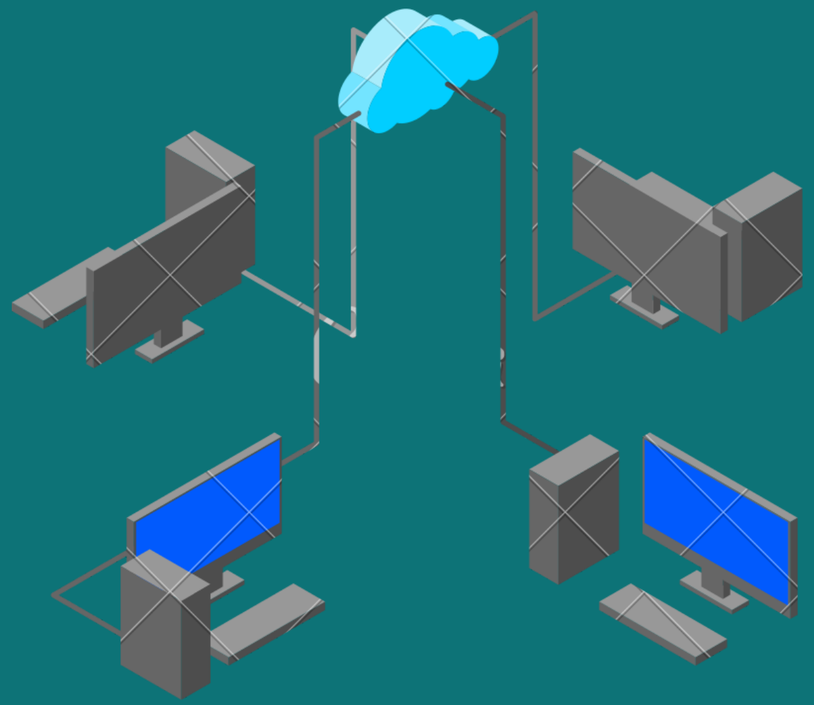
Using Modem and PSTN

Public Switched Telephone Network (PSTN) is an agglomeration of an interconnected network of telephone lines owned by both governments as well as commercial organizations.

Using ISDN

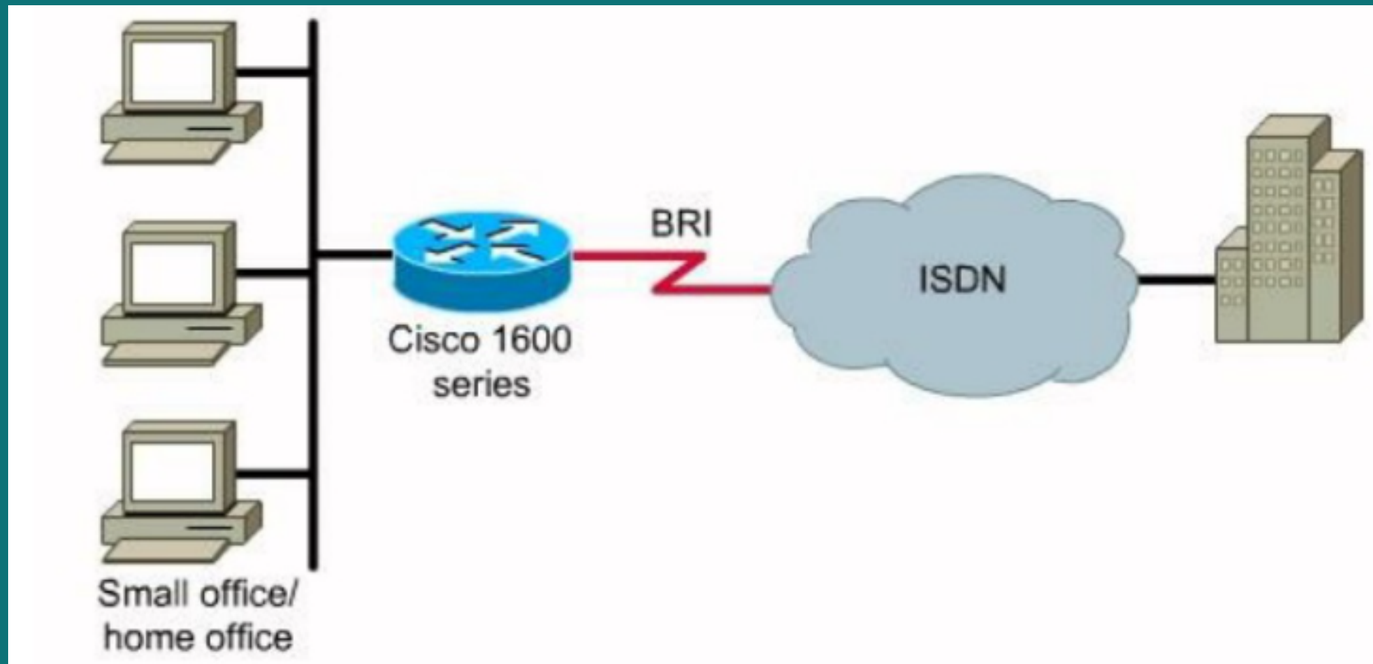
From an enterprise perspective, the technology is fully suited for most remote access objectives, offering BRI services (2B+D channels) for end users, with an overall bandwidth of 112/128 kbps for user data. Service providers usually offer ISDN service with two data/voice channels for the end user.

Telecommuter / Remote Office

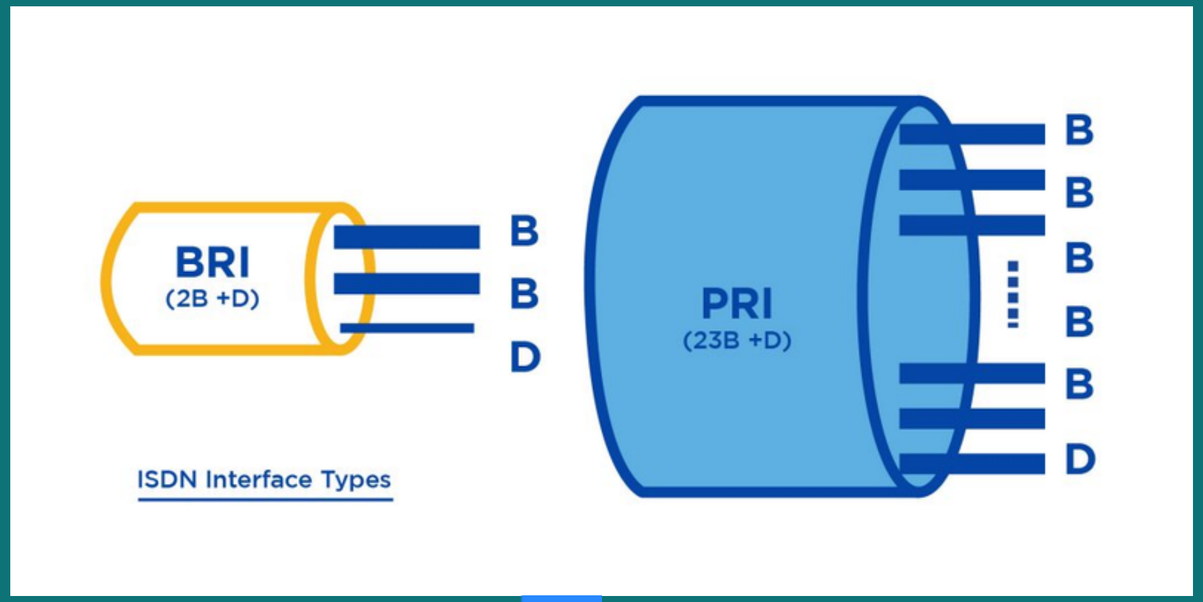


Components and considerations

- ISDN Router
- Multiple Remote users at same location



ISDN Service



- **Basic Rate Interface (BRI) –**

There are two data-bearing channels (‘B’ channels) and one signaling channel (‘D’ channel) in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps.

- **Primary Rate Interface (PRI) –**

Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country you are in. PRI is not supported on the iSeries..

Dail on Demand Routing

- Dial-On-Demand Routing (DDR) is a technique whereby a router can automatically initiate and close a circuit-switched session as transmitting stations demand. The router spoofs keep alives so that end stations treat the session as active. DDR permits routing over ISDN or telephone
- DDR enables remote WAN data connections that automatically terminate after transmission activity ends. DDR is used with primary and backup connections.

ISDN PROTOCOLS

Protocols start with the following letters :

E — Protocols recommend telephone network standards for ISDN

I — Protocols for Concepts , Terminology and General Methods

Q — Protocols , how switching and signaling should operate , Call setup .

Advantages and Disadvantages of ISDN

Advantages of ISDN:

- **ISDN channels have a reliable connection.**
- **ISDN is used to facilitate the user with multiple digital channels.**
- **It has faster data transfer rate.**

Disadvantages of ISDN:

- **ISDN lines costlier than the other telephone system.**
- **It requires specialized digital devices.**
- **It is less flexible.**