Basics of Computer Networks - Part I

Complete Course on Computer Networks for GATE 2021

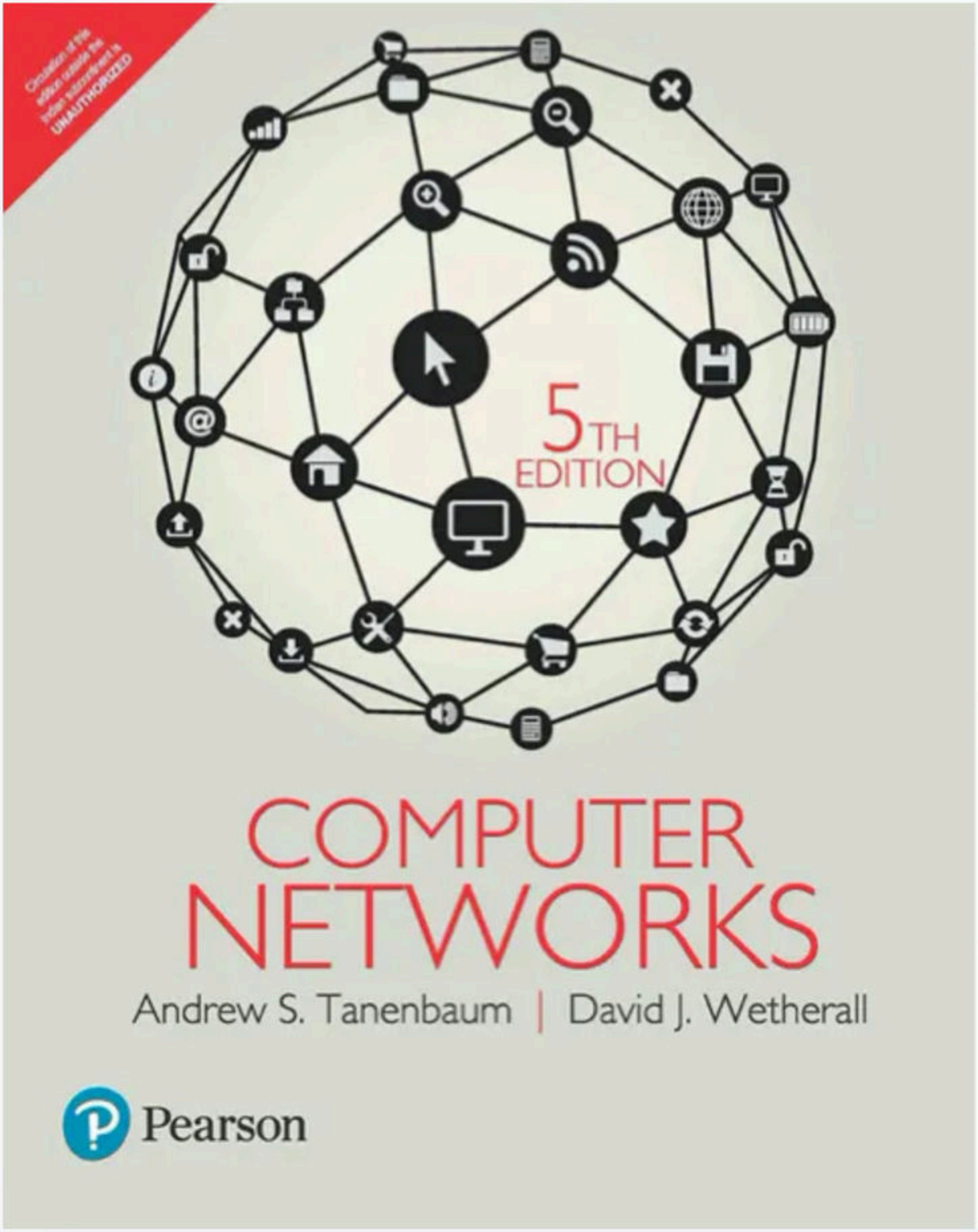
Sanchit Jain • Lesson 1 • Oct 14, 2020

Computer networks

Computer networks

- Core subjects for CS/IT Students
- In GATE 7-8 Marks out of 100 Marks, and 5-6 questions on an average
- In NET 20-22 Marks out of 200 marks and 10-12 questions
- Mostly Numerical type questions
- Needs a little time, good scoring
- Applied in Specific Industry

- Book Name
  - Data Communications and Networking
- Writers
  - Behrouz A. Forouzan
- Publisher
  - McGraw Hill
- Edition – 4th



- **Book Name**
  - Computer Networks
- **Writers**
  - ANDREW S. TANENBAUM
  - David J. Wetherall
- **Publisher**
  - Pearson
- **Edition**
  - 5th

Syllabus

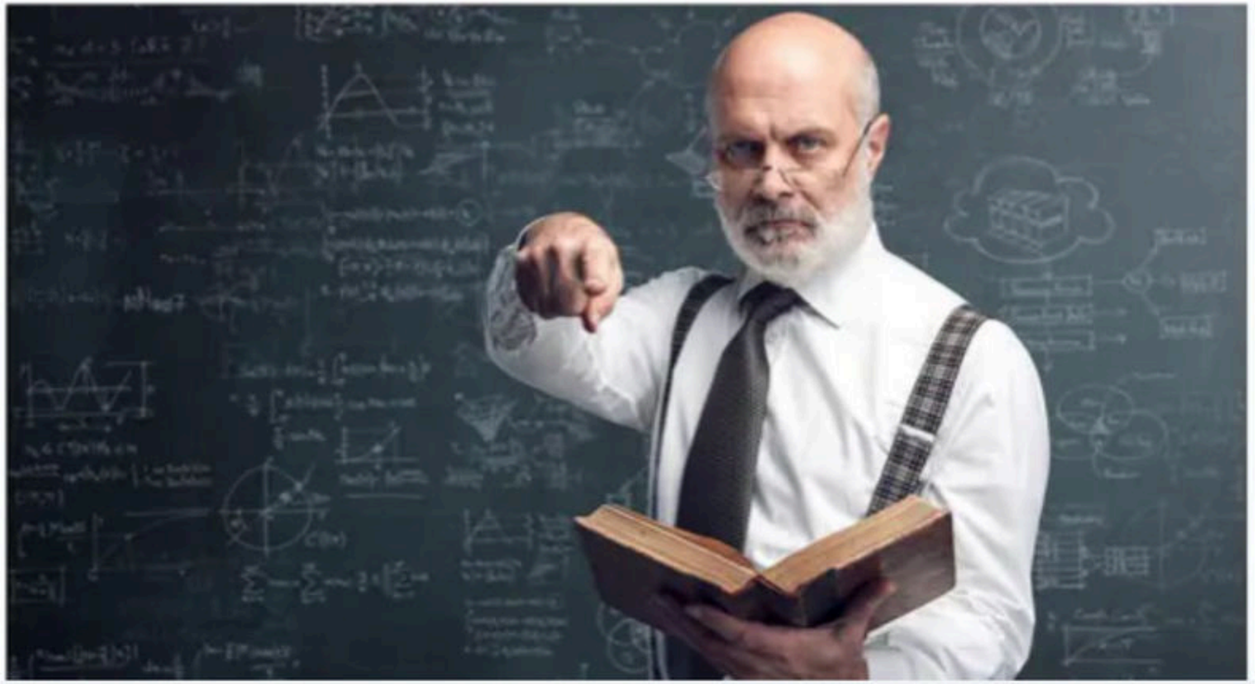
- Concept of layering
- LAN technologies (Ethernet), Flow and error control techniques, switching.
- IPv4/IPv6, routers and routing algorithms (distance vector, link state).
- TCP/UDP and sockets, congestion control.
- Application layer protocols (DNS, SMTP, POP, FTP, HTTP).
- Basics of Wi-Fi.
- Network security: authentication, basics of public key and private key cryptography, digital signatures and certificates, firewalls.

What you can expect from me

- Will take care of theory and numerical both
- Will give more weightage to the topics that are asked more frequently in GATE
- Will not emphasize more than required, on a topic
- Will provide PDF of related books

What i expect from you

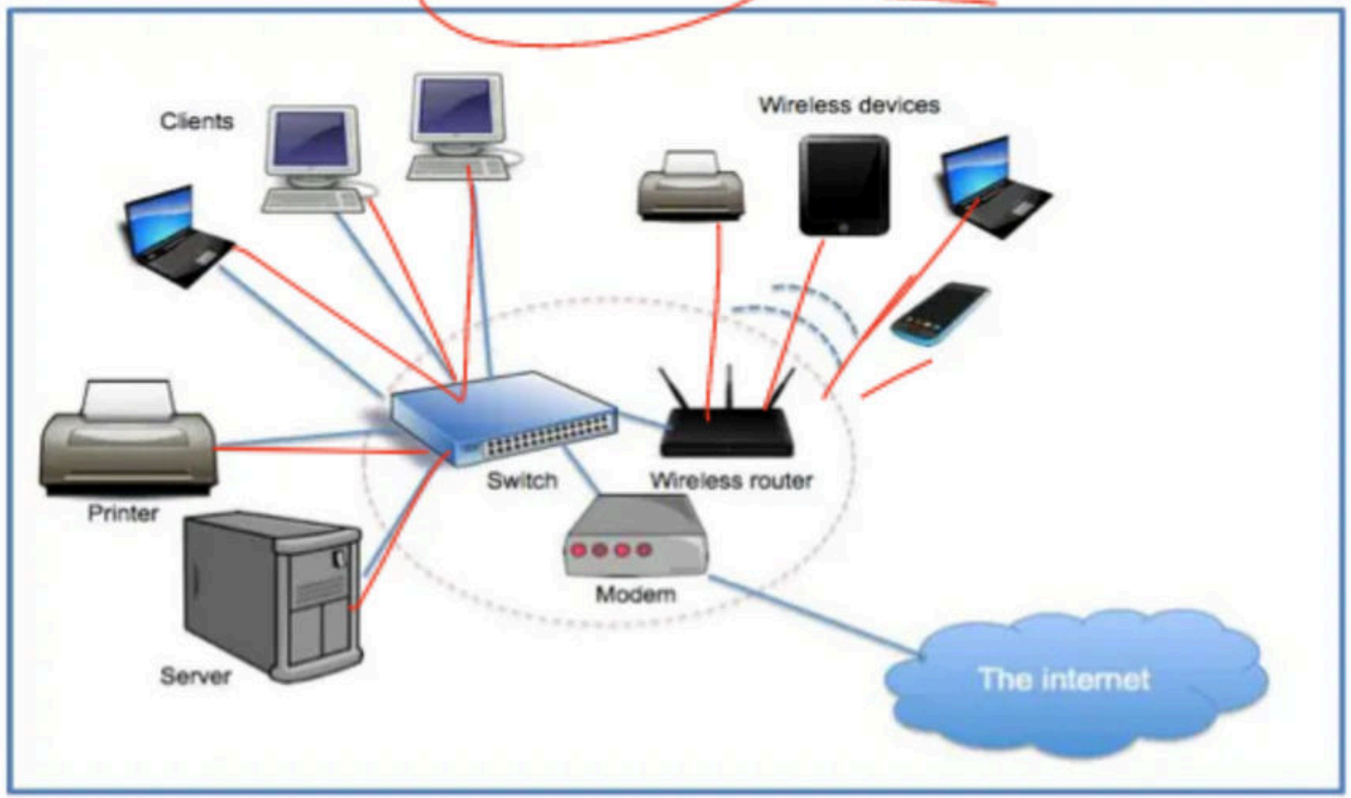
- There is no hurry, feel free to ask questions any time through out the class, but first listen
- Please revise the entire lecture before and after the class
- Be regular, Consistency is most important
- More you practice, more clarity you will get
- If we follow all the above specified points Success in guaranteed



Break

Basics of Computer Networks

- A **computer network** is a telecommunications network, which allows digital devices(nodes) to exchange data between each other using either wired or wireless connections to share resources (h/w or s/w) e.g. internet.
- A collection of autonomous computers interconnected by a single technology.



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

in billions

3.89

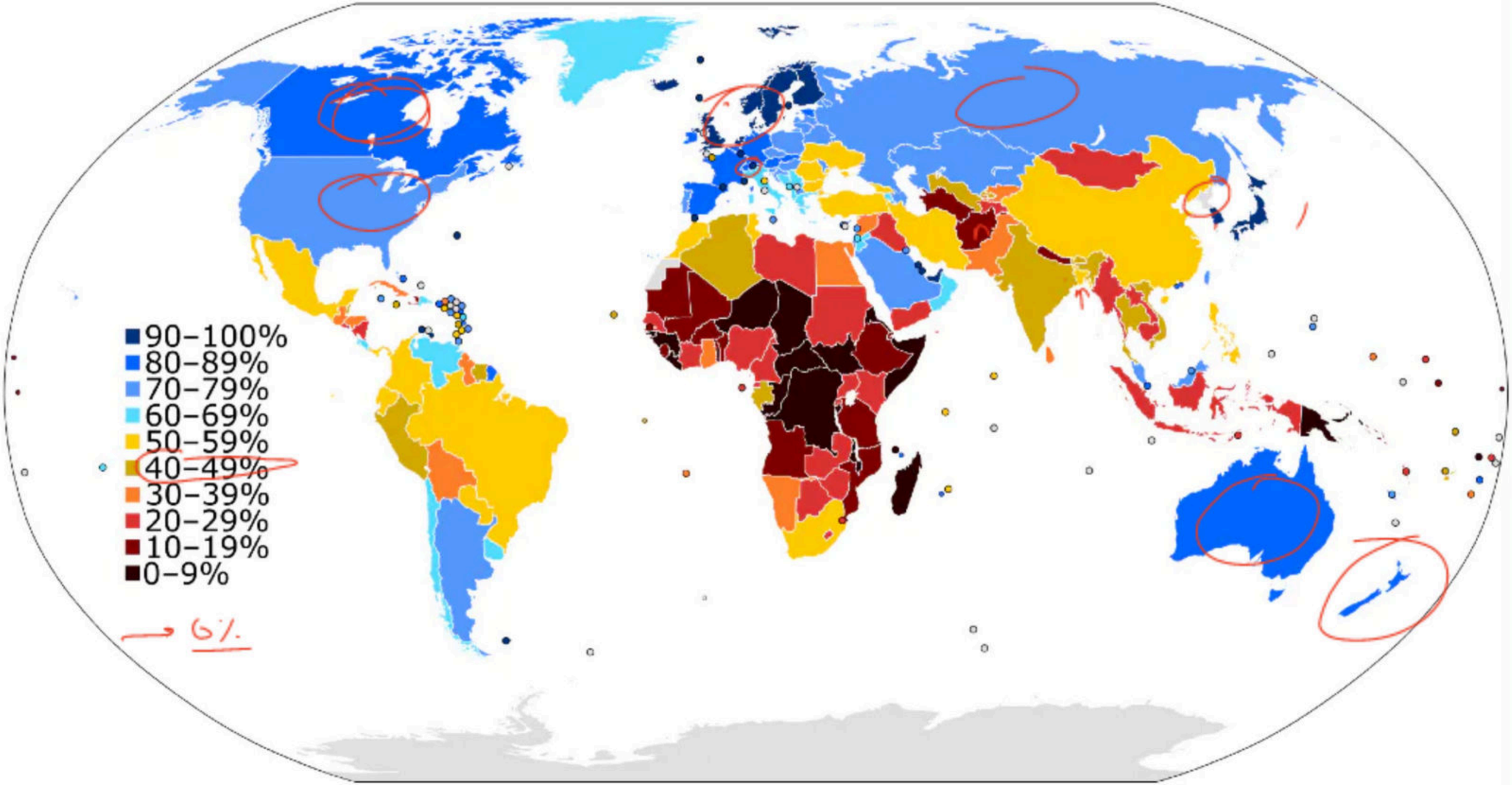
in 2012

4.83

in 2016

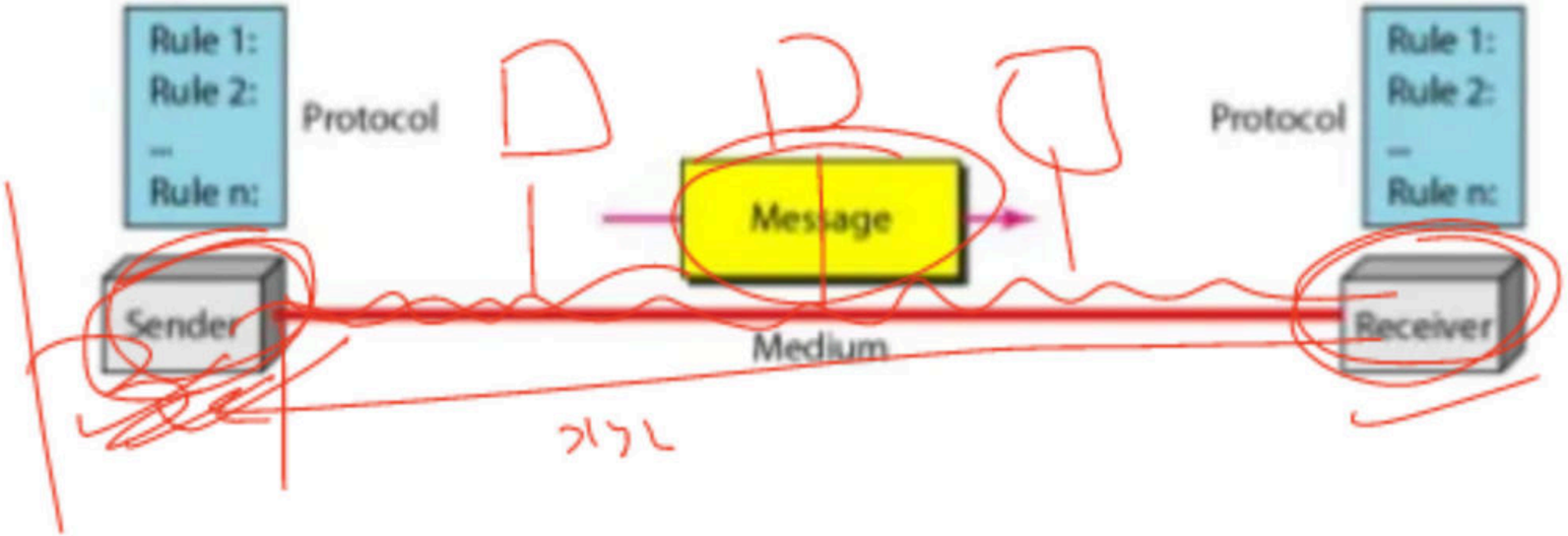
5.69

in 2020

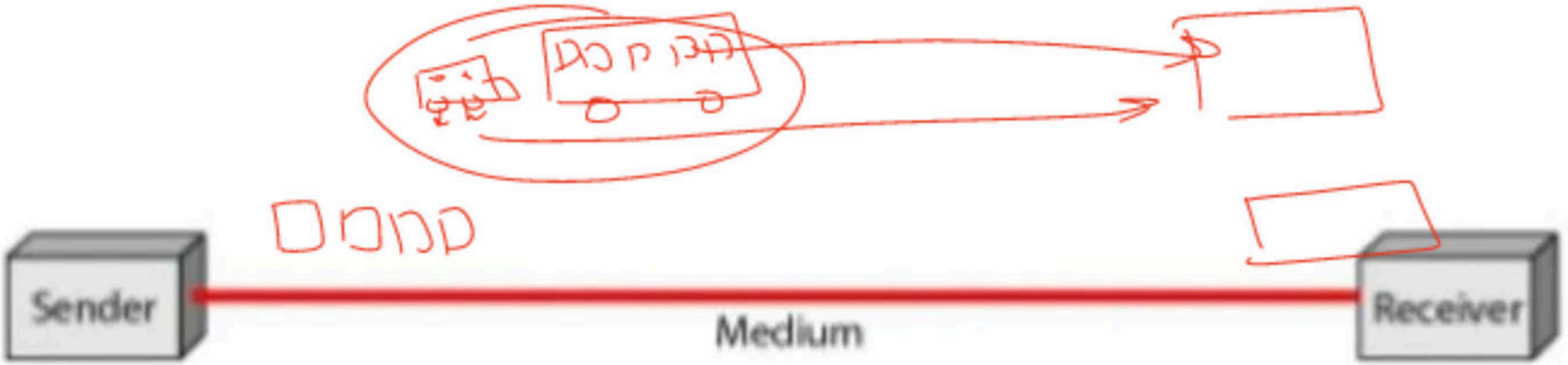


Data communications are the exchange of data between to two devices via some transmission medium. A data communication system has five components

1. **Message**- information (data) to be communicated e.g. text, audio, video.
2. **Sender**- device how sends the message (computer, phone, camera etc.)
3. **Receiver**- device how receives the message (computer, phone, television etc.)
4. **Transmission medium** – is the physical path by which a message travels from sender to receiver.
5. **Protocol** – the set of rules that governs the data communication.

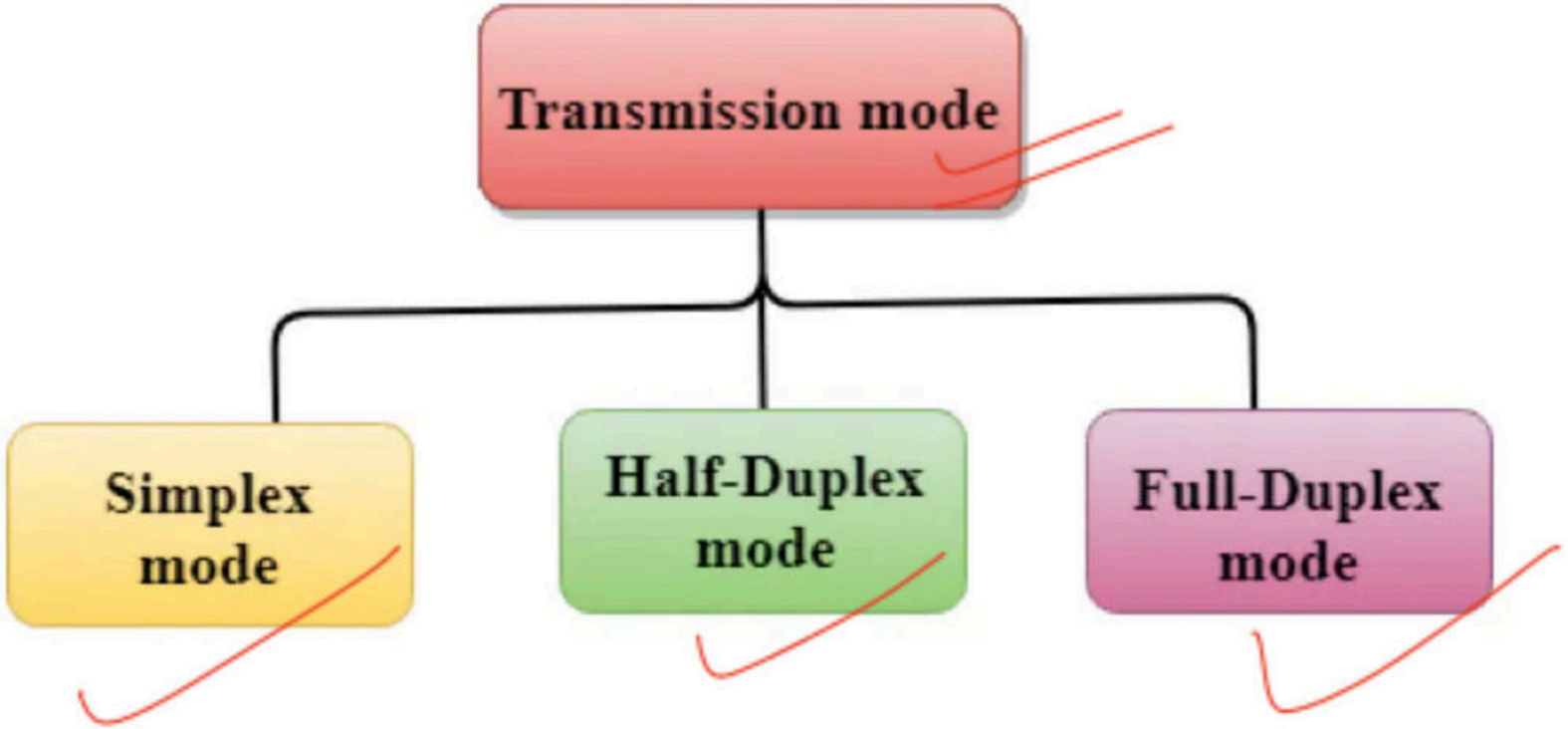


- Effectiveness of the data communications system depends on four fundamental characteristics
  1. **Delivery**- must deliver the data to correct destination.
  2. **Accuracy**- must be delivered accurately without any error
  3. **Timeliness**- must deliver the data in a timely manner, sometime time in real time applications data delivered after time is useless.
  4. **Jitter**- Refers to variation in the packet arrival time i.e. the uneven delay between the packets (mismatch in audio and picture in a video)

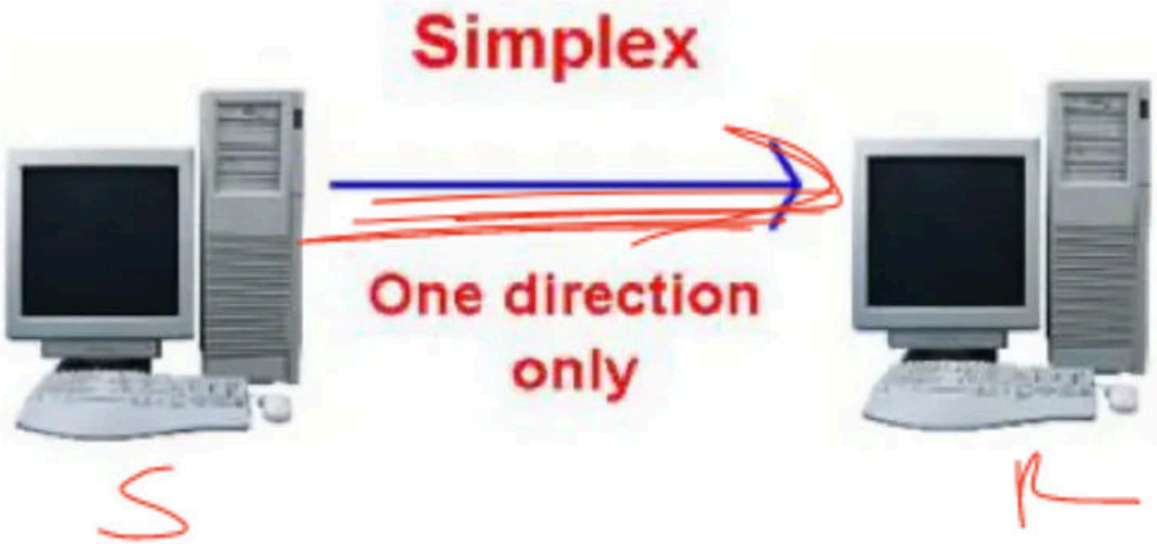


Break

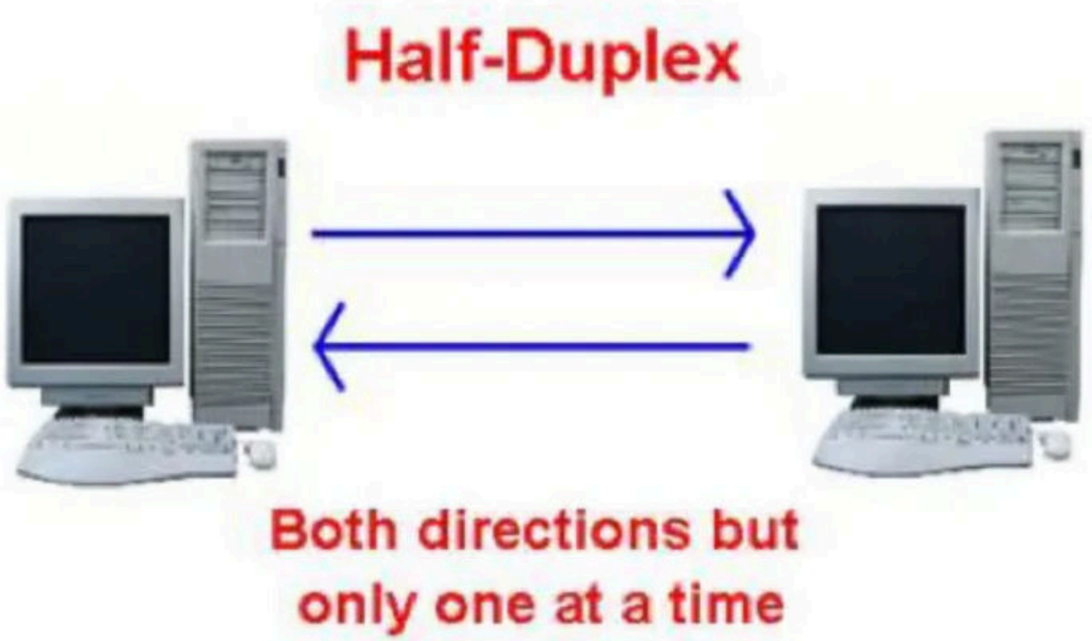
- Data flow between two systems can be categorised into three types –



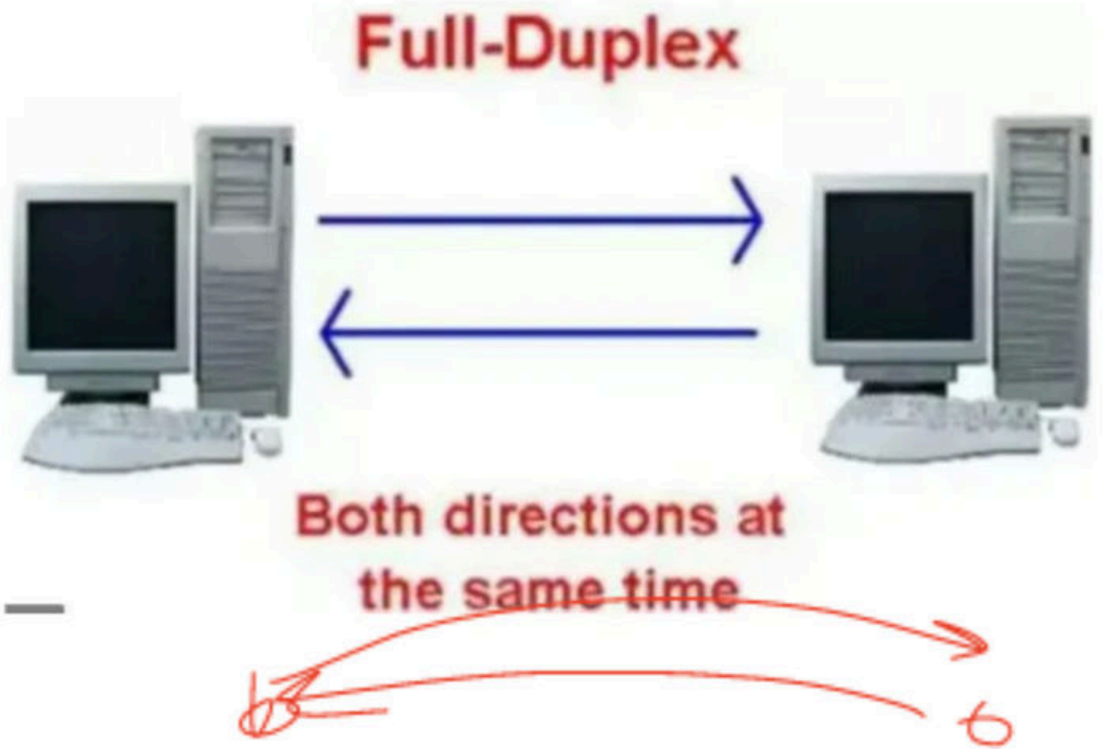
- Data flow between two systems can be categorised into three types –
  - **Simplex** – the communication is unidirectional, as a one-way street.one device always sends can always send other can always receive. E.g. radio, mouse.
  - The simplex mode can use the entire capacity of the channel to send data in one direction.



- **Half duplex** – each station can both transmit and receive, but not at the same time. E.g. like a one lane road, walkie-talkie etc.
  - When one device is sending, the other can only receive, and vice versa.
  - In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
  - Walkie-talkies are both half-duplex systems.



- **Full duplex** – both stations can transmit and receive at the same time. Actually, it is two half duplex connections.
- Telephone network is an example of full-duplex mode, when two people are communicating by a telephone line, both can talk and listen at the same time.
- The capacity of the channel, must be divided between the two directions.

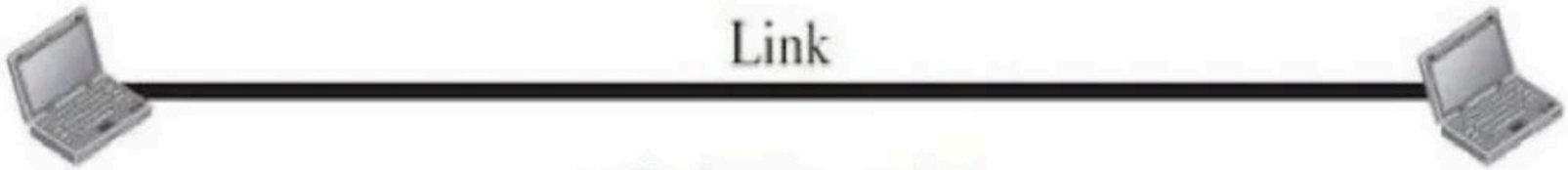


Break

- Network criteria- a network must be able to meet a certain number of criteria. The most important of these are performance, reliability and security.
  1. **Performance** – can be measured in many ways including transit time, response time, number of users, type of transmission medium, capabilities of connected hardware's and efficiency of software.
  2. **Reliability** – is a measure of frequency of failure and the time taken to resolve from the failure.
  3. **Security** – includes protecting data from unauthorised access, protecting data from damage and development.

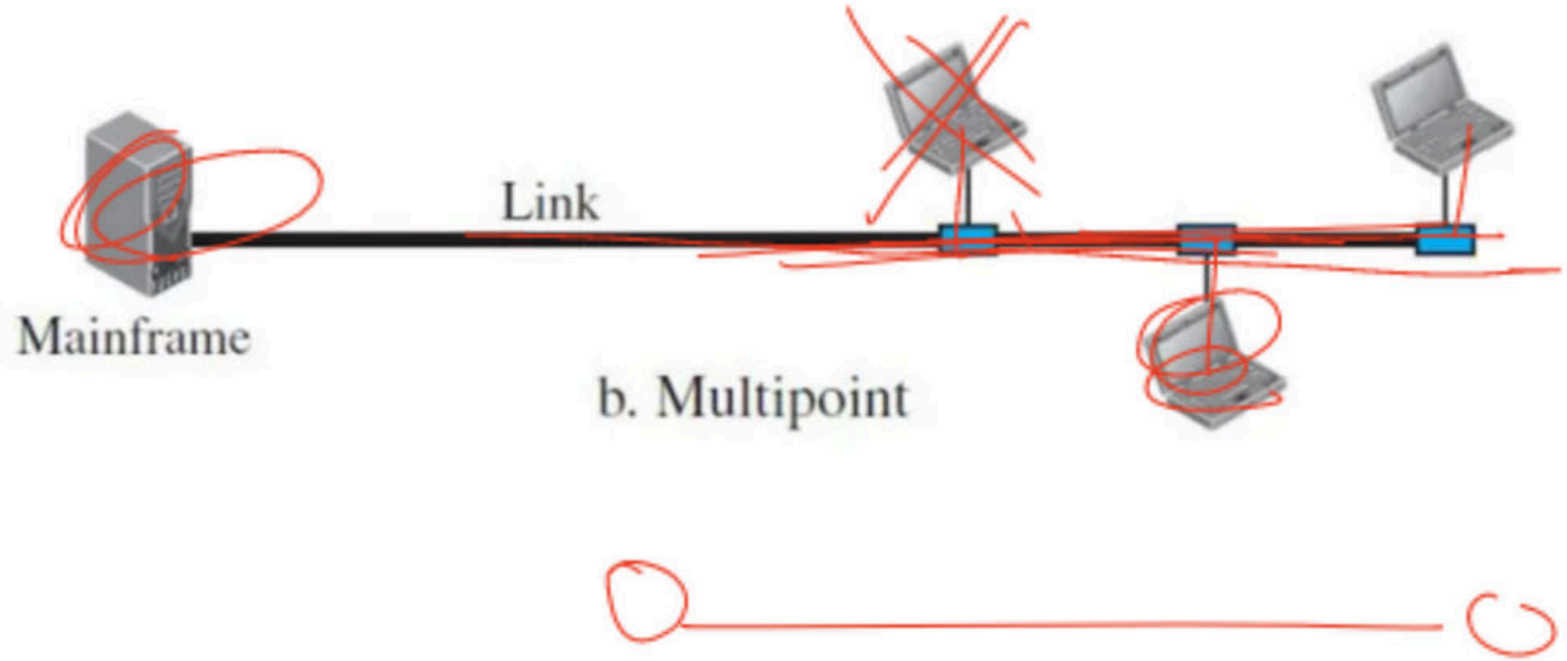
Types of connection-

- **Point to point-** A point-to-point connection provides a dedicated link between two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.



a. Point-to-point

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



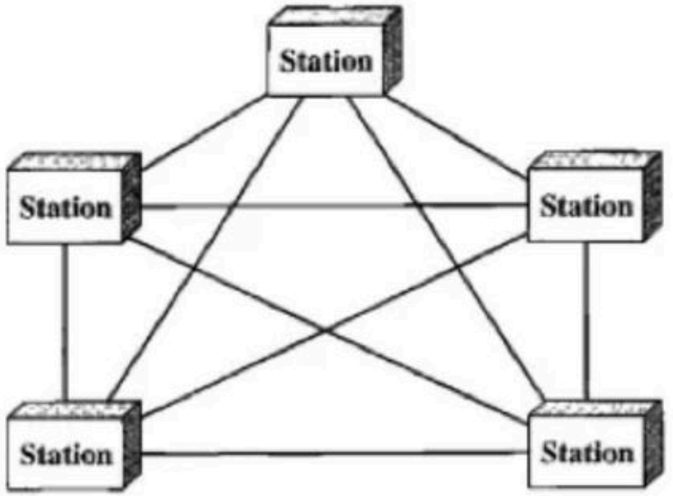
b. Multipoint

Break

Physical topology - Refers to the way in which a network is laid out physically. Topology of a network is the geometric representation of the relationship of all the links and linking devices to one another.

Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- In mesh topology, we need, **n (n -1) /2,** duplex-mode links, where n is number of nodes.

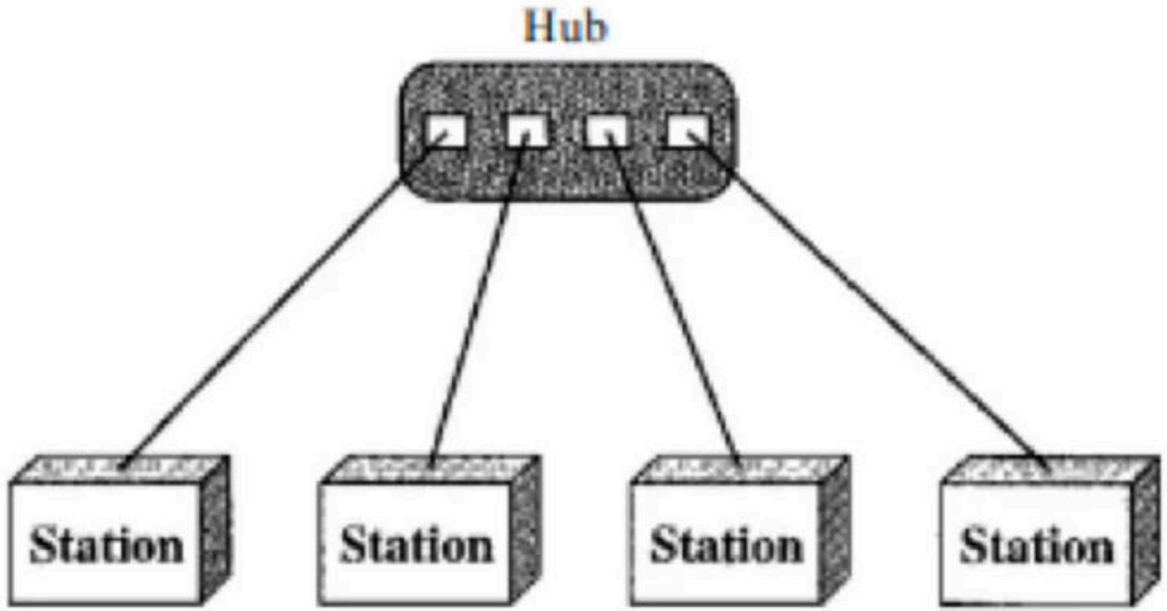


- **Advantages**
  1. The use of dedicated links guarantees that each connection can carry its own data load, thus **eliminating the traffic problems** that can occur when links must be shared by multiple devices.
  2. A mesh topology is **robust**. If one link becomes unusable, it does not incapacitate the entire system.
  3. There is the advantage of **privacy or security**. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
  4. Point-to-point links make **fault identification and fault isolation easy**. Traffic can be routed to avoid links with suspected problems.

- **Disadvantage**
  1. Since every device must be connected to every other device, **installation and reconnection are difficult.**
  2. The **sheer bulk** of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
  3. The hardware required to connect each link (I/O ports and cable) can be prohibitively **expensive**.

Star Topology

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



Advantages

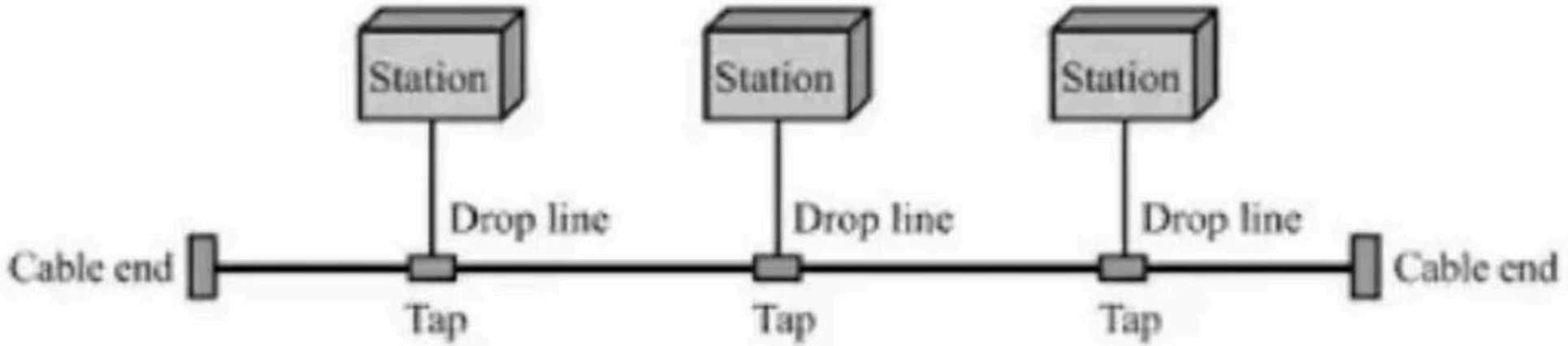
1. A star topology is less expensive than a mesh topology.
2. It is easy to install and reconfigure and less costly.
3. It is robust. If one link fails, only that link is affected.
4. Easy fault identification and fault isolation.

Disadvantage

1. Dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Often more cabling is required in a star than in some other topologies.

Bus Topology

- A bus topology, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



Advantages

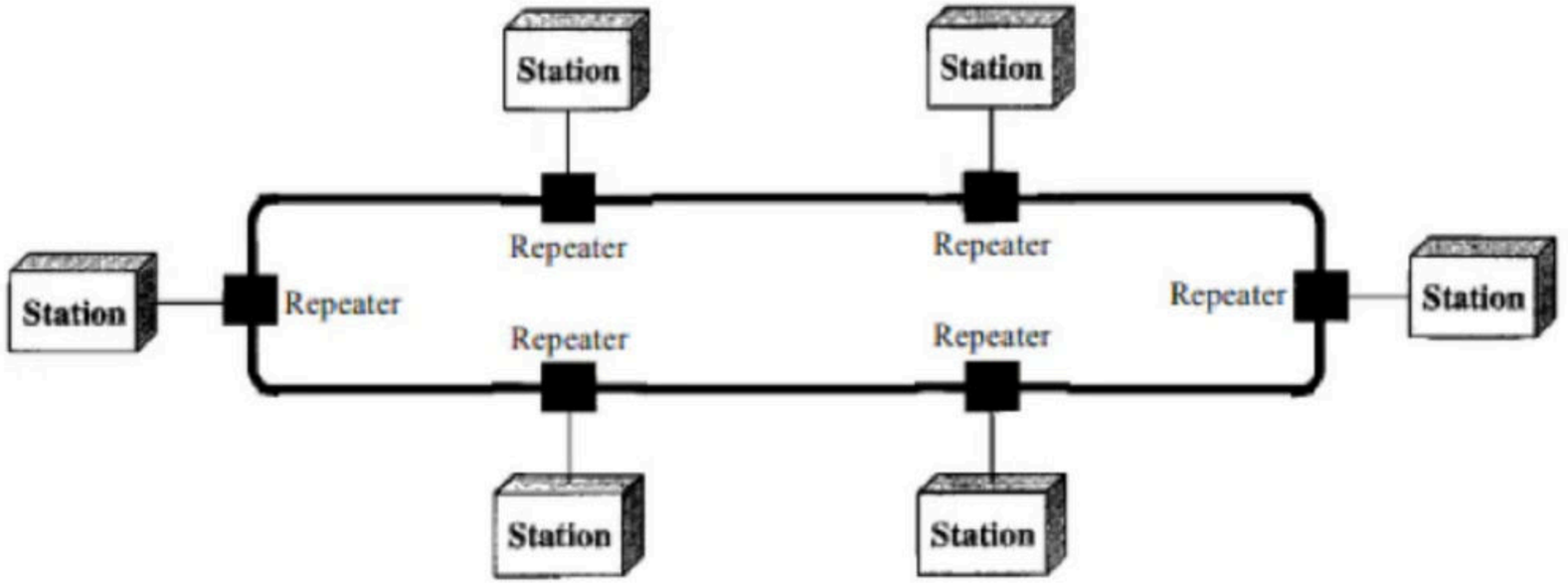
- Advantages of a bus topology include ease of installation.
- Uses less cabling than mesh or star topologies.

Disadvantage

- Disadvantages include difficult reconnection and fault isolation.
- Difficult to add new devices to network.
- A fault or break in the bus cable stops all transmission.

Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages

- A ring is relatively easy to install and reconfigure.
- Fault isolation is simplified.

Disadvantages

- A break in the ring (such as a disabled station) can disable the entire network.

Break

- Protocols and Standards-
  - Syntax
  - Semantics
  - Timing
  - De facto, De jure

Network Models

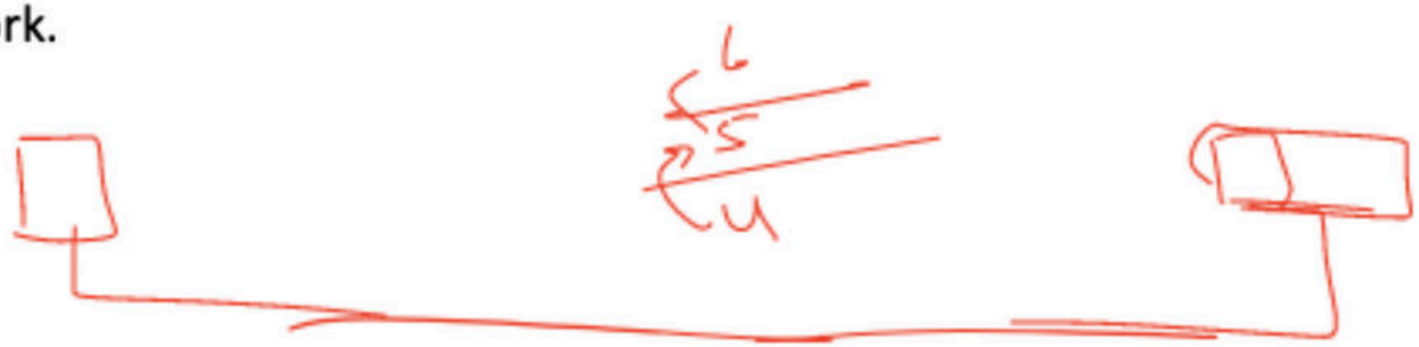
1. Layered Task- International standard organization (ISO)- open system interconnection (OSI) model- allows two system to communicate regardless of their architecture. - which has seven layers with following duties

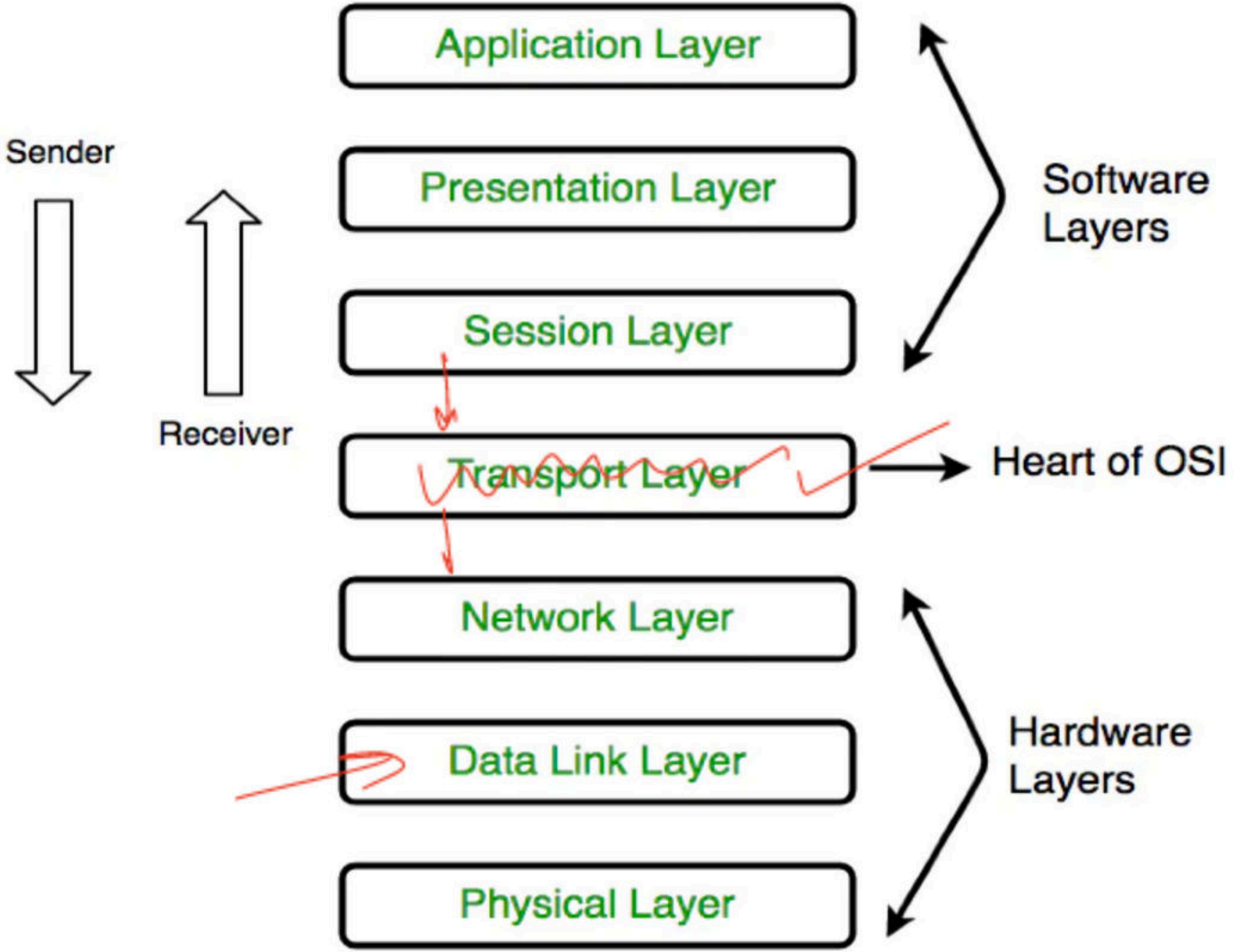
2. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

3. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

4. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

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





Layered Architecture

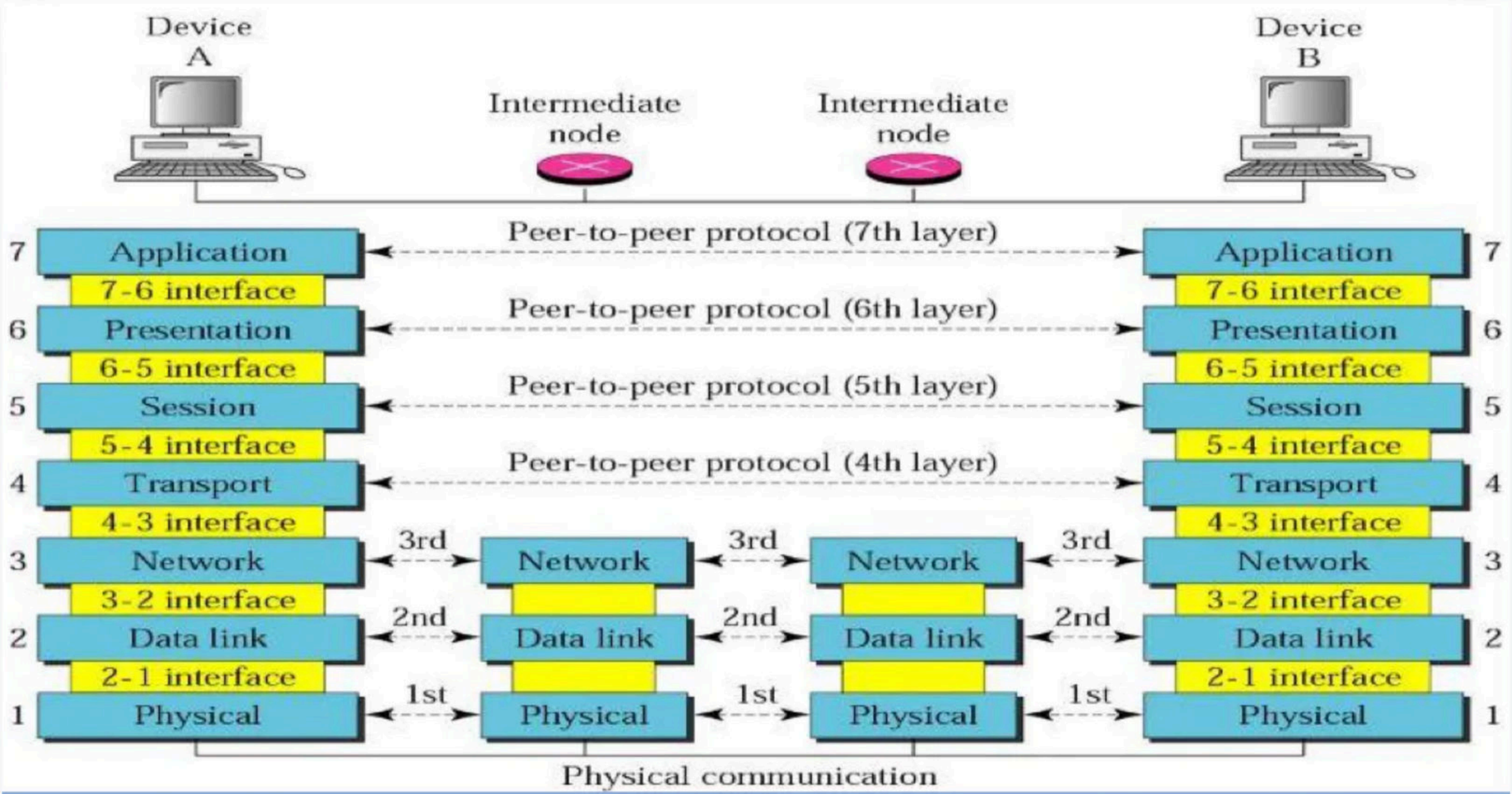
1. The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).

2. Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.

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

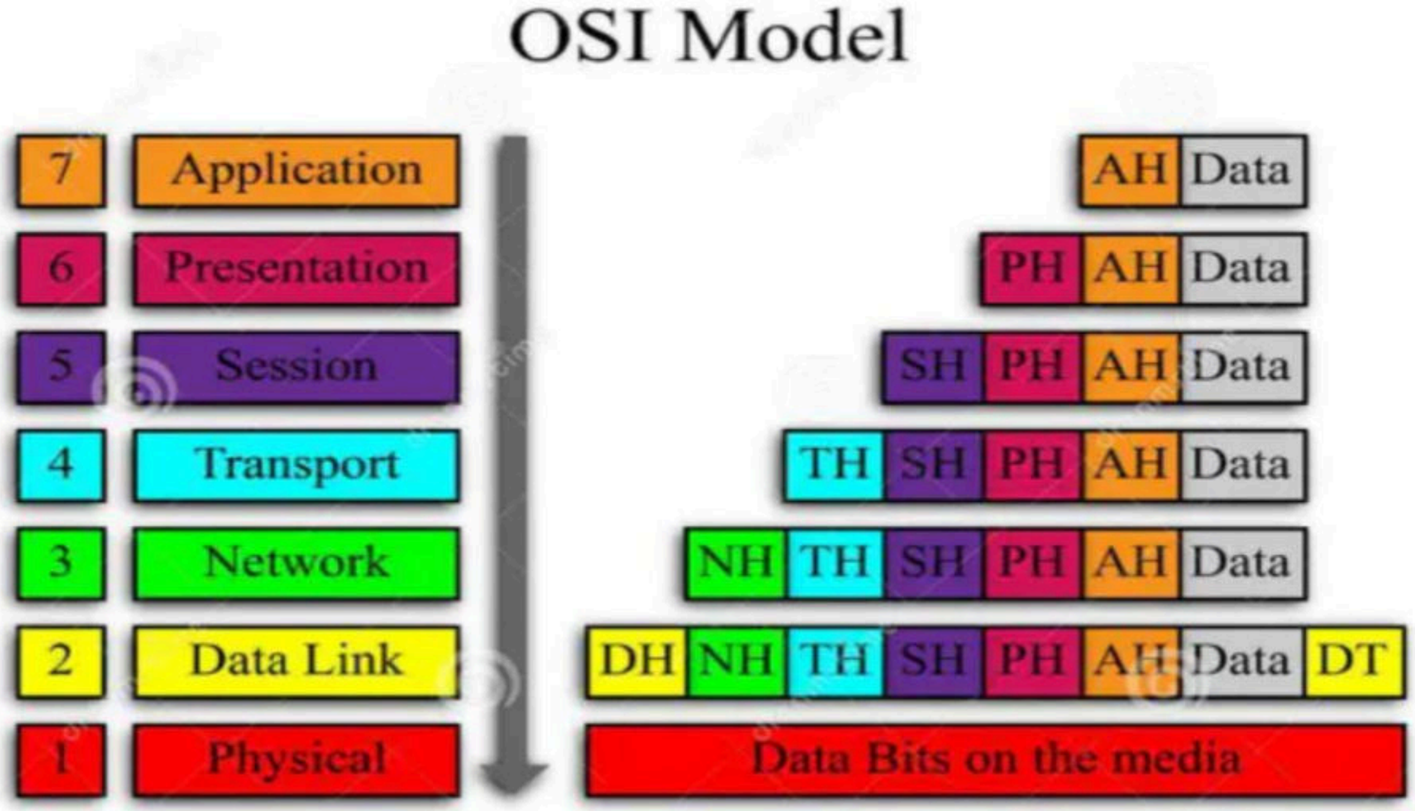
4. This communication is governed by an agreed-upon series of rules and conventions called protocols.

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



Peer-to-Peer Processes

- At the physical layer, communication is direct: device A sends a stream of bits to device B (through intermediate nodes).
- At the higher layers, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.



Break

Physical layer

1. The physical layer defines the **characteristics of the interface** between the devices and the transmission medium.
2. **Representation of bits**: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals- electrical or optical.
3. **Data rate:** The transmission rate-the number of bits sent each second-is also defined by the physical layer.
4. **Line configuration**: The physical layer is concerned with the connection of devices to the media.
5. **Physical topology**: The physical topology defines how devices are connected to make a network.
6. **Transmission mode**: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data link layer

1. **Framing**: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
2. **Physical addressing**: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
3. **Flow control**: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
4. **Error control**: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
5. **Access control**: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Network layer

1. The network layer is responsible for the **source-to-destination delivery** of a packet, possibly across multiple networks (links).
2. **Logical addressing:** If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
3. **Routing:** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport layer

1. **Service-point addressing**: The transport layer header must include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer. The transport layer is responsible for process-to-process delivery of the entire message.
2. **Segmentation and reassembly**: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
3. **Connection control**: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
4. **Flow control**: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
5. **Error control**: Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Session layer

1. The session layer is the **network dialog controller**. It establishes, maintains, and synchronizes the interaction among communicating systems.
2. The session layer is responsible for **dialog control and synchronization**.
3. **Dialog control**: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
4. **Synchronization**: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

Presentation layer

1. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
2. **Translation**: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
3. **Encryption**: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
4. **Compression**: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application layer

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

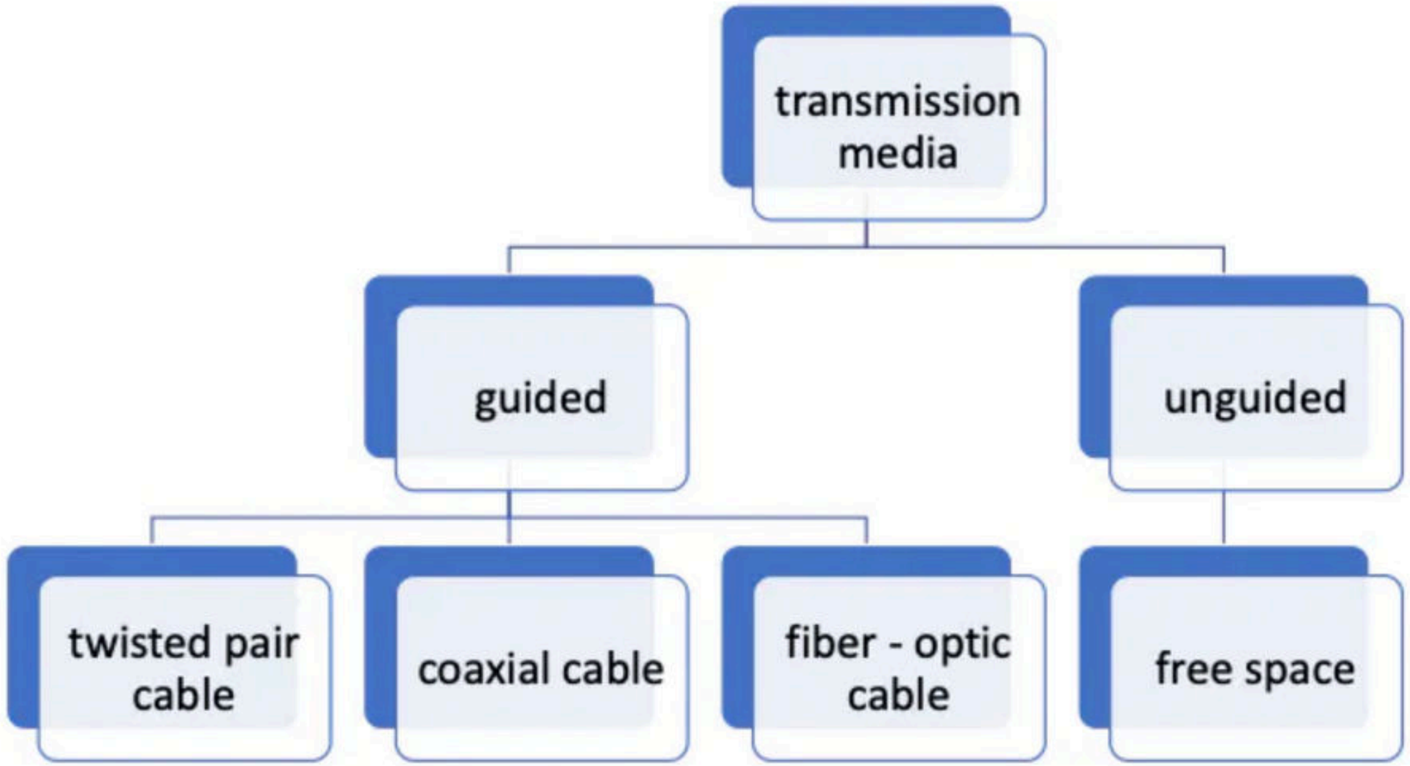
Services

1. **Network virtual terminal**: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
2. **File transfer, access, and management**: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
3. **Mail services**: This application provides the basis for e-mail forwarding and storage.
4. **Directory services**: This application provides distributed database sources and access for global information about various objects and services.

Break

Transmission media

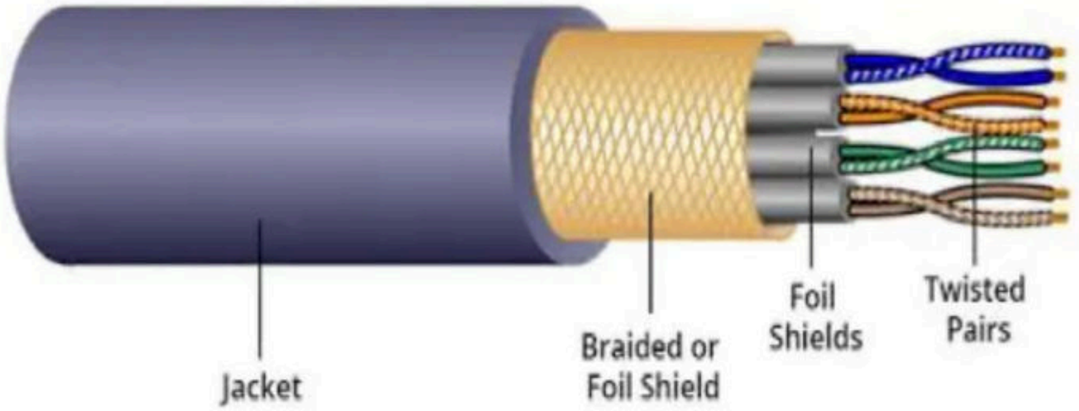
- (layer-0) can broadly be defined anything that can carry information from source to destination.



Guided media

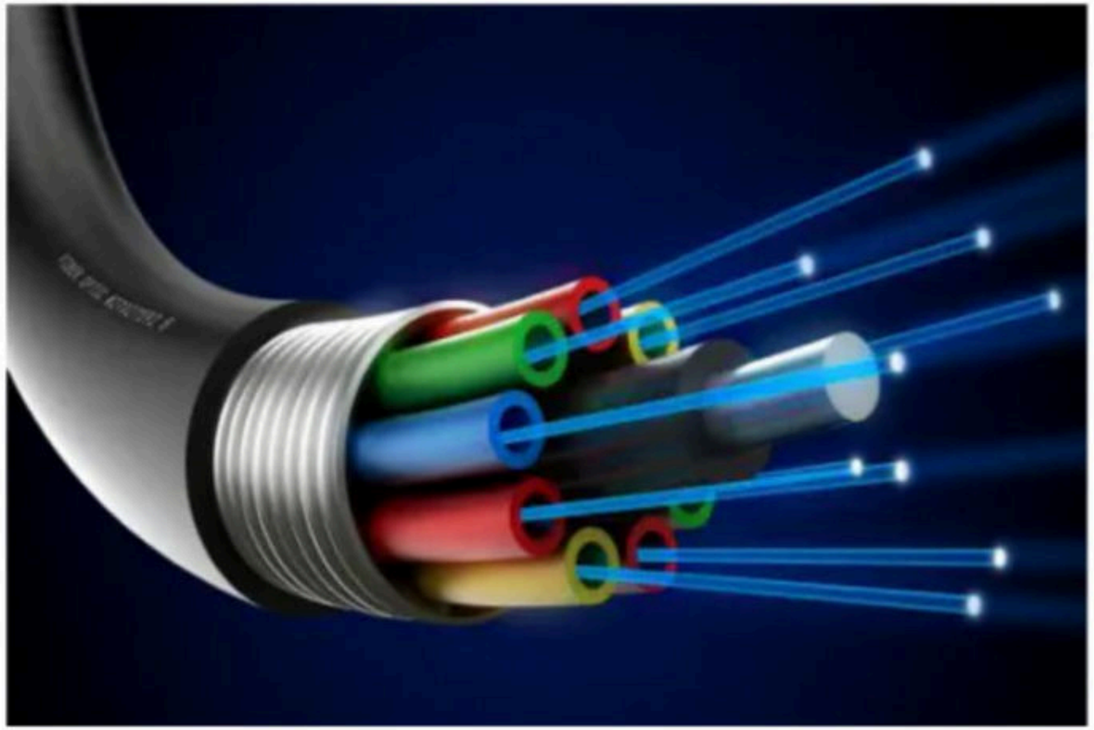
- Guided media – Are those which provide a connection from one device to another, include twisted pair cable, coaxial cable and fibre optic cable.

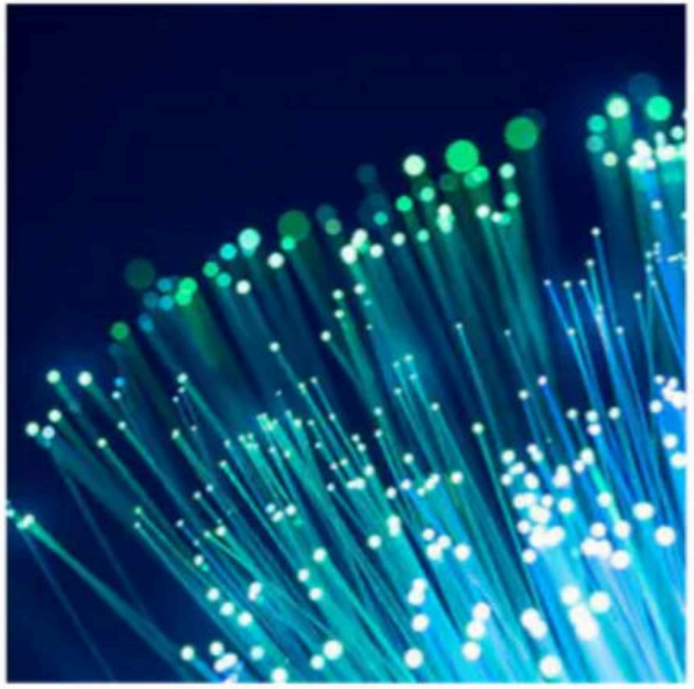
- **Twisted pair cable** - Consists of two conductors (copper), each with it's own plastic insulation, twisted together. (shielded and unshielded twisted pair of cables)(telephone line)



- **Coaxial Cable** – Has a central core conductor of solid wire enclosed in an insulating sheath, which in turn, encased in an outer conductor of metal foil, braid or a combination of two. (Cable tv)

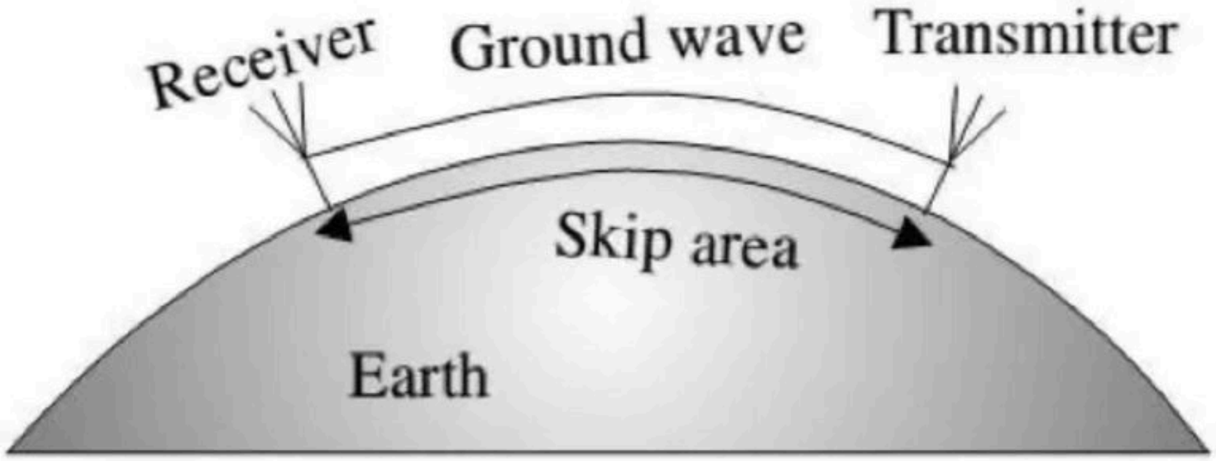
- **Fibre optic** - made of glass or plastic and transmit signal in the form of light, using the principle of total internal reflection, a glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- Backbone network cost effective can go up to 1600 Gbps (higher bandwidth, less signal attenuation, no noise problem, no corrosion, light weight, greater immunity to tapping) (installation and maintenance, unidirectional light propagation, cost)





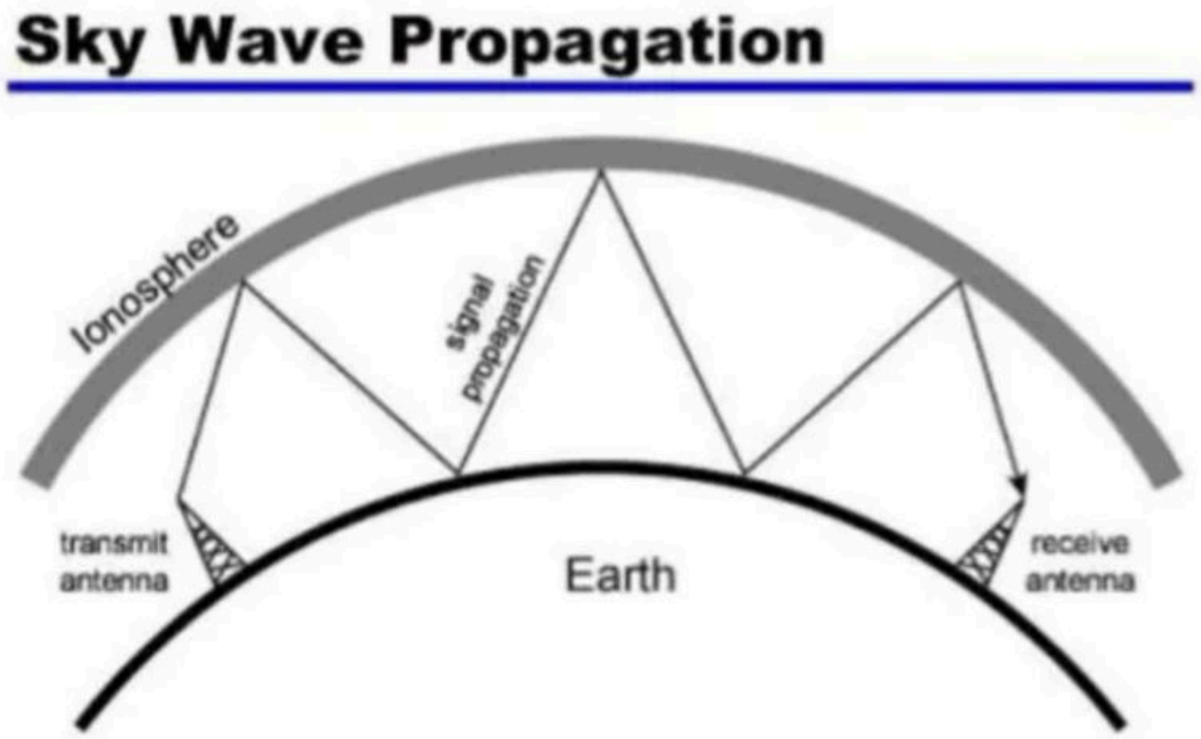
Unguided Media: Wireless

- **Ground propagation** – Waves travel through lower portion of the atmosphere hugging the earth, they are omni directional, distance depends on the amount of power.
- Will having low frequency and large wave length (Khz - Mhz)
- Bend round the obstructions, because large of Wave Length(e.g. light and sound)
- Attenuate in short range.



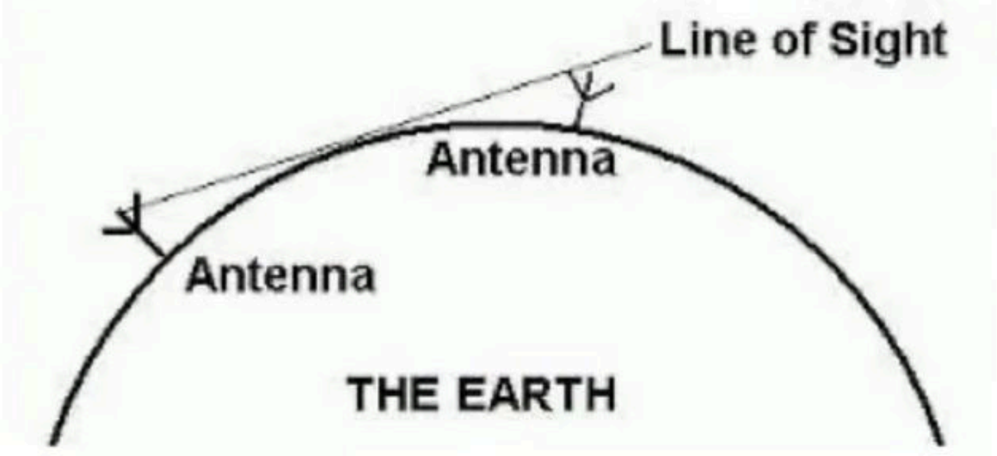
Unguided Media: Wireless

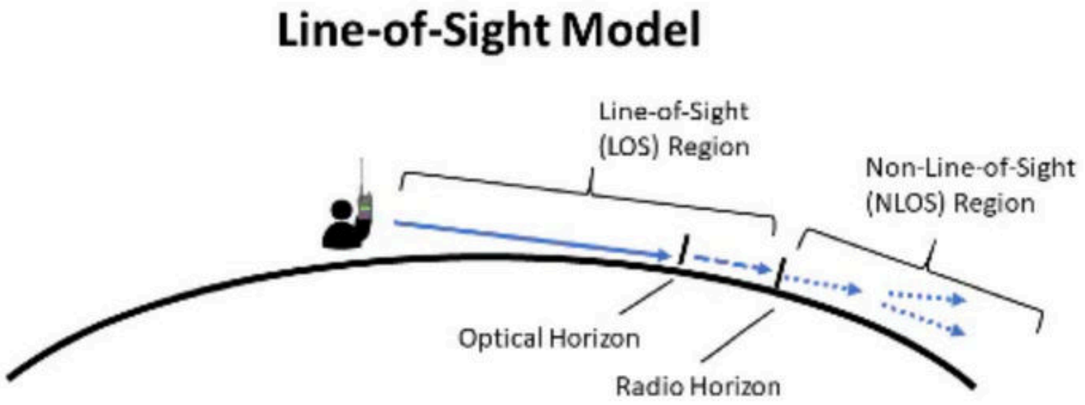
- **Sky propagation** – high frequency radio waves, radiated upward into the ionosphere where they are reflected back to earth. greater distance with lower output.
- 3 Mhz to 32 Mhz
- Range go up to 5000 km

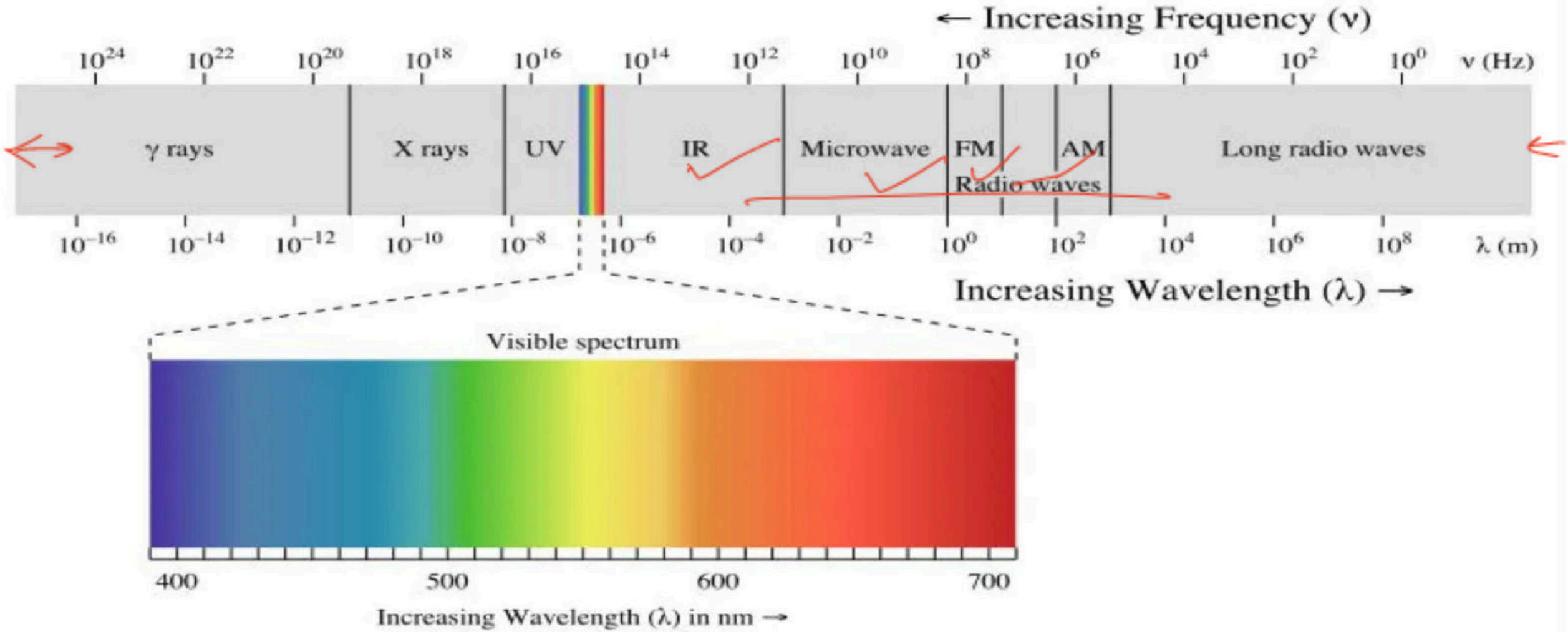


Unguided Media: Wireless

- **Line of sight propagation** – very high frequency signals transmitted in straight lines directly from antenna to antenna.
- Microwaves used







1. Radio Waves – (3KHz- 1GHz) (omnidirectional) (interference problem because of omnidirectional) (sky mode) (long distance) (AM radio) (can penetrate through wall) (managed by government)
2. Microwaves – (1GHZ- 300GHz) (unidirectional) (can be focused narrowly) (sending and receiving antenna needed to be aligned) (cannot penetrate wall) (wide band so high data rates are possible) (managed by government)
3. Infrared – (300GHz- 400THz) (short range communication) (home appliances)