Computer Networks

Third Year of Computer Engineering

(2015 Course)

Subject Code:**310245**

Prof. Mohini G. Devikar

Course Objectives:

- To understand the fundamental concepts of networking standards, protocols and technologies.
- To learn different techniques for framing, error control, flow control and routing.
- To learn role of protocols at various layers in the protocol stacks.
- To learn network programming.
- To develop an understanding of modern network architectures from a design and performance perspective

Course Outcomes:

On completion of the course, student will be able to–

- Analyze the requirements for a given organizational structure to select the most appropriate networking architecture, topologies, transmission mediums, and technologies
- Demonstrate design issues, flow control and error control
- Analyze data flow between TCP/IP model using Application, Transport and Network Layer Protocols.
- Illustrate applications of Computer Network capabilities, selection and usage for various sectors of user community.
- Illustrate Client-Server architectures and prototypes by the means of correct standards and technology.
- Demonstrate different routing and switching algorithms

Books

Text Books:

- **Andrew S. Tanenbaum, *Computer Network*, Prentice-Hall**
- **Fourauzan B., "Data Communications and Networking"**

Unit I Physical Layer

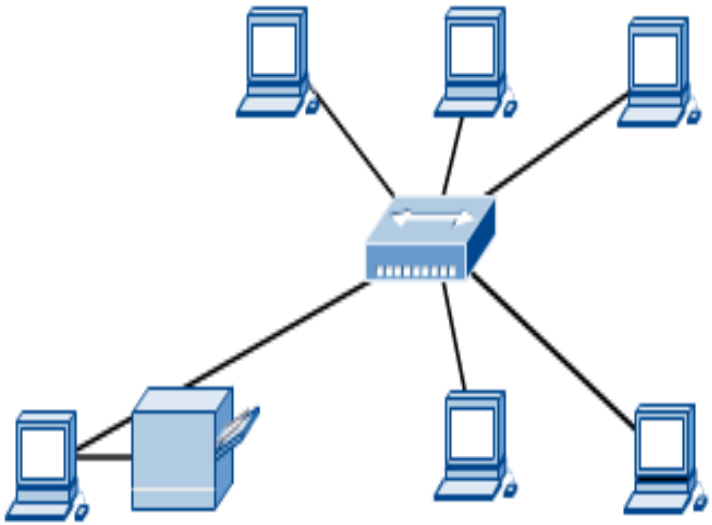
Introduction of LAN; MAN; WAN; PAN, Ad-hoc Network, Network Architectures: Client-Server; Peer To Peer; Distributed and SDN, OSI Model, TCP/IP Model, Topologies: Star and Hierarchical; Design issues for Layers, Transmission Mediums: CAT5, 5e, 6, OFC and Radio Spectrum, Network Devices: Bridge, Switch, Router, Brouter and Access Point, Manchester and Differential Manchester Encodings; IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Network

A 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 Networks

- Computer network connects two or more autonomous computers.
- If two computers are able to share the information it means they are in a network.
- The computers can be geographically located anywhere.



Data Communication

- The term telecommunication means communication at a distance.
- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Components of data communication

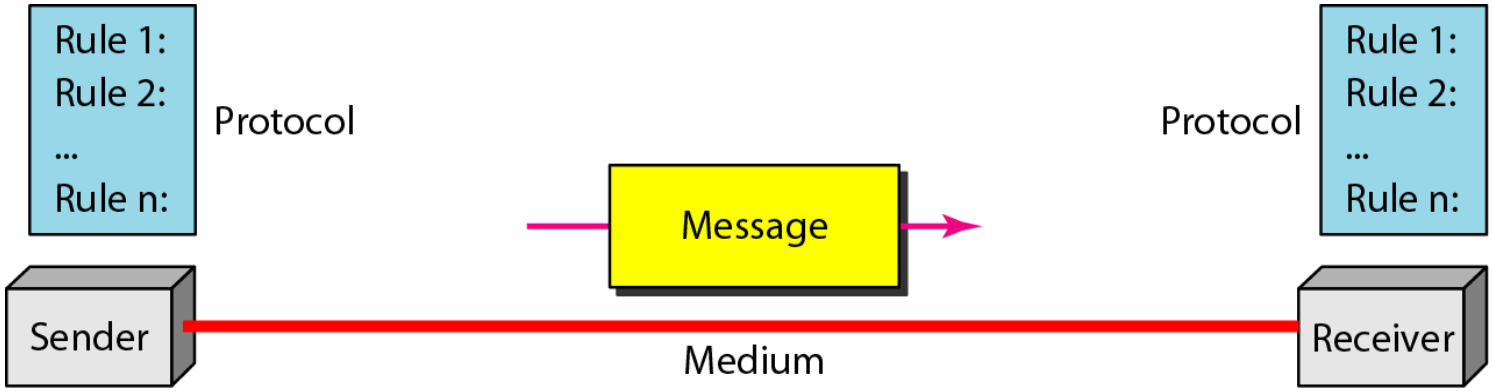


Fig.1 Five components of data communication

Components of data communication

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

Components of data communication

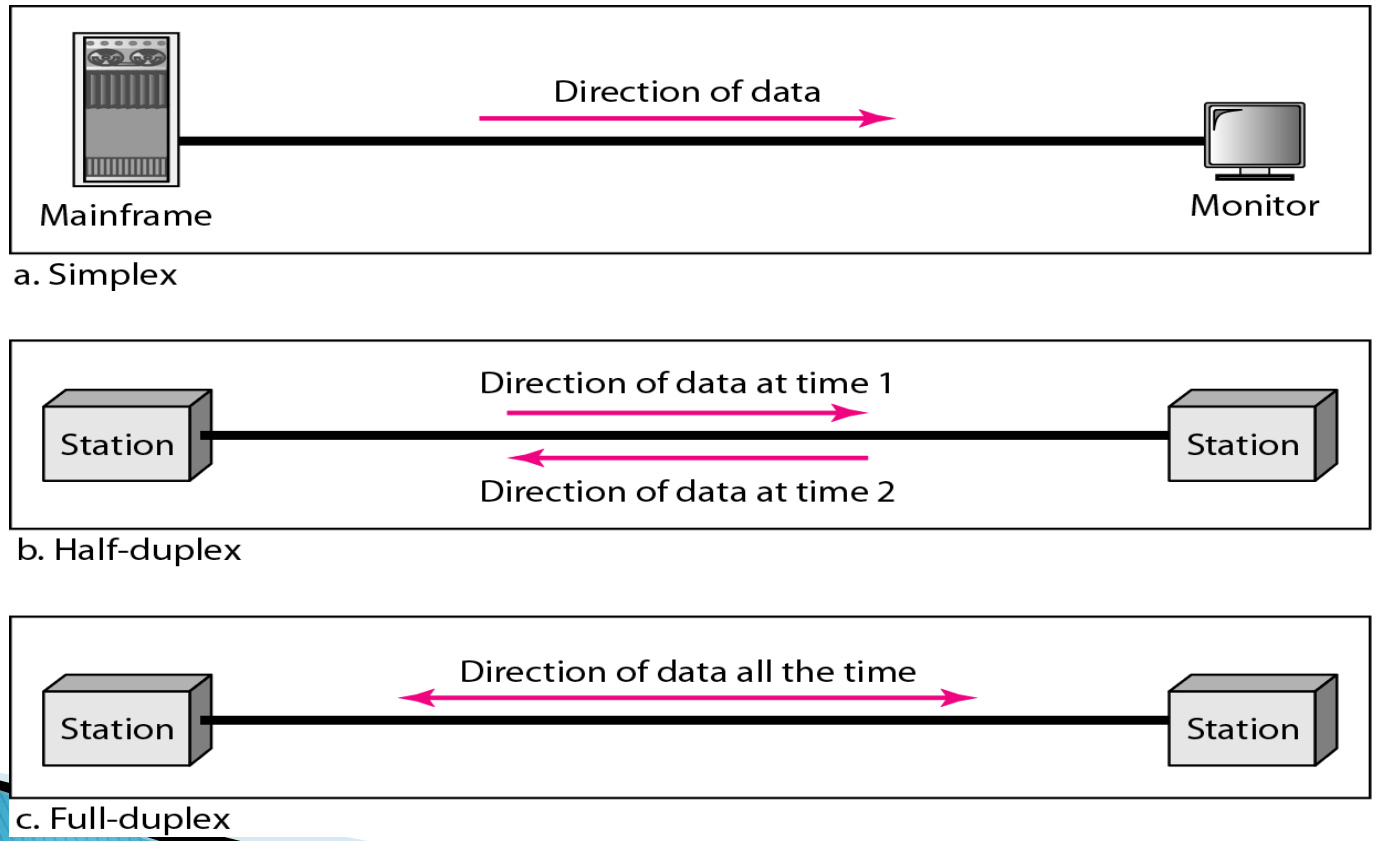
4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver.

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 Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure.



Data Flow

a. Simplex

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.

Eg. Keyboards and traditional monitors are examples of simplex devices.

b. Half-Duplex

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 .

Eg. Walkie-talkies and speakerphone are both half duplex systems.

c. Full-Duplex

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.

PAN, LAN, MAN & WAN

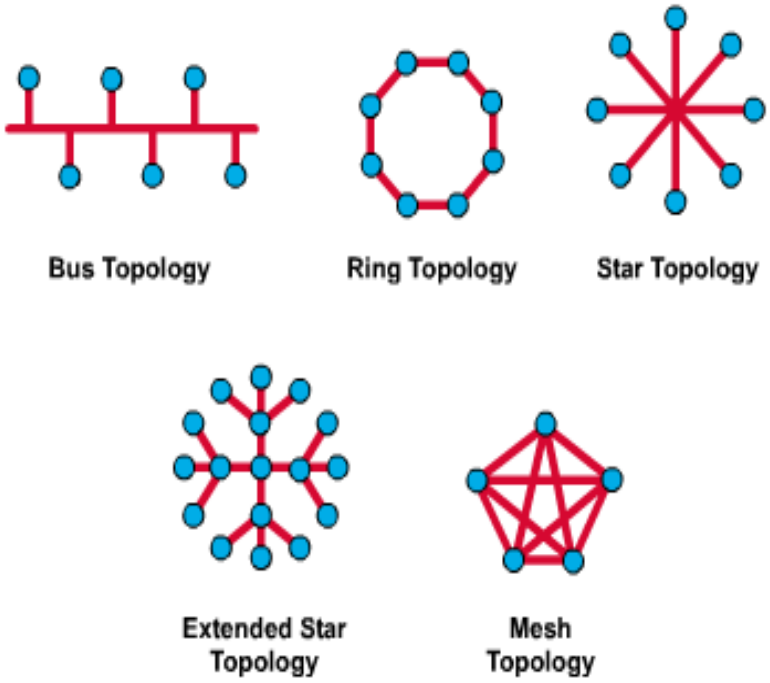
- A personal area network (PAN) is a computer network for interconnecting devices on an individual person's workspace.
- Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- Network in a City is call MAN (Metropolitan Area Network)
- Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)

Applications of Networks

- **Resource Sharing**
  - Hardware (computing resources, disks, printers)
  - Software (application software)
- **Information Sharing**
  - Easy accessibility from anywhere (files, databases)
  - Search Capability (WWW)
- **Communication**
  - Email
  - Message broadcast

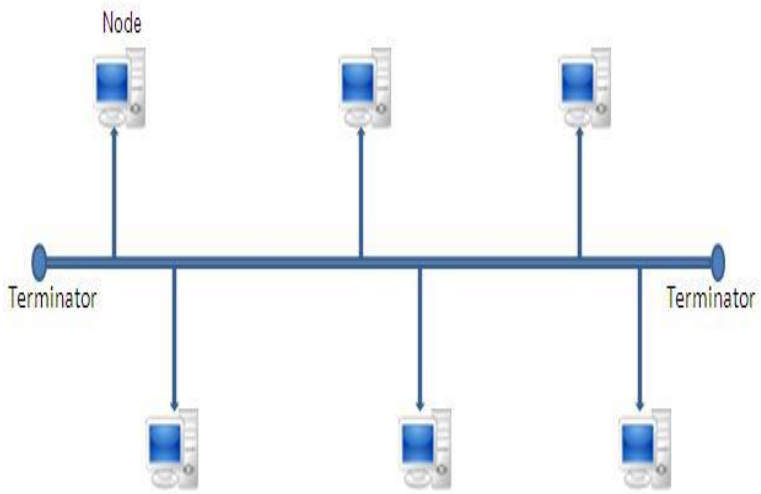
Network Topology

The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



Bus Topology

- Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



Advantages of Bus Topology

1)Easy to implement and extend

2)Well suited for temporary networks that must be set up in a hurry

3)Typically the least cheapest topology to implement

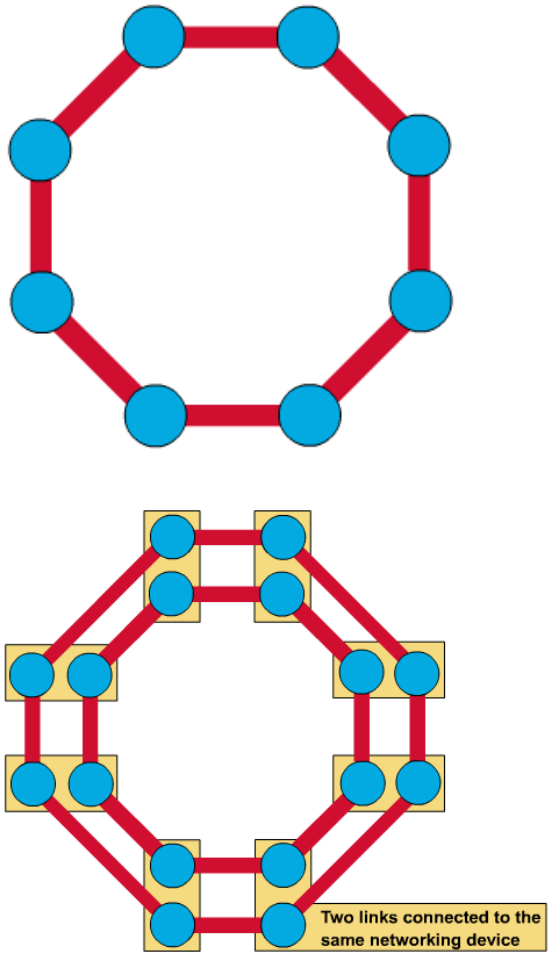
4)Failure of one station does not affect others

Disadvantages of Bus Topology

1) Difficult to administer/troubleshoot
2) Limited cable length and number of stations
3) A cable break can disable the entire network; no redundancy
4) Maintenance costs may be higher in the long run
5) Performance degrades as additional computers are added

Ring Topology

- A frame/token travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.
- The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.
  - Single ring – All the devices on the network share a single cable
  - Dual ring – The dual ring topology allows data to be sent in both directions.



Advantages of Ring Topology

1) This type of network topology is very organized

2)Performance is better than that of Bus topology

3)No need for network server to control the connectivity between workstations

4)Additional components do not affect the performance of network

5)Each computer has equal access to resources

Disadvantages of Ring Topology

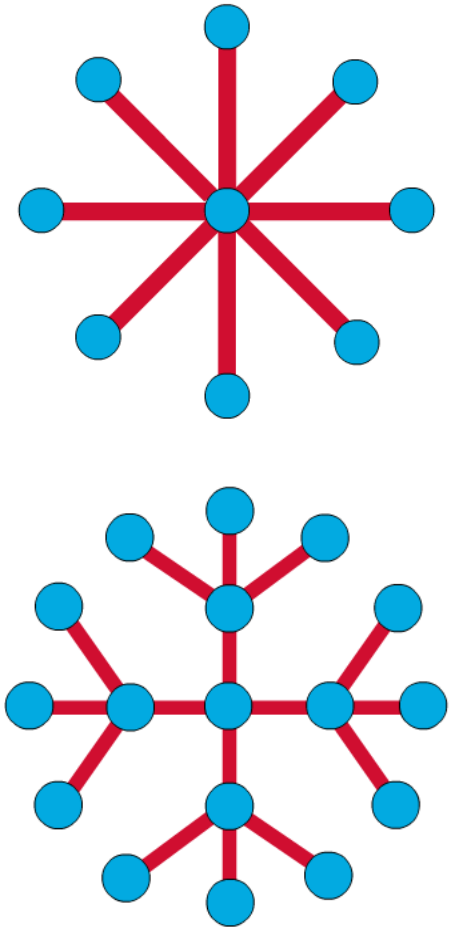
1)Each packet of data must pass through all the computers between source and destination, slower than star topology

2)If one workstation or port goes down, the entire network gets affected

3)Network is highly dependent on the wire which connects different components

Star & Tree Topology

- The star topology is the most commonly used architecture in Ethernet LANs.
- When installed, the star topology resembles spokes in a bicycle wheel.
- Larger networks use the extended star topology also called tree topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



Advantages of Star Topology

1)Compared to Bus topology it gives far much better performance

2)Easy to connect new nodes or devices

3)Centralized management. It helps in monitoring the network

4)Failure of one node or link doesn’t affect the rest of network

Disadvantages of Star Topology

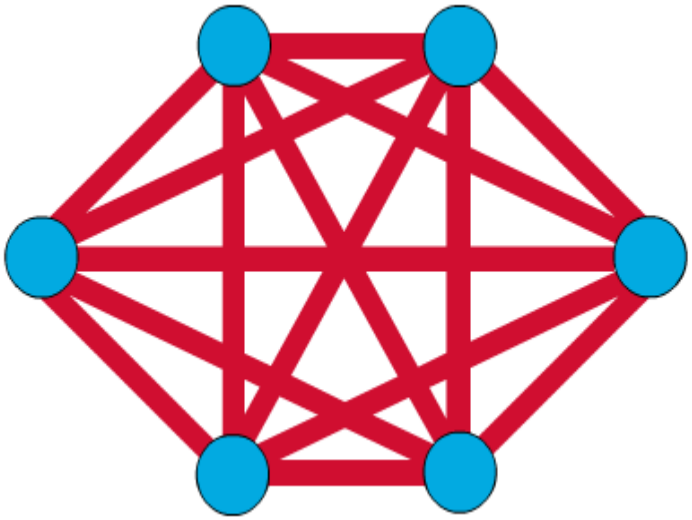
1)If central device fails whole network goes down

2)The use of hub, a router or a switch as central device increases the overall cost of the network

3)Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- Every networked node is directly connected to every other networked node
- It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- Implementing the mesh topology is expensive and difficult.



Advantages of Mesh Topology

1)Manages high amounts of traffic, because multiple devices can transmit data simultaneously.

2)A failure of one device does not cause a break in the network or transmission of data.

3)Adding additional devices does not disrupt data transmission between other devices.

Disadvantages of Mesh Topology

1) The cost to implement is higher than other network typologies, making it a less desirable option.

2)Building and maintaining the topology is difficult and time consuming.

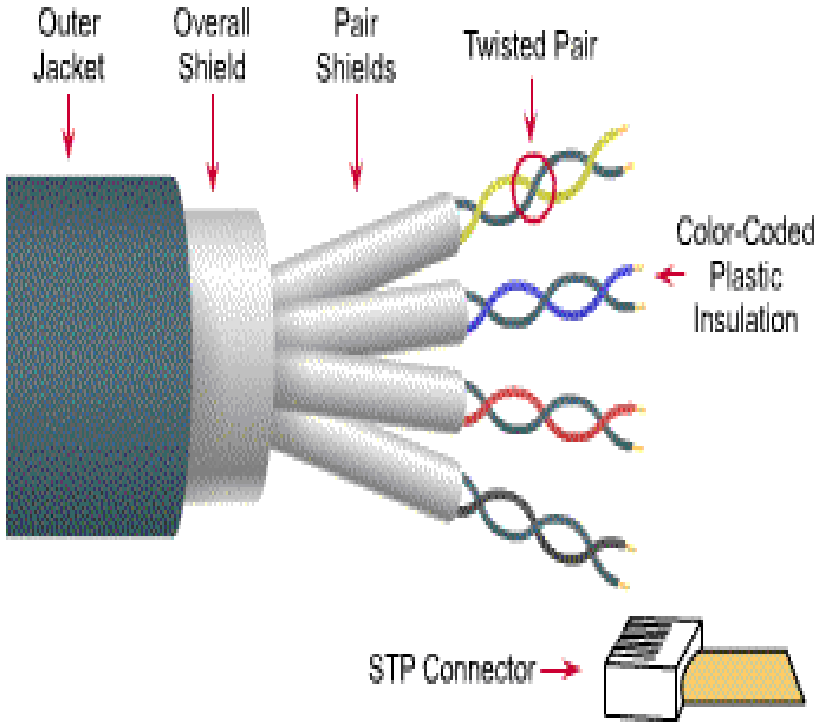
3)The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

Network Components

- Physical Media
- Interconnecting Devices
- Computers
- Networking Software
- Applications

Networking Media

- Networking media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).



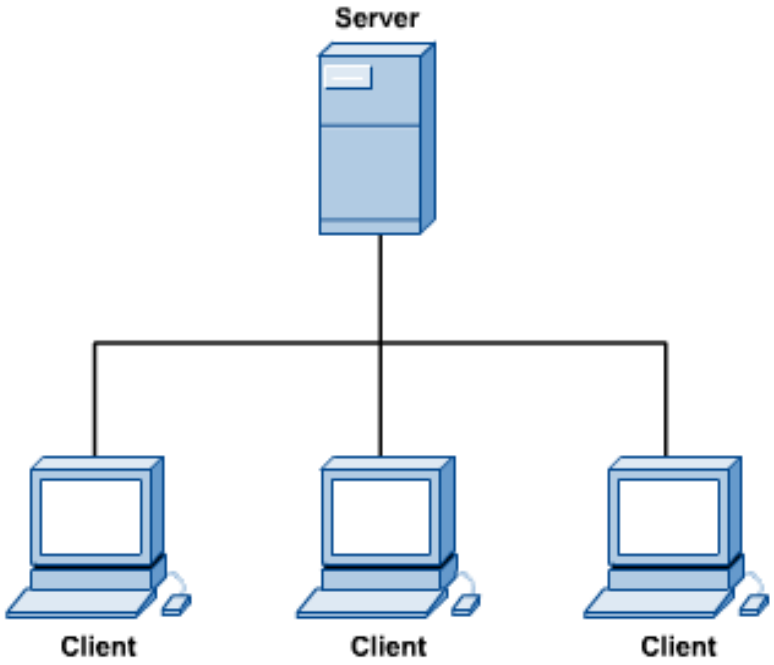
- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

Networking Devices

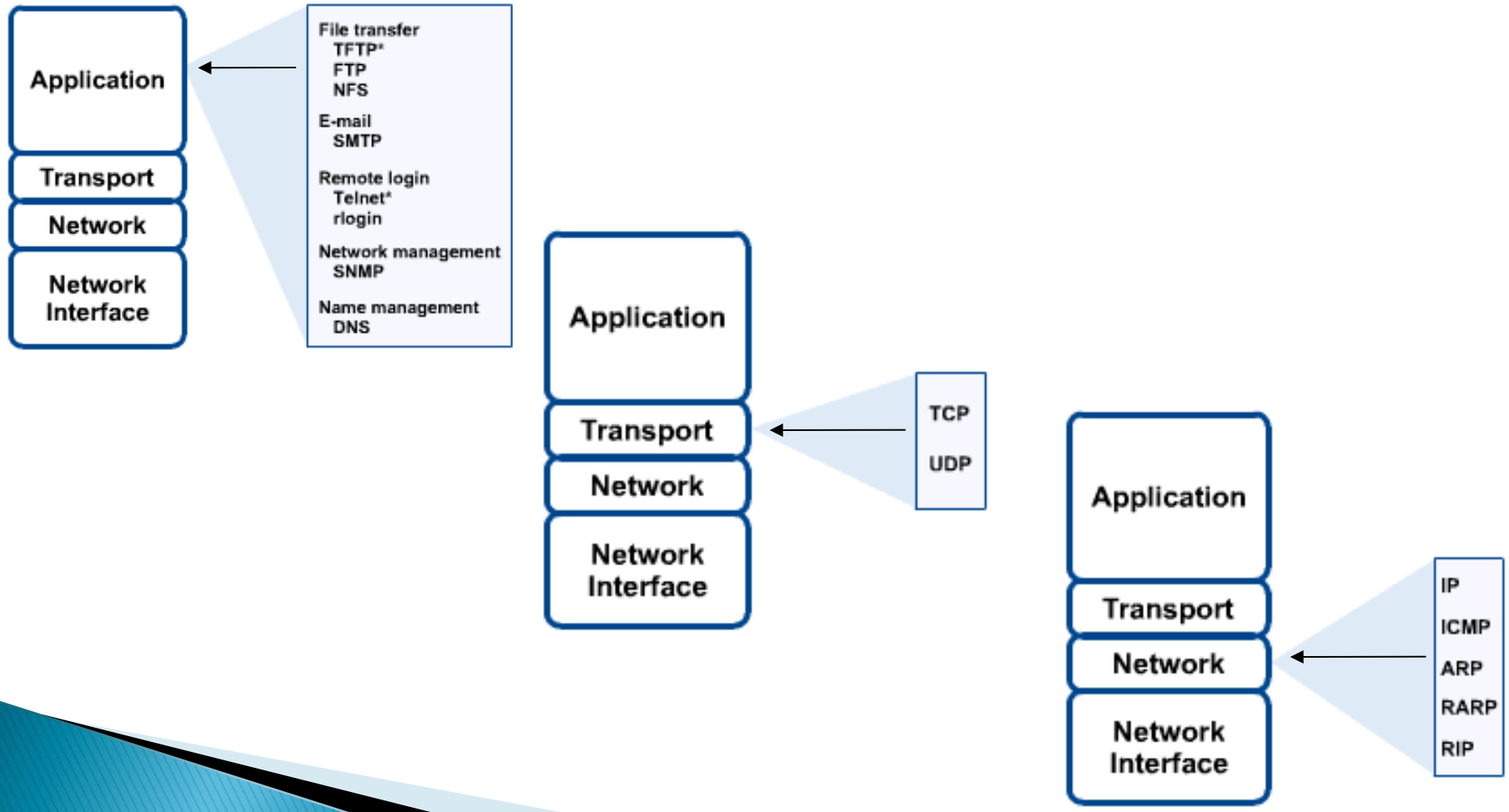
- HUB,
- Switches,
- Routers,
- Wireless Access Points,
- Modems etc.

Computers: Clients and Servers

- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.
- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.



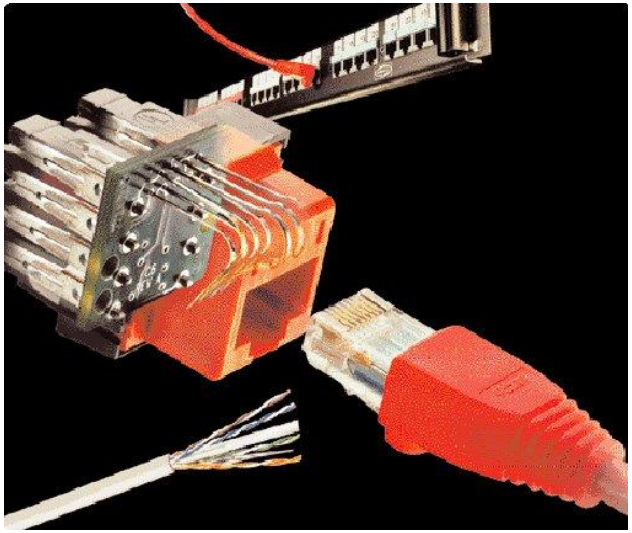
Networking Protocol: TCP/IP

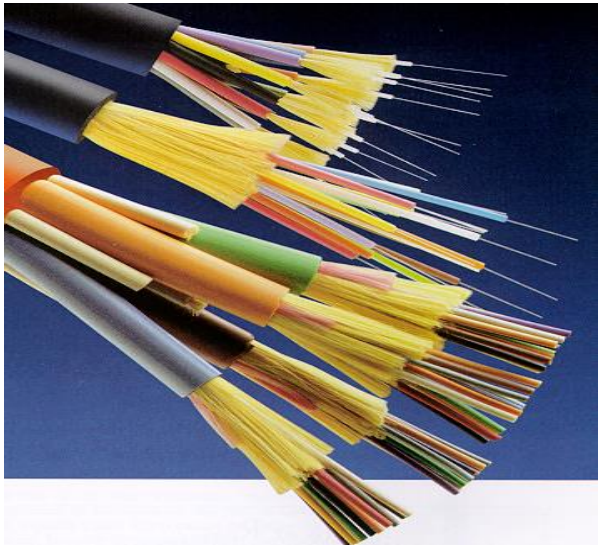


Applications

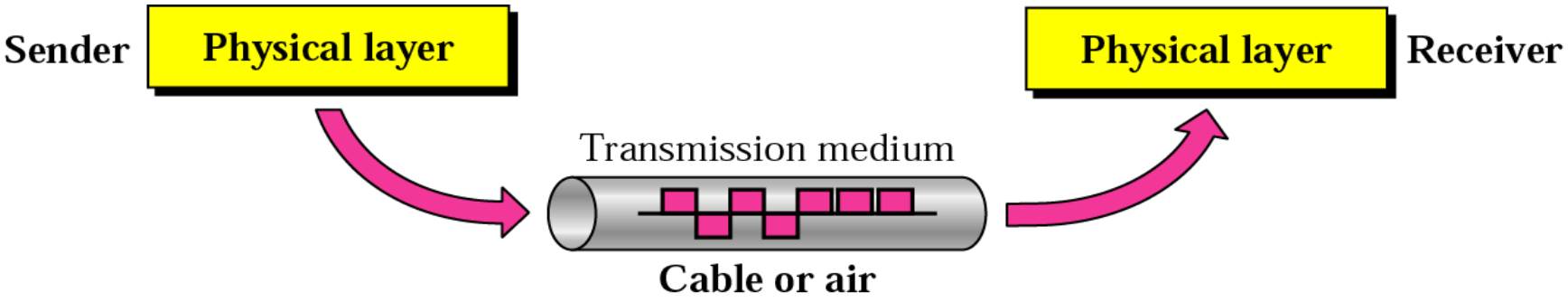
- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio

PHYSICAL MEDIA





Physical Media



Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.

Physical Media

- The main functionality of the transmission media is to carry the information in the form of bits.
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits are in the form of electrical signals.
- In a fibre based network, the bits are in the form of light pulses.

Physical Media

- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.

`

Physical Media

Some factors need to be considered for designing the transmission media:

Bandwidth: All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.

Transmission impairment: When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.

Interference: An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

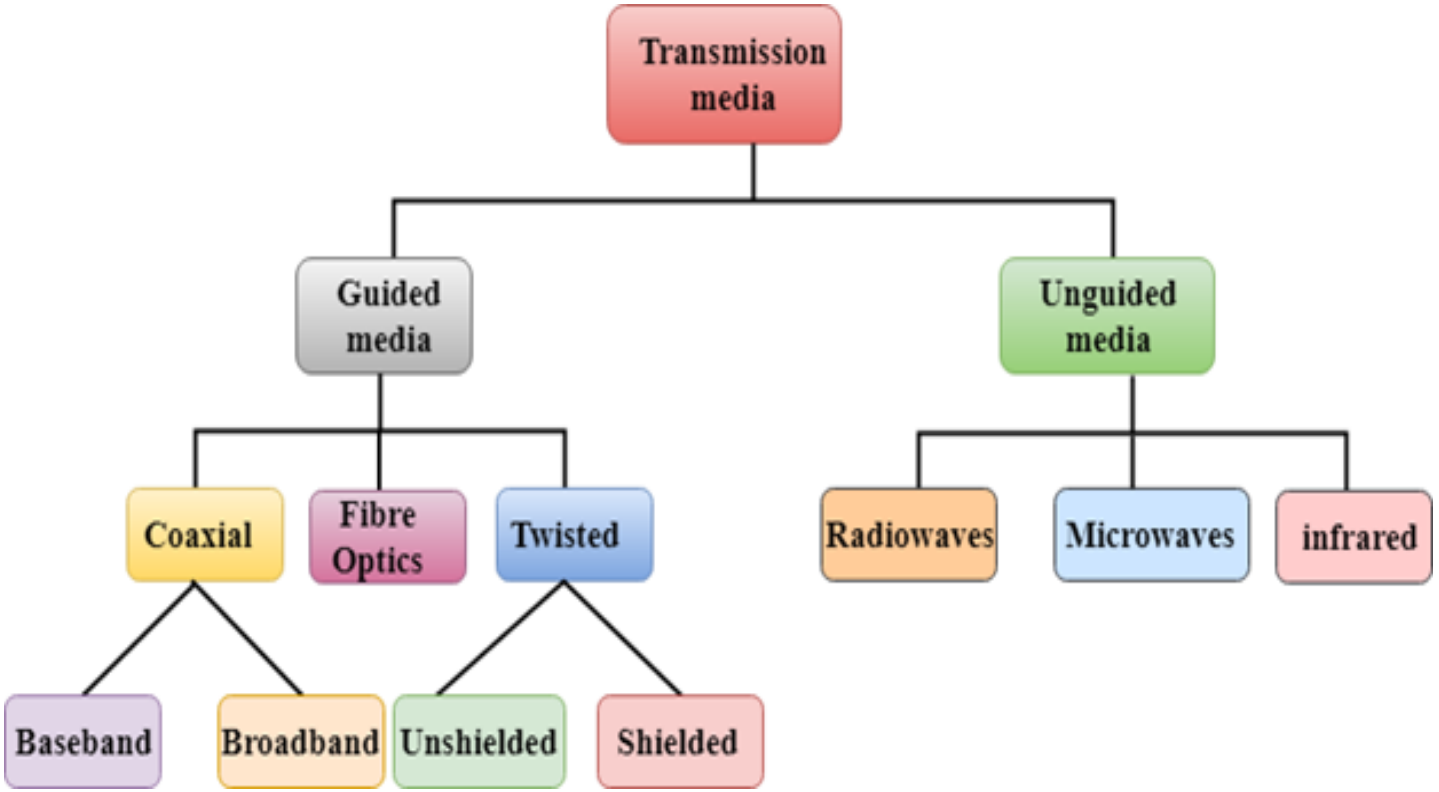
Causes Of Transmission Impairment

Attenuation: Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.

Distortion: Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.

Noise: When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Physical/Transmission Media



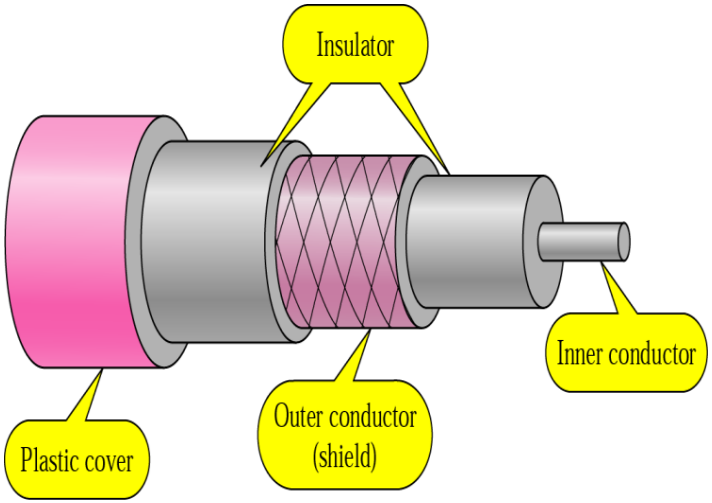
Copper Media: Coaxial Cable

Coaxial cable is a copper-cored cable surrounded by a heavy shielding and is used to connect computers in a network. Coaxial cable is also known as coax,

- Coaxial cables tend to carry signals at a greater distance and are a good choice for weak signals, due to their layered protection.

- Repeater is used to regenerate the weakened signals.

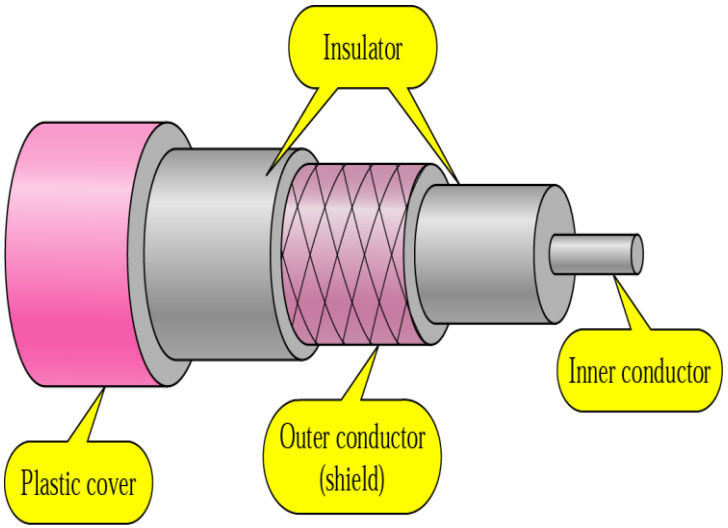
- It is used by cable TV service providers



Copper Media: Coaxial Cable

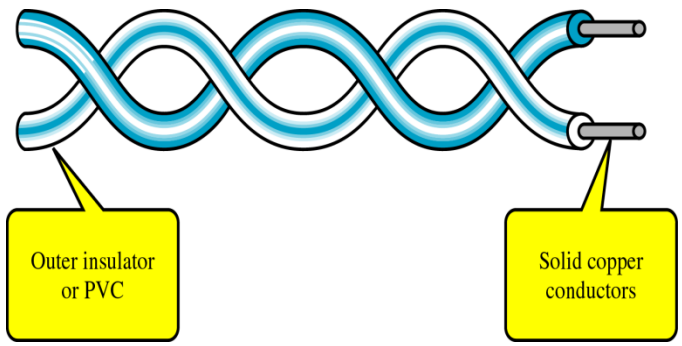
It consists of four primary components, as follows:

- A core copper wire, which serves as the primary channel
- A dielectric plastic insulator, which surrounds the copper
- A braided copper/aluminum sheath beneath the insulator. This is used to protect from external electromagnetic interference.
- The last layer, which is made of Teflon or plastic coating, is used to protect the inner layers from physical damage such as fire, water etc

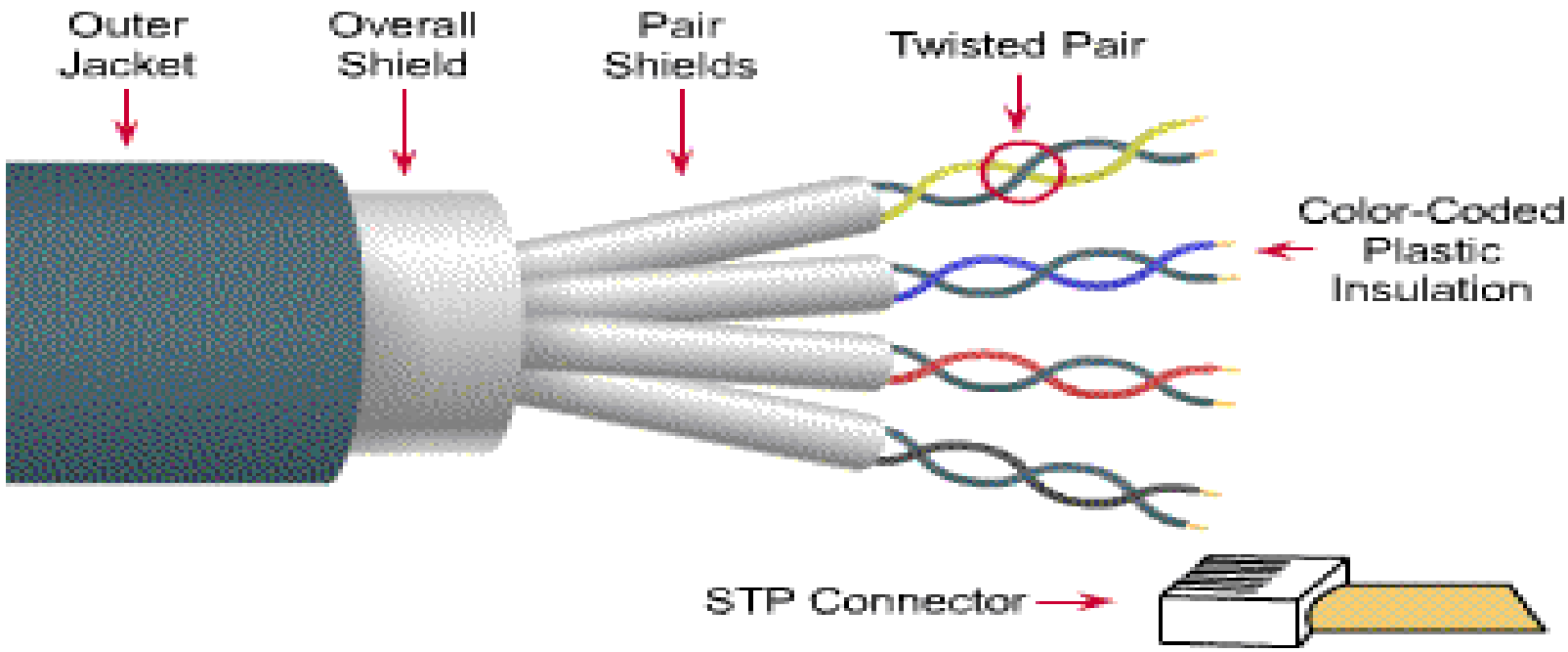


Copper Media: Twisted Pair

- Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks.
- Twisted pair is a physical media made up of a pair of cables twisted with each other.
- A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, and the noise generated by adjacent pairs.
- There are two basic types, shielded twisted-pair (STP) and unshielded twisted pair (UTP).



Shielded Twisted Pair (STP)

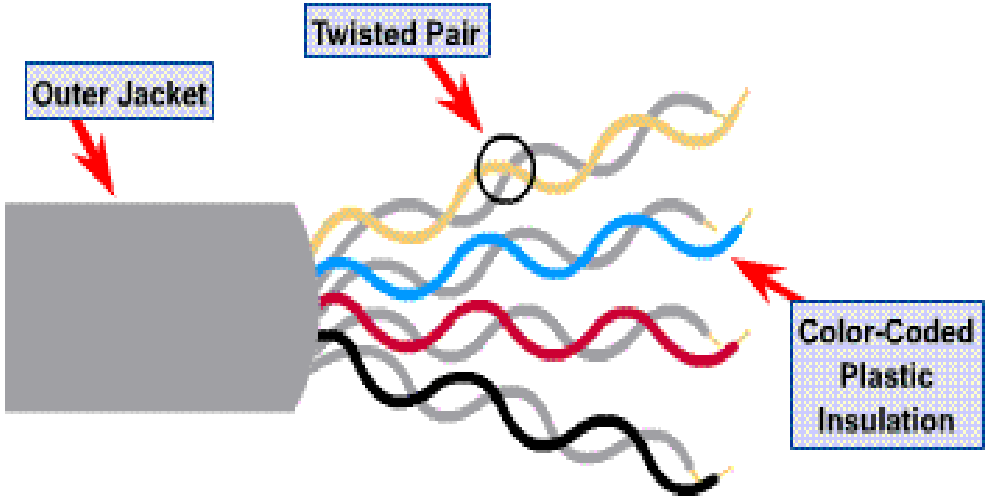


- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

Shielded Twisted Pair (STP)

- Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding, which prevents electromagnetic interference, thereby transporting data faster.
- It contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference.
- STP cables are costlier when compared to UTP, but has the advantage of being capable of supporting higher transmission rates across longer distances.
- The best use for STP cables are in industrial settings with high amounts of electromagnetic interference, such as a factory with large electronic equipment, where they can be properly installed and maintained.

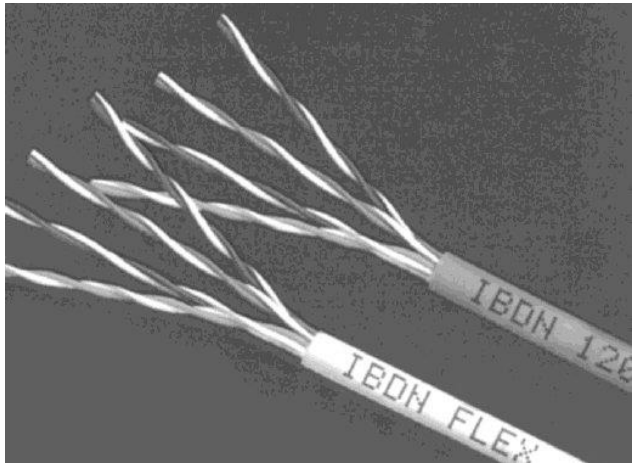
Unshielded Twisted Pair (UTP)

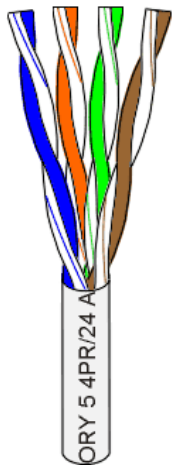


- Speed and throughput: 10-100 Mbps
- Cost per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m (short)

Unshielded Twisted Pair (UTP)

- Consists of 4 pairs (8 wires) of insulated copper wires typically about 1 mm thick.
- The wires are twisted together in a helical form.
- Twisting reduces the interference between pairs of wires.
- High bandwidth and High attenuation channel.
- Flexible and cheap cable.
- Category rating based on number of twists per inch and the material used
- CAT 3, CAT 4, CAT 5, Enhanced CAT 5 and now CAT 6.





Categories of UTP

- UTP comes in several categories that are based on the number of twists in the wires, the diameter of the wires and the material used in the wires.
- Category 3 is the wiring used primarily for telephone connections.
- Category 5e and Category 6 are currently the most common Ethernet cables used.

Categories of UTP: CAT 3

- Bandwidth 16 Mhz
- 11.5 dB Attenuation
- 100 ohms Impedance

Electrical Impedance, is the total opposition that a circuit presents to alternating current.

- Used in voice applications and 10baseT (10Mbps) Ethernet

Categories of UTP: CAT 4

- 20 MHz Bandwidth
- 7.5 dB Attenuation
- 100 ohms Impedance
- Used in 10baseT (10Mbps) Ethernet

Categories of UTP: CAT 5

- 100 MHz Bandwidth
- 24.0 dB Attenuation
- 100 ohms Impedance
- Used for high-speed data transmission
- Used in 10BaseT (10 Mbps) Ethernet & Fast Ethernet (100 Mbps)

Categories of UTP: CAT 5e

- 150 MHz Bandwidth
- 24.0 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps)

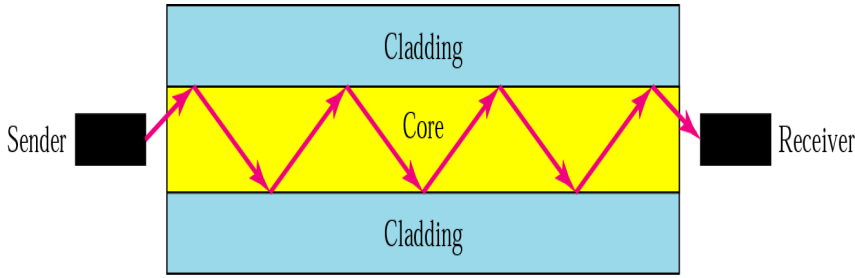
Categories of UTP: CAT 6

- 250 MHz Bandwidth
- 19.8 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Gigabit Ethernet (1000 Mbps) & 10 Gig Ethernet (10000 Mbps)

Fibre Media

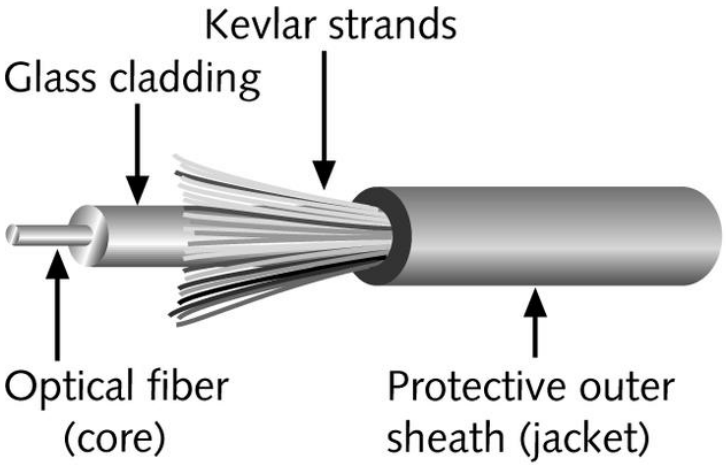
Optical fibre's use light to send information through the optical medium.

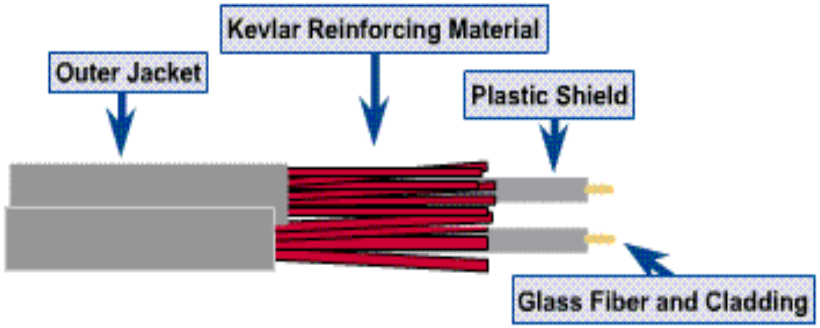
- Fibre optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires..
- Modulated light transmissions are used to transmit the signal.

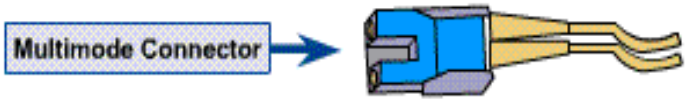


Fiber-Optic Cable

- Contains one or several glass fibers at its core
- Surrounding the fibers is a layer called cladding







- Speed and throughput: 100+ Mbps
- Cost per node: Most Expensive
- Media and connector size: Small
- Single mode, maximum cable length: Up to 3000m
- Multimode mode, maximum cable length: Up to 2000m
- Single mode: One stream of laser-generated light
- Multimode: Multiple streams of LED-generated light

Fiber Optic Cable

- FO Cable may have 1 to over 1000 fibers
- Internet infrastructure and telecom networks are now generally based on fiber optics.
- Optical fiber can be used to transmit power as light.
- Optical fibers are used in sensors to measure temperature and pressure.

Advantages of Fibre Optic cable over Copper:

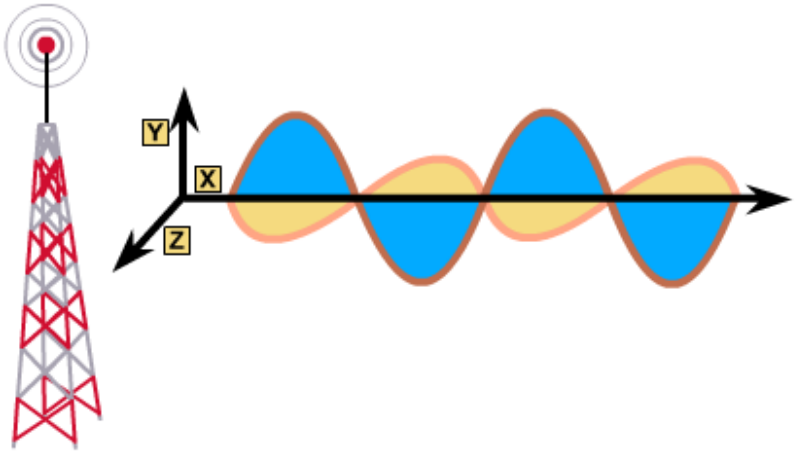
- Greater Bandwidth: The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- Faster speed: Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- Longer distances: The fibre optic cable carries the data at a longer distance as compared to copper cable.
- Better reliability: The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- Thinner and Sturdier: Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Unguided/Wireless Media

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Wireless Media

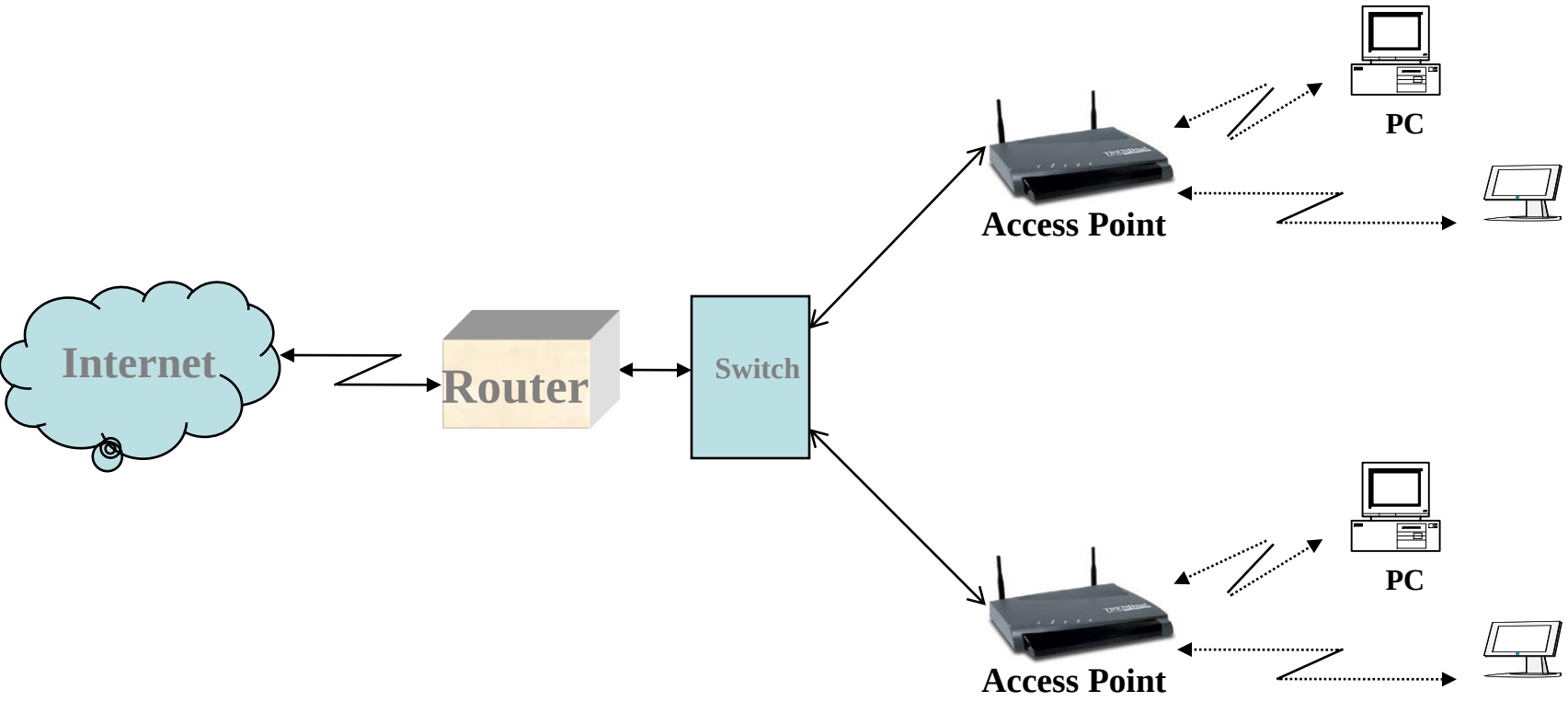
- Very useful in difficult terrain where cable laying is not possible.
- Provides mobility to communication nodes.
- cable laying costs can be reduced.
- Susceptible to rain, atmospheric variations and Objects in transmission path.



Wireless Media

- Indoor : 10 – 50m : BlueTooth, WLAN
- Short range Outdoor : 50 – 200m: WLAN
- Mid Range Outdoor : 200m – 5 Km : GSM, WLAN Point-to-Point, Wi-Max
- Long Range Outdoor : 5 Km – 100 Km : Microwave Point-to-Point
- Long Distance Communication : Across Continents : Satellite Communication

Wireless LAN



Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 300GHz to 3 KHz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is FM radio.

Application Radio waves

- A Radio wave is useful for multi casting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Radio waves

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Application Radio waves

- A Radio wave is useful for multi casting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Microwave

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- Frequency range: The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- Bandwidth: It supports the bandwidth from 1 to 10 Mbps.
- Short distance: It is inexpensive for short distance.
- Long distance: It is expensive as it requires a higher tower for a longer distance.
- Attenuation: Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

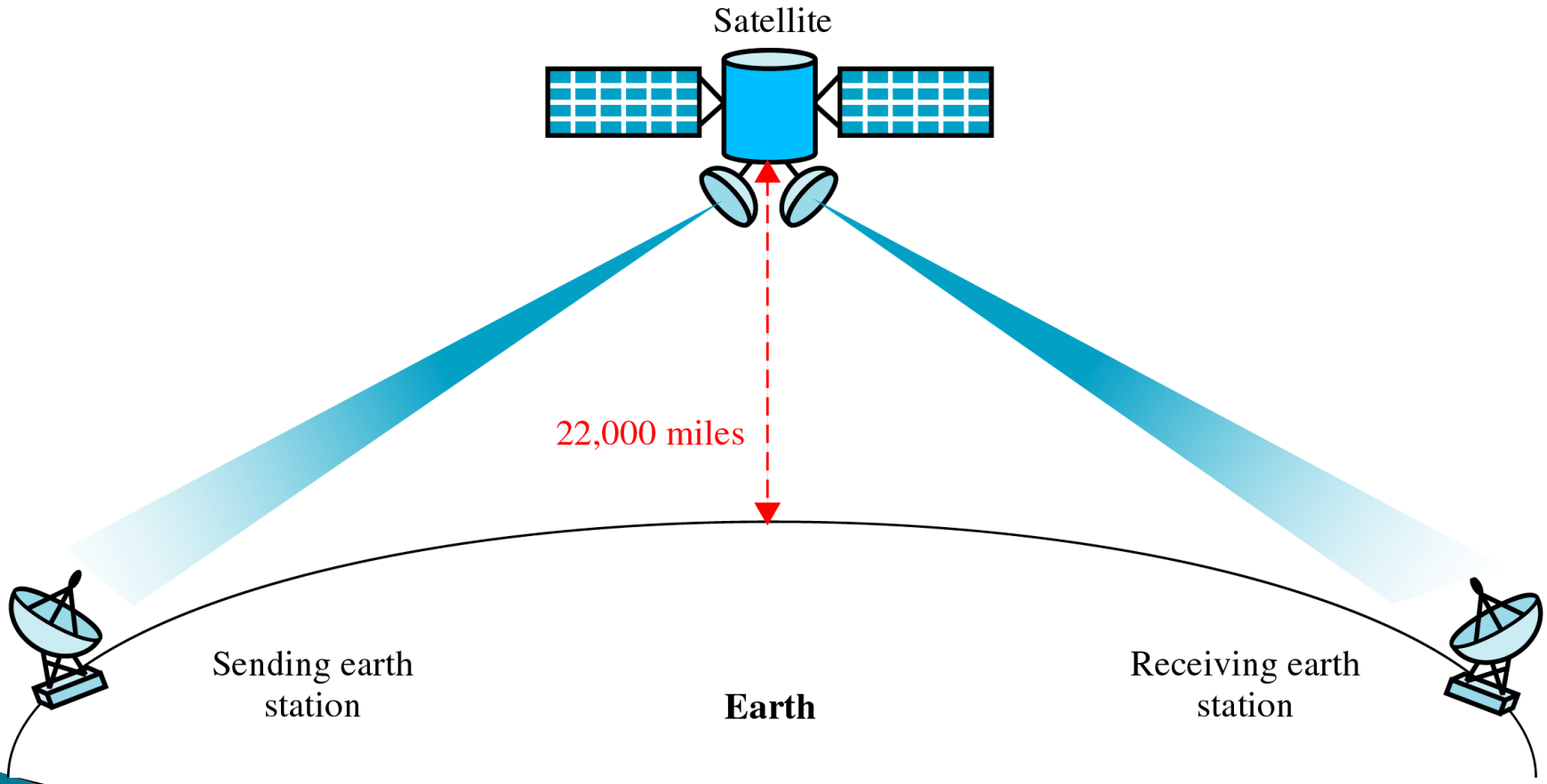
Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages Of Microwave:

- Eavesdropping: An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- Out of phase signal: A signal can be moved out of phase by using microwave transmission.
- Susceptible to weather condition: A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- Bandwidth limited: Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Communication



Satellite Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

- The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Satellite Communication

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Satellite Communication

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

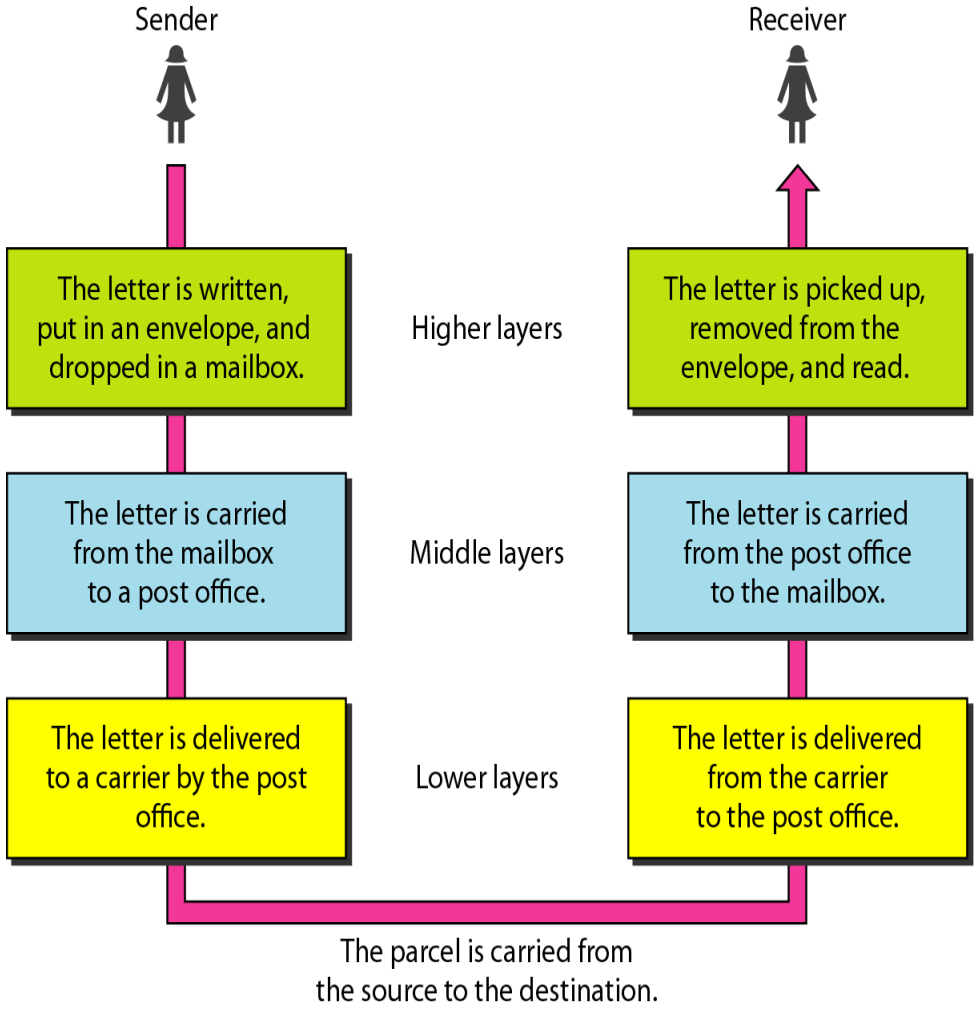
- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

OSI MODEL

LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail.

The process of sending a letter to a friend would be complex if there were no services available from the post office.



Layer Architecture

- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

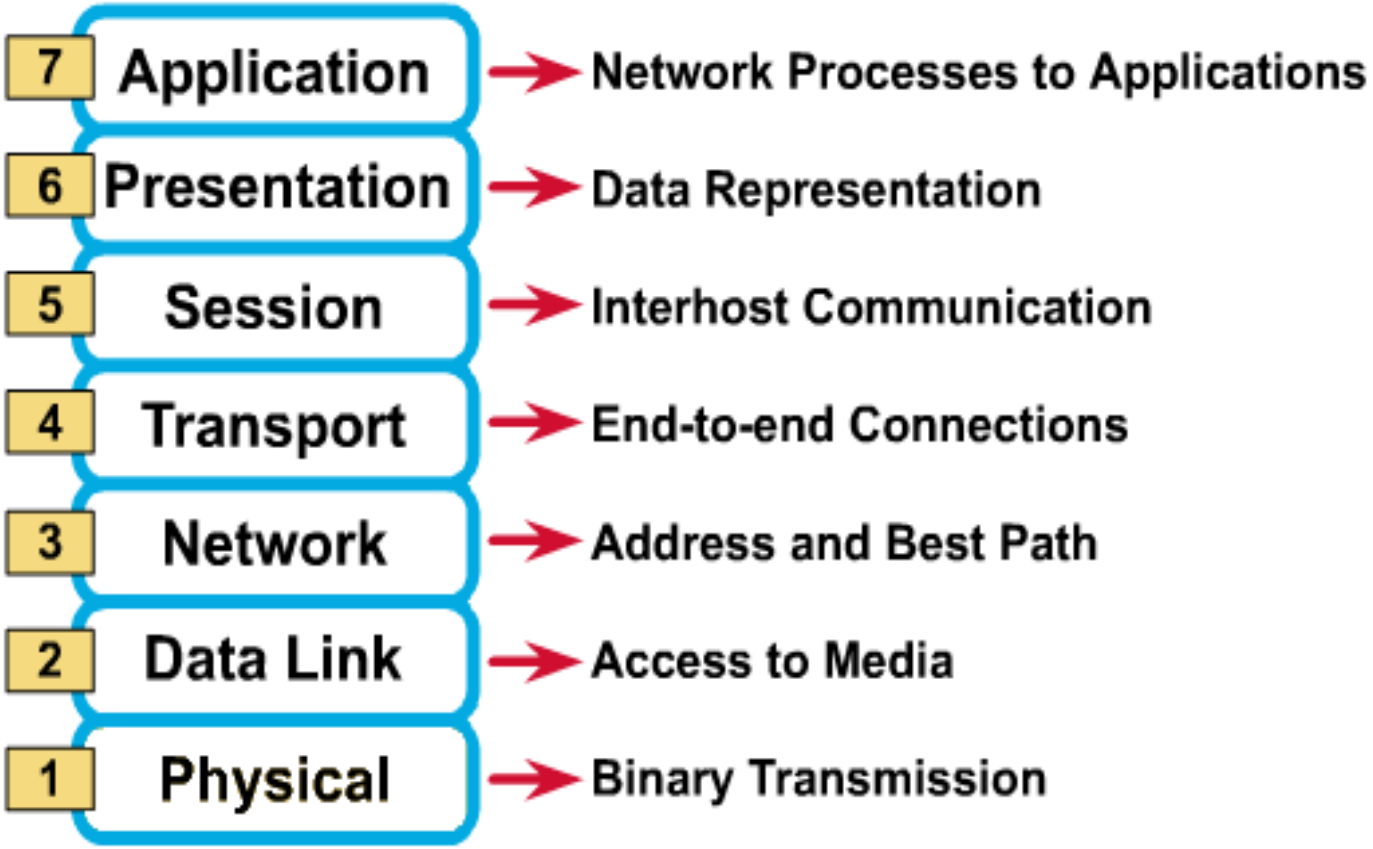
Open Systems Interconnection (OSI)

- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.

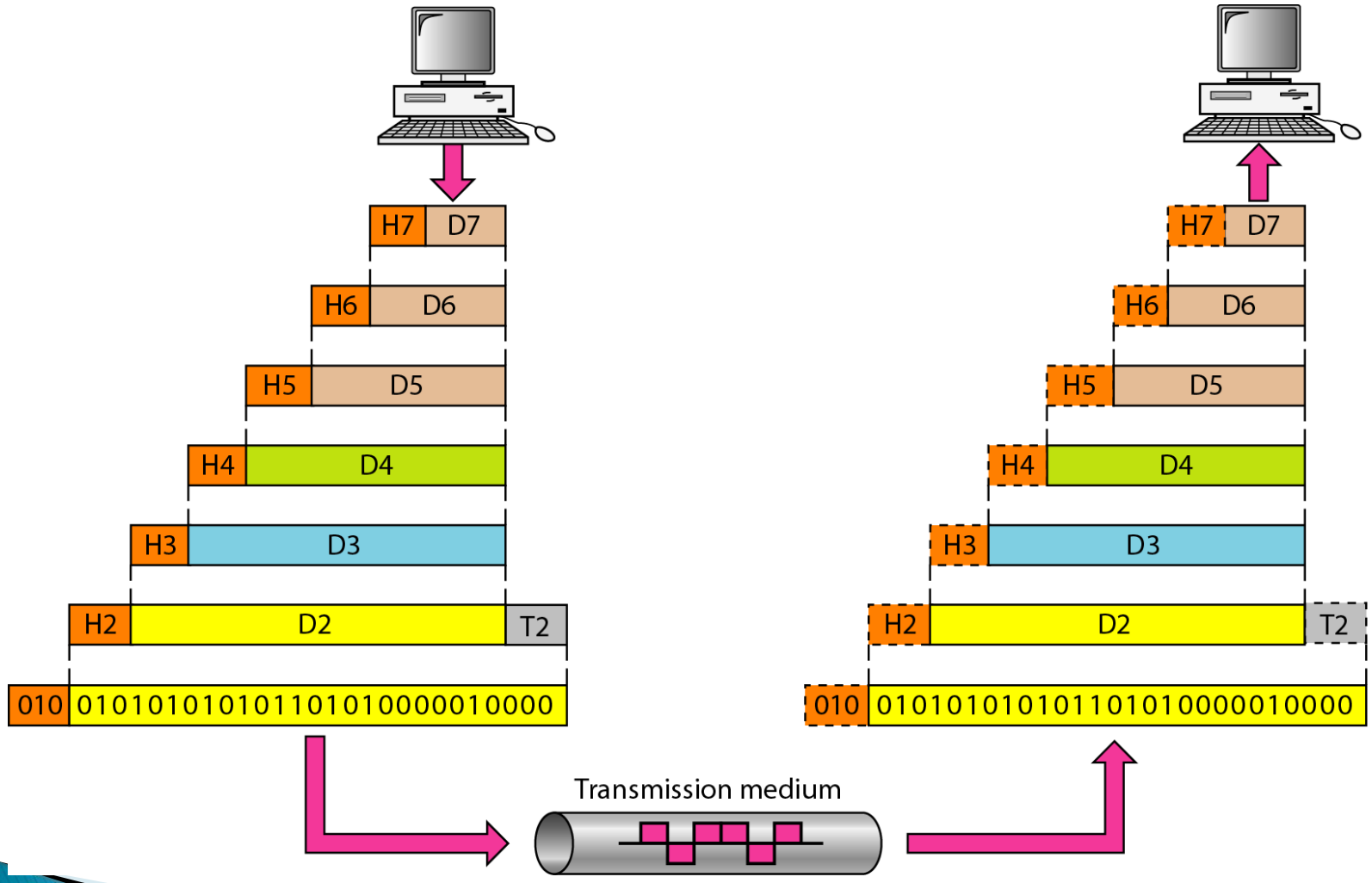
OSI Reference Model

- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .
- This separation into smaller more manageable functions is known as layering.

OSI Reference Model: 7 Layers



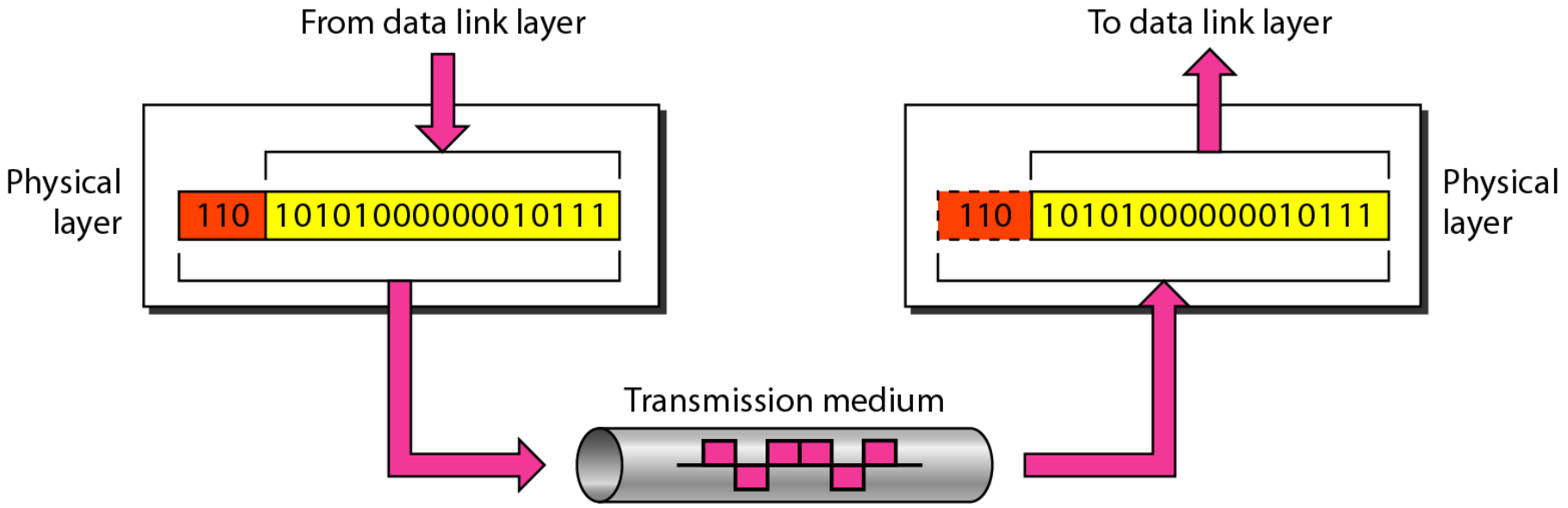
An exchange using the OSI model



OSI: A Layered Network Model

- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 4 layers (transport, network, data link and physical — Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

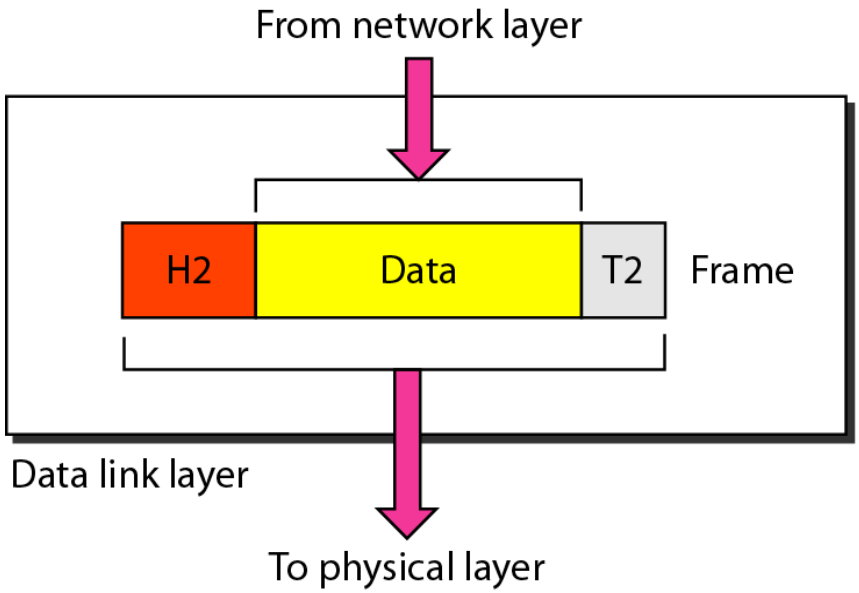
Physical Layer

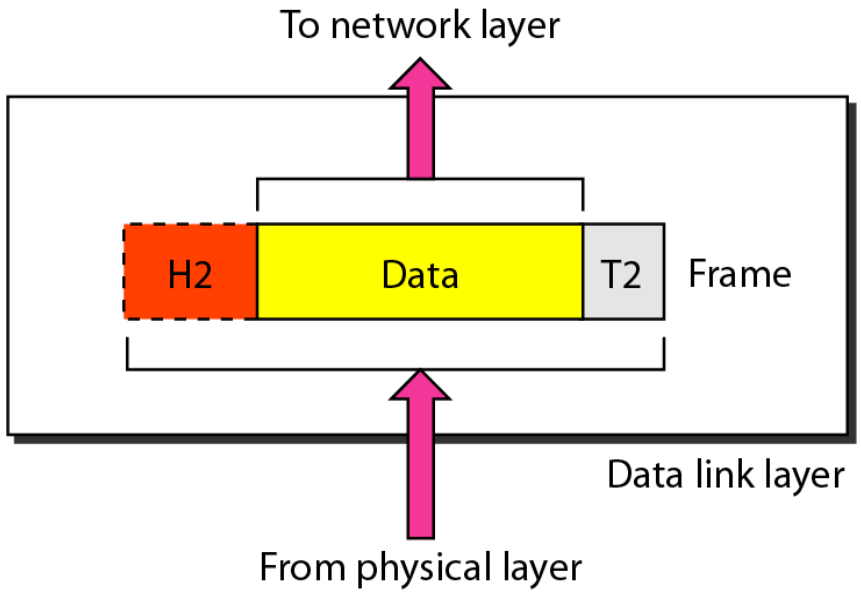


Physical Layer

- Provides physical interface for transmission of information.
- Defines rules by which bits are passed from one system to another on a physical communication medium.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Data Link Layer



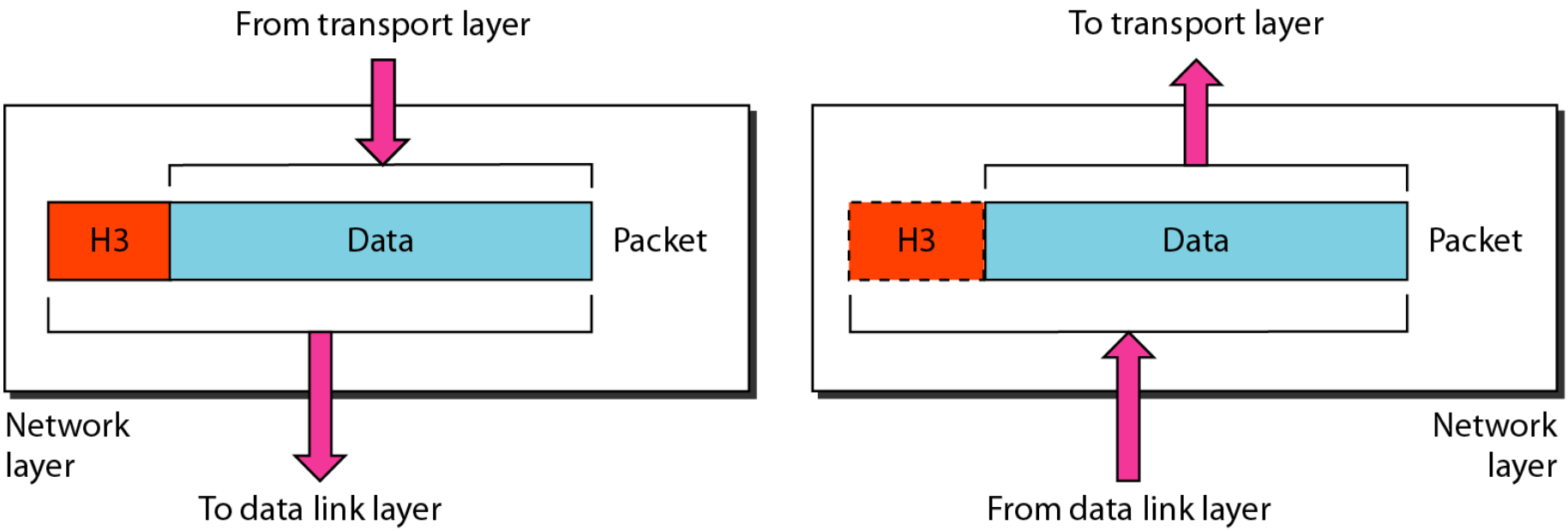


Data Link Layer

- Data link layer attempts to provide reliable communication over the physical layer interface.

- Breaks the outgoing data into frames and reassemble the received frames.
- Create and detect frame boundaries.
- Handle errors by implementing an acknowledgement and retransmission scheme.
- Implement flow control.
- Supports points-to-point as well as broadcast communication.
- Supports simplex, half-duplex or full-duplex communication.

Network Layer



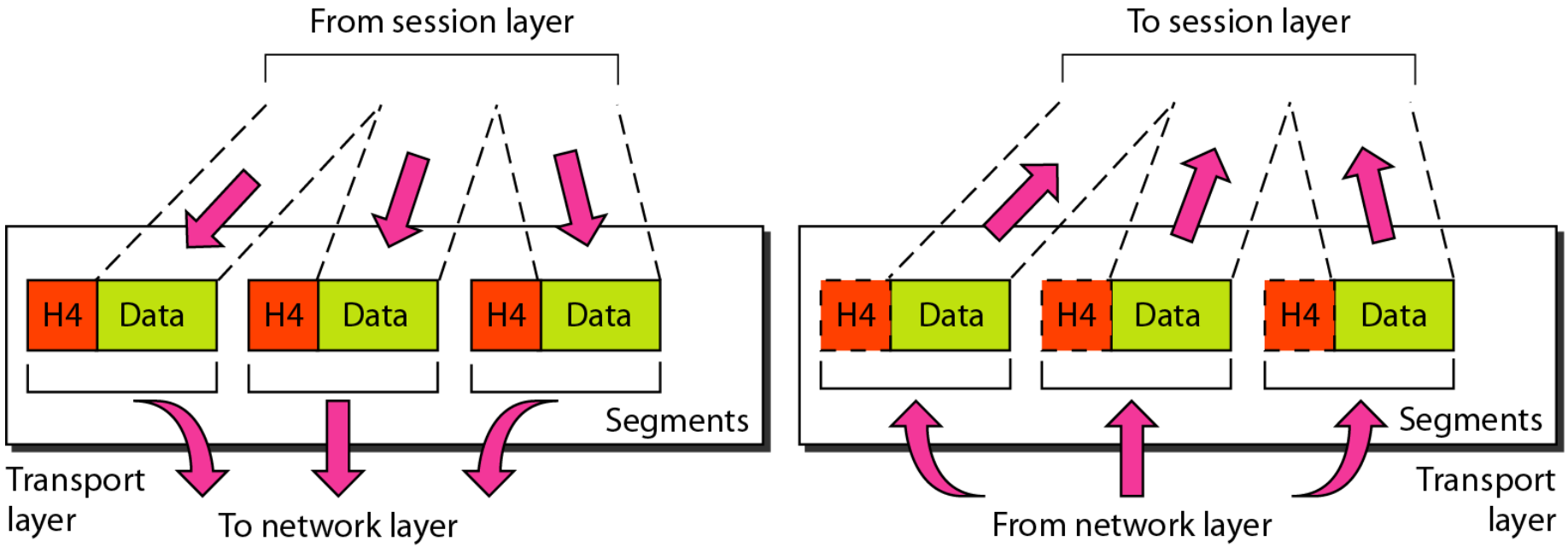
Network Layer

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination
- Defines logical addressing so that any endpoint can be identified.
- Handles congestion in the network.
- Facilitates interconnection between heterogeneous networks (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

Transport Layer

- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensures that the data units are delivered error free.
- Ensures that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.
- Provides for the connection management.
- Multiplex multiple connection over a single channel.

Session Layer

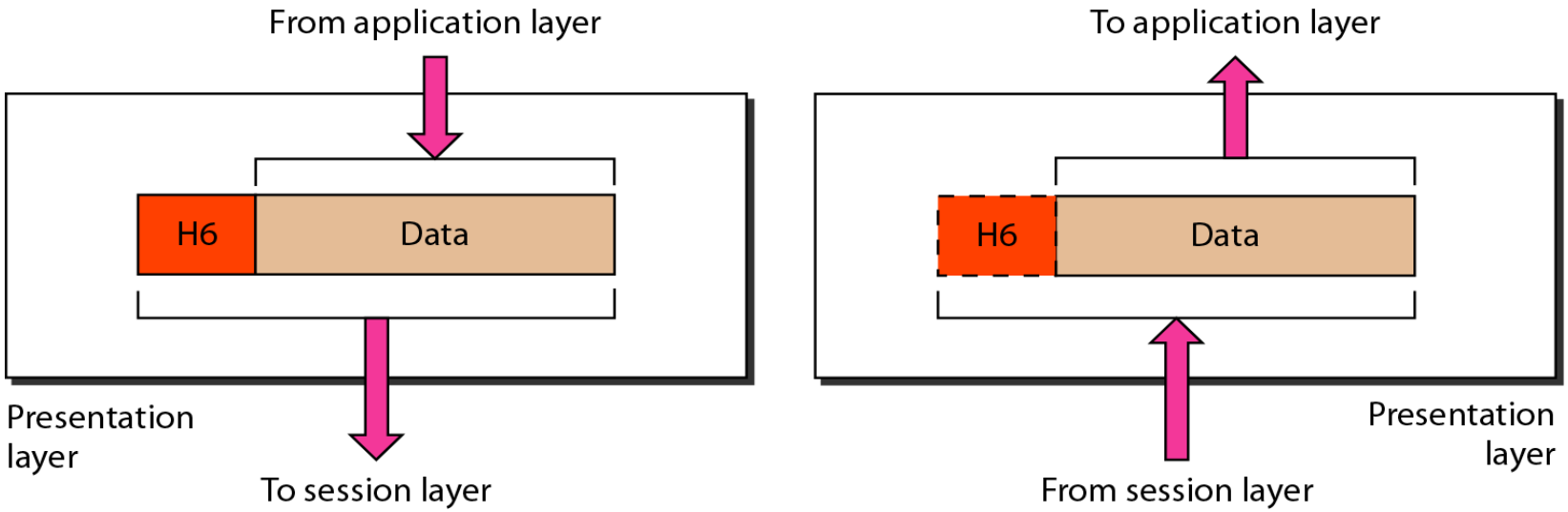


Session Layer

- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Presentation Layer

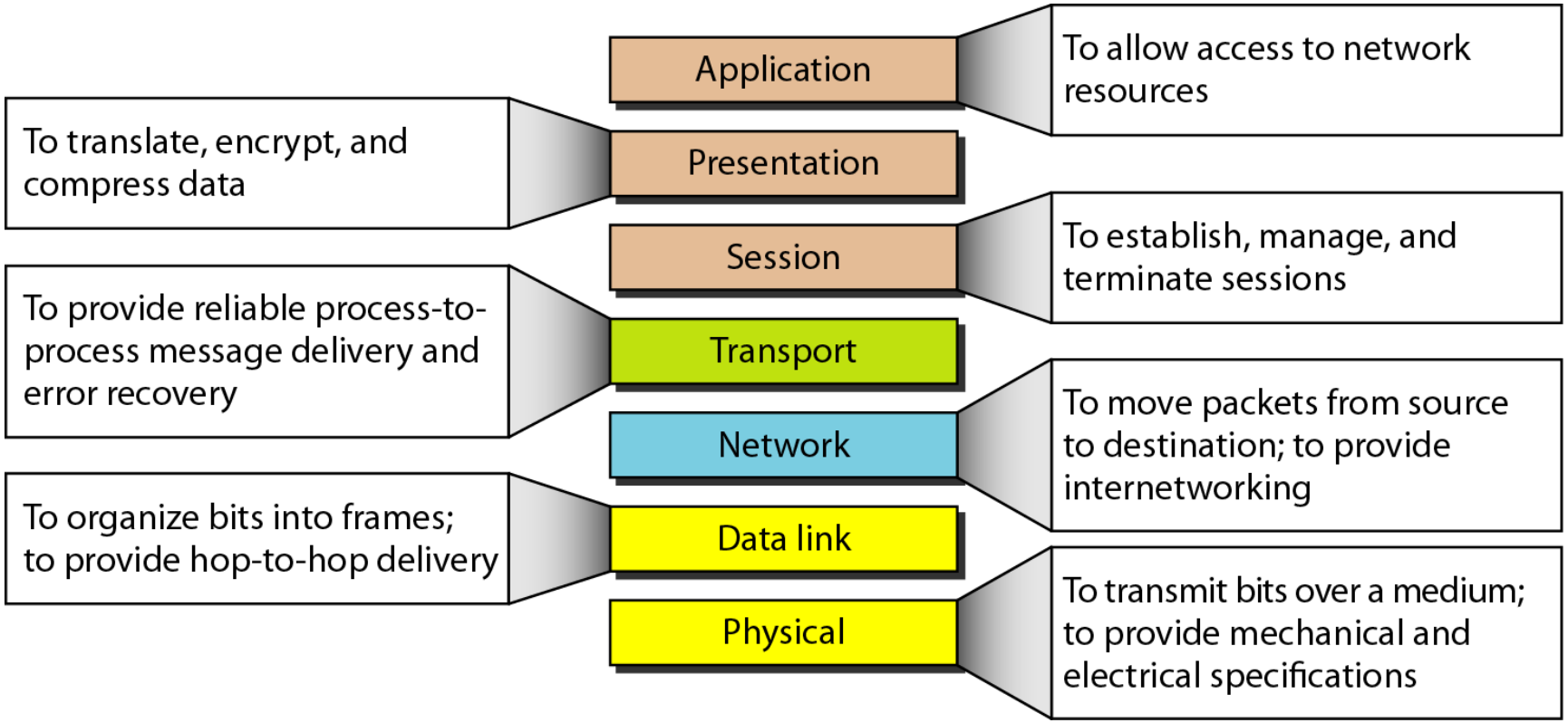
- Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.
- Also handles data compression and data encryption (cryptography).



Application Layer

- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications.
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

Summary of Layers

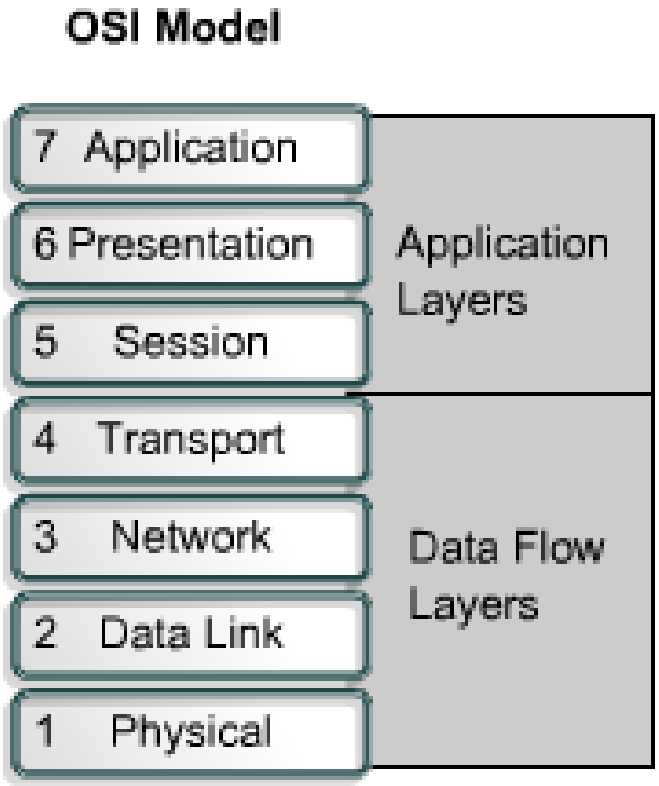


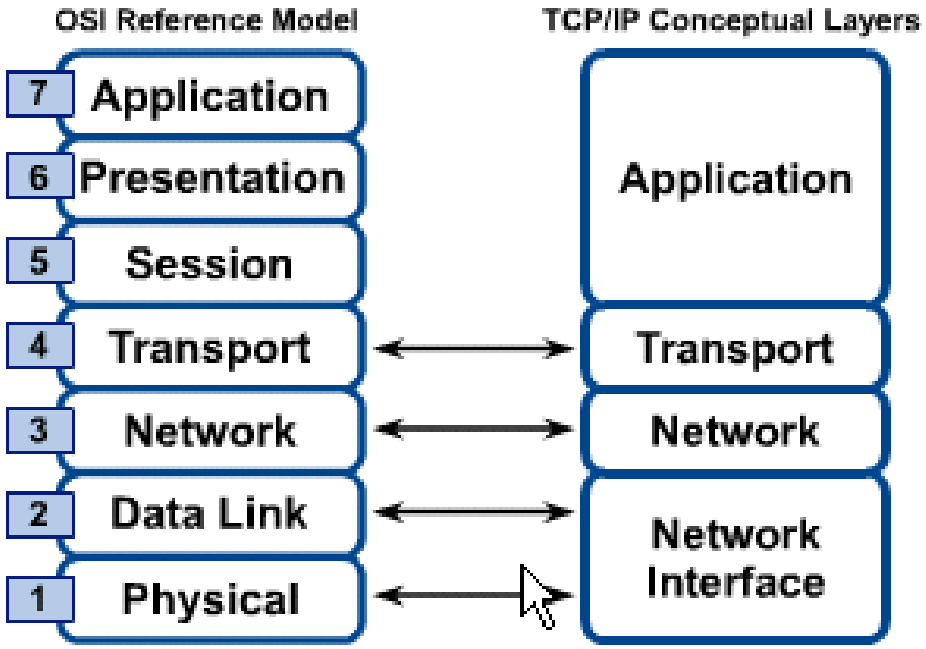
TCP/IP MODEL

TCP/IP PROTOCOL SUITE

- 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 TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

OSI & TCP/IP Models





TCP/IP Model

Application Layer
Application programs using the network

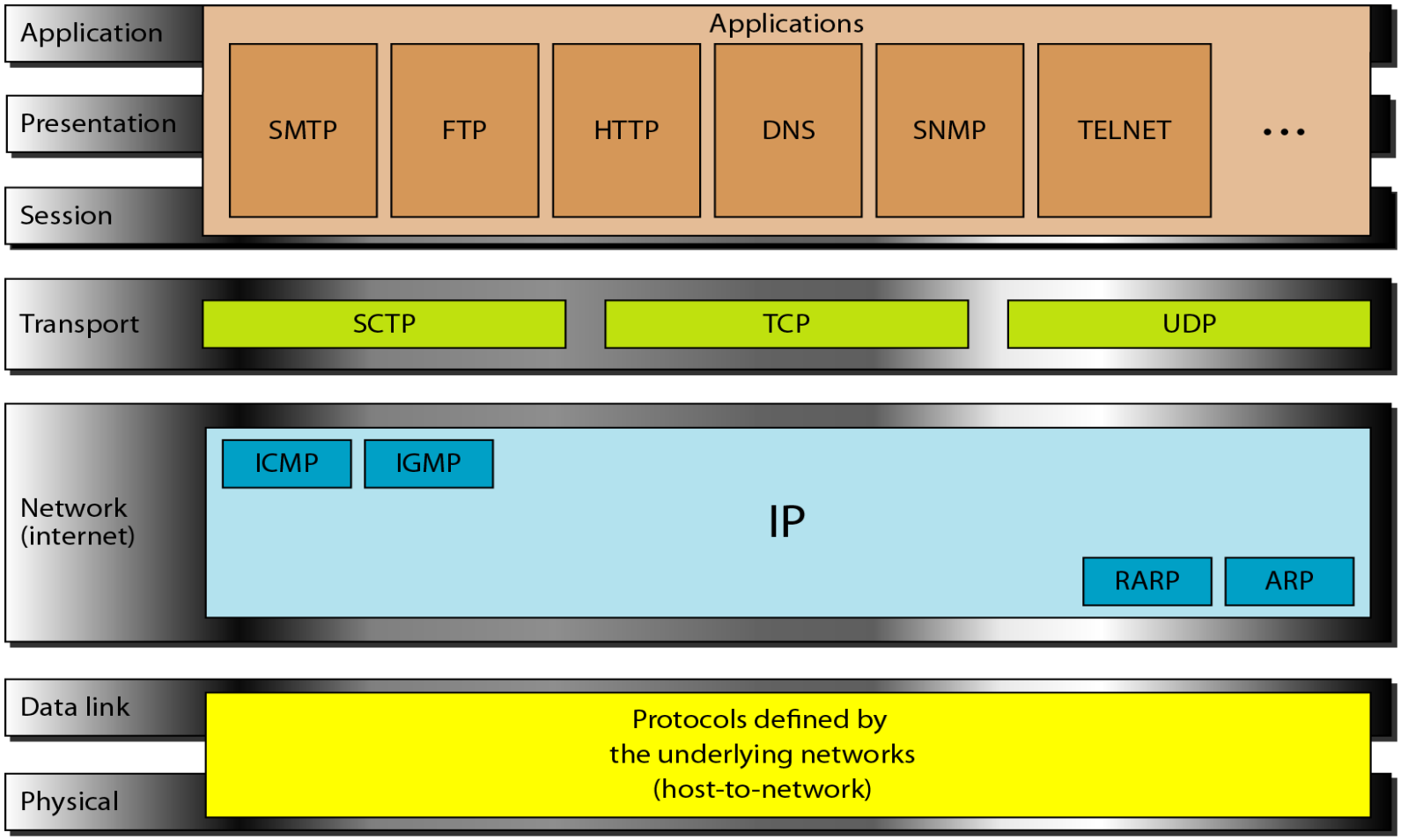
Transport Layer (TCP/UDP)
Management of end-to-end message transmission, error detection and error correction

Network Layer (IP)
Handling of datagrams : routing and congestion

Data Link Layer
Management of cost effective and reliable data delivery, access to physical networks

Physical Layer
Physical Media

TCP/IP and OSI model



- Study the difference between OSI Model and TCP/IP Model.

- **Ad Hoc Network**
- **Network Architecture**
- **Computer Network Devices/Components**

Ad Hoc Network

"Ad Hoc" is actually a Latin phrase that means "for this purpose."

In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.

An ad hoc network is a network that is composed of individual devices communicating with each other directly.

Ad Hoc Network

For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other.

If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes.

Ad Hoc Network

Many ad hoc networks are local area networks where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes.

Wireless Ad Hoc Network

- A wireless ad hoc network (WANET) or MANET (Mobile ad hoc network) mobile devices communicating directly with one another.
- The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.
- Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" – anywhere, anytime.

Wireless Sensor Network

- A wireless sensor network (WSN) employs sensor based devices to jointly observe physical or environmental settings such as sound, pressure, climatic changes, andso on.

- Wireless sensor networks are used in a wide range of areas: traffic control,vehicle detection, greenhouse monitoring and so on.

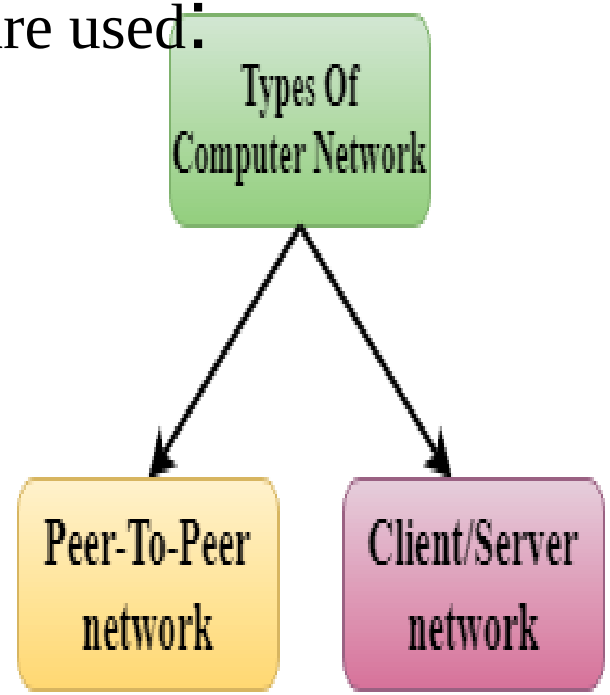
Network Architecture

- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
- Simply we can say that how computers are organized and how tasks are allocated to the computer.

Network Architecture

- The two types of network architectures are used:

  - Peer-To-Peer network
  - Client/Server network

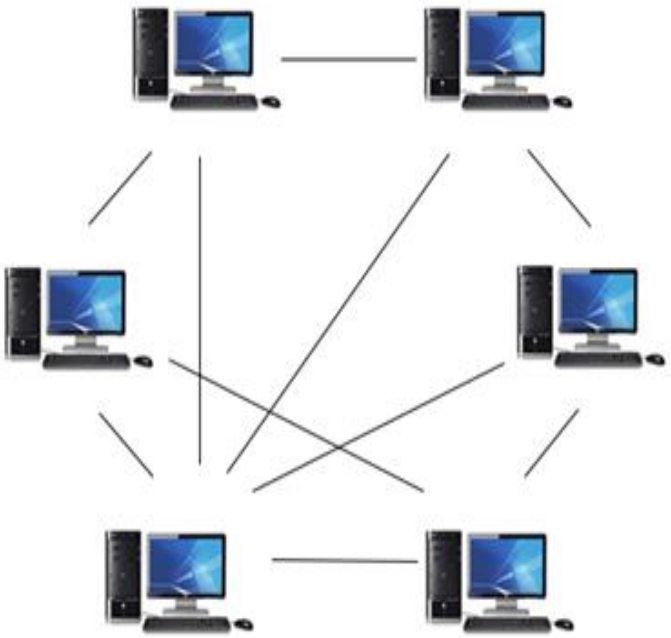


Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.

- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Peer-To-Peer network



Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.

Client/Server Network

- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

Client/Server Network

Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Network Devices:

- NIC
- Repeater
- Hub
- Bridge
- Switch
- Router
- Gateways
- Brouter

Network Interface Card(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 or manufacturer to identify a network card uniquely.
- The MAC address is stored in the PROM (Programmable read-only memory).

Network Interface Card(NIC):

There are two types of NIC:

- Wired NIC
- 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.

Repeater:

- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- The repeaters do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

Hub:

- Hub – A hub is basically a multiport repeater.
- 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.

Bridge:

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

Switch :

- Switch is data link layer device. A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub and bridge.
- 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.

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.

Gateway:

- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models or different networking protocols.
- If a network node wants to communicate with a node/network that resides outsides of that network or autonomous system, the network will require the services of a gateway, which is familiar with the routing path of other remote networks.
- They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system

Gateway:

- Gateways are network protocol converters. Often the two networks that a gateway joins use different base protocols. The gateway facilitates compatibility between the two protocols.
- Gateways are generally more complex than switch or router.

Brouter:

- It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer.
- Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

Software Defined Networks

- Basically, traditional networks can’t cope up and meet current networking requirements like dynamic scalability, central control and management, on the fly changes or experiments, lesser error-prone manual configurations on each networking node, handling of network traffic (which has massively increased due to boom of mobile data), and server virtualization traffic in data centers.
- Traditional networks are tightly coupled with highly expensive network elements that don’t offer any kind of openness or ability to customize internals.
- To deal with such issues, open source communities came together to define a networking approach for future. And that’s how the concept of SDN came to life.

Software Defined Networks

- SDN is implemented through software.
- Software-defined networking (SDN) is still a relatively new model used to design, build, and manage networks.
- SDN is a software layer, it provides advantages such as reduced manual efforts, dynamic scalability, and central management of network devices.
- Here,you can configure/monitor/troubleshoot network devices with ease from central point, avoiding a lot of manual effort, hence saving time and money in the process.

Distributed Networks

- Distributed networking is a distributed computing network system over which computer programming, software, and its data are spread out across more than one computer, but communicate complex messages through their nodes (computers), and are dependent upon each other.
- With distributed network architecture a single central control system can be maintained, but the load can be distributed among several local sites. These sites can be physically separated from each other but connected via the internet. And, if one system fails, the others can continue to work without being affected.

Distributed Networks

- With single servers, there is always the possibility of an overload as the network grows. Single servers are also prone to the whole network going down if the server is affected. With a distributed system the load is shared among the different systems which makes networking quicker and more efficient.
- There is no loss of configuration if the central server experiences any problems because it is distributed among the secondary systems.
- Each node on the system has an administrator, and the tasks that each administrator has control over can be determined by the central node.

Benefits of Distributed Network

Scalable:

- A distributed network architecture makes scalability a lot simpler than single networks. Because the load is distributed, new devices can be added and configured to the network without much disruption to the whole network.
- In case of a single network, too many devices can slow the system down and overwhelm the server. This won't happen with a distributed network.

More efficient:

- The administrator of the central network can have as much or as little control as required at each time. This administrator can delegate tasks to node administrators and concentrate on other tasks at hand.

More reliable:

- Because of the way the distributed network architecture is set up the system is more robust and reliable. If files on one system get corrupted, it doesn't affect the entire system.

Spread Spectrum

- The Spread spectrum signal occupies a larger bandwidth than a normal signal. Hence the name spread spectrum.
- The original signal is coded at the transmitter. This coding is independent of the original signal
- It is spread at the source and dispread at the receiver.
- The spread spectrum signal is pseudo random in nature. Looks like random noise signal.
- Only special receiver can recover the original information. Hence, other intended receivers find this signal as noise.

Spread Spectrum

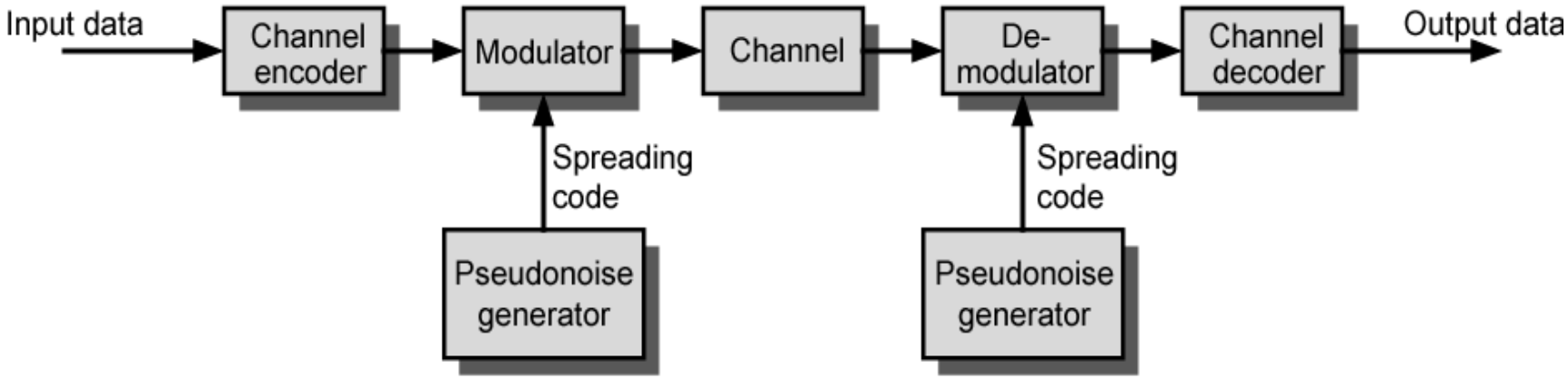


Fig. Block diagram of a Spread Spectrum System

Spread Spectrum

These are of two types.

- Frequency Hopped Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)