Savitribai Phule Pune University
Third Year of Computer Engineering (2019 Course)
310244: Computer Networks and Security

Home

Teaching Scheme:	Credit: 03	Examination Scheme:
TH: 03 Hours/Week		Mid-Semester (TH) : 30 Marks End-Sem (TH): 70 Marks

Prerequisites Courses:

Companion Course: Computer Networks and Security Laboratory (310247)

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 different layer protocols in the protocol stacks
- To understand modern network architectures with respect to design and performance
- To learn the fundamental concepts of information security

Sinhgad Institutes

Prof. Mandar Diwakar
Asst. Professor
Dept. of Computer Engineering
Smt. Kashibai Navale College of Engineering, Pune

Computer Network and Security

T.E. Computer Engineering Semester I

Unit I

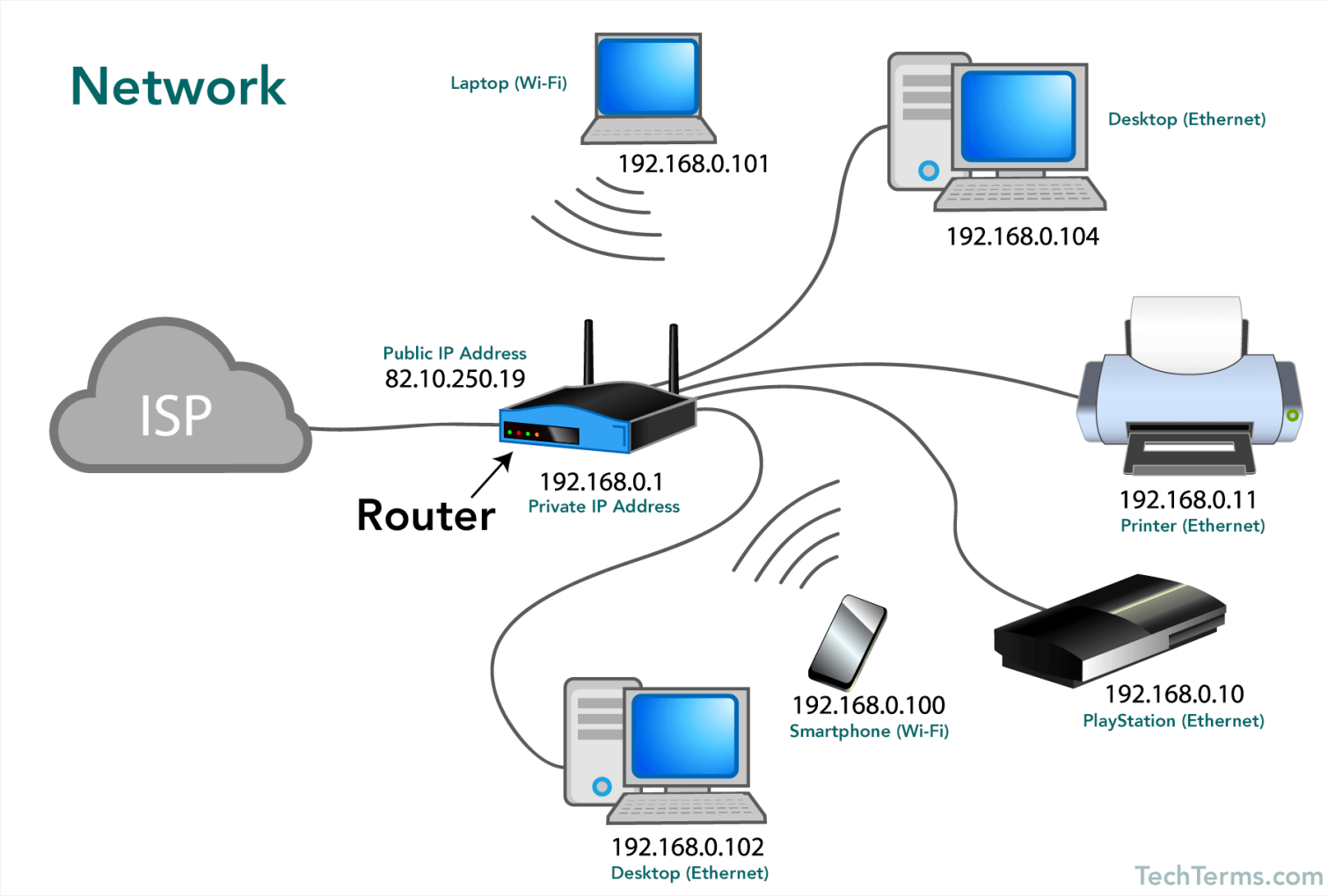
Introduction To Computer Networks

Unit I	Introduction To Computer Networks	07 Hours

Definition, **Types of Networks**: Local area networks (LAN), Metropolitan area networks (MAN), Wide area networks (WAN), Wireless networks, Networks Software, Protocol, Design issues for the Network layers, **Network Models**: The OSI Reference Model, TCP/IP Model, Network Topologies. Types of Transmission Medium, **Network Architectures**: Client-Server, Peer To Peer, Hybrid. **Network Devices**: Bridge, Switch, Router, Gateway, Access Point. **Line Coding Schemes**: Manchester and Differential Manchester Encodings. Frequency Hopping (FHSS) and Direct Sequence (DSSS) spread spectrum.

What is a Computer Network?

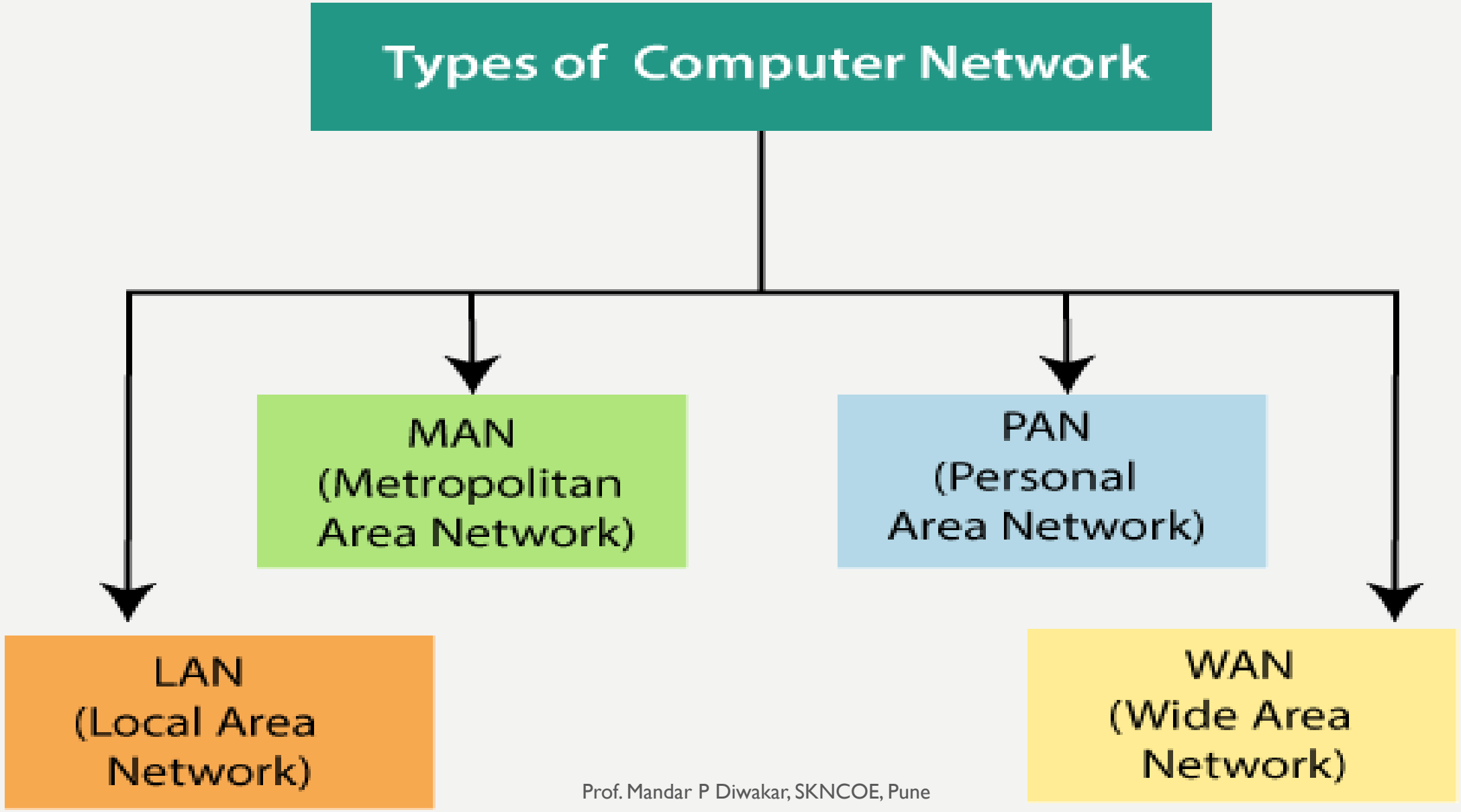
- **Computer Network** is a group of computers connected with each other through wires, **optical fibers** or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the **sharing of resources among various devices.**
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.



What is need of Computer Network?

1. **Information exchange :-**To exchange data and information between different individual users, it is necessary to interconnect the individual users' computers**.**
2. **Resource sharing :-** The cost of computer has come down. However, the cost of a laser printer, bulk storage, and large enterprise software remains high. When computers are interconnected, there is a possibility that, users connected to the network may share the above mentioned resources.
3. **Back up and Roll back : -** Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server
4. **Security : -** Network allows the security by ensuring that the user has the right to access the certain files and applications
5. **Distribution of Working** can possible using computer network.
6. **Centralize control** can possible.
7. **Maximum** performance using **minimum** cost.

Types of Computer Networks

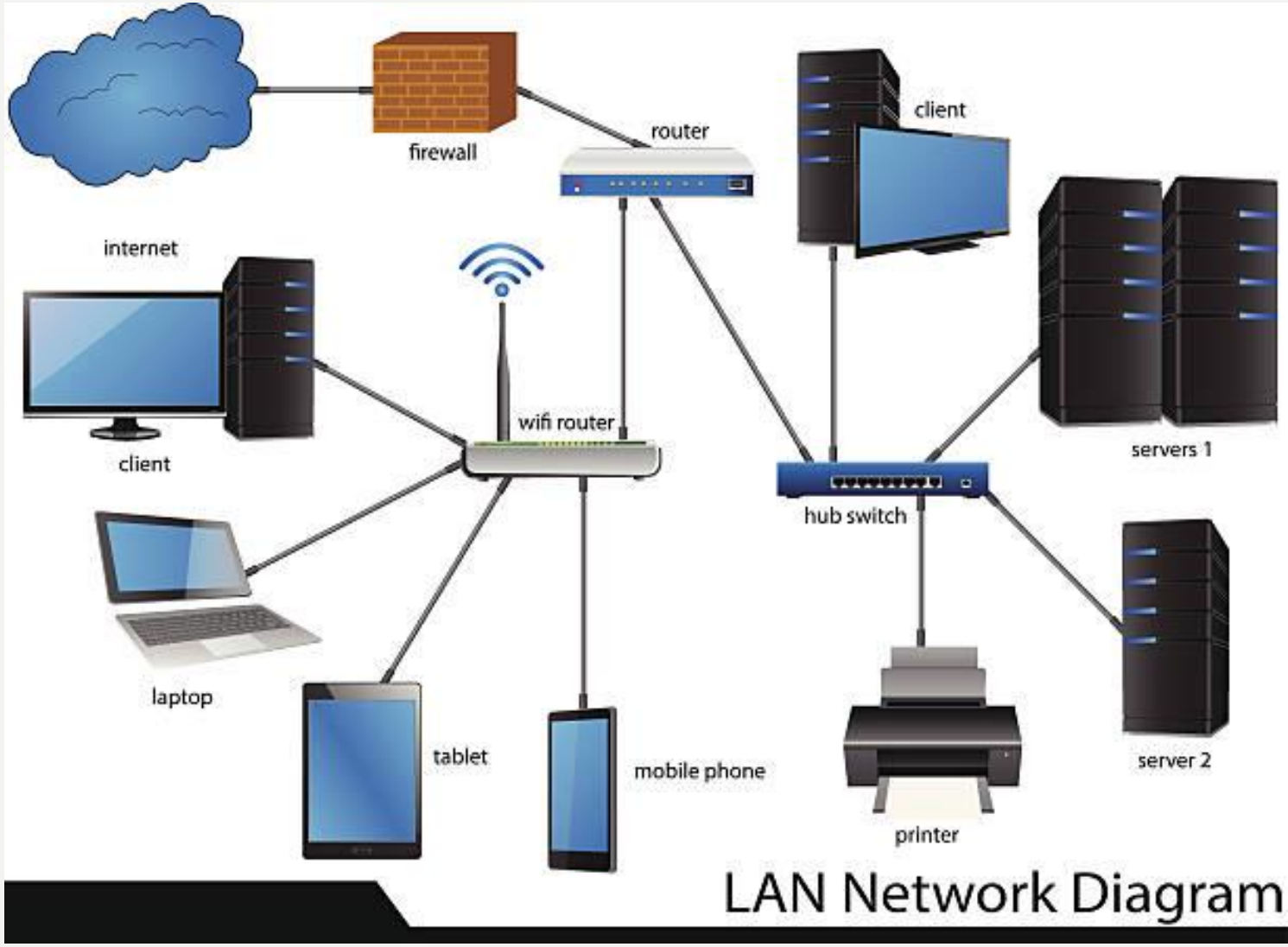


PAN (Personal Area Network)

- **Personal Area Network** is a network arranged within an individual person, typically within a range of 10meters.
- **PAN** is used for connecting the computer devices of personal**.**
- **Thomas Zimmerman** was the first research scientist to bring the idea of the **PAN.**
- **Personal Area Network** covers an area of 30 feet .
- This may include **Bluetooth enabled devices** or **infra-red enabled devices**.
- **PAN** may include **wireless computer keyboard** and **mouse**, **Bluetooth enabled headphones**, **wireless printers**, **mobiles** and **TV remotes**.

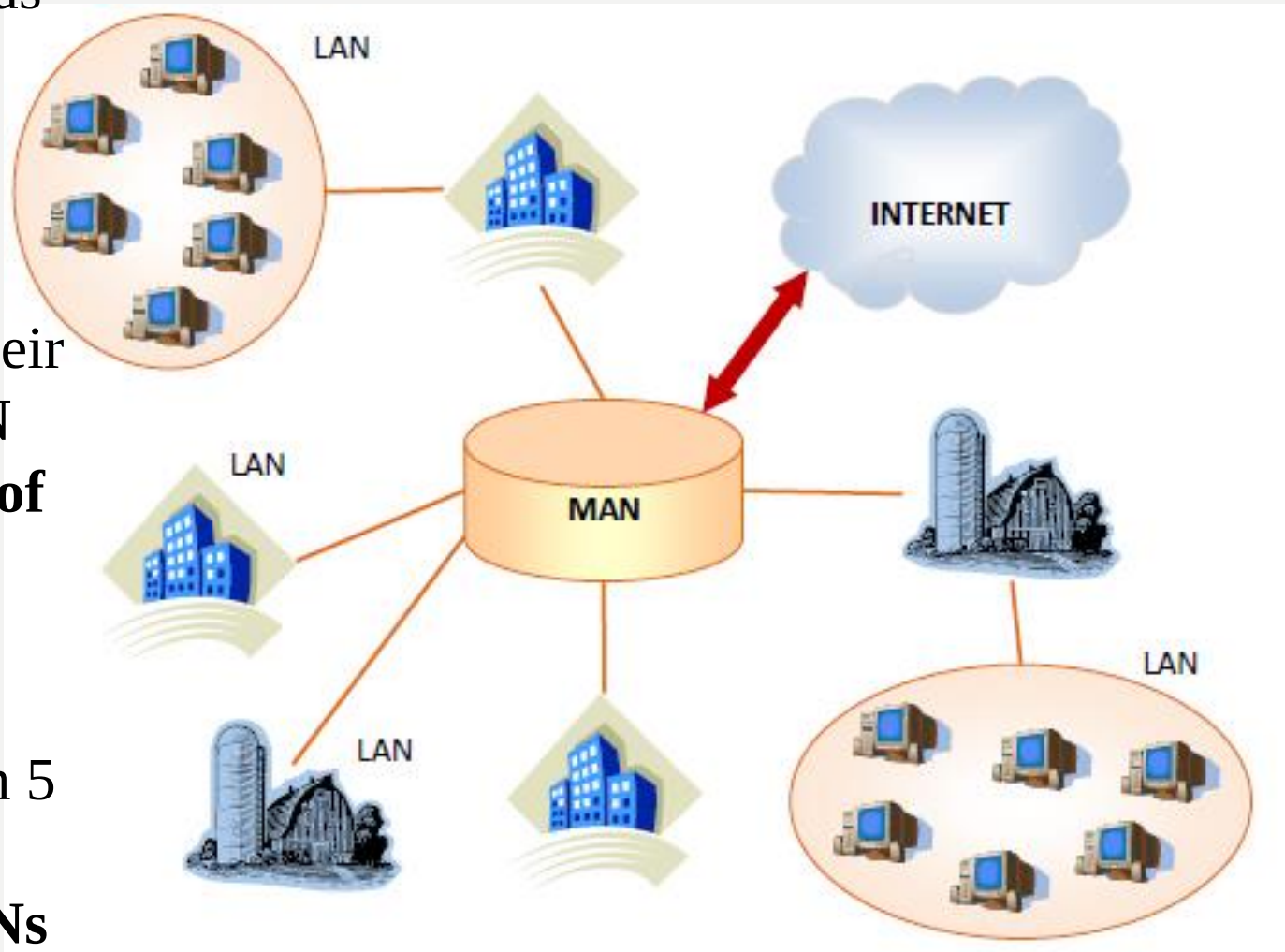
LAN (Local Area Network)

- **Local Area Network** is a group of computers connected to each other in a small area such as building, office.
- **LAN** is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- **LAN** provides a useful way of sharing the resources between end users.
- The resources such as **printers**, **file servers**, **scanners**, and **internet** are easily sharable among computers.
- **LAN** covers an **organization offices**, **schools**, **colleges** or **universities**.



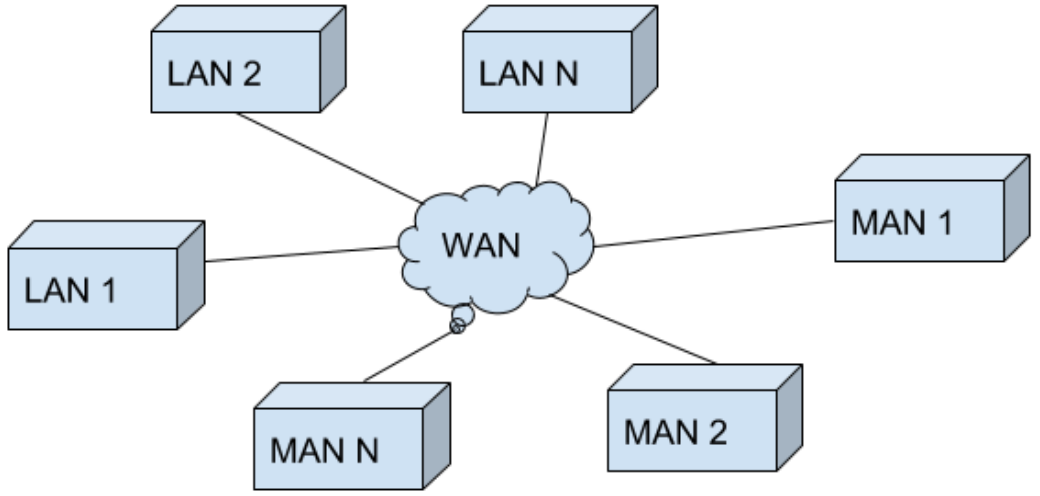
MAN (Metropolitan Area Network)

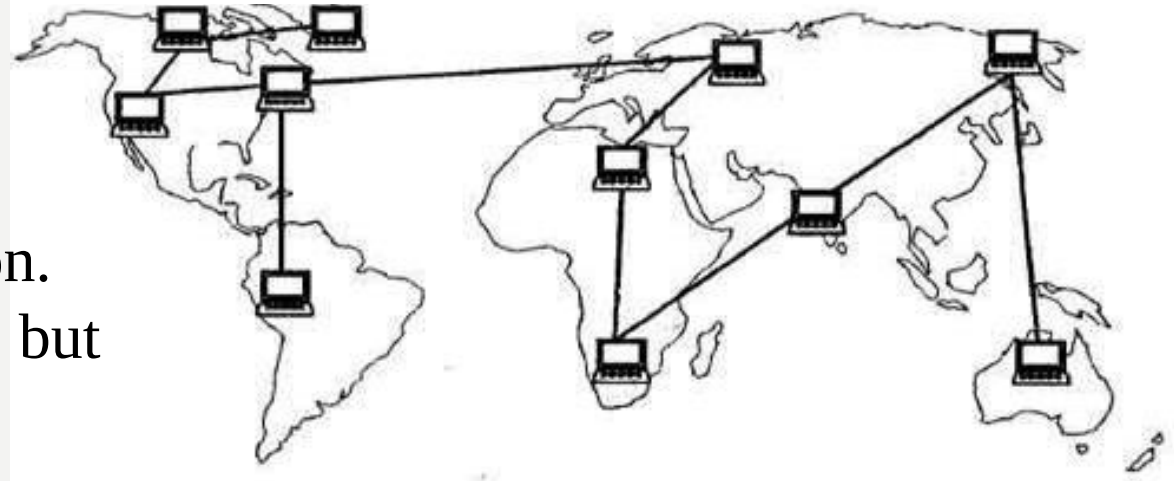
- **The Metropolitan Area Network (MAN)** generally expands throughout a city such as **cable TV network**.
- It can be in the form of **Ethernet**, **Token-ring**, **ATM**, or **Fiber Distributed Data Interface (FDDI).**
- This service enables its users to expand their Local Area Networks. For example, **MAN can help an organization to connect all of its offices in a city.**
- Backbone of **MAN** is **high-capacity** and **high-speed fiber optics.**
- **MAN** Network size generally ranges from 5 to 50 km.
- They provide **uplinks** for connecting **LANs** to **WANs** and **Internet.**



Wide Area Network (WAN)

- As the name suggests, the **Wide Area Network (WAN)** covers a wide area which may span across provinces and even a whole **country** or whole **Globe**.
- Generally, **telecommunication networks** are **Wide Area Network**.
- These networks provide connectivity to **MANs** and **LANs**.
- Since they are equipped with very **high speed backbone**, **WANs** use very **expensive network equipment**.
- **WAN** may be managed by multiple administration.
- **WANs** can be vital for **international businesses**, but they are also essential for everyday use, as the **internet** is considered the **largest WAN** in the **world**.





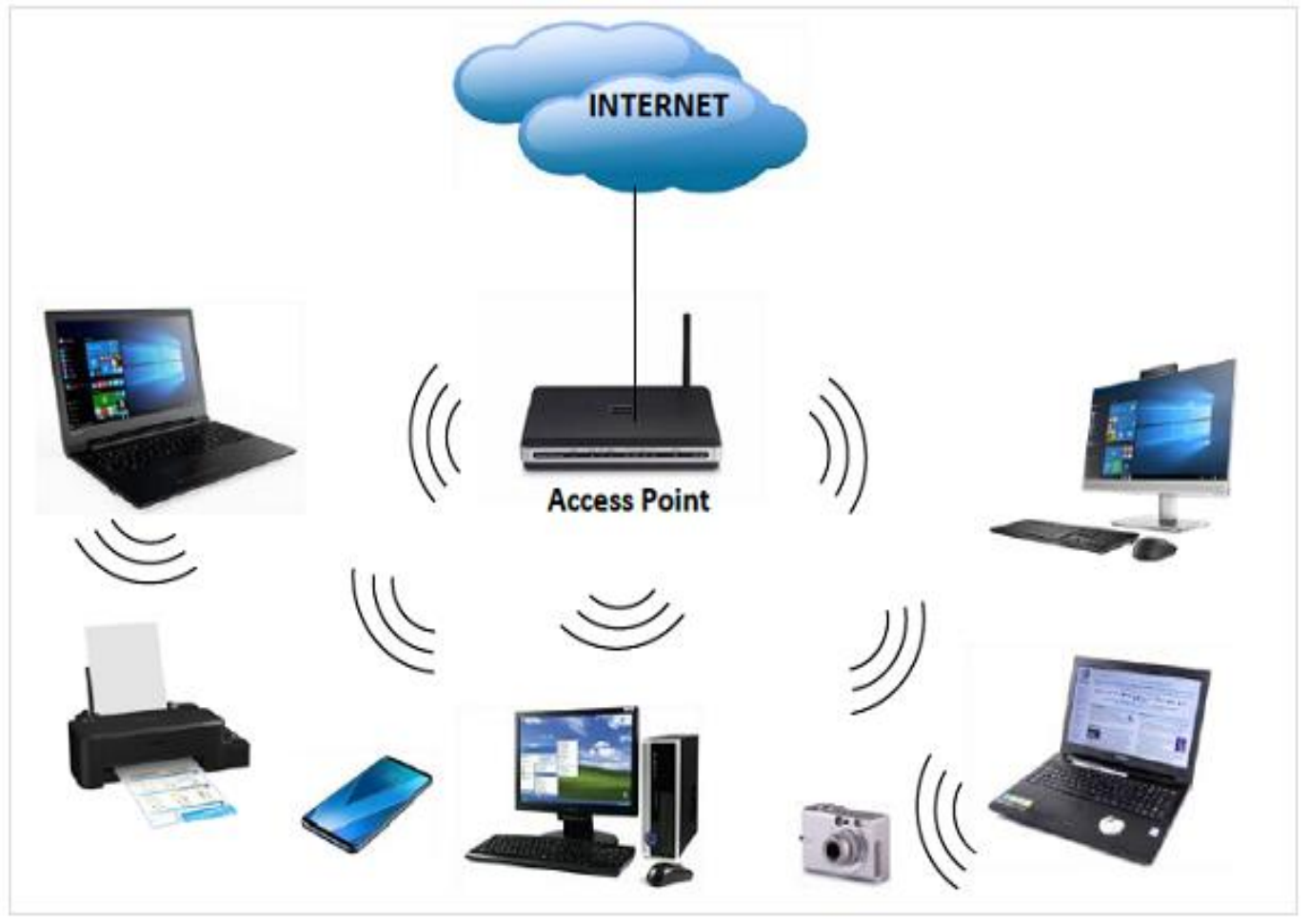
Wide area network

Wireless networks

- **System interconnection** is all about interconnecting the **components of a computer** using **short-range radio**.
- Some companies got together to design a short-range **wireless network** called **Bluetooth** to connect these components without wires**(Bluetooth mouse, keyboard, printer).**
- **Bluetooth** also allows digital **cameras, headsets, scanners**, and other devices to connect to a computer by merely being brought within range.
- **No cables, no driver installation**, just put them down, turn them on, and they work.

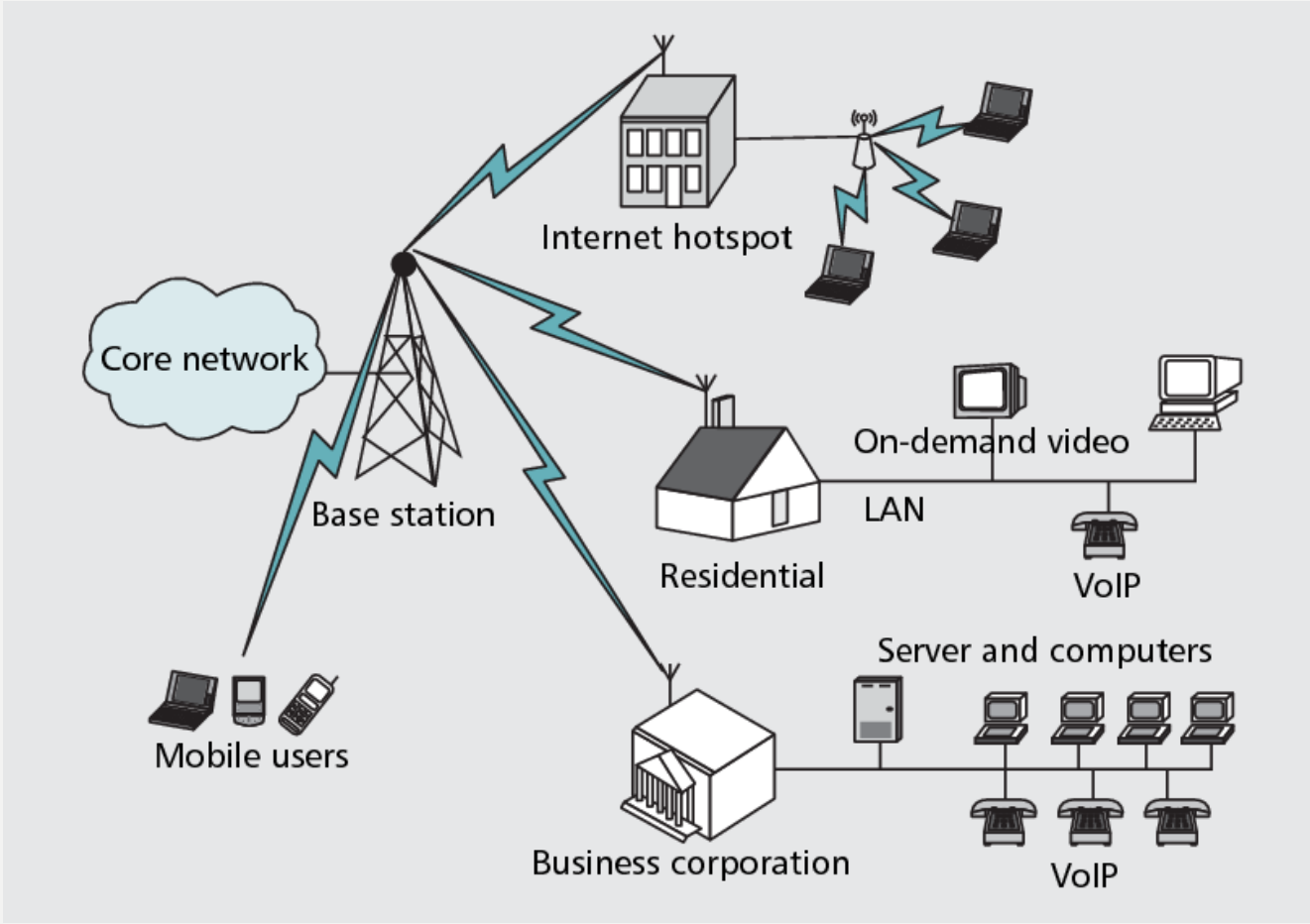
Wireless networks

- **Wireless LANs (WLANs)** are wireless computer networks that use **high-frequency radio waves** instead of cables for connecting the devices within a limited area forming **LAN** (Local Area Network).
- Users connected by **wireless LANs** can move around within this limited area such as home, school, campus, office building, railway platform, etc.
- Most **WLANs** are based upon the standard **IEEE 802.11 standard or Wi-Fi**.



Wireless networks

- **WWAN** (Wireless Wide Area Network) is a WAN (Wide Area Network) and the only thing is that the connectivity is wireless.
- It provides **regional**, **nationwide** and **global wireless** coverage.
- Where **Local Area Network** can be wired or wireless the Wireless Wide Area Network connections are completely wireless.
- In our day today life we are using the Wireless Wide Area Network of different sizes and depending on it **delivery of telephonic calls**, **Web pages** and **streaming video, data sharing occurs.**
- **WiMAX, GSM, GPS**



Networks Software

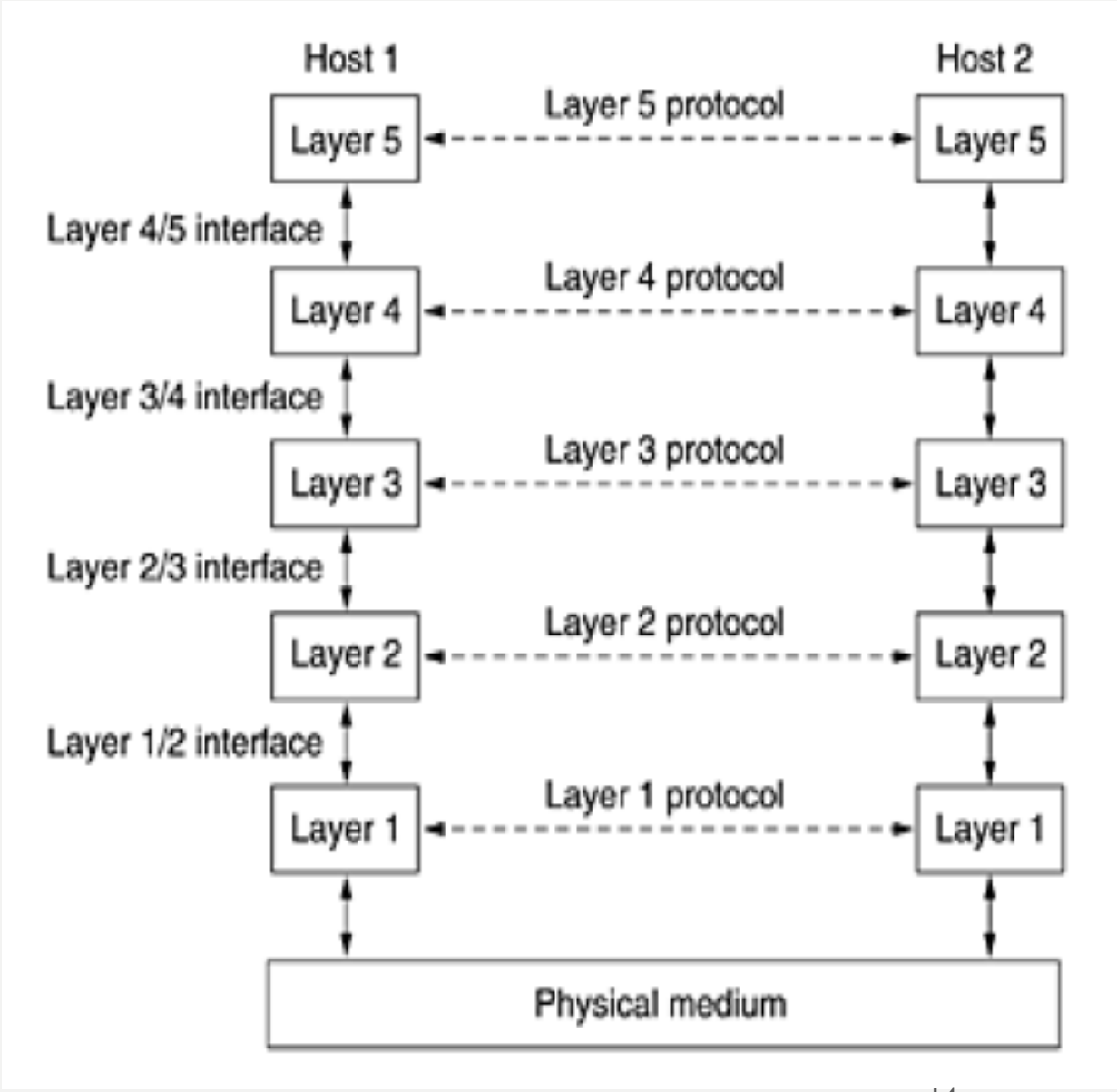
- The first computer networks were designed with the **hardware** as the main concern and the **software** as an afterthought.
- This strategy no longer works.
- **Network software** is now highly structured.

Protocol

- To reduce their design complexity, most networks are organized as a **stack of layers or levels**, each one built upon the one below it.
- The **number** of layers, the **name** of each layer, the **contents** of each layer, and the **function** of each layer **differ** from network to network.
- **The purpose of each layer** is to **offer certain services** to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
- In a sense, each layer is a kind of **virtual machine**, **offering certain services to the layer above it.**
- The fundamental idea is that a particular **piece of software (or hardware)** provides a service to its users but **keeps the details of its internal state and algorithms hidden from them(abstraction)**.

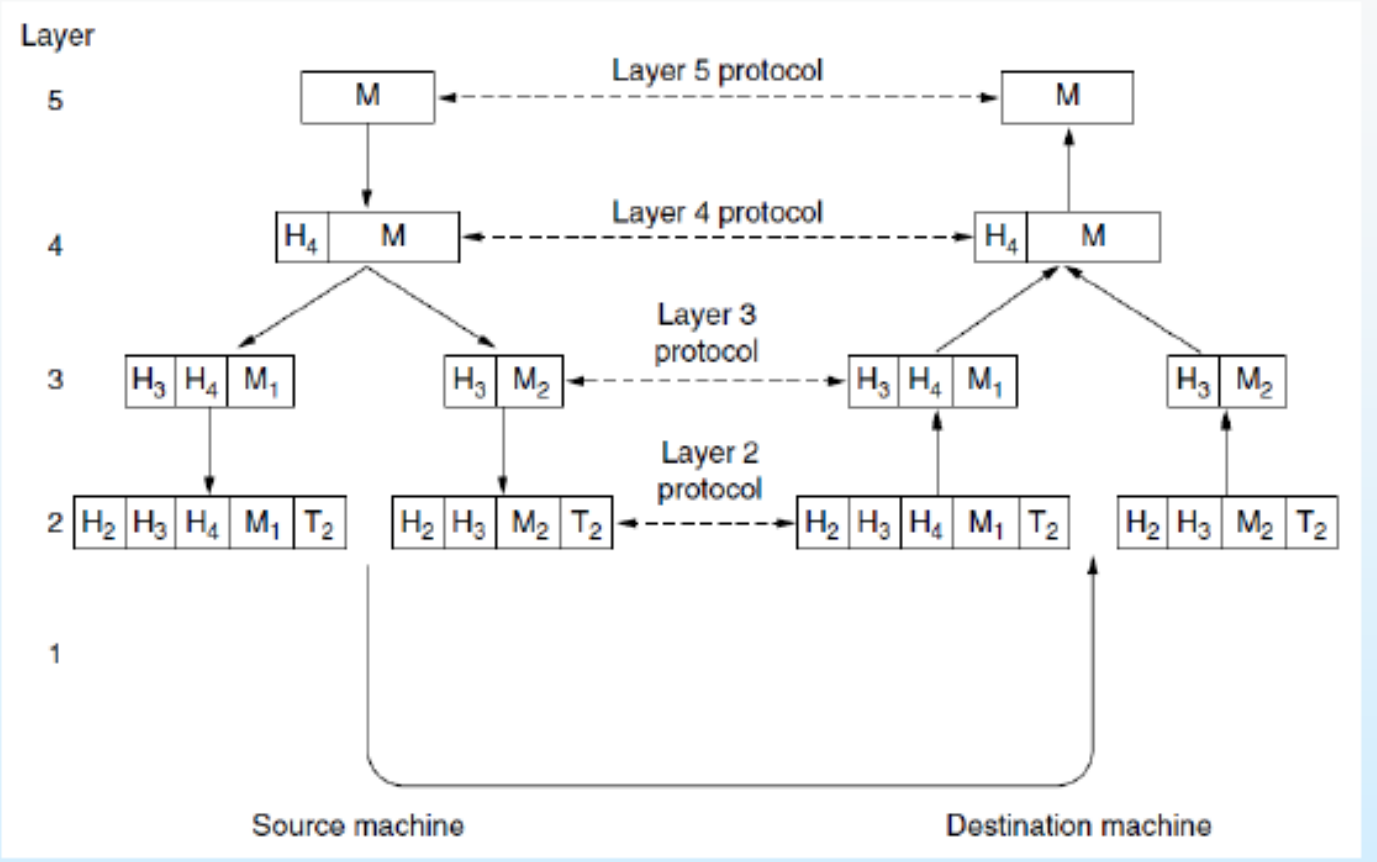
Networks Software

- A **five-layer network** is illustrated in Fig.
- The **entities** comprising the corresponding layers on different machines are called **peers**.
- The **peers** may be **processes, hardware devices, or even human beings.**
- In reality, no data are directly transferred from layer n on one machine to layer n on another machine.
- Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs.
- In Fig. , virtual communication is shown by dotted lines and physical communication by solid lines.
- Between each pair of adjacent layers is an interface.
- The interface defines which primitive operations and services the lower layer makes available to the upper one.
- A set of layers and protocols is called a network architecture.



Communication Flow

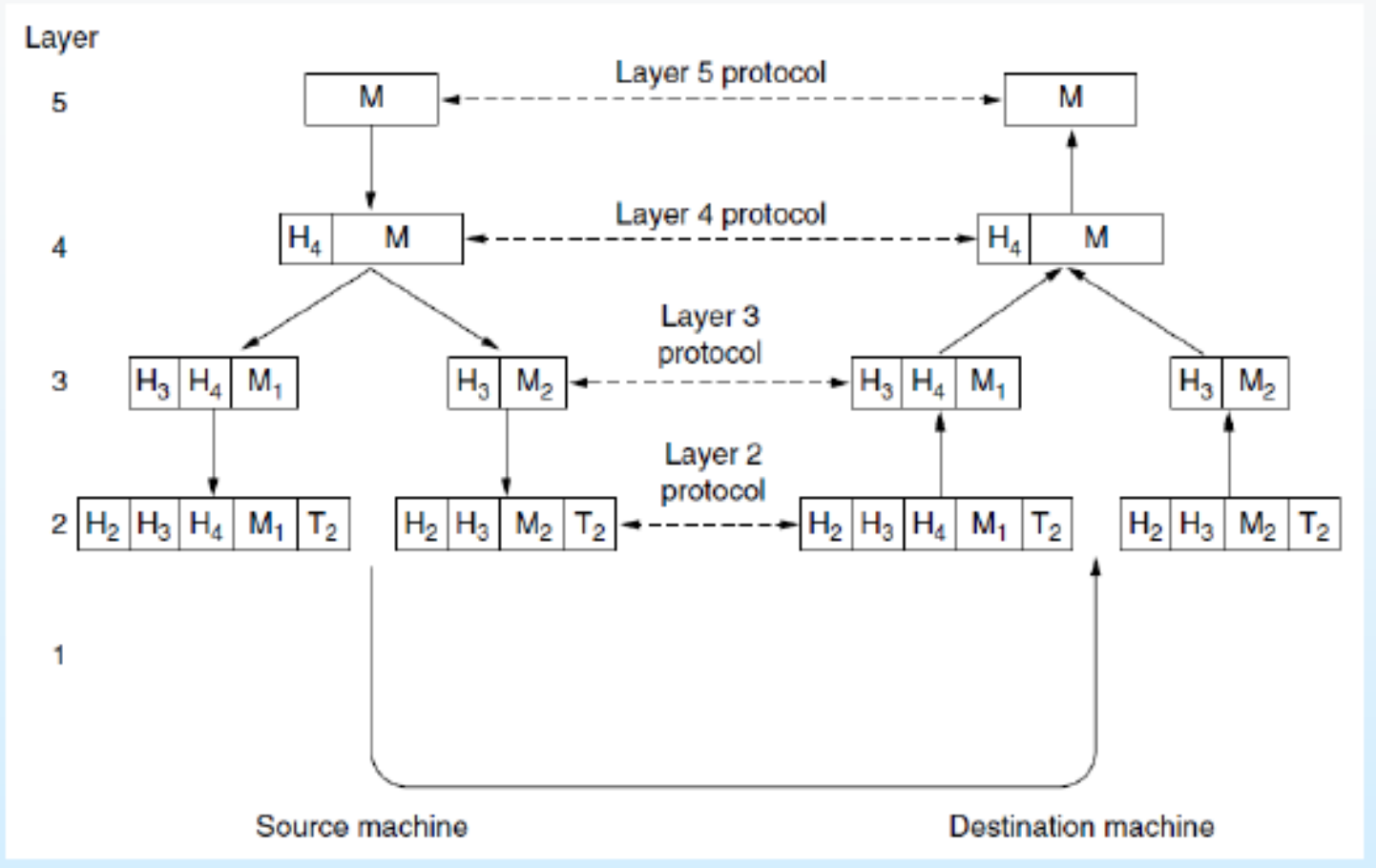
- A message, **M**, is produced by an application process running in **layer 5** and given to **layer 4** for transmission.
- **Layer 4** puts a header in front of the message to identify the message and passes the result to **layer 3**
- The header includes control information, such as address/port, to allow **layer 4** on the destination machine to deliver the message.
- Other examples of control information used in some layers are sequence numbers, sizes, and times.



- **layer 3** must break up the incoming messages into smaller units, packets, prepending a **layer 3** header to each packet

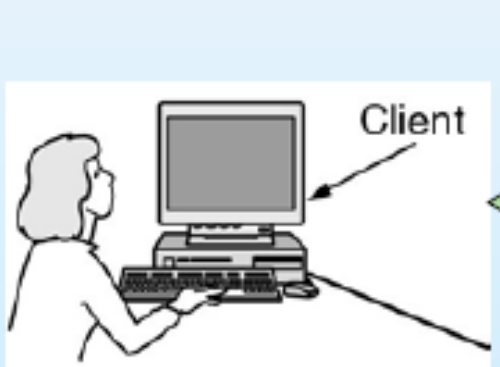
Communication Flow

- **Layer 3** decides which lines to use and passes the packets to **layer 2**.
- **Layer 2** adds to each piece not only a header but also a trailer, and gives the resulting unit to layer 1 for physical transmission.
- At the receiving machine the message moves upward, from **layer** to **layer**, with headers being stripped off as it progresses



Communication Protocol

- **Definition 1**: A protocol is an agreement between the communicating parties on how communication is to proceed
- **Definition 2**: A protocol is a set of communication "rules" between two processes.
- **Example: A** "grades database query" protocol
- (We may make a small project out of it later …)

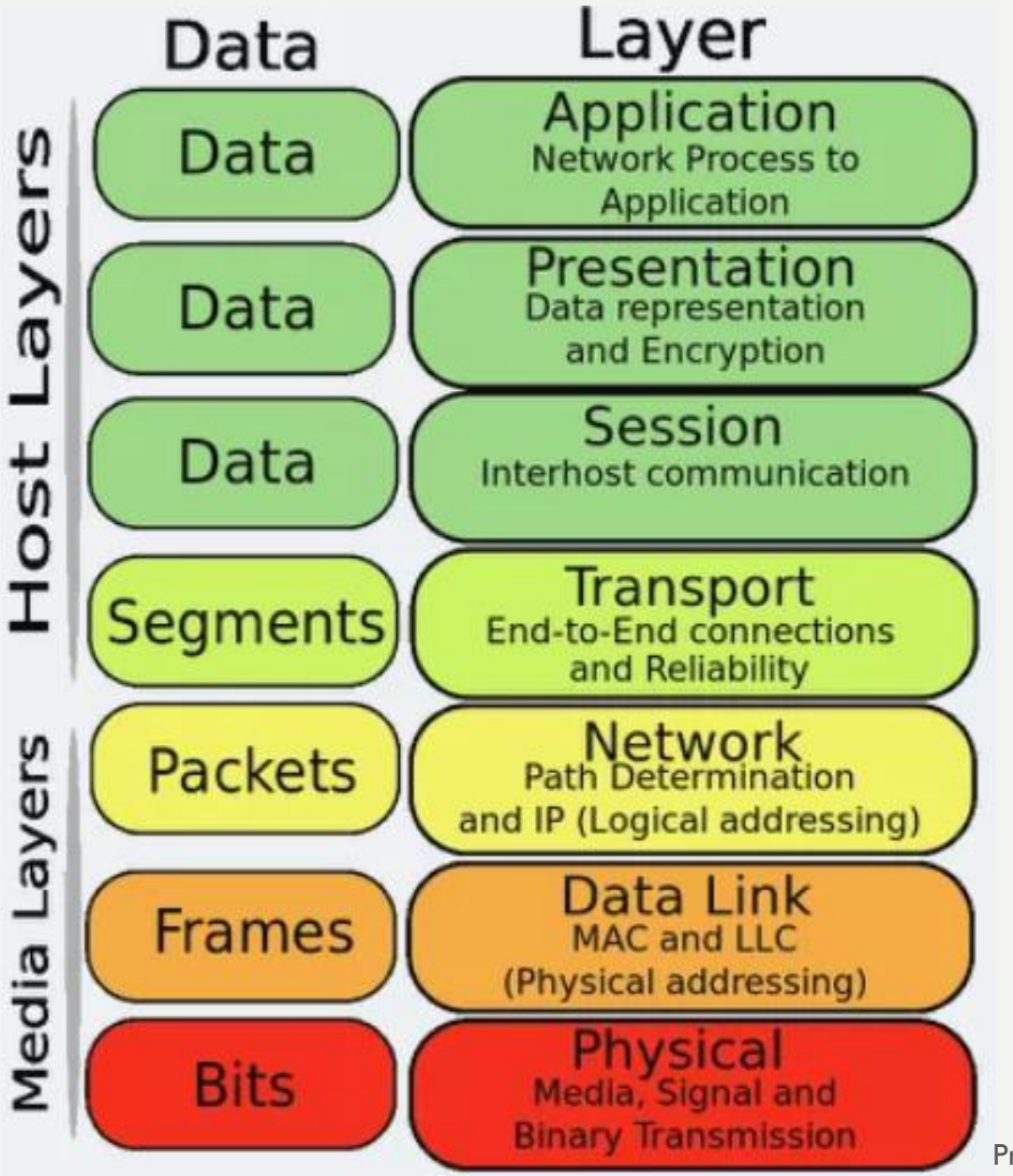


Client: HELLO	Server: READY
Client: NAME 051883261\n	Server: DAN HACKER\n
Client: GRADE MATH\n	Server: 87\n
Client: GRADE HISTORY\n	Server: 93\n
Client: END	Server: BYE

Design issues for the Network layers,

- Every layer needs a mechanism for **identifying senders and receivers.**
- The protocol must also determine **how many logical channels the connection corresponds to and what their priorities are**?
- **Error control is an important issue** because physical communication circuits are not perfect.
- Not all communication channels **preserve the order of messages sent** on them.
- An issue that occurs at every level is how to **keep a fast sender from swamping a slow receiver with data.**
- Another problem that must be solved at several levels is the **inability of all processes to accept arbitrarily long messages.**
- **Multiplexing is needed in the physical layer**, for example, where all the traffic for all connections has to be sent over at most a few physical circuits.
- When there are **multiple paths between source and destination**, a route must be chosen.

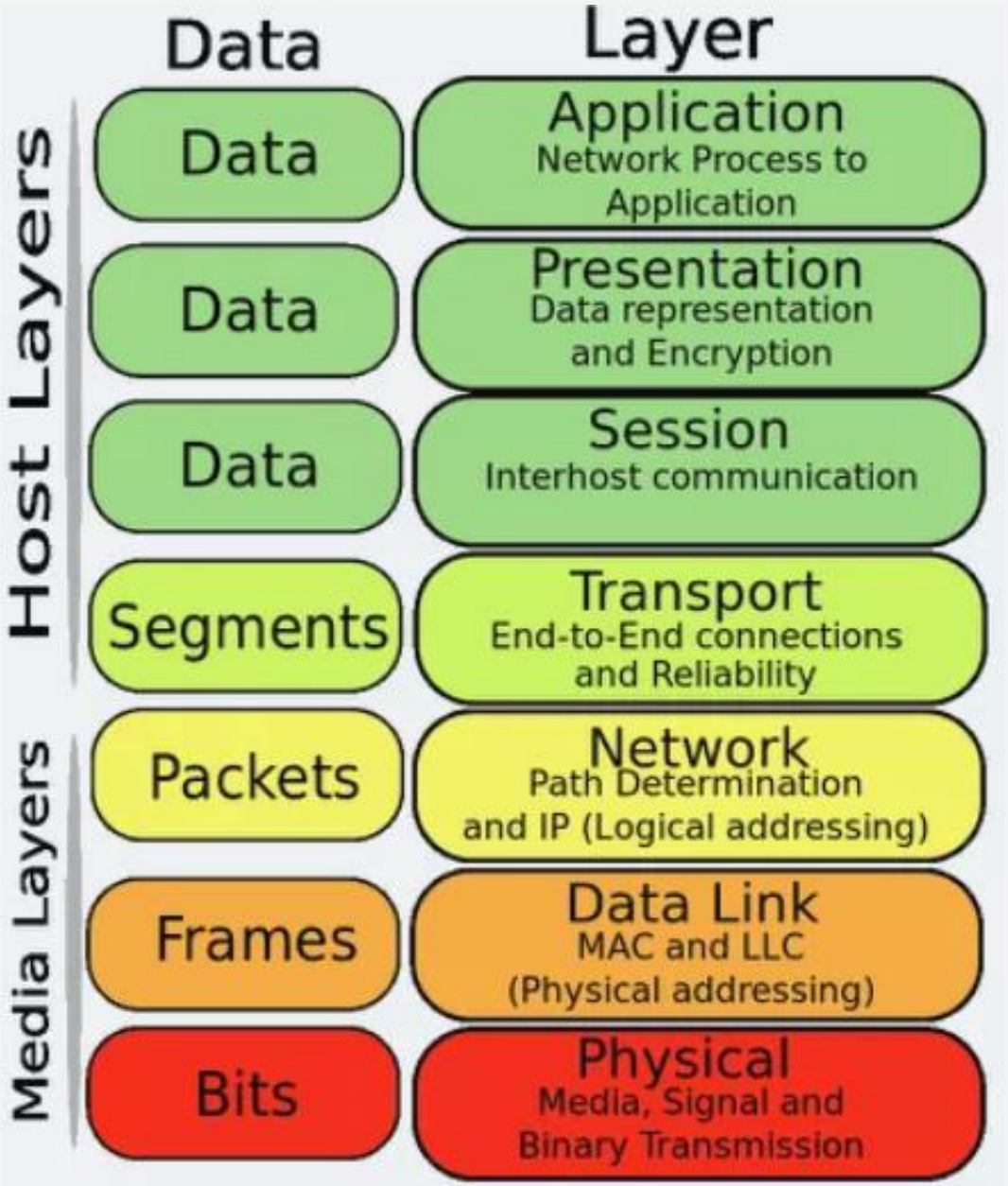
The OSI reference model



- Open Systems Interconnection (OSI)
- Proposed by the International Standards Organization (ISO)
- The OSI model has **seven layers**

- The **physical layer** is concerned with transmitting raw bits over a communication channel.
- **Data Link layer** is responsible for the error-free transfer of data frames. It defines the format of the data on the network.
- **Network Layer** determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.

The OSI reference model



- The **Transport layer** is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The **Session layer** is used to establish, maintain and synchronizes the interaction between communicating devices.
- A **Presentation layer** is mainly concerned with the syntax and semantics of the information
- An **Application layer** serves as a window for users and application processes to access network service.

The Physical layer (OSI)

- The main functionality of the physical layer is to **transmit the individual bits from one node to another node.**
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer

- **Line Configuration**: It defines the way how two or more devices can be connected physically.
- **Data Transmission** : It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology** : It defines the way how network devices are arranged.
- **Signals**: It determines the type of the signal used for transmitting the information.

Data Link layer (OSI)

- **Encoding** and **decoding** of **data frames into bits** (as the physical layer may use waves or other type of media). At the receiving side: Collects a stream of bits into a larger aggregate called a frame.
- **Segmentation** of upper layer **datagrams (packets) into frames** in sizes that can be handled by the communications hardware
- Takes care of any errors in the physical layer (electricity presence, voltage drop, no power, connection, etc.)
- Provides **reliable transit of the data** through a physical network
- **Synchronization** of various physical devices that will transmit the data
- It makes sure that the **frames are transferred in correct order** and asks for retransmission in case of error
- The **frame formatting issues such as stop and start bits**, bit order, parity and other functions are handled here. Management of big-endian/little-endian issues are also managed at this layer.
- Usually **implemented on Hardware** (network interface card):

Network Layer (OSI)

- Provide **switching technologies** and **routing technologies.**
- It is the network layer's job to figure out the network topology, **handle routing** and to **prepare data for transmission**.
- **Establishes the route** between the sending and receiving nodes for data transmission.
- **Encapsulation** of transport data into network layer protocol data units.
- Also responsible for **handling errors, packet sequencing, controlling network congestion** and **addressing.**
- In short: this layer is responsible for the **setting up the required network for transferring data from one node to other**

Transport Layer (OSI)

- Responsible for **delivering the data or the messages** between the two nodes.
- **Divide the data in packets** at the sender side.
- **Re-assemble packets** at the receiver side
- Third task: **error free data transmission**
- Uses checksums for **error correction or rejection**
- **Drop corrupt packets** and requests retransmission
- Fourth task: **guarantee data integrity**
- **Make sure all packets have arrived**
- UDP, SPX, TCP are some of the protocols that operate on this layer with one exception: UDP is unreliable

Session Layer (OSI)

- In practice, this layer is often not used or services within this layer are sometimes incorporated into the transport layer.
- Establishing, maintaining and terminating the connection between two end nodes (not used in TCP/IP)
- Controls the communication between the source user and the destination user and also decides the time of communication
- It determines **one-way or two-way communications** and manages the dialog between both parties; for example, making sure that the previous request has been fulfilled before the next one is sent
- Any error report related to application layer, presentation layer and session layer, are provided by this layer

Presentation Layer (OSI)

- Convert the data into a format that could be easily recognized by the application layers of other end users.
- For example: translation between ASCII and EBCDIC machines as well as between different floating point and binary formats. Integer size (16,32, or 64 bit?). Floating point representations.
- Compression/decompression, conversion, encryption/decryption, coding, decoding, etc.
- Converts the data obtained from the application layer into a format that can be easily identified by other network layers

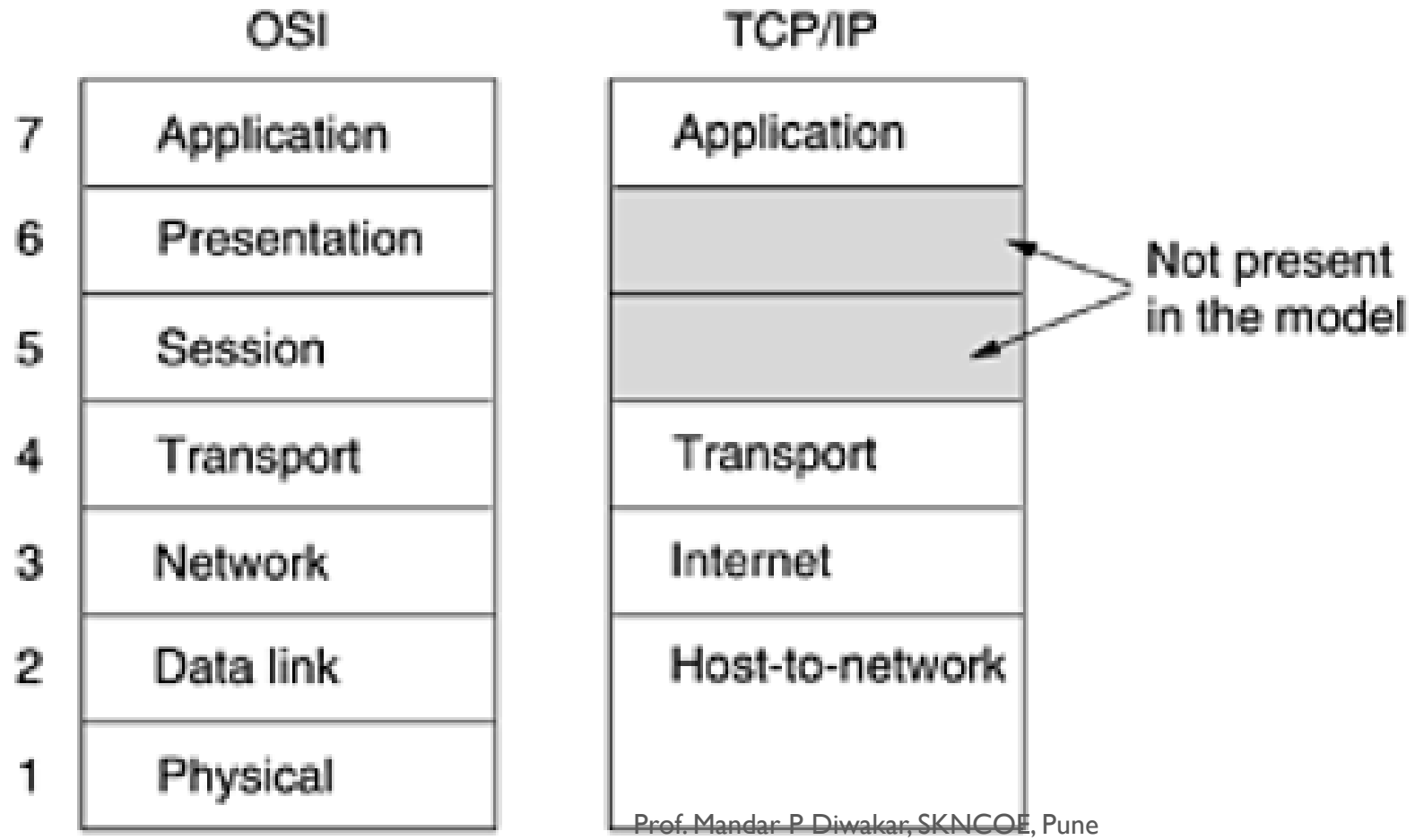
Application Layer (OSI)

- The closest layer to the user: Outlook, Explorer, Firefox, Skype (HTTP, POP, SMTP, FTP, TELNET).
- In this layer that a user interacts with the software application that does data transfer
- **The main tasks:**

- Identify/authenticate the user who wants to communicate
- Determine whether the data and networks sources are available
- Synchronize communication between the two nodes

TCP/IP Model

- TCP/IP model has been developed much later after OSI model.
- OSI was developed as theoretical model, while TCP/IP was more practical.
- TCP/IP is having just four layers in oppose to seven layers of OSI.



The Internet Layer (TCP/IP)

- The Internet layer is responsible for logical transmission of data packets over the internet. It can be compared to the network layer of the OSI model.
- **The main functions of the internet layer are −**
- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- It reassembles the out-of-order packets when they reach the destination.
- It handles the error in transmission of data packets and fragmentation of data packets..

The Transport Layer (TCP/IP)

- The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host.
- It corresponds to the transport layer of the OSI model.
- **The functions of the transport layer are −**

- It facilitates the communicating hosts to carry on a conversation.
- It provides an interface for the users to the underlying network.
- It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.

The Application Layer (TCP/IP)

- The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.
- **The functions of the application layer are −**

- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
- It is also concerned with error handling and recovery of the message as a whole.

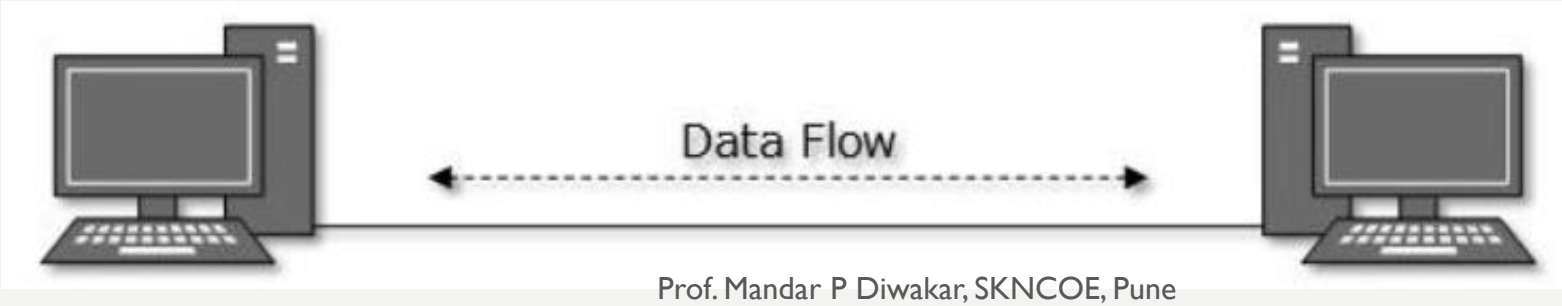
The Host-to-Network Layer (TCP/IP)

- The host-to-network layer is the lowest layer of the TCP/IP model and is concerned with the physical transmission of data. It is also called a network interface layer or link layer. It can be considered as the combination of physical layer and data link layer of the OSI model.
- **The functions of this layer are −**

- It defines how bits are to be encoded into optical or electrical pulses.
- It accepts IP packets from the network layer and encapsulates them into frames. It synchronizes the transmission of the frames as well as the bits making up the frames, between the sender and the receiver.
- It states the transmission mode, i.e. simplex, half duplex or full duplex
- It states the topology of the network, i.e. bus, star, ring etc.

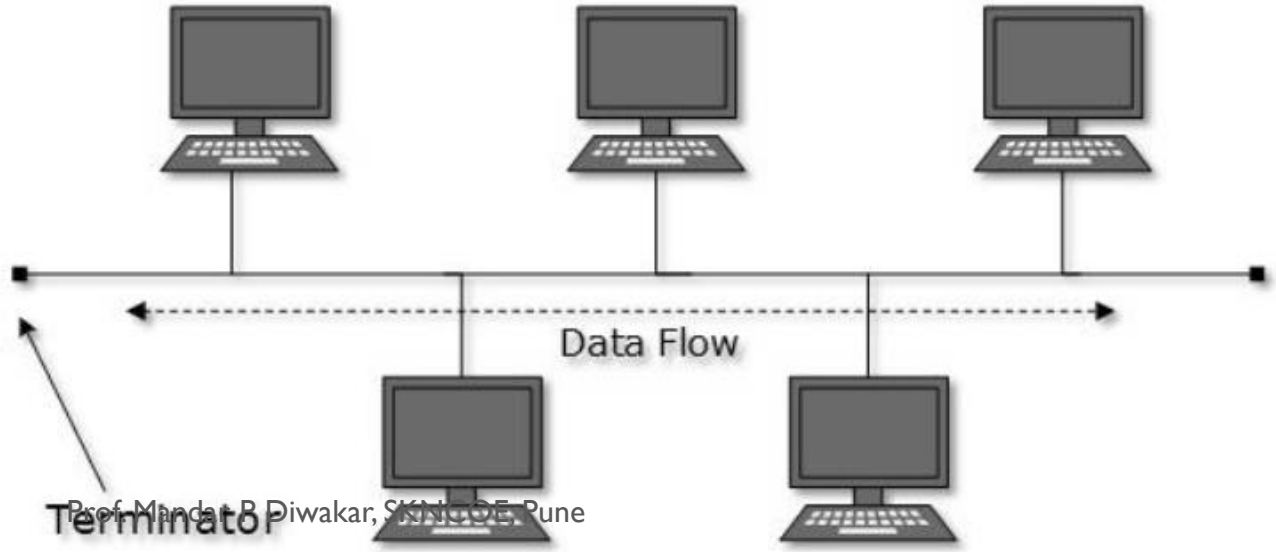
COMPUTER NETWORK TOPOLOGIES

- A **Network Topology** is the arrangement with which computer systems or network devices are connected to each other.
- **Topologies** may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.
- **Point-to-Point**
- Point-to-point networks contains exactly two hosts such as computer, switches, routers, or servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice versa.



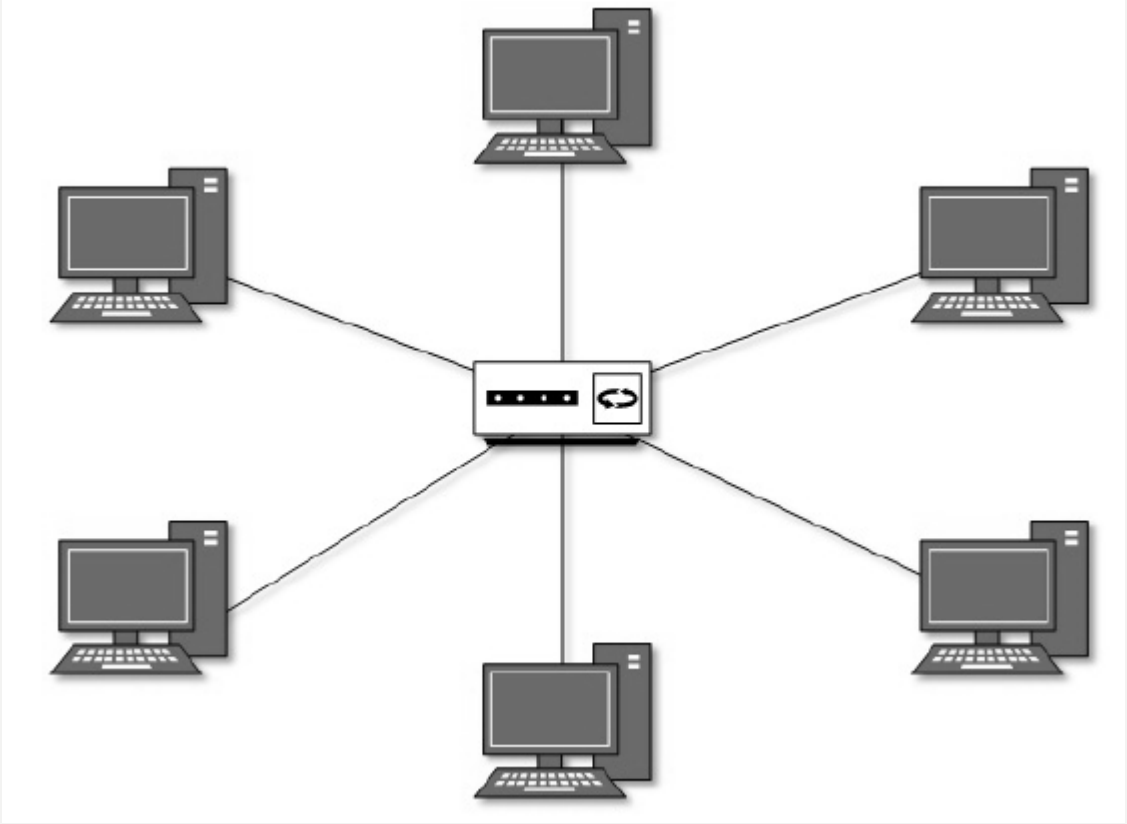
Bus Topology

- In case of Bus topology, all devices share single communication line or cable.
- Bus topology may have problem while multiple hosts sending data at the same time.
- Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



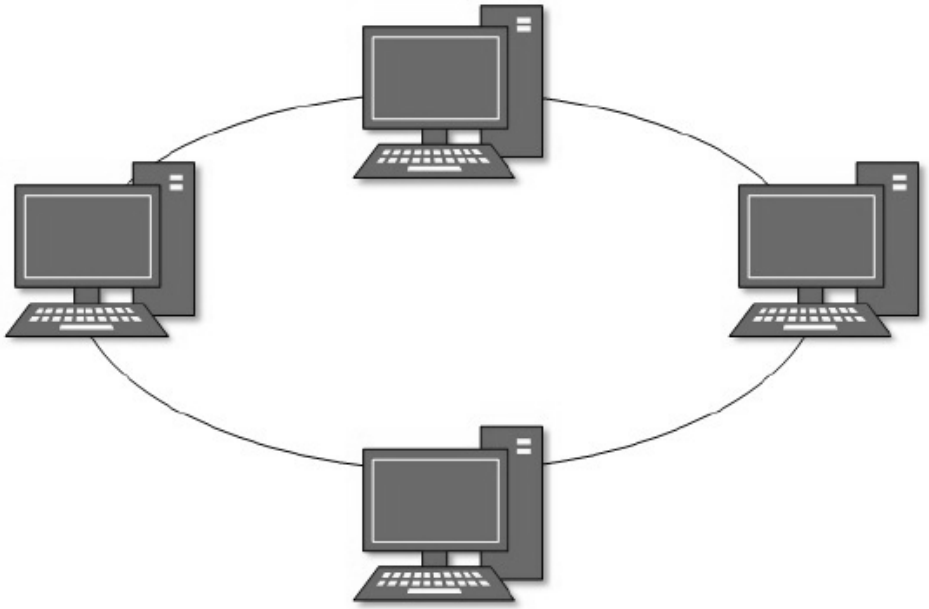
Star Topology

- All hosts in Star topology are connected to a central device, known as hub/switch device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub.
- If hub fails, connectivity of all hosts to all other hosts fails.
- Every communication between hosts takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.



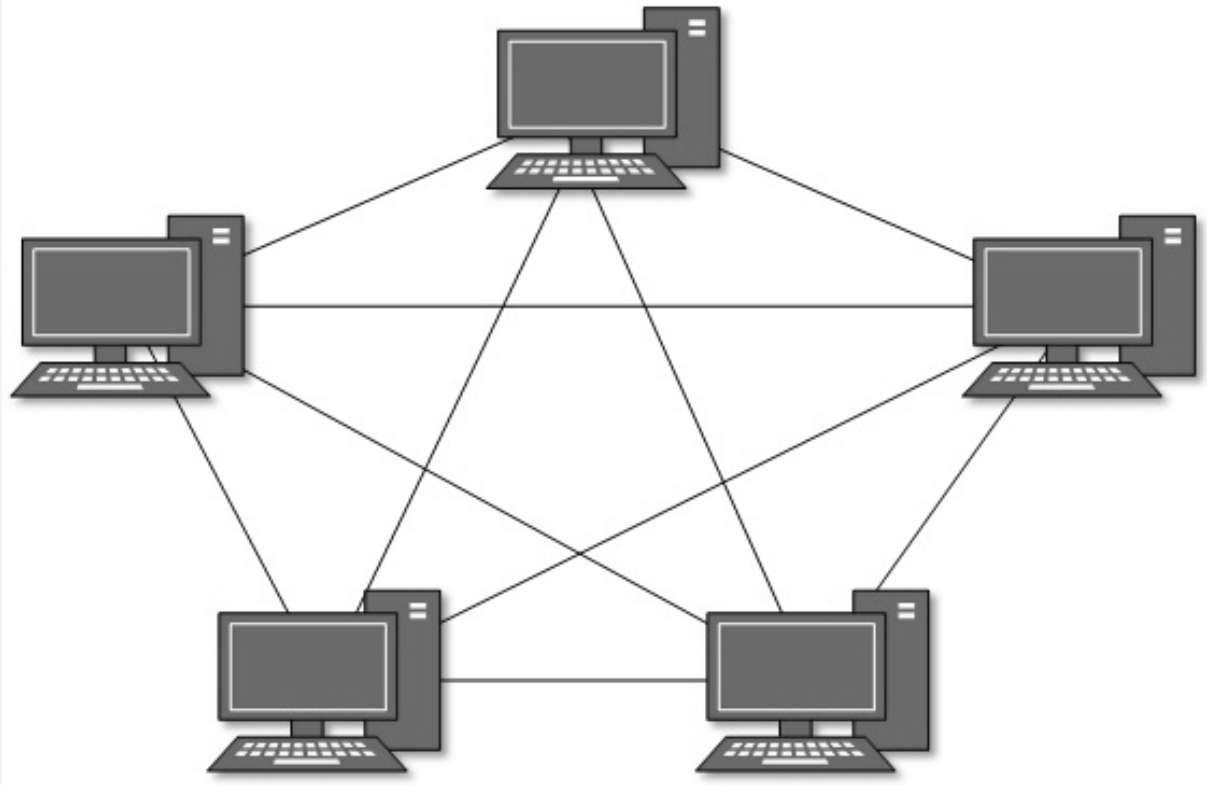
Ring Topology

- In ring topology, each host machine connects to exactly two other machines, creating a circular network structure.
- When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts.
- To connect one more host in the existing structure, the administrator may need only one more extra cable.
- Failure of any host results in failure of the whole ring.
- Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.



Mesh Topology

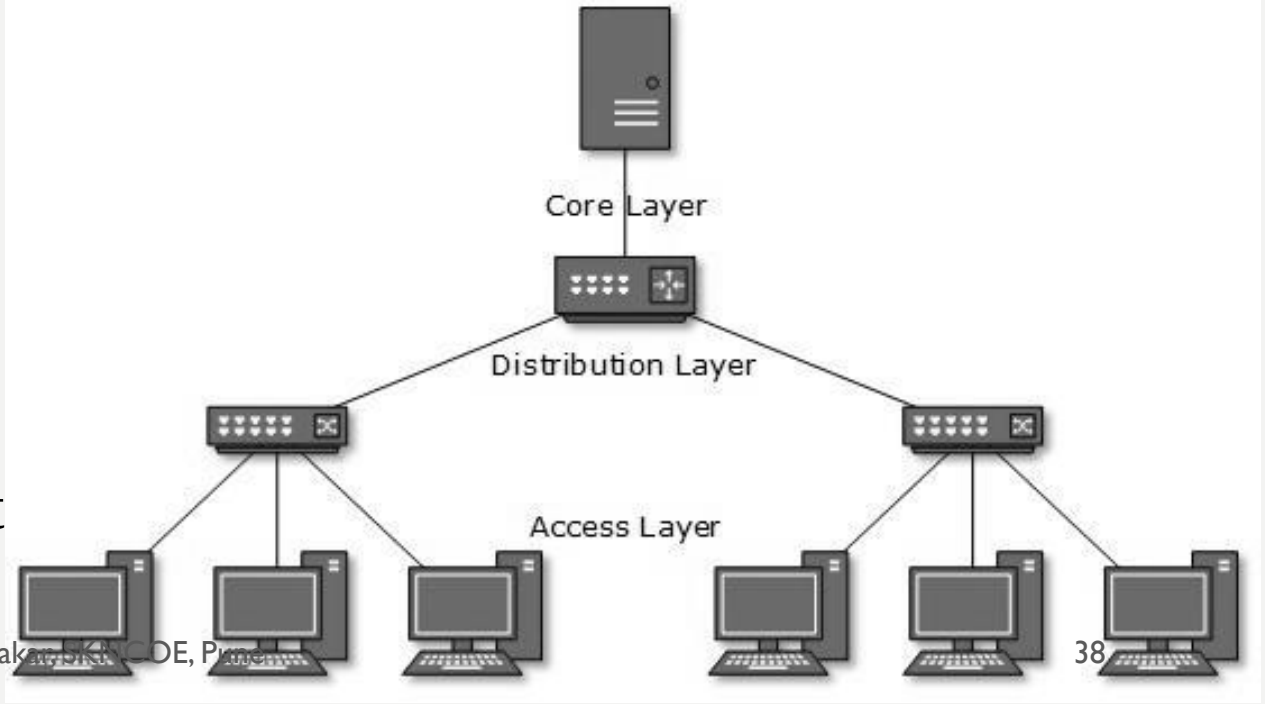
- In this type of topology, a host is connected to one or multiple hosts.
- This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection with few hosts only.
- All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required
- It provides the most reliable network structure among all network topologies.



Tree Topology

- Also known as Hierarchical Topology, this is the most common form of network topology in use presently.
- This topology imitates as extended Star topology and inherits properties of Bus topology.
- This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices.

- The lowermost is access-layer where computers are attached.
- The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer.
- The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



Transmission Media

- **Transmission media** is a pathway that carries the information from sender to receiver.
- We use different types of cables or waves to transmit data.
- Data is transmitted normally through electrical or electromagnetic signals.
- An electrical signal is in the form of **current**.
- An electromagnetic signal is series of **electromagnetic energy pulses** at various **frequencies**.
- These signals can be transmitted through **copper wires, optical fibers, atmosphere, water and vacuum.**
- Different Medias have different properties like **bandwidth, delay, cost and ease of installation and maintenance.**
- Transmission media is also called **Communication channel.**

Types of Transmission Media

1. Wired or Guided Media or Bound Transmission Media

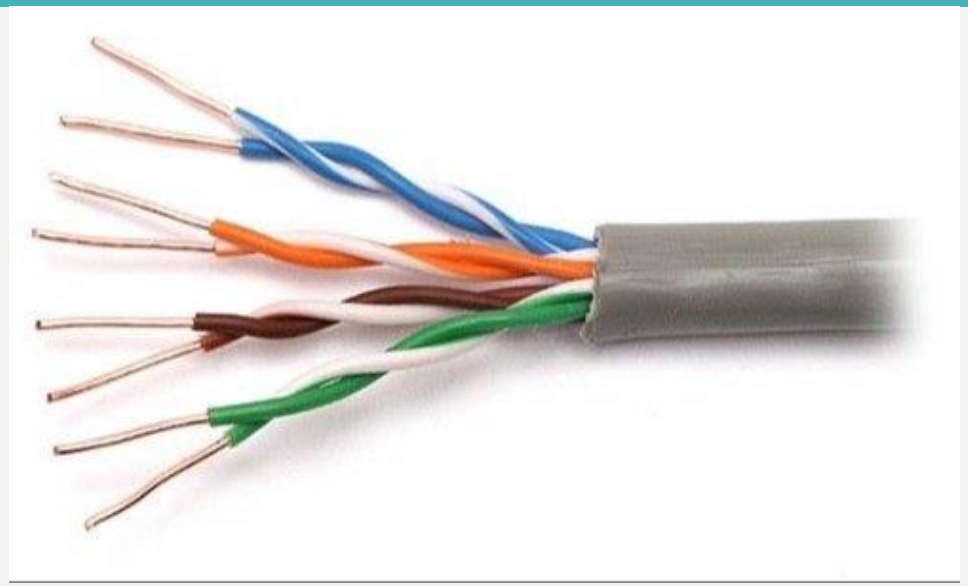
- Twisted Pair Cable
- Coaxial Cable
- Fiber Optic Cable

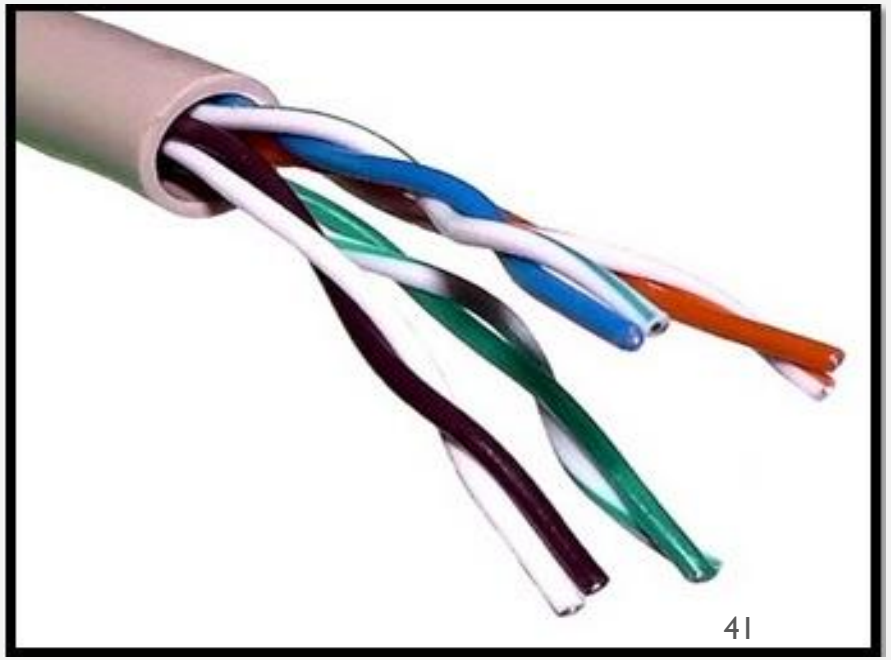
2. Wireless or Unguided Media or Unbound Transmission Media

- Radio Waves
- Microwaves
- Infrared Waves

Twisted pair cable

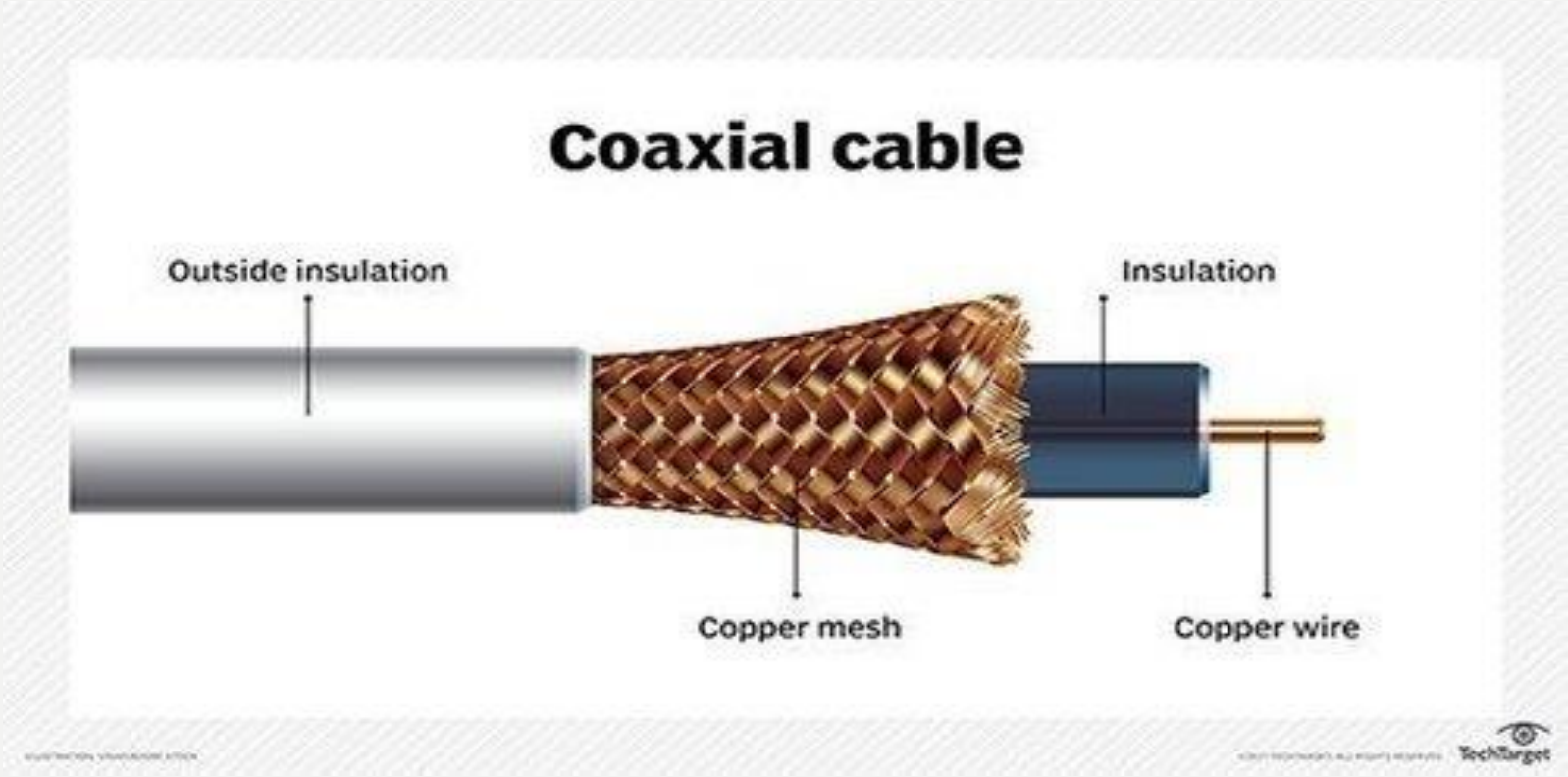
- **A twisted pair cable** comprises of two separate insulated copper wires, which are twisted together and run in parallel.
- The copper wires are typically 1mm in diameter.
- One of the wires is used to transmit data and the other is the ground reference.
- When the wires are **twisted**, some part of the noise signals is in the direction of data signals while the other parts are in the opposite directions.
- Thus the external waves cancel out due to the different twists.





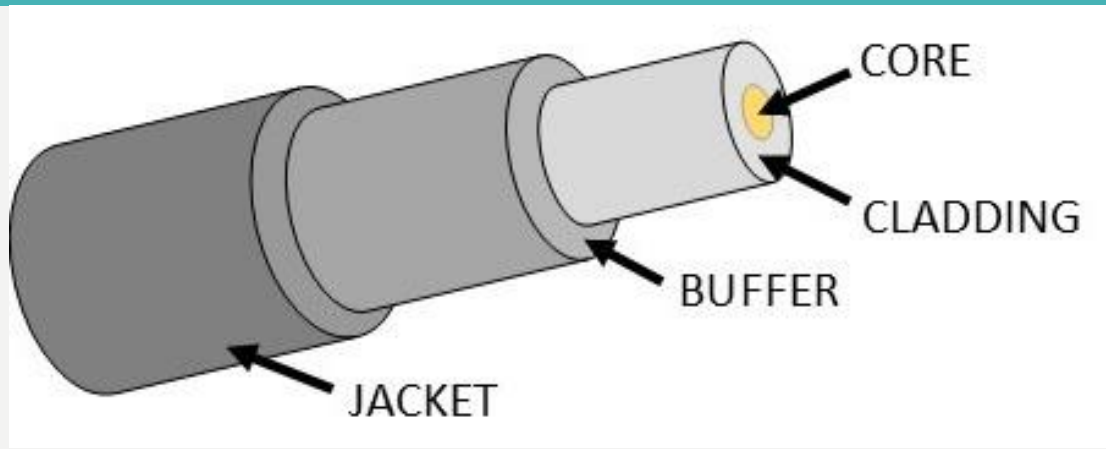
Co-axial Cables

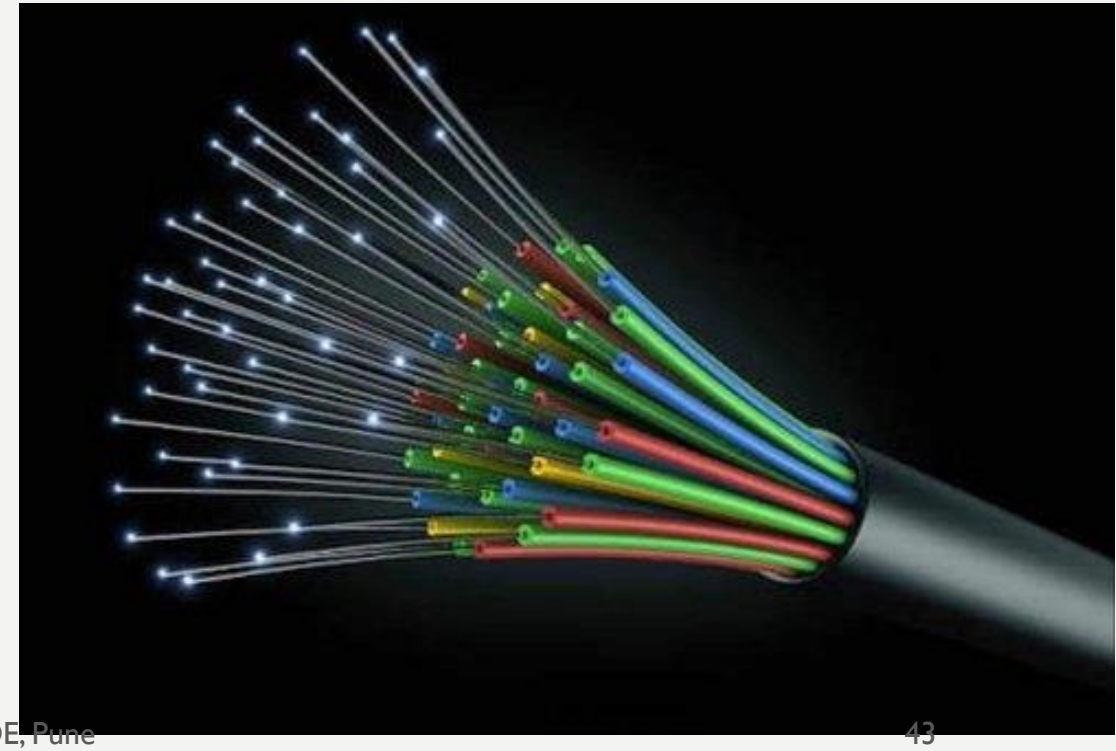
- **Co-axial** includes a central copper wire surrounded by PVC insulation over which a copper mesh sleeve is placed.
- Again, the **metal sleeve** is shielded by an **outer shield** of thick PVC material, as shown in the figure**.**
- It has a huge bandwidth and low losses.
- This cable is appropriate for point to point or point to multipoint software. This is the most broadly used medium for local area networks.
- These cables are valuable than twisted-pair cables, but they are economical than optical fiber cables.



Fiber optic cabling

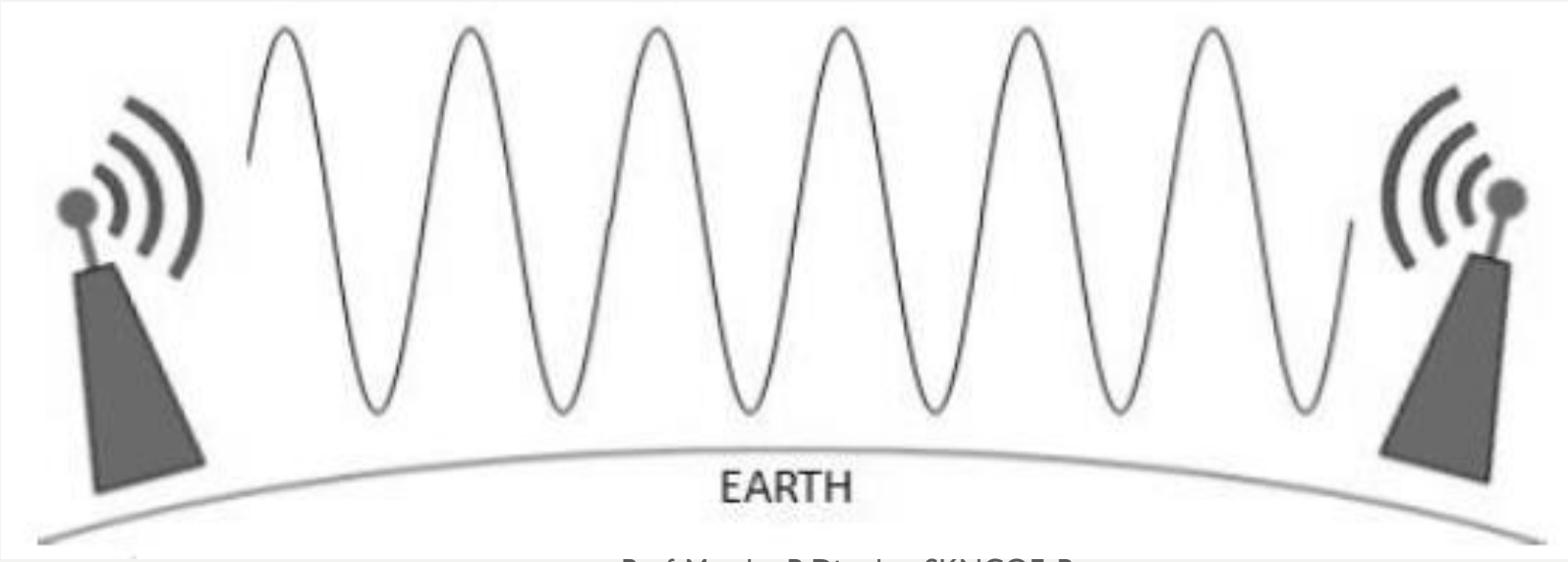
- A **fiber optic** cable is made of glass or plastic and transmits signals in the structure of light signals.
- The structure of an **optical fiber cable** is displayed in the figure.
- It involves an inner glass core surrounded by a glass cladding that reflects the light into the core.
- Each **fiber** is encircled by a plastic jacket.
- **Fiber optic cabling** can support too high bandwidths in the range from 100 Mbps to 2 gigabytes and more because light has a much greater frequency than electricity.





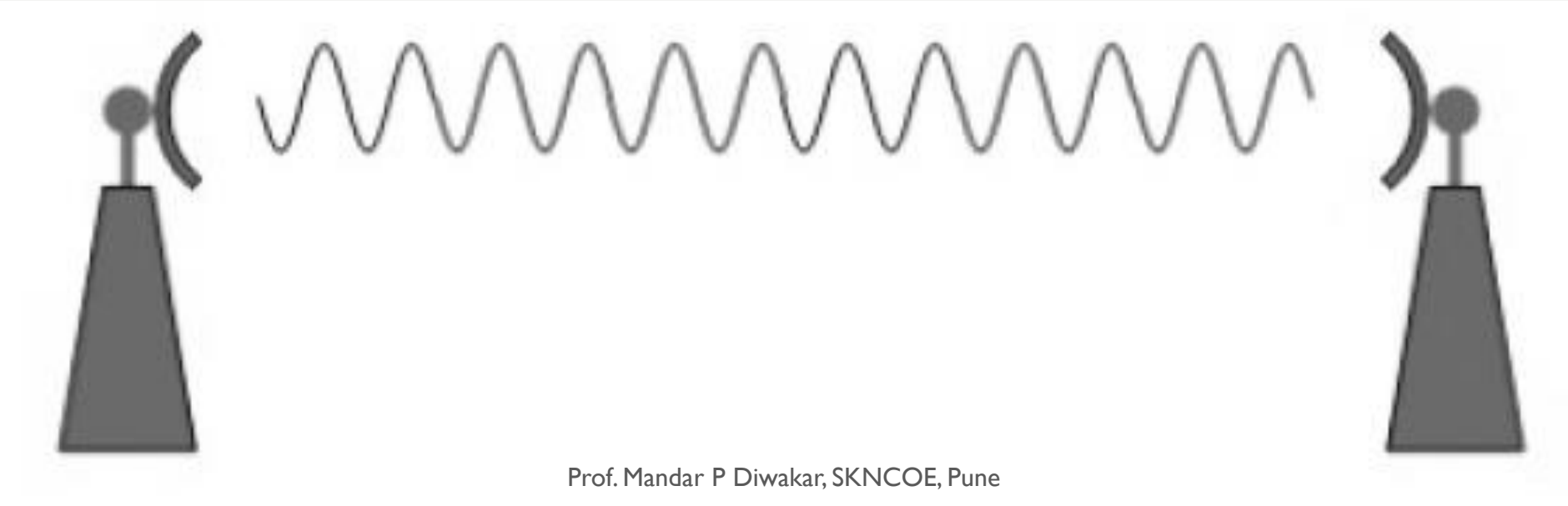
Radio Transmission

- Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.
- These are easy to generate and can penetrate through buildings.
- The sending and receiving antennas need not be aligned.
- Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



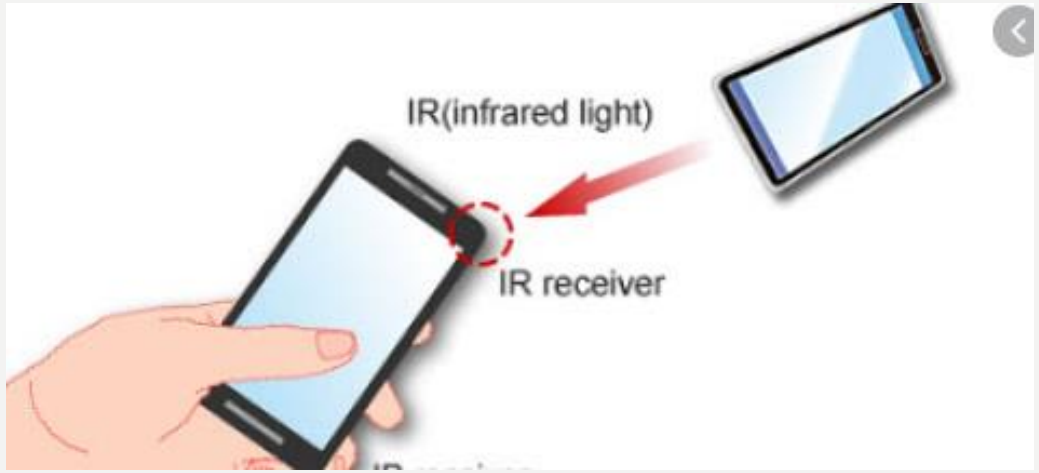
Microwave Transmission

- It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other.
- The distance covered by the signal is directly proportional to the height of the antenna.
- Frequency Range:1GHz – 300GHz.
- These are majorly used for mobile phone communication and television distribution.



Infrared Transmission

- Infrared wave lies in between visible light spectrum and microwaves.
- It has wavelength of 700nm to 1mm and frequency ranges from 300GHz to 430THz.
- Infrared wave is used for very short range communication purposes such as television and its remote.
- Infrared travels in a straight line hence it is directional by nature.
- Because of high frequency range, Infrared cannot cross wall-like obstacles.



Network Architectures

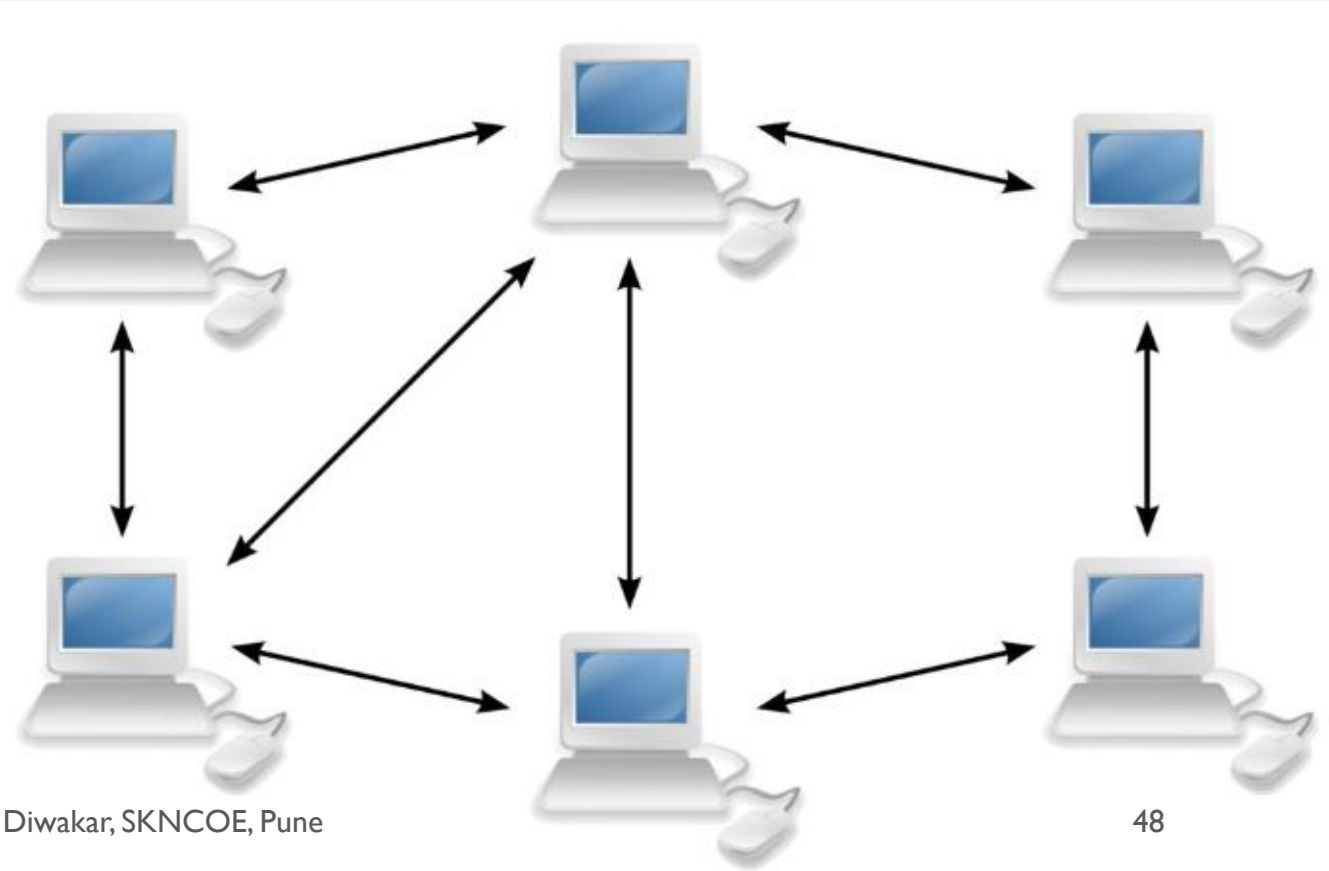
- Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
- Simply we can say that how computers are organized and how tasks are allocated to the computer.

- The two types of network architectures are used:

- Peer-To-Peer network
- Client/Server network
- Hybrid.

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.
- If one computer stops working but, other computers will not stop working.
- it does not contain the centralized system Therefore, it cannot back up the data as the data is different in different locations.

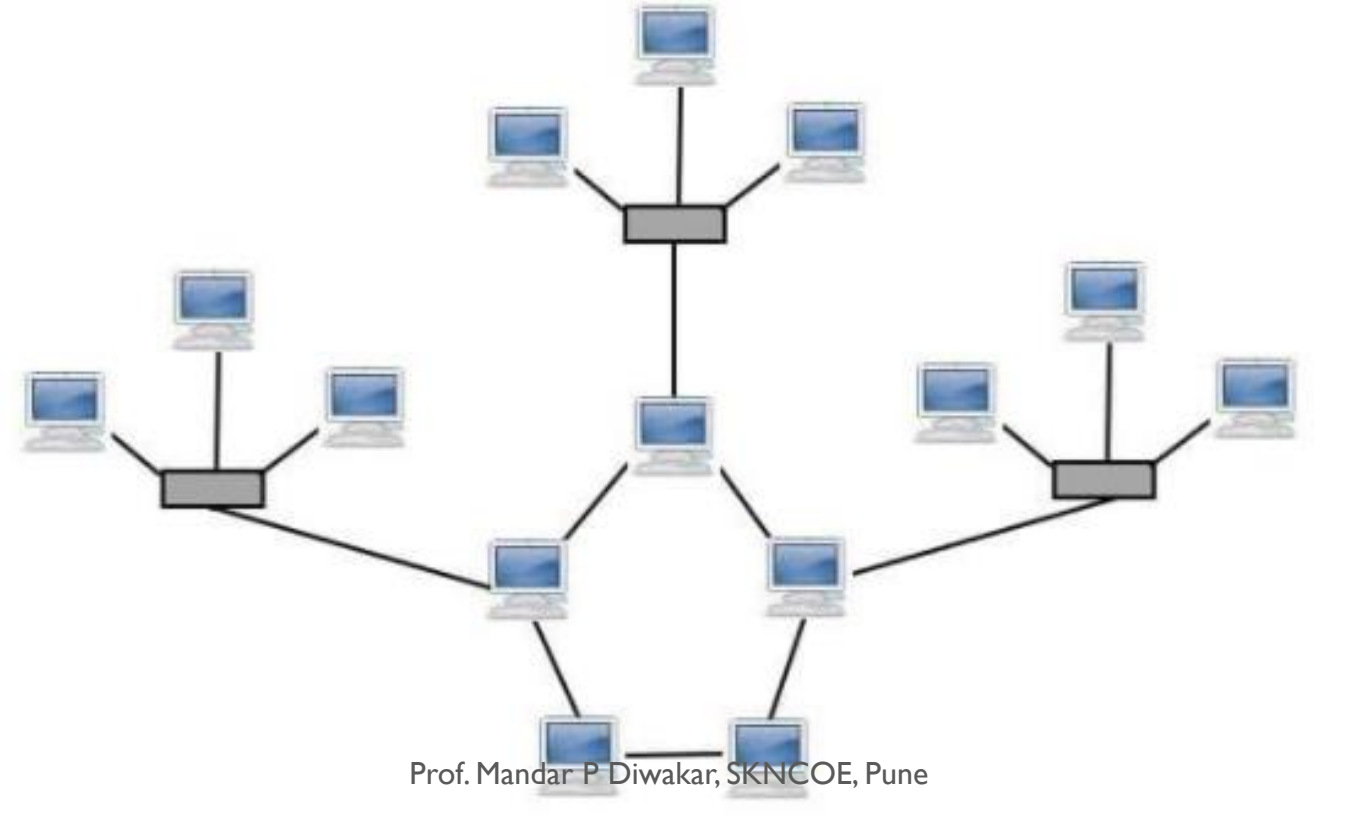


Client/Server network

- 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.
- 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.

Hybrid Network

- A hybrid topology is a kind of network that is a combination of two or more network topologies, such as mesh topology, bus topology, and ring topology.
- Its usage and choice are dependent on its deployments and requirements like the performance of the desired network, and the number of computers, their location.
- The below figure is describing the structure of hybrid topology that contains more than one topology.



Network Devices

- Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices.
- These devices transfer data in a fast, secure and correct way over same or different networks.
- Network devices may be inter-network or intra-network.
- Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

- Hub.
- Switch.
- Router.
- Bridge.
- Gateway.
- Modem.
- Access Point.

NIC (Network interface card)

- A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network.
- It is a circuit board installed in a computer that provides a dedicated network connection to the computer.
- It is also called network interface controller, network adapter or LAN adapter.

- **Purpose**

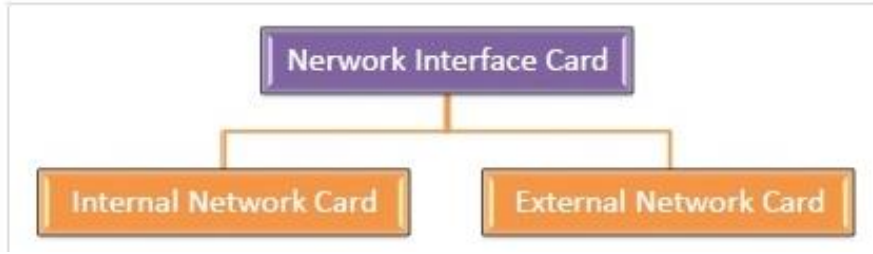
1. NIC allows both wired and wireless communications.
2. NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
3. NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

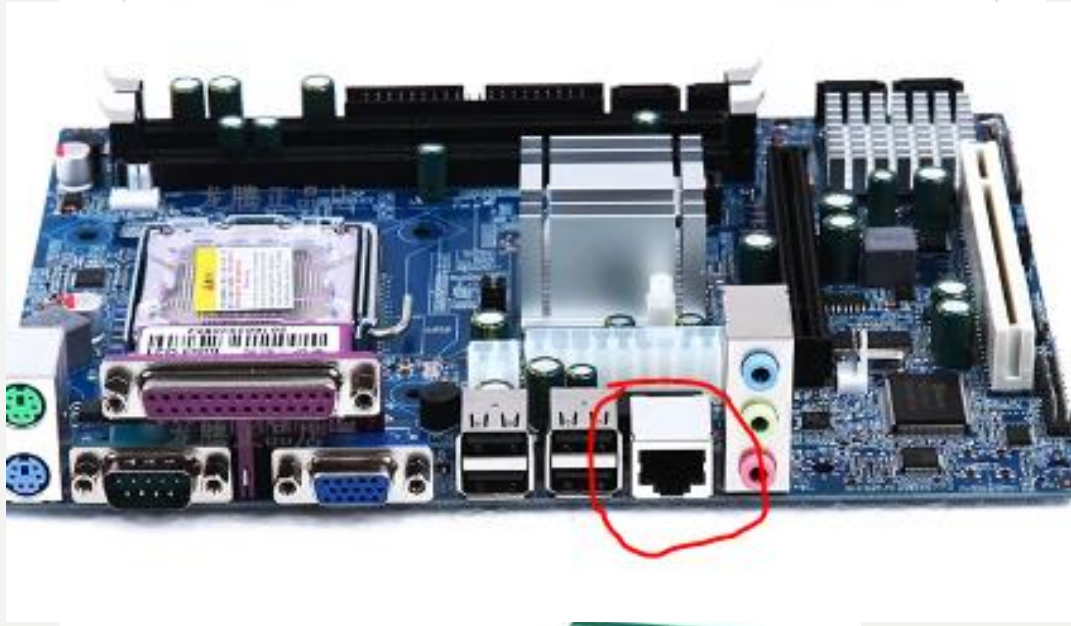
NIC (Network interface card)

Types of NIC Cards

Internal Network Cards

- In internal networks cards, motherboard has a slot for the network card where it can be inserted.
- It requires network cables to provide network access.
- Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).





NIC (Network interface card)

Types of NIC Cards

External Network Cards

- In desktops and laptops that do not have an internal NIC, external NICs are used.
- External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

NIC (Network interface card)

Types of NIC Cards

Wireless Network NIC

- Wireless network NIC cards consist of a small antenna integrated onto the card, where the communication between various devices is set up wirelessly using the router and various network protocols.
- It is usually connected to a wireless radio-based computer network and under this type of NIC cables are not necessary for connectivity of various devices. Rather than cables, radio waves are used for the same.
- For a wireless network to work there must be a router which has antennae that enables connectivity. A router is the main thing under making a wireless network connection

NIC (Network interface card)

RJ45

- RJ45 is a type of connector commonly used for Ethernet networking.
- Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires.
- The "RJ" in RJ45 stands for "registered jack," since it is a standardized networking interface. The "45" simply refers to the number of the interface standard.
- Ethernet cables have an RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables.

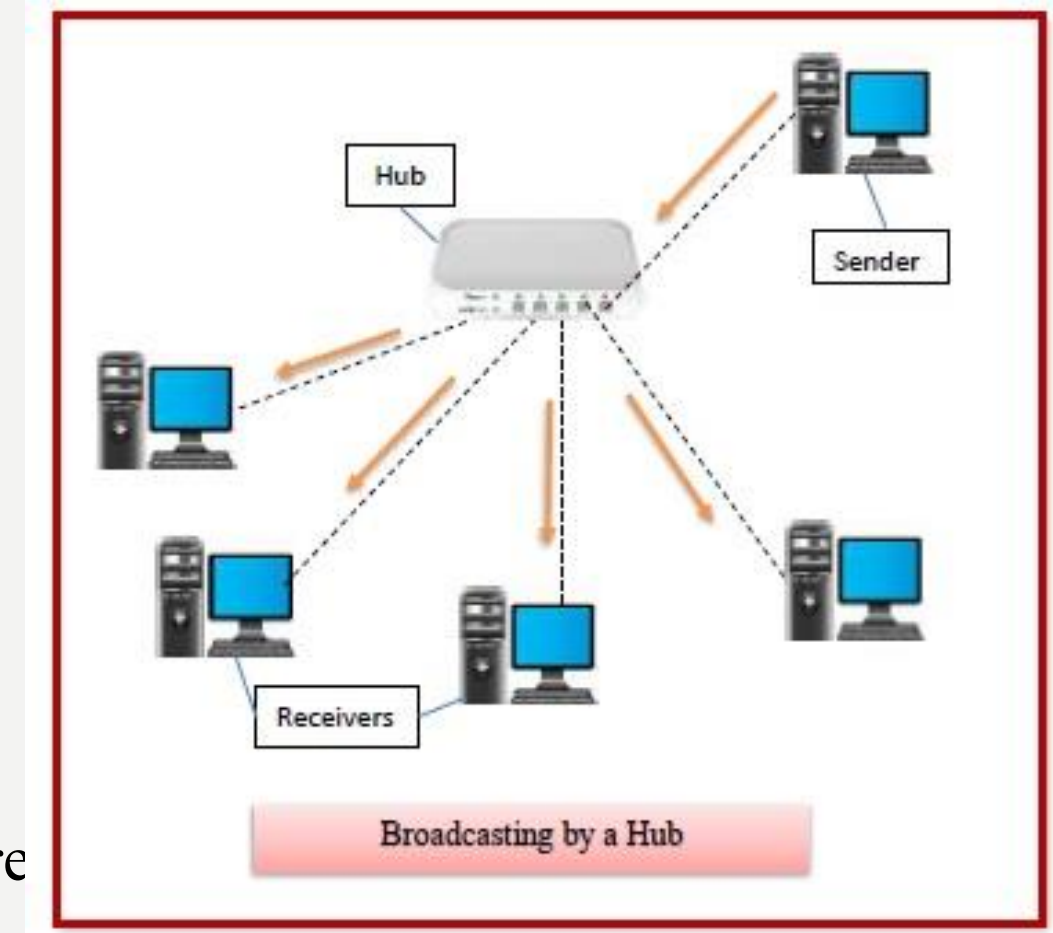
HUB

- Hubs are networking devices operating at a physical layer of the OSI model that are used to connect multiple devices in a network.
- They are generally used to connect computers in a LAN.
- A hub has many ports in it.
- A computer which intends to be connected to the network is plugged in to one of these ports.
- When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.

HUB

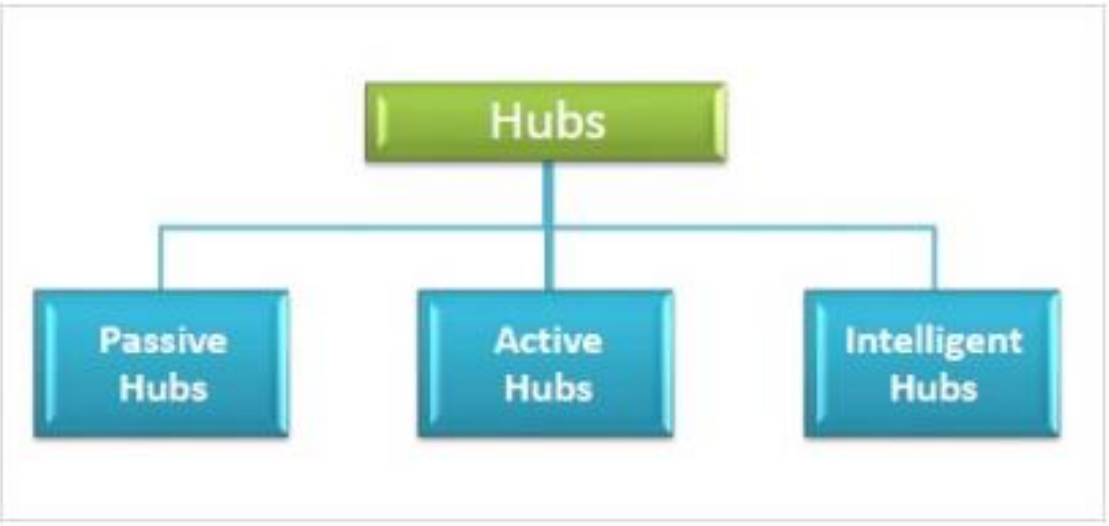
➢ Features of Hubs

1. A hub operates in the physical layer of the OSI model.
2. A hub cannot filter data.
3. It is a non-intelligent network device that sends message to all ports.
4. It primarily broadcasts messages.
5. Transmission mode is half duplex.
6. Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.
7. Since they lack intelligence to compute best path for transmission of data packets, inefficiencies and wastage occur.
8. They are passive devices, they don't have any software associated with it.
9. They generally have fewer ports of 4/12.



HUB

➢ Types of Hubs



1. **Passive Hubs** – Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.

2. **Active Hubs** – Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting center. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.

3. **Intelligent Hubs** – Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc.

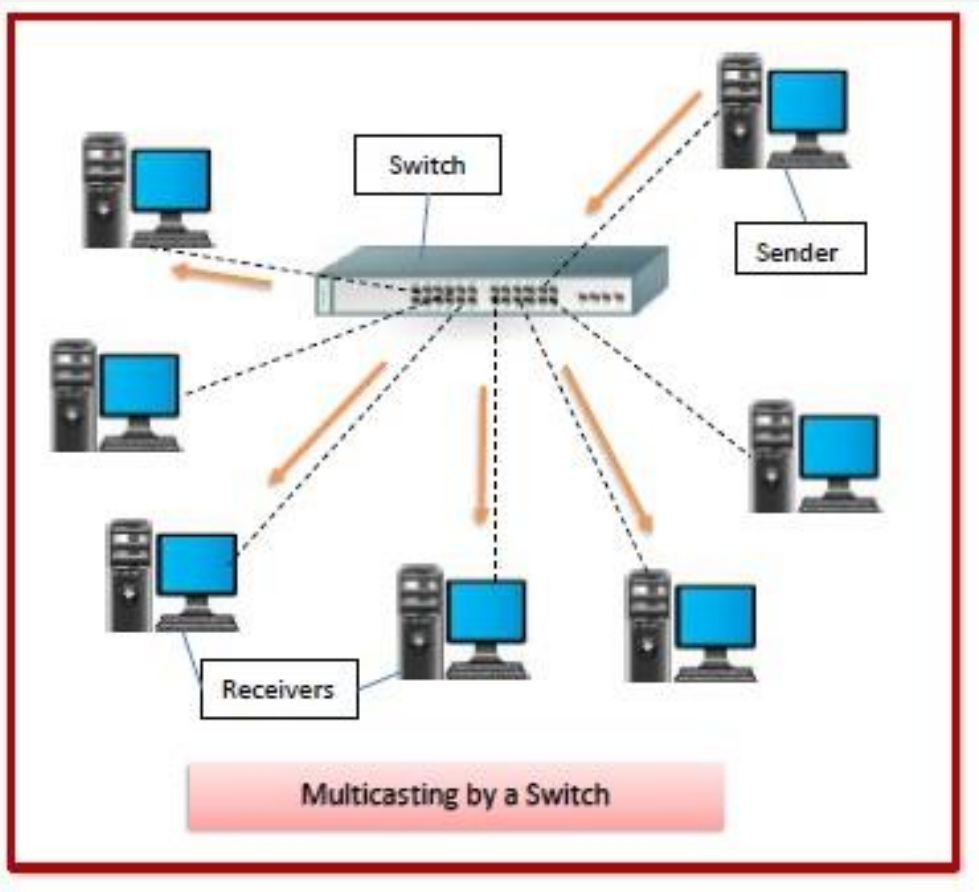
Switches

- Switches are networking devices operating at layer 2 or a data link layer of the OSI model.
- They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.
- A switch has many ports, to which computers are plugged in.
- When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).
- It supports unicast, multicast as well as broadcast communications.

Switches

Features of Switches

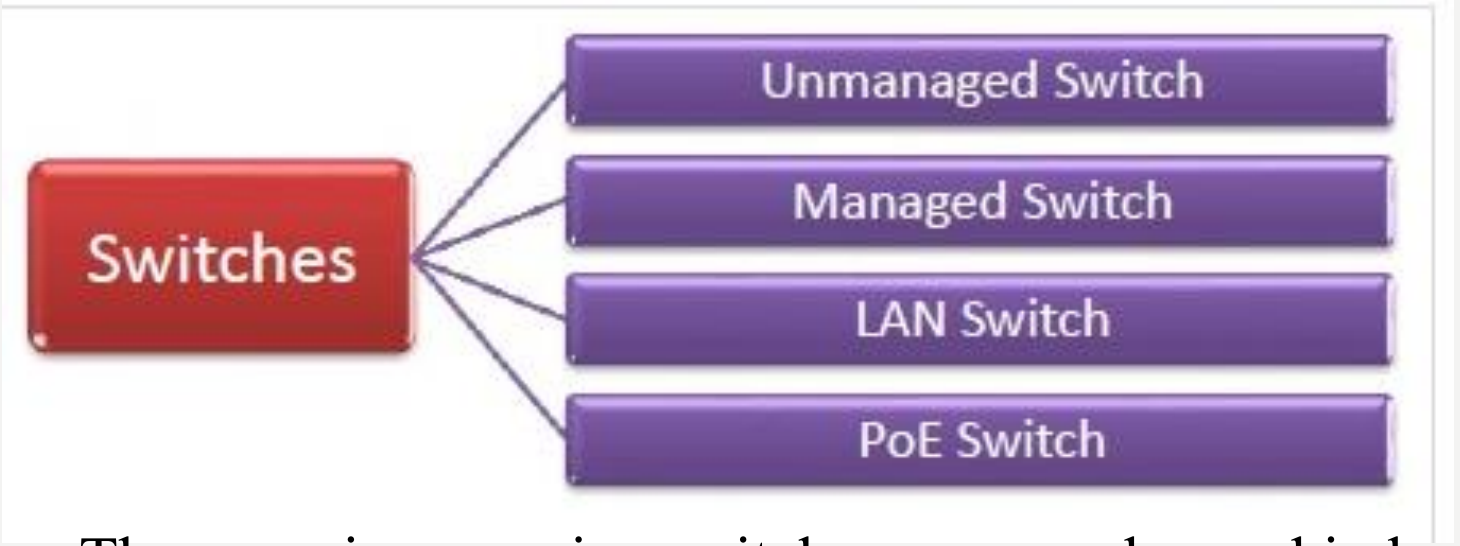
- A switch operates in the layer 2, i.e. data link layer of the OSI model.
- It is an intelligent network device that can be conceived as a multiport network bridge.
- It uses MAC addresses to send data packets to selected destination ports.
- It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
- Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.



- Switches are active devices, equipped with network software and network management capabilities.
- Switches can perform some error checking before forwarding data to the destined port.
- The number of ports is higher – 24/48

Switches

- **Types of Switches**



- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating. When more devices needs to be added, more switches are simply added by this plug and play method.

- **Managed Switch** − These are costly switches that are used in organizations with large and complex networks. They can be customized to augment the functionalities of a standard switch. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility.

Switches

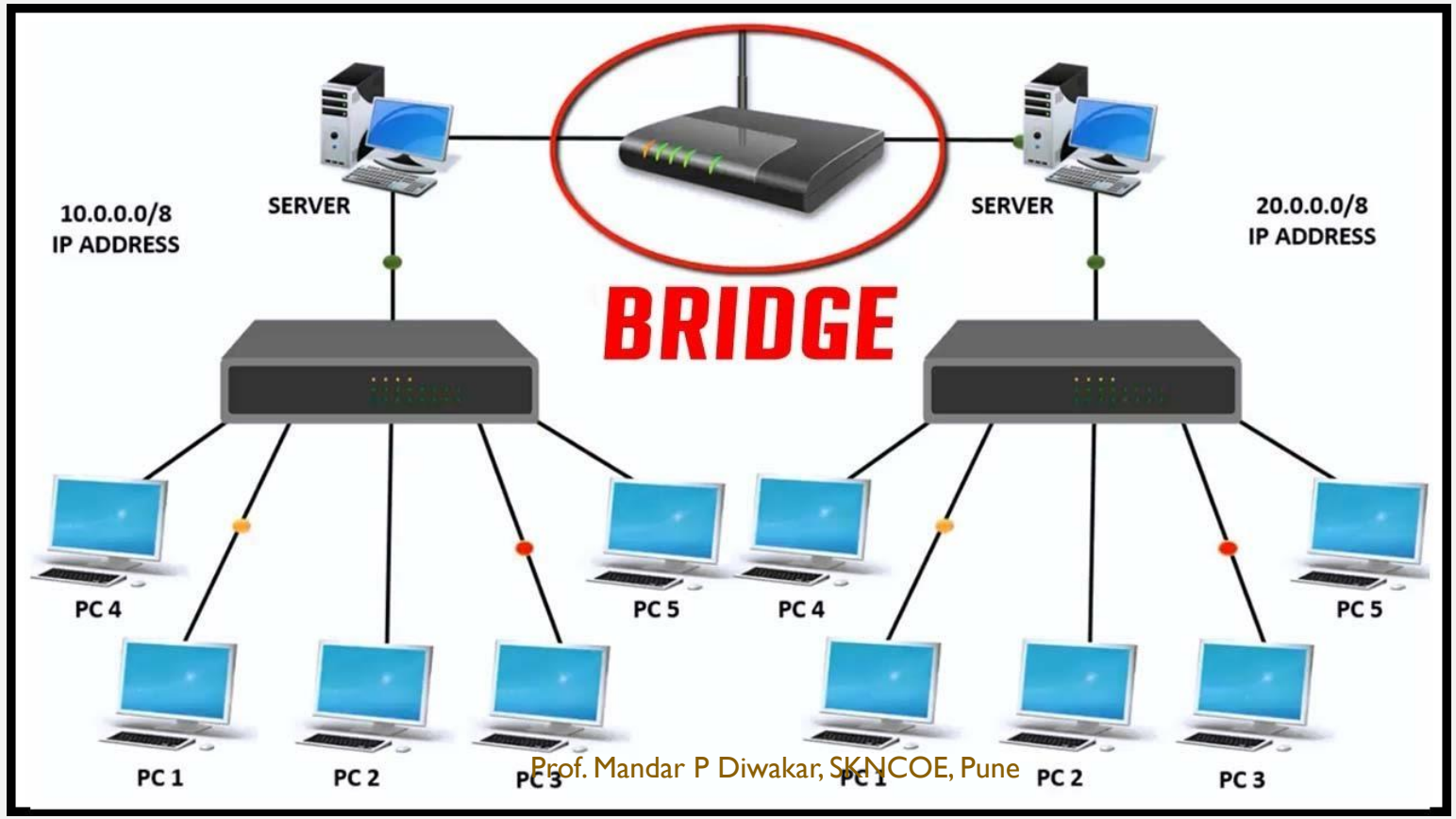
Types of Switches

- **LAN Switch** − Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.

- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line. PoE switches offer greater flexibility and simplifies the cabling connections

Bridges

- A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN.
- The process of aggregating networks is called network bridging.
- A bridge connects the different components so that they appear as parts of a single network.
- Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.



Bridges

- **Working Principle**

- The working principle of a bridge is, it blocks or forwards the data depending on the destination MAC address and this address is written into every data frame.
- In a computer network, a bridge separates a LAN into different segments like segment1 & segment2, etc. and the MAC address of all the PCs can be stored into the table.

- For instance, PC1 transmits the data to PC2, where the data will transmit to the bridge first. So the bridge reads the MAC address & decides whether to transmit the data to segment1 or segment2. Therefore, the PC2 is accessible in segment1, which means the bridge transmits the data in segment1 only & eliminates all the connected PCs in segment2. In this way, the bridge reduces traffic in a computer network.

Bridges

- **Functions of Bridges in Network**

- This networking device is used for dividing local area networks into several segments.
- In the OSI model, it works under the data link layer.
- It is used to store the address of MAC in PC used in a network and also used for diminishing the network traffic.

- **Advantages/Disadvantages of Bridge in Computer Network**

- It acts as a repeater to extend a network.
- Network traffic on a segment can be reduced by subdividing it into network communications Collisions can be reduced.
- Bridges increase the available bandwidth to individual nodes
- It avoids waste BW (bandwidth)
- The length of the network can be increased.
- Connects different segments of network transmission

Router

- Routers are networking devices operating at **layer 3** or a **network layer** of the **OSI model**.
- They are responsible for **receiving**, **analyzing**, and **forwarding** data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its **routing tables** to decide the **optimal route** and then transfers the packet along this route.

Router

➢ Features of Routers

1. A router is a layer 3 or network layer device.
2. It connects different networks together and sends data packets from one network to another.
3. A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
4. It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
5. Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
6. In order to prepare or refresh the routing table, routers share information among each other.
7. Routers provide protection against broadcast storms.
8. Routers are more expensive than other networking devices like hubs, bridges and switches.

Routers are manufactured by some popular companies like − **Cisco, D-Link, HP, 3Com, Juniper & Nortel**

Router

- **Routing Table**
- The functioning of a router depends largely upon the routing table stored in it.
- The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent.
- **A routing table typically contains the following entities −**

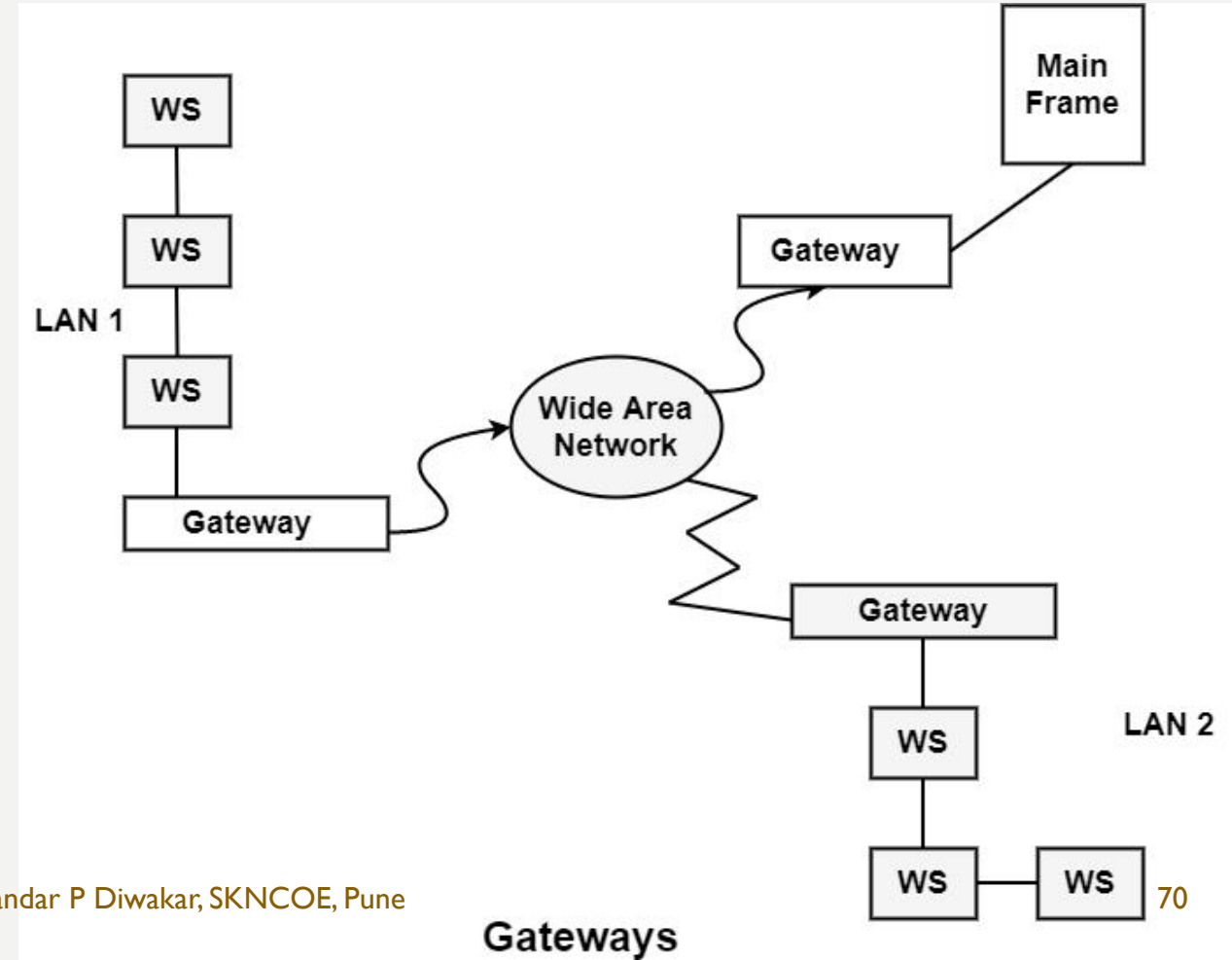
1. IP addresses and subnet mask of the nodes in the network
2. IP addresses of the routers in the network
3. Interface information among the network devices and channels

- **Routing tables are of two types −**

1. **Static Routing Table** − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
2. **Dynamic Routing Table** − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

Gateways

- A device that can bridge several network structure is called a gateway.
- Thus gateways can link two dissimilar LANs. The major difference between gateways and routers is that routers operate at the OSI model's network layer.
- In contrast, gateways operate from the lowest to the topmost layer, i.e., the application layer to the OSI model's network layer.
- A gateway is a connecting device that can relate to multiple networks.
- They perform at the application layer of the OSI model.
- They manage messages, locations, and protocol conversion to deliver a packet to its terminal between two connections.
- The main disadvantage of the gateway is that gateways are slow because they need to perform intensive conversions.



Gateways

Gateways

➢ Characteristics of Gateways

1. It can support complete protocol transformation from one proprietary computer network technology to other technology. It means ethernet to token ring or FDDI or some different model or protocol instead of encapsulation.
2. It needs higher layers of the OSI model, possible by layer 7, the application layer. IBM SNA, DEC net, Internet TCP/IP and other protocols can be transformed from connection to connection.
3. Unlike bridges and routers, gateways work casually due to protocol conversion. Therefore, they can generate bottlenecks of the blockage during the time of peak operation.

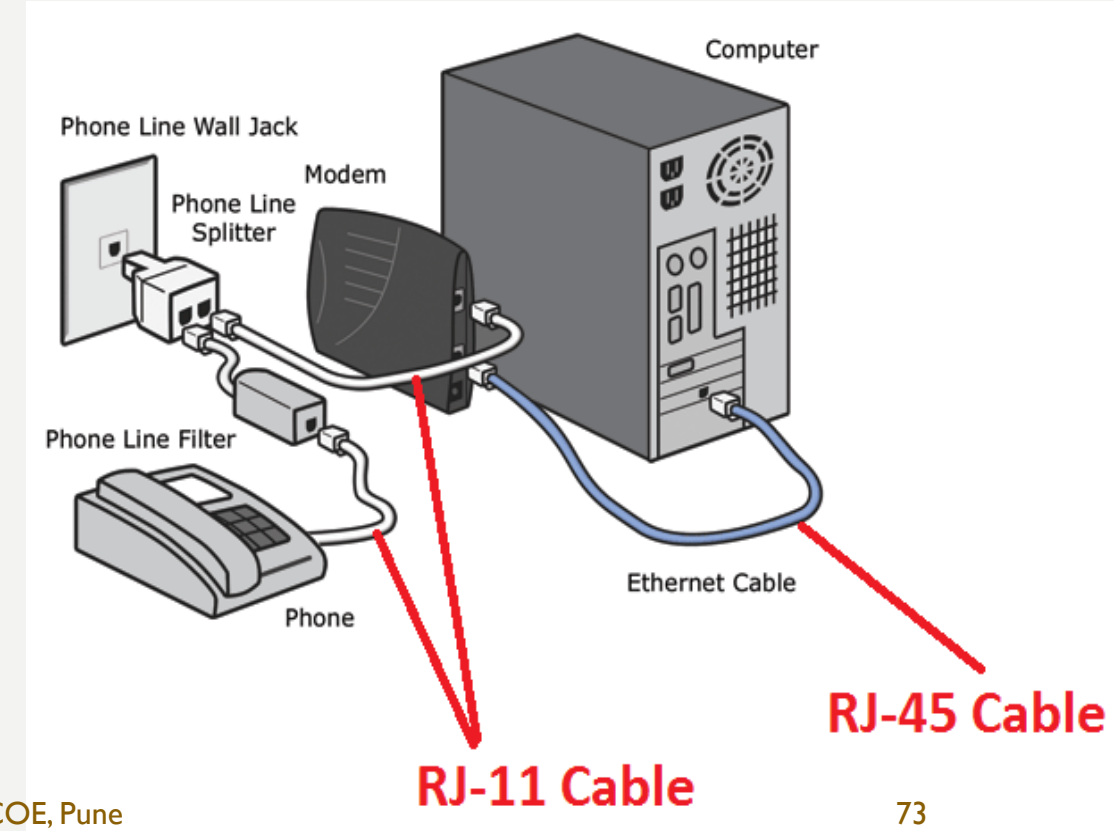
Gateways

➢ Advantages of Gateways

1. It can connect the devices of two several networks having a different design.
2. It is an intelligent tool with filtering capabilities.
3. It has control over both collisions and the advertisement area.
4. It needs a full-duplex mode of connection.
5. It can make data translation and protocol conversion of the data packet according to the destination network's requires.
6. It is used to encapsulate and decapsulate the data packets.
7. It has enhanced security over any other network relating device.

Modem

- Modem is a device that enables a computer to send or receive data over telephone or cable lines.
- The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.
- The main function of the modem is to convert digital signal into analog and vice versa.
- Modem is a combination of two devices − modulator and demodulator.
- The modulator converts digital data into analog data when the data is being sent by the computer.
- The demodulator converts analog data signals into digital data when it is being received by the computer.



Modem

- **Types of Modem**

- Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

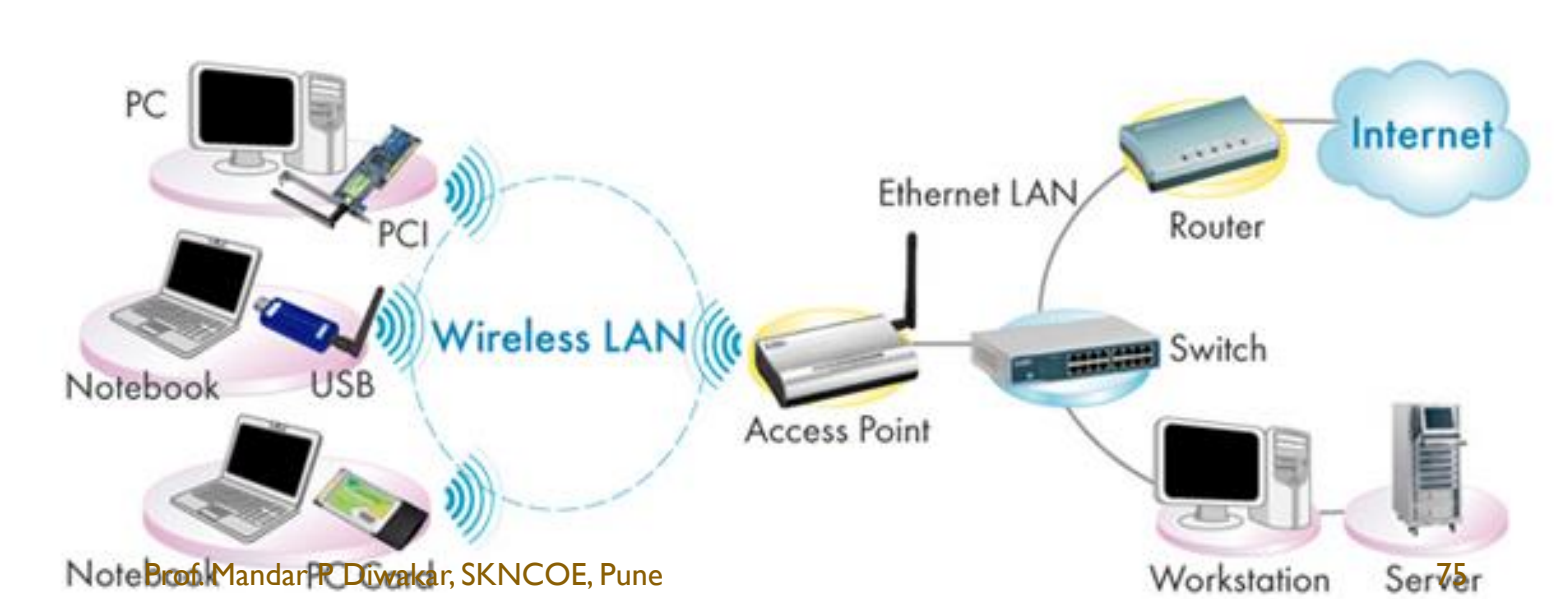
1. **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).

2. **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.

3. **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

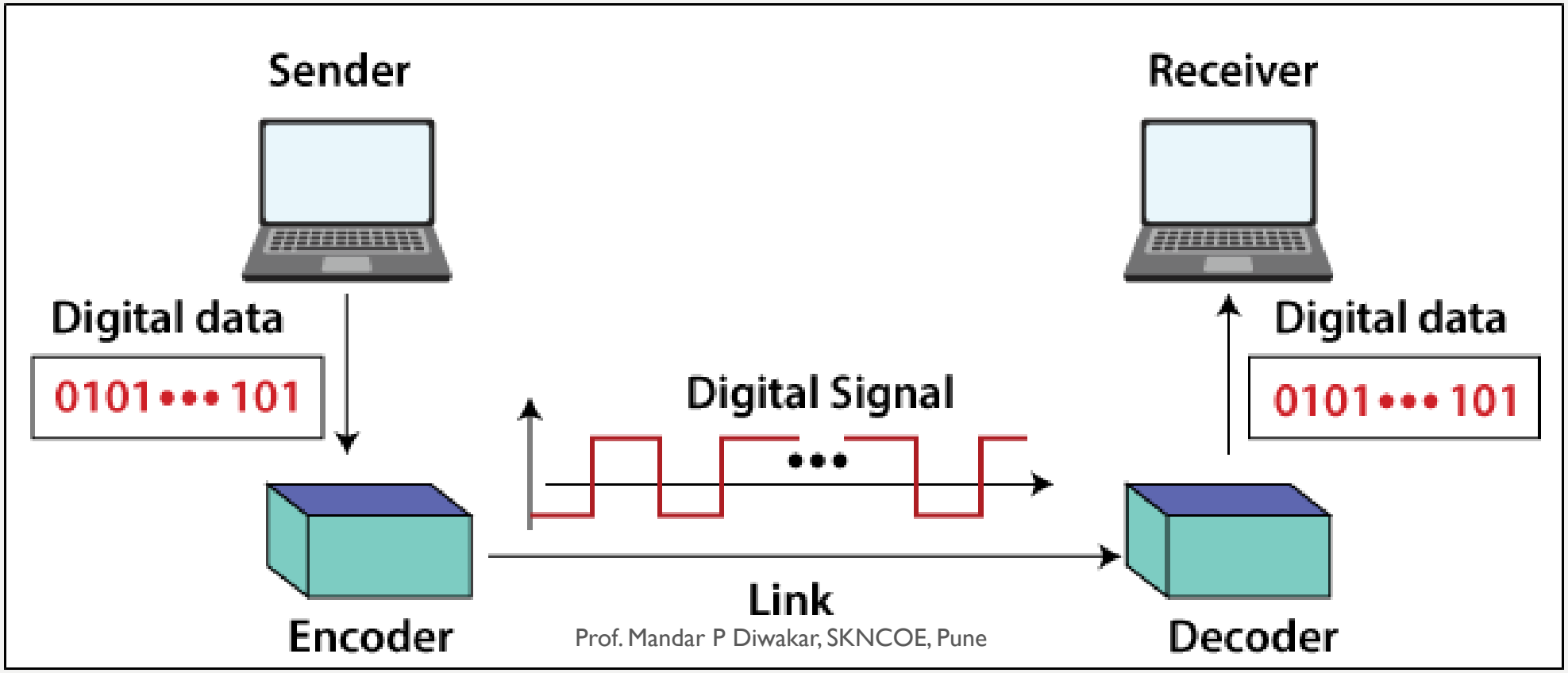
Access Point

- An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.
- An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.
- For example, if you want to enable Wi-Fi access in your company's reception area but don’t have a router within range, you can install an access point near the front desk and run an Ethernet cable through the ceiling back to the server room



Line Coding

- A line code is the code used for data transmission of a digital signal over a transmission line. This process of coding is chosen so as to avoid overlap and distortion of signal such as inter-symbol interference.
- A line code is an assignment of a symbol or pulse to each **zero** or **one** to be transmitted. Digital data is represented by baseband data formats known as line codes



Properties of Line Coding

➢ **Following are the properties of line coding −**

- As the coding is done to make more bits transmit on a single signal, the bandwidth used is much reduced.
- For a given bandwidth, the power is efficiently used.
- The probability of error is much reduced.
- Error detection is done and the bipolar too has a correction capability.
- Power density is much favorable.
- The timing content is adequate.
- Long strings of 1s and 0s is avoided to maintain transparency.

➢ **Types of Line Coding**

1. Manchester Encoding **2. Differential Manchester Encoding**

Manchester Encoding

- Manchester Encoding is a form of Data Encoding in which each data bit is expressed as Either low followed by high or high followed by low.
- It is also known as Phase Encoding(PE).
- It is a Special case of Binary Phase Shift Keying(BPSK).
- In this technique, the signal synchronizes itself resulting in minimizing the error rate.
- The DC Component of the signal carries no information.

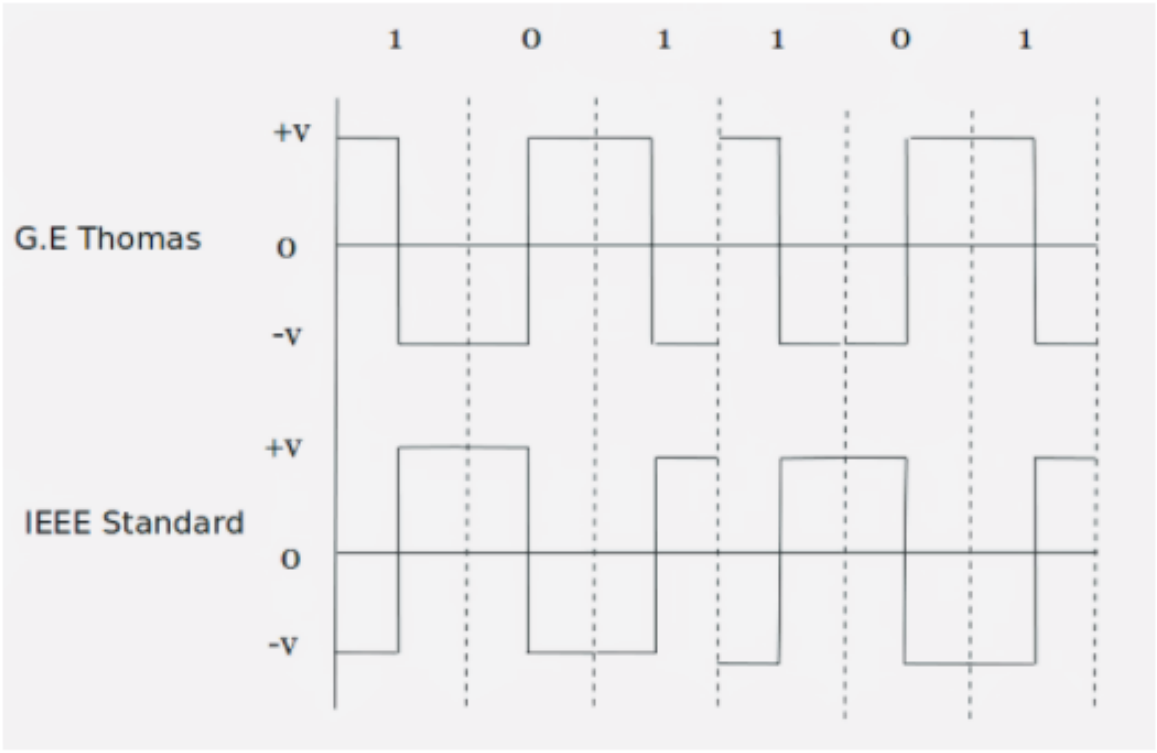
Manchester Encoding

- **Manchester Encoding (Acc. to G.E Thomas)**

  In this approach Data is encoded as For 0 the signal level will be low in the first half and high in the second half of that period. For 1 the signal level will be high in the first half and low in the second half of that period.

- **Manchester Encoding (Acc.to IEEE Standard)**

  In this approach Data is encoded as For 0 the signal level will be high in the first half and low in the second half of that period. For 1 the signal level will be low in the first half and high in the second half of that period.

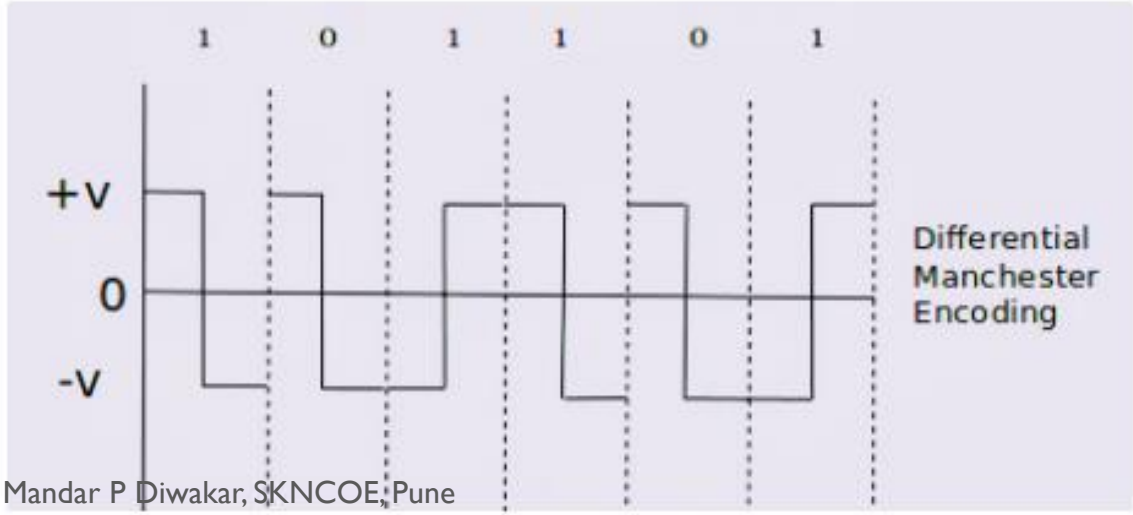


Comparison between M.E according to G.E Thomas and IEEE Standard

Differential Manchester Encodings

- In Differential Manchester Encoding the Bit 0 represent Inversion whereas 1 represents no inversion.
- The transition at the middle bit is used only for Synchronization.
- At 0 Transition will be there at the beginning of the Bit interval.
- At 1 Transition will be absent at the beginning of the Bit interval.
- Used in 802.5 with Twisted Pair.

- For 1 the signal is from high to low.
- As 0 so there will be a transition as shown in the figure.
- for 1 there is no transition.
- As 1 there is no transition.
- for 0 there is a transition.
- for 1 there is no transition.



Spread Spectrum Signals

- **Spread spectrum** is a technique used for wireless communications in telecommunication and radio communication.
- In this technique, the frequency of the transmitted signal, i.e., an electrical signal, electromagnetic signal, or acoustic signal, is deliberately varied and generates a much greater bandwidth than the signal would have if its frequency were not varied.
- In other words, **"Spread Spectrum** is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth.“.
- Now, spread spectrum technology is widely used in radio signals transmission because it can easily reduce noise and other signal issues.

Spread Spectrum Signals

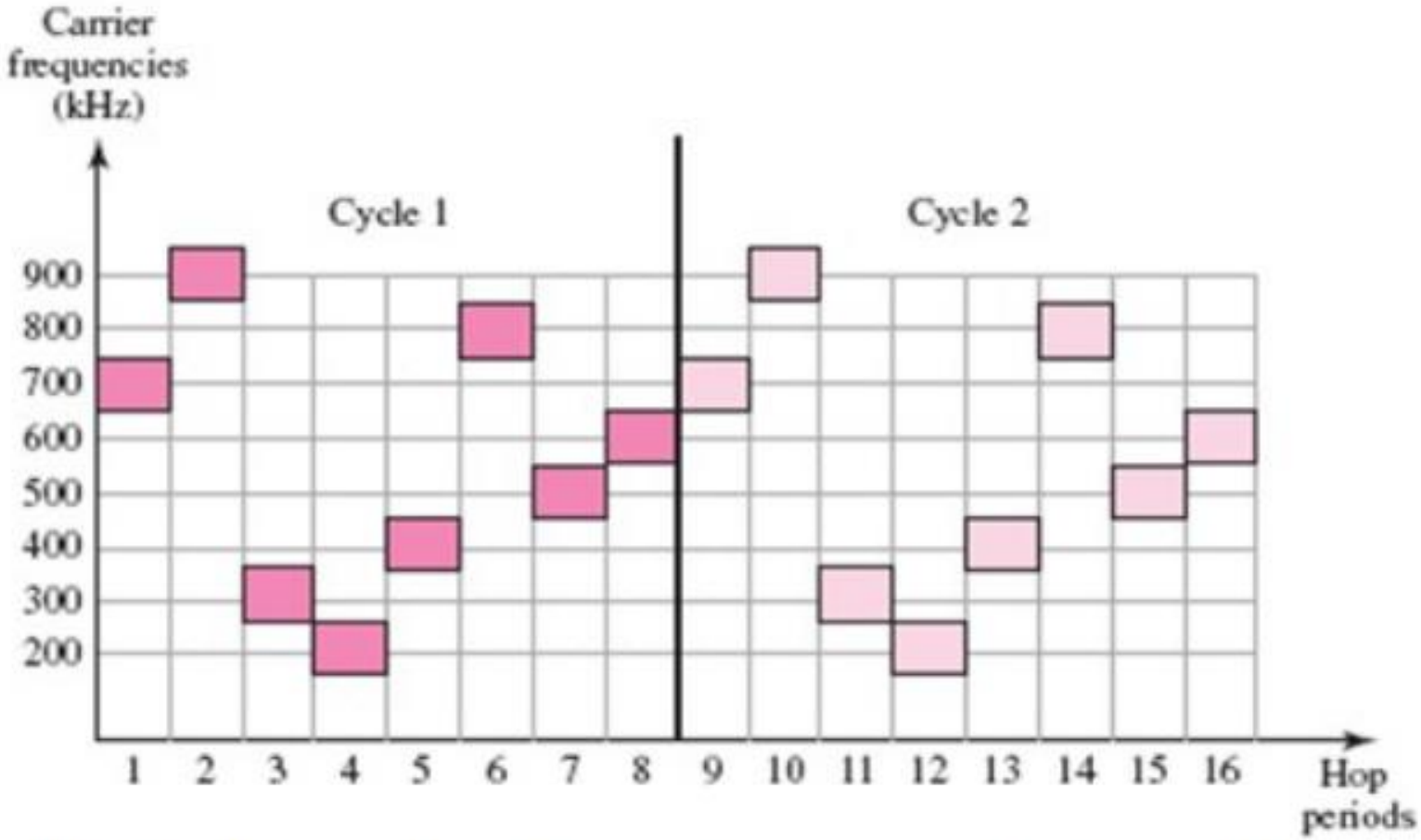
- **Spread spectrum** is a technique used for wireless communications in telecommunication and radio communication.
- **Spread Spectrum** is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth.“.
- Now, spread spectrum technology is widely used in radio signals transmission because it can easily reduce noise and other signal issues.
- **Types of Spread Spectrum**

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

Frequency Hopped Spread Spectrum FHSS

- The **Frequency Hopping Spread Spectrum** or **FHSS** allows us to utilize bandwidth properly and maximum.
- In this technique, the whole available bandwidth is divided into many channels and spread between channels, arranged continuously.
- The frequency slots are selected randomly, and frequency signals are transmitted according to their occupancy.
- The transmitters and receivers keep on hopping on channels available for a particular amount of time in milliseconds.
- So, you can see that it implements the frequency division multiplexing and time-division multiplexing simultaneously in FHSS.

Frequency Hopped Spread Spectrum FHSS



In FH Data is divided into chunks and transmitted at different frequencies at different times.

Advantages FHSS

1. The biggest advantage of Frequency Hopping Spread Spectrum or FHSS is its high efficiency.
2. FHSS signals are highly resistant to narrowband interference because the signal hops to a different frequency band.
3. It requires a shorter time for acquisition.
4. It is highly secure.
5. Its signals are very difficult to intercept if the frequency-hopping pattern is not known; that's why it is preferred to use in Military services.
6. It provides a very large bandwidth.

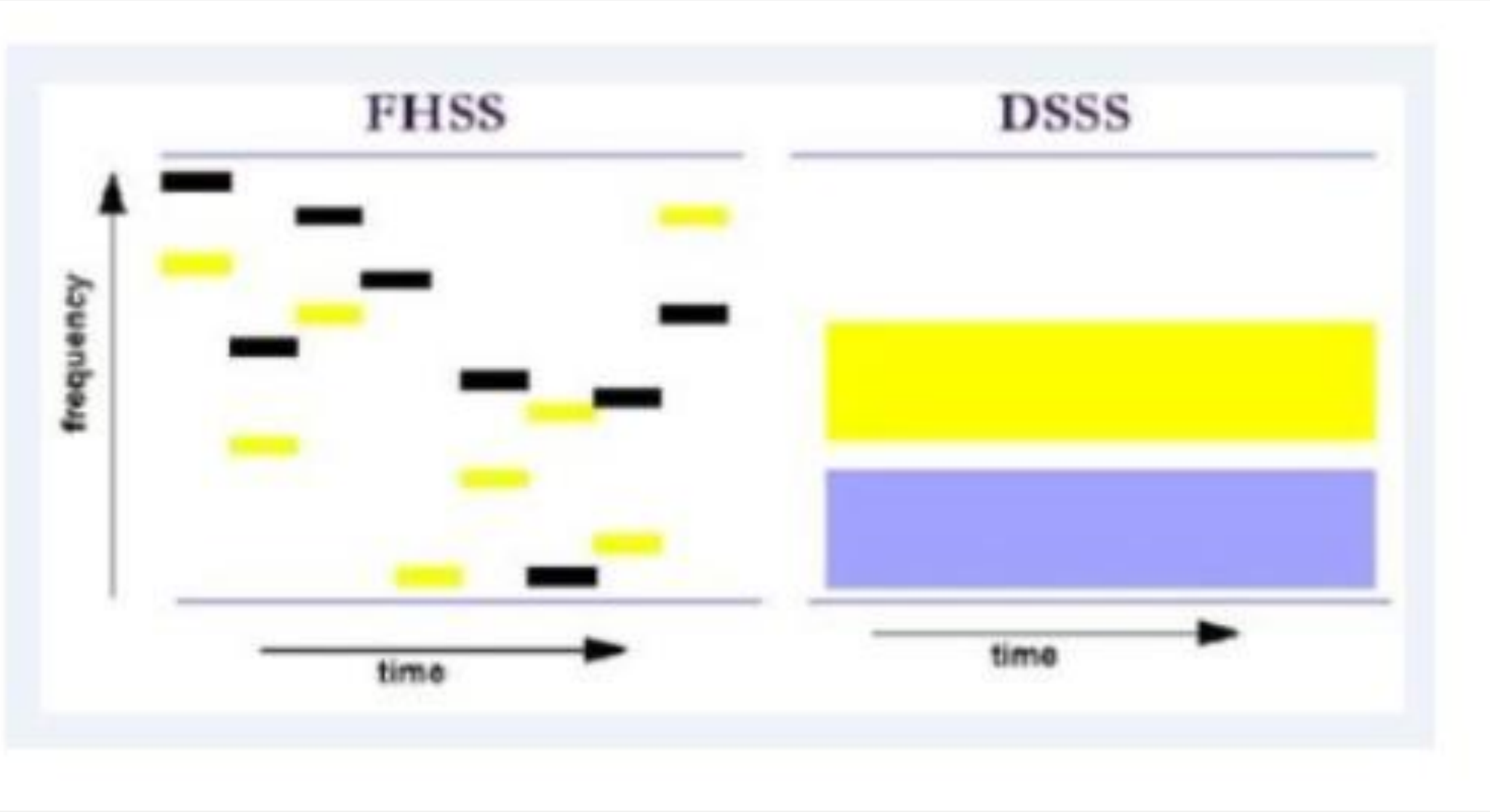
Applications FHSS

1. The Frequency Hopping Spread Spectrum or FHSS is used in wireless local area networks (WLAN) standard for Wi-Fi.
2. FHSS is also used in the wireless personal area networks (WPAN) standard for Bluetooth.

Direct Sequence Spread Spectrum (DSSS)

- The **Direct Sequence Spread Spectrum (DSSS)** is a spread-spectrum modulation technique primarily used to reduce overall signal interference in telecommunication.
- The **Direct Sequence Spread Spectrum** modulation makes the transmitted signal wider in bandwidth than the information bandwidth.
- In **DSSS**, the message bits are modulated by a bit sequencing process known as a spreading sequence.
- This spreading-sequence bit is known as a chip.
- It has a much shorter duration (larger bandwidth) than the original message bits.

Direct Sequence Spread Spectrum (DSSS)



Advantages (DSSS)

- DSSS is less reluctant to noise; that's why the DSSS system's performance in the presence of noise is better than the FHSS system.
- DSSS, signals are challenging to detect.
- It provides the best discrimination against multipath signals.
- In Direct Sequence Spread Spectrum, there are very few chances of jamming because it avoids intentional interference such as jamming effectively.

Applications (DSSS)

- Direct Sequence Spread Spectrum or DSSS is used in LAN technology.
- Direct Sequence Spread Spectrum or DSSS is also used in Satellite communication technology.
- DSSS is used in the military and many other commercial applications.

Question Bank Unit 1

1. What are different transmission modes?[4]
2. Encode the following binary data stream into Manchester and differential Manchester codes 1 1 0 0 1 0 1 0 [8]
3. What are different topologies [4]
4. Explain different components required for wireless Network[4]
5. What is need of Access Point in wireless Network[4]
6. Explain TCP/IP Reference Model [8]
7. Explain OSI reference model [8]
8. Compare TCP/IP and OSI model [6]
9. Explain fiber optics modes of propagation. [8]

Question Bank Unit 1

10. List and write the use of different network connecting devices. [8]
11. What is switch? Explain difference between manageable and non manageable switch.[8]
12. Describe the network components (Connectors, Hubs, Switches, Repeaters, and bridges) [6]
13. Explain various internetworking devices. State at which layer that work?[8]
14. Compare between Hub and Switch.[4]
15. Explain working of Hubs, Switches and Routers. [6]
16. Differentiate between Bridge, Router and Switches. [6]
17. Explain the types of frequency hopping. [8]
18. Give brief description of
    1. Twisted Pair Cable
    2. Co-axial cable
    3. Fiber Optic cable [8]