Unit 1

COMPUTER NETWORKS

RCS-601

UNIT 1

Introduction Concepts: Goals and Applications of Networks, Network structure and architecture, The OSI reference model, services, Network Topology Design - Delay Analysis, Back Bone Design, Local Access Network Design. Physical Layer Transmission Media, Switching methods, ISDN, Terminal Handling.

INTRODUCTION

Networking is the sharing of information and services. Networking is possible when individuals or groups have information or abilities that they wish to share with others.

UNDERSTANDING NETWORK

A network is simply a collection of computers or other hardware devices that are connected together using special software and hardware

Each workstation is called as node and communication media between two nodes is called as Link.

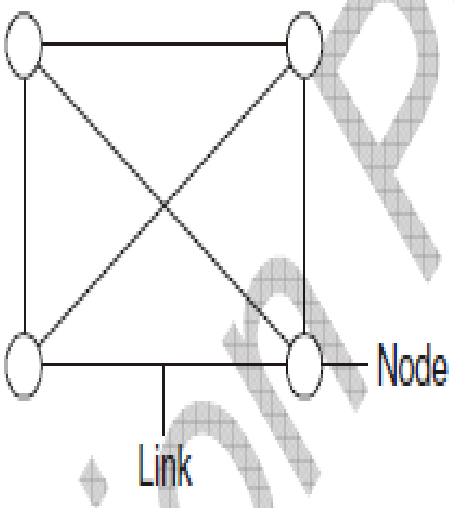
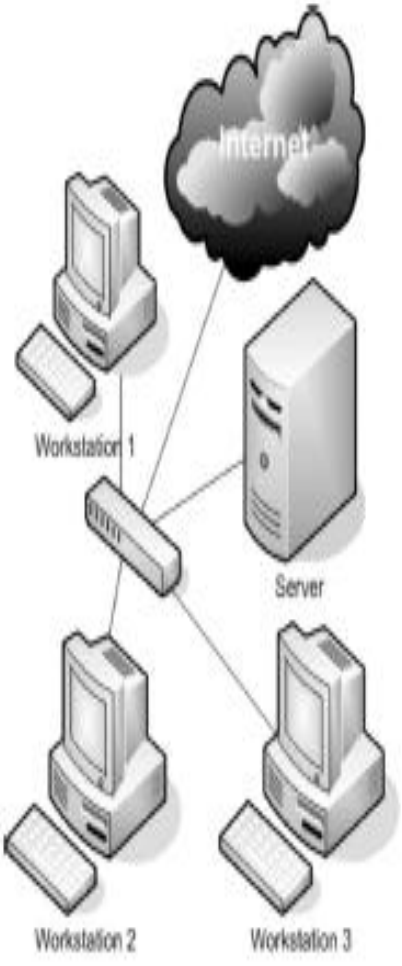
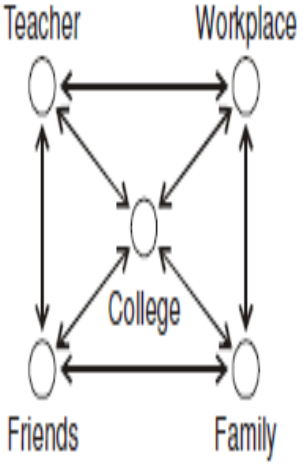


Figure 1.1: Basic Network Concept



Human Network –Real Life Example

Human network is network of human beings. Human network means social structure which consists of human beings, schools, colleges, hospitals, universities, etc connected through technology.



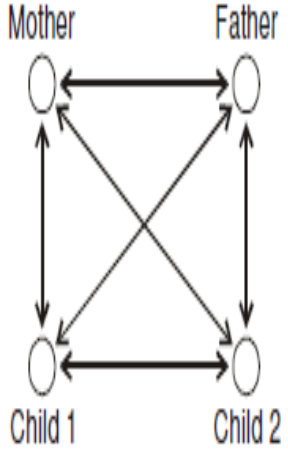
Human Network

Example of human network

i. Family network

ii. Client server network (restaurant network)

iii. Contact network



Family Network

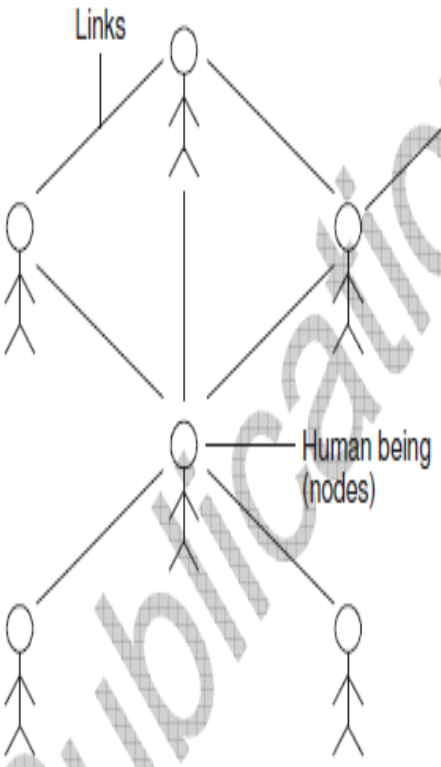


Figure 1.2: Human network

Given figure shows a human network. In this case, human beings act as nodes. Links between the nodes are of different types such as mobile phones audio links, emails, roads, emotions, relations etc.

Publications

Computer Network

A computer network is defined as the interconnection of two or more computers for sharing information and sharing resources.

Computers are connected to each other so that they can share files and folders, applications or resources like printers, scanners, web-cams etc. Fig. 1.3 shows basic concept of computer network.

Example: Internet is the best example of computer network. Millions of computers are networked together to form the Internet.

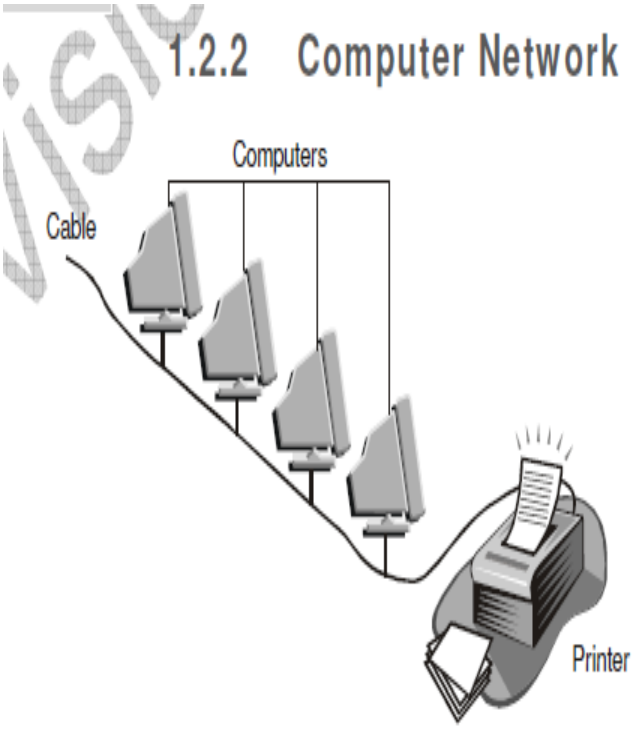


Figure 1. 3: Computer network

Applications of computer Network

i. Banking

ii. Colleges

iii. School

iv. Universities

v. Hospitals

vi. Hotels etc.

Need of Computer Network

i. Communication from one computer to the other.

ii. Exchange of data and information among the users, via the network.

iii. Sharing of information over the geographically wide areas.

iv. For educational purpose.

v. For connecting the computers between various buildings of an organization.

vi. Sharing of expensive software, hardware and databases.

vii. Sharing the resources such as scanner and printer among all the users.

It means that, need of computer network is everywhere where computers are used.

Components of Computer Network

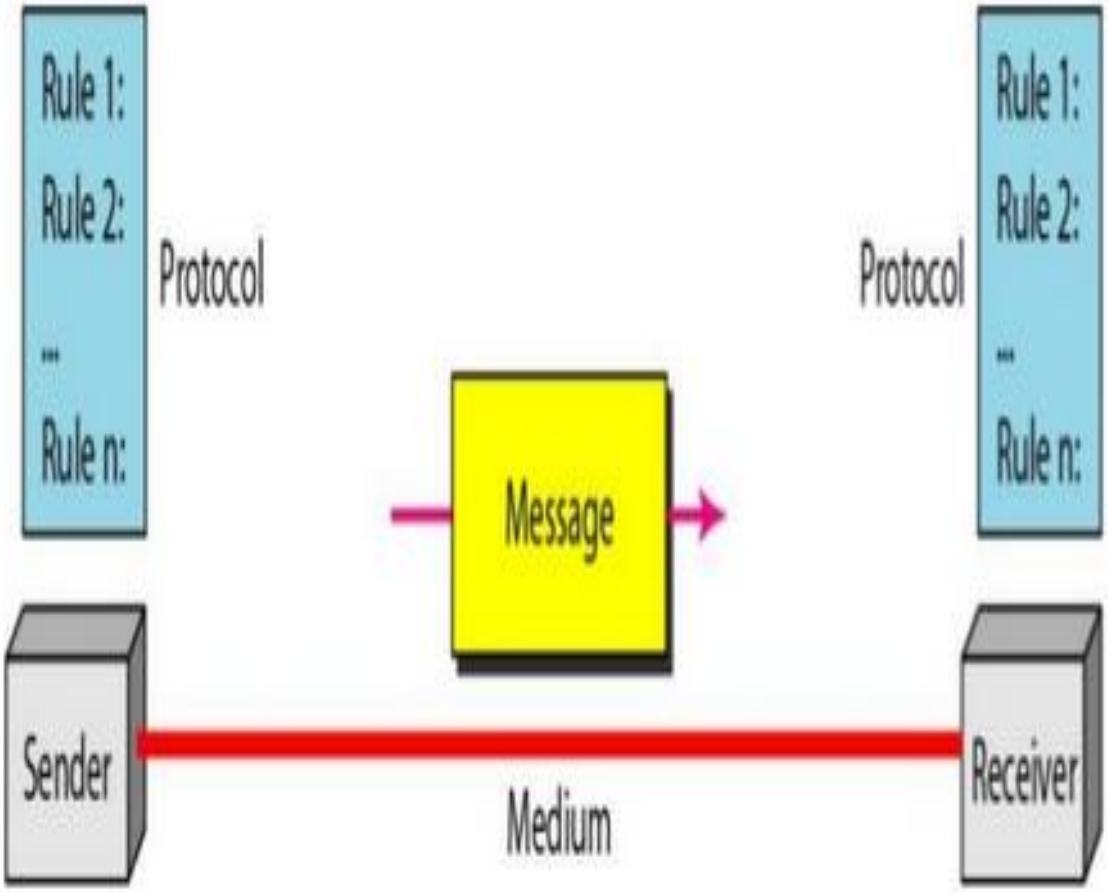
The components of computer network are as follows:

1. **Computers** (at least two) – **Sender & Receiver**
2. **Message:** It is the information to be communicated i.e Image, Text etc
3. **Transmission media:** Transmission media are the medium that carry data from one computer to another. Example, Twisted pair cable, Co-axial cable, Optical fiber cable
4. **Network Interface Card (NIC):** The NIC acts as the physical interface or connection between the computer and the network cable.
5. **Network operating system:** A network of computers cannot operate without a network operating system. Without a network operating system, computers cannot share resources and other users cannot make use of those resources.
6. **Network control devices:** Network control devices are also called as connecting devices. In computer network many computers are connected to one another. For each connection, we need to use the network control devices.
7. **Power supply:** The power supply unit converts general purpose electric current from the mains to direct current for the other components of the computer.

Components of a data communication system

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.



Protocol

Protocol is nothing but rules for communication. The term "protocol" is used in a variety of applications.

Rules of protocol apply in the same way in the computer environment. When several computers are networked, the rules and technical procedures that govern their communications and interactions are called protocol.

Advantages of Computer Network

- File Sharing: Networks offer a quick and easy way to share files directly.
- Resource Sharing: All computers in the network can share resources such as printers, fax machines, modems and scanners.
- Communication: Those on the network can communicate with each other via e-mail, instant messages etc.
- Flexible Access: Networks allow their users to access files from computers throughout the network.
- Sharing of Information: Computer networks enable us to share data and information with the computers that are located geographically large distance apart.

Disadvantages of Computer Network

i. Security issues

ii. Dependency on the main file server.

iii. Rapid spread of computer viruses.

iv. Expensive set up

v. Cable faults.

Network Services

The different services provided by the network, for organizations are:

i. Resource sharing

a.Hardware resources

b. Software resources

ii. Cost

iii. Communication

medium

iv. High reliability

Services provided by network to people

i. Interactive entertainment e.g games, audio/video

on demand etc.

ii. Person-to-person communication

a. E-mail

b. News group

c. Video conferencing

iii. Access to remote information

a. E-banking b. Digital library

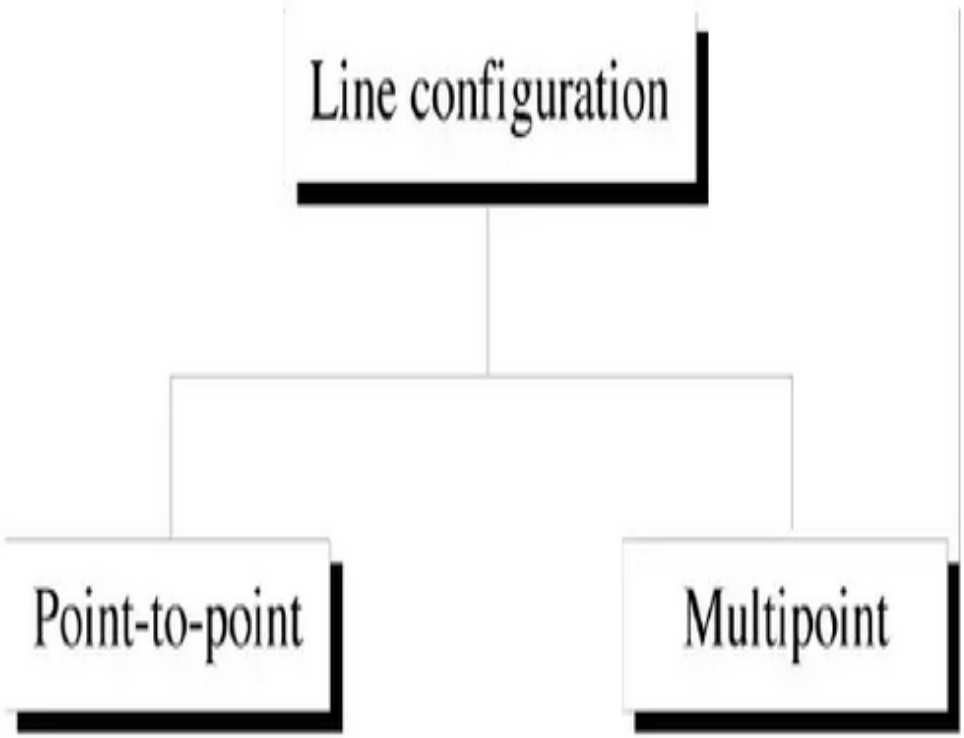
c. Home shopping d. On line share market

Social Issues

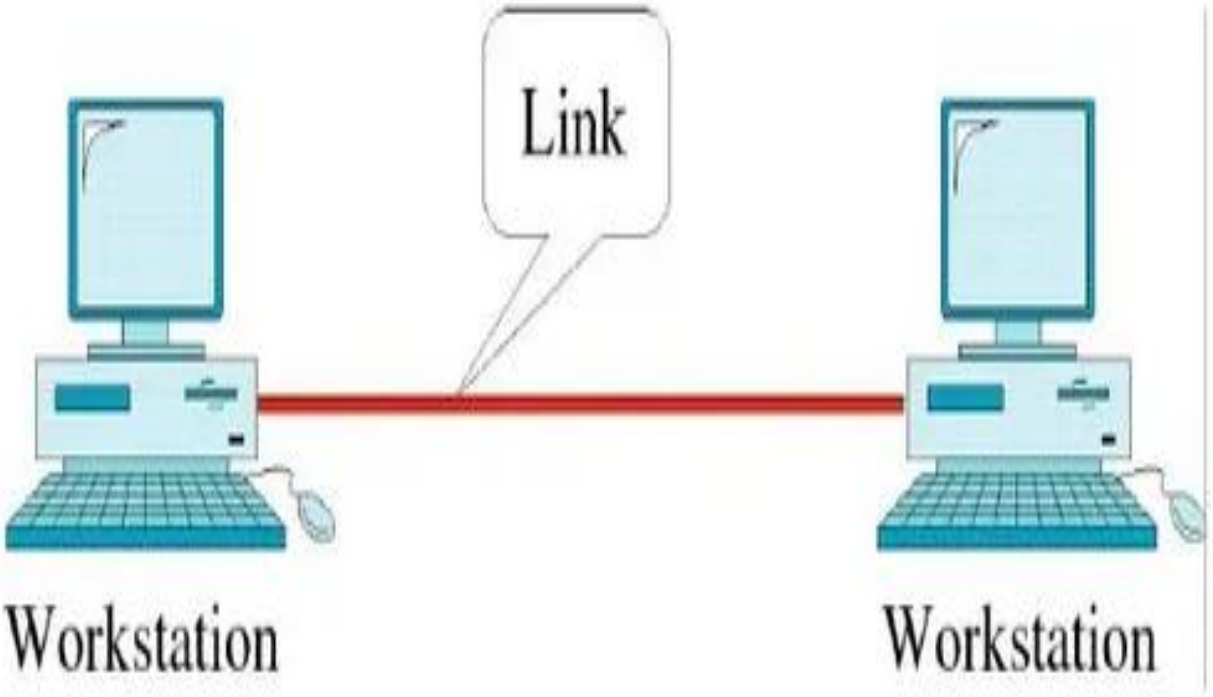
- Privacy
- Copyright
- Pornography
- Anonymity
- Freedom of speech vs. censorship
- Responsibility of the service providers

Basic Concepts

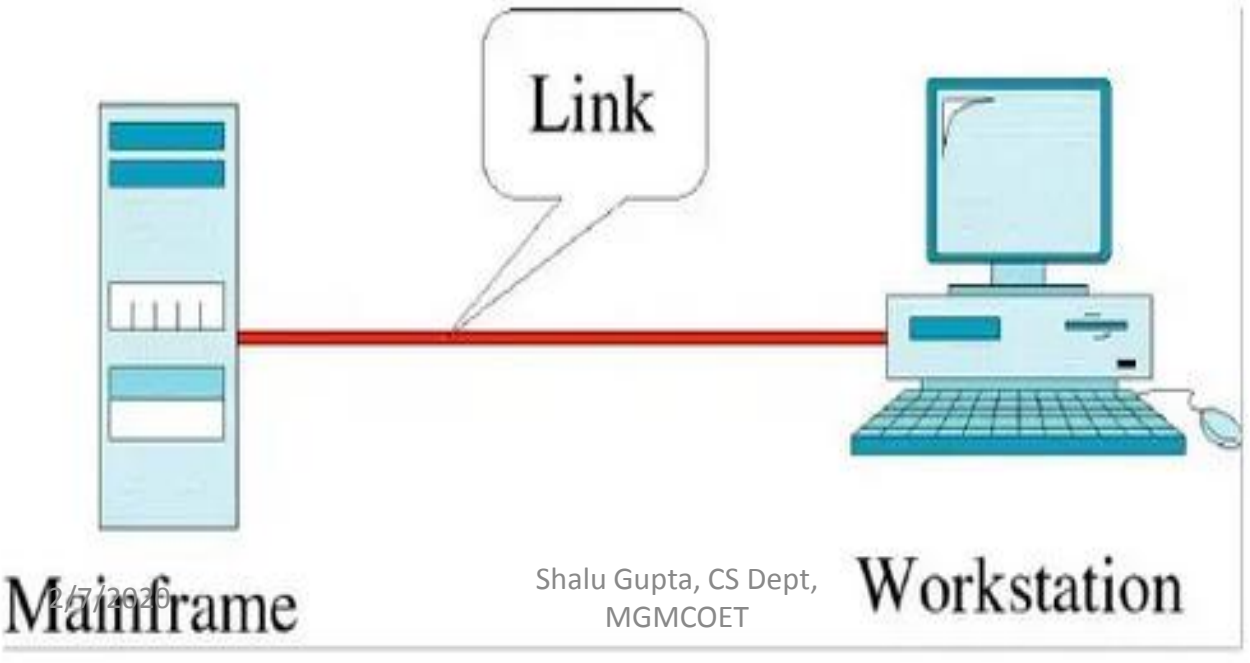
- • Line Configuration
- • Topology
- • Transmission Mode
- • Categories of Networks
- • Internetworks


Line configuration
Point-to-point
Multipoint

Point-to-Point Line Configuration

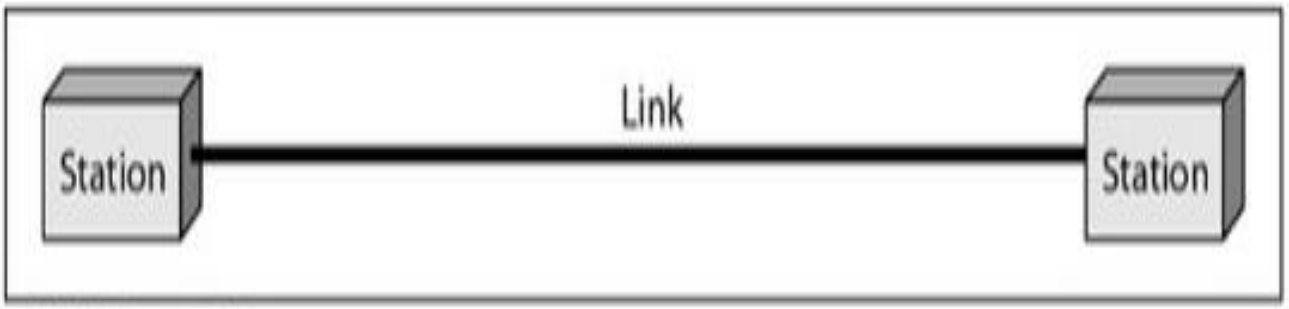


Point-to-Point Line Configuration



Point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

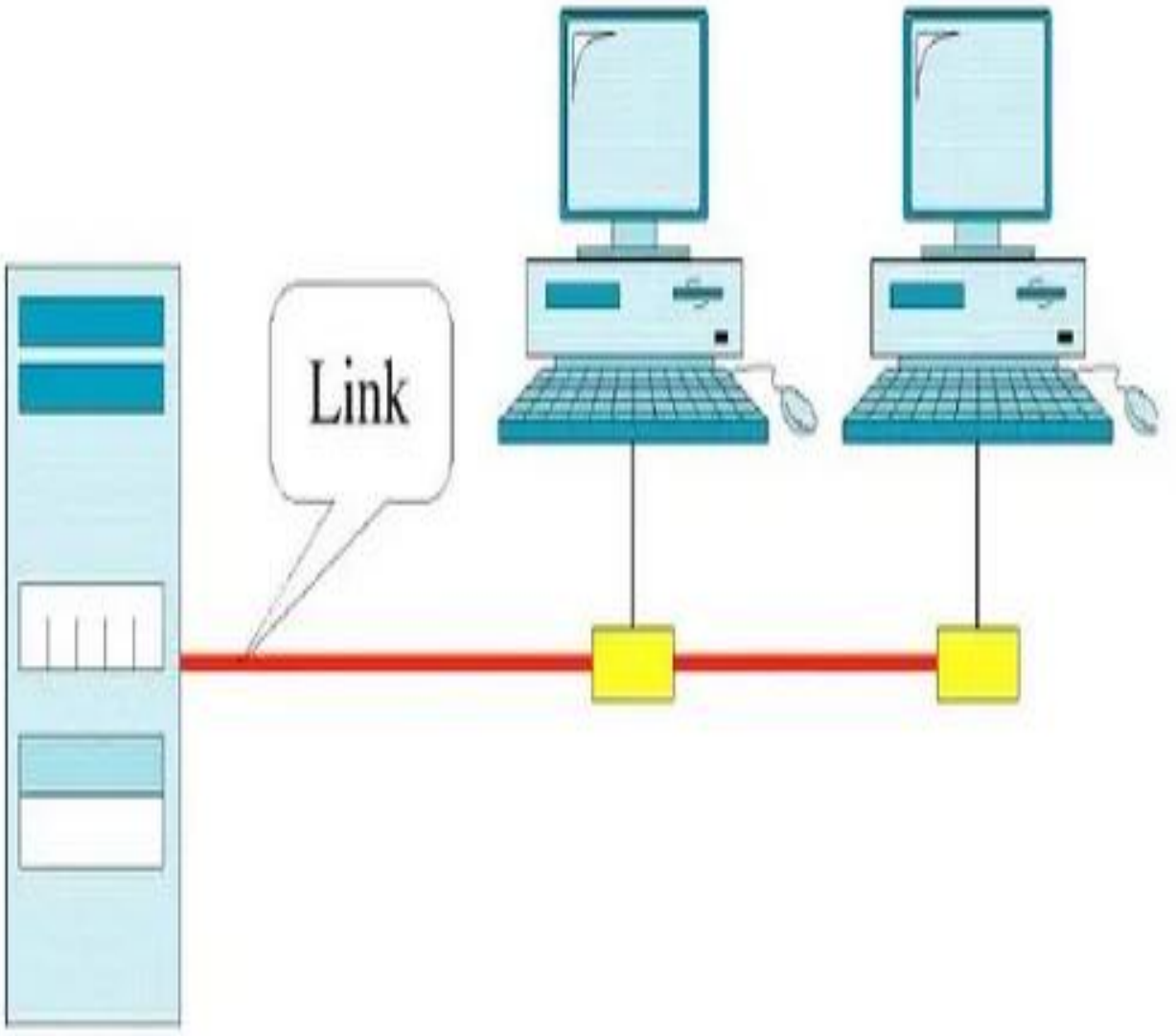
This network provides a dedicated link between any two stations . Such a transmission is called **unicasting**.



Point-to-point

Point-to-Point Line Configuration

Multipoint Line Configuration



Multi point Line Configuration

There are two types of transmission technology:

1. Broadcast Networks

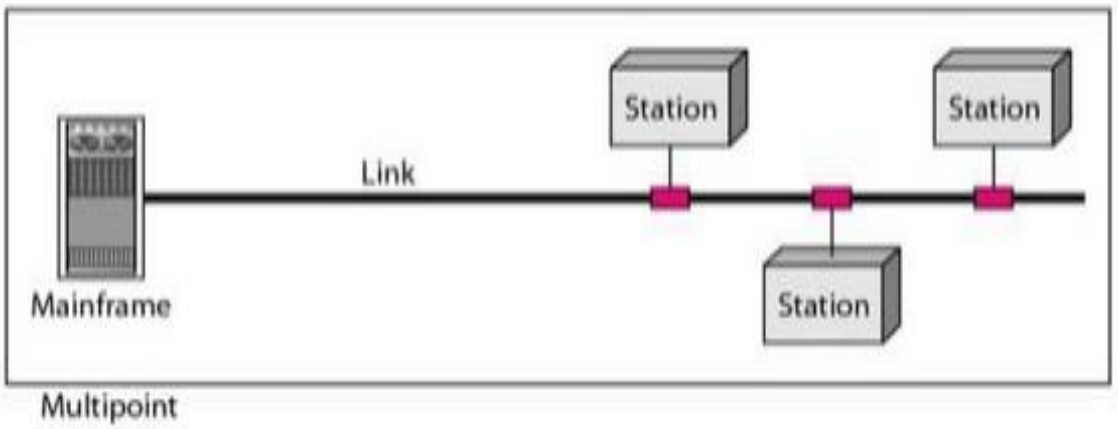
This has a single communication channel that is shared by all the machines on the network.

The data transmitted is converted in small packets form. Each packet contains address field of the destination station.

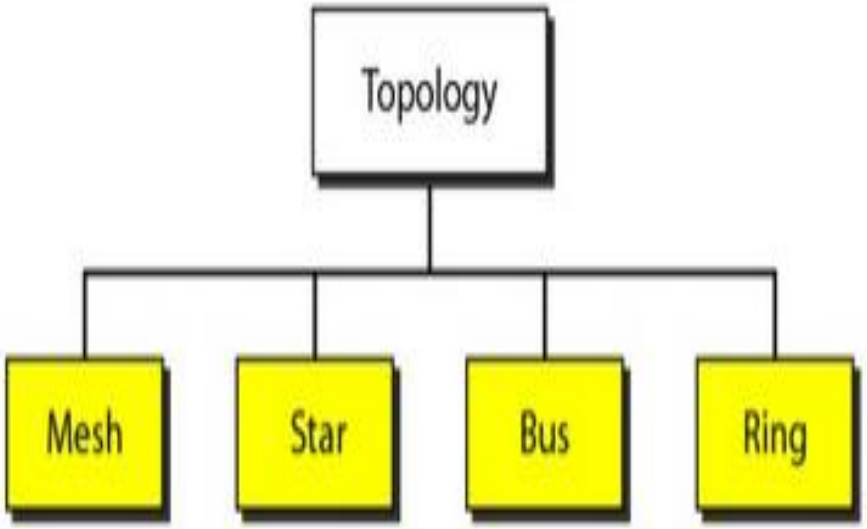
Ex:- a person standing at corridor "watson, come here. I want you"

sending same packets to all the stations within a network is called as **broadcasting**.

When data packets are sent to a specific group of stations it is called as **multicasting**. This is a selective process



Categories of topology



- The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a **link**; two or more links form a **topology**.

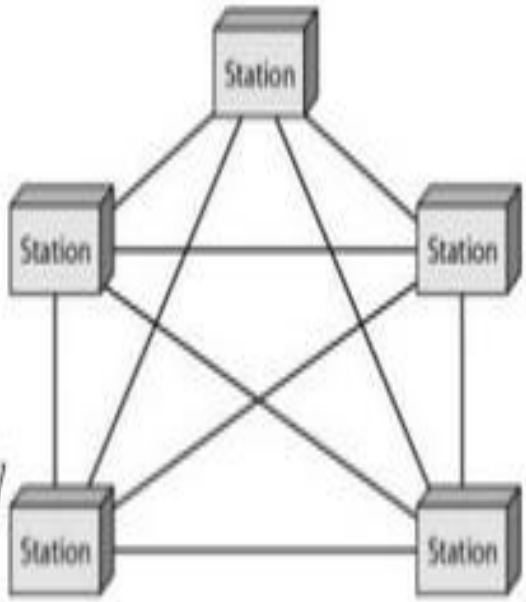
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

- There are four basic topologies possible: mesh, star, bus, and ring.

Mesh Topology

A fully connected mesh topology (five devices)

- In mesh topology every device has a dedicated point-to-point link to every other device.
- The link carries traffic only between the two devices it connects.
- Duplex-mode
- Advantages:
  - guaranteed dedicated links
  - eliminates traffic problems
  - privacy and security
  - this makes fault identification easy



- Disadvantages:
  - cabling and number of IO ports required
  - wiring is greater than available space
  - hardware is required for each link – expensive

Star Topology

A star topology connecting four stations

•In star topology, each device has a dedicated point-to-point link only to a central controller called hub.

•The controller acts as an exchange: if one device wants to send data to another , it sends the data to controller, which then relays the data to the another connected device.

•Advantages:

less expensive

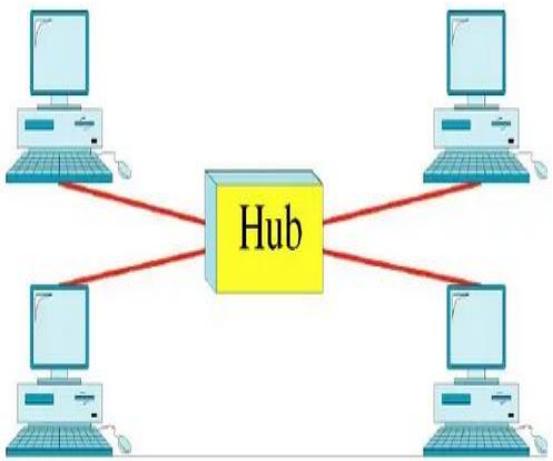
robustness – if one link fails, only that link is affected, other links remain active.

•Disadvantages:

dependency of the whole topology on one single point.

star requires less than mesh, each node is linked to the hub. So more cabling is required .

Star Topology



Bus Topology

- A bus topology is a multipoint .
- One long cable acts as a backbone to link all the devices in the network.
- Nodes are connected by bus cable by drop line and taps.

  a drop line is a connection running between the device and the main cable

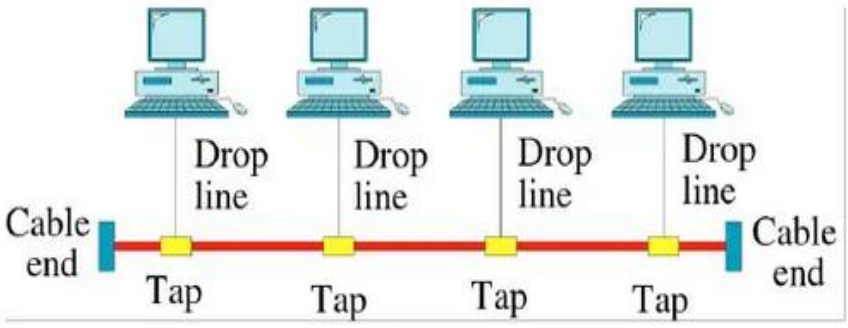
  a tap is a connector that either splices or punctures.
- Advantages:

  easy of installation
- Disadvantages:

  difficult reconnection

  addition of new devices require modification or replacement of the backbone.

Bus Topology



Ring Topology

•In ring topology each device has a point-to-point connection with only the two devices on either side of it.

•A signal is passed along a ring in one direction, from device to device until it reaches its destination.

•Advantages:

easy to install and reconfigure

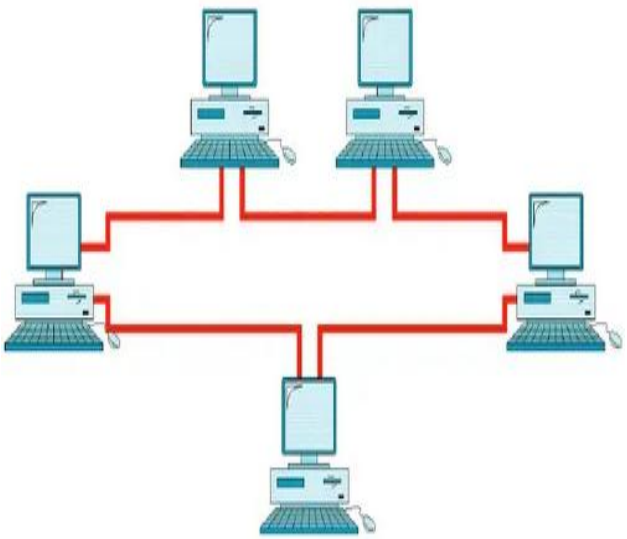
to add or delete a device requires changing only two connections. The only constraints are media and traffic.

•Disadvantages;

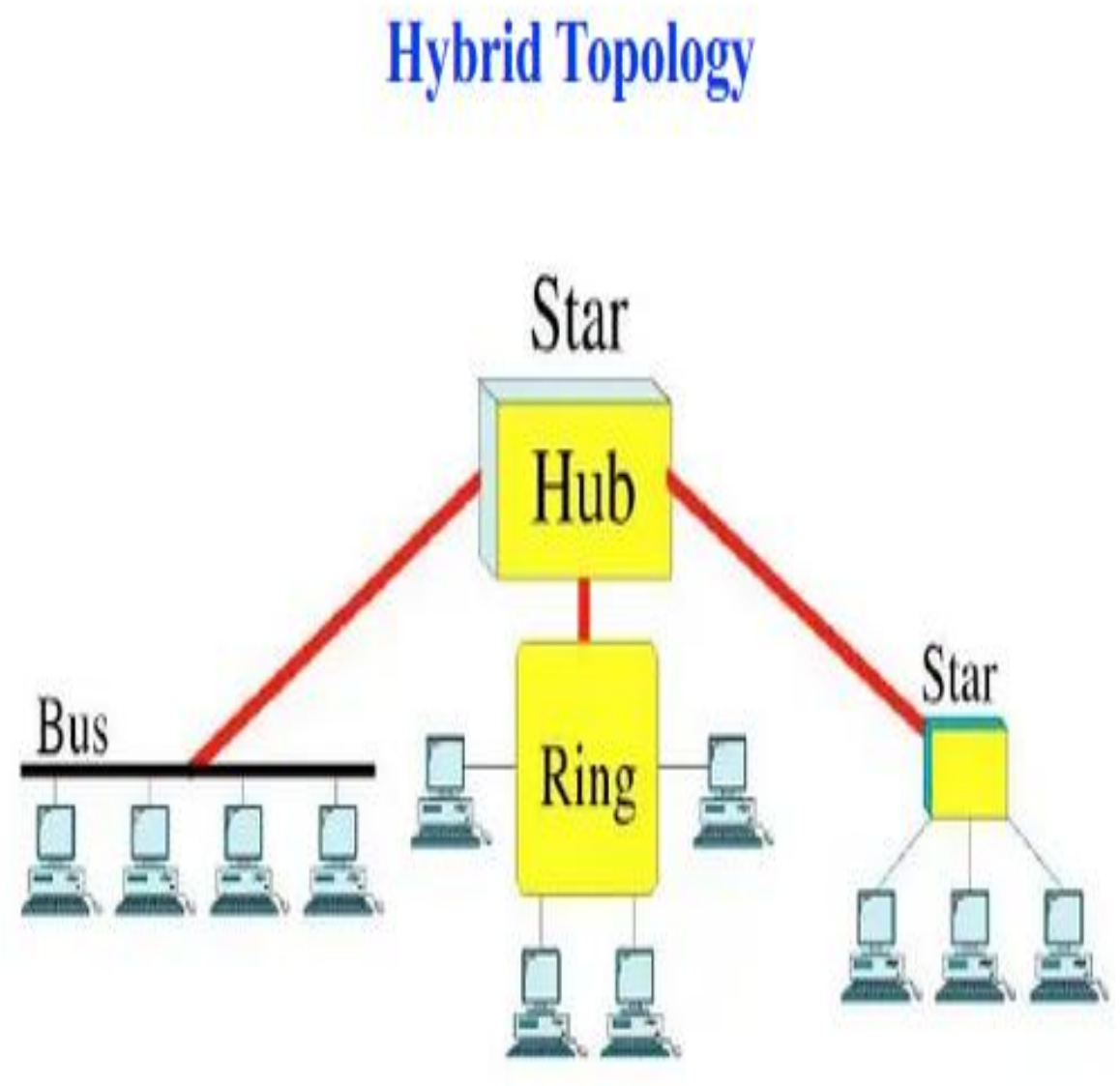
unidirectional

a break in a ring can disable the entire network

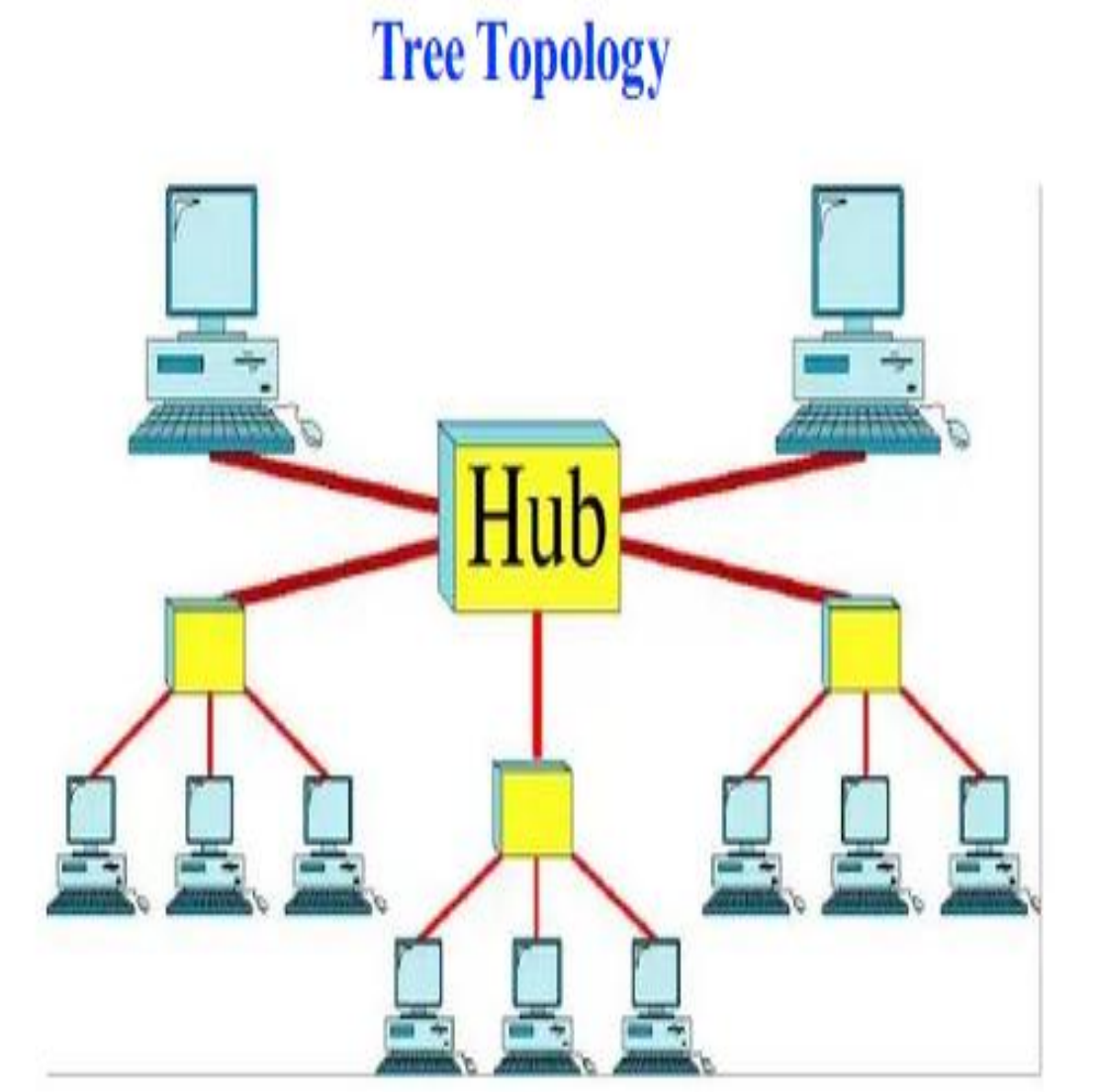
Ring Topology

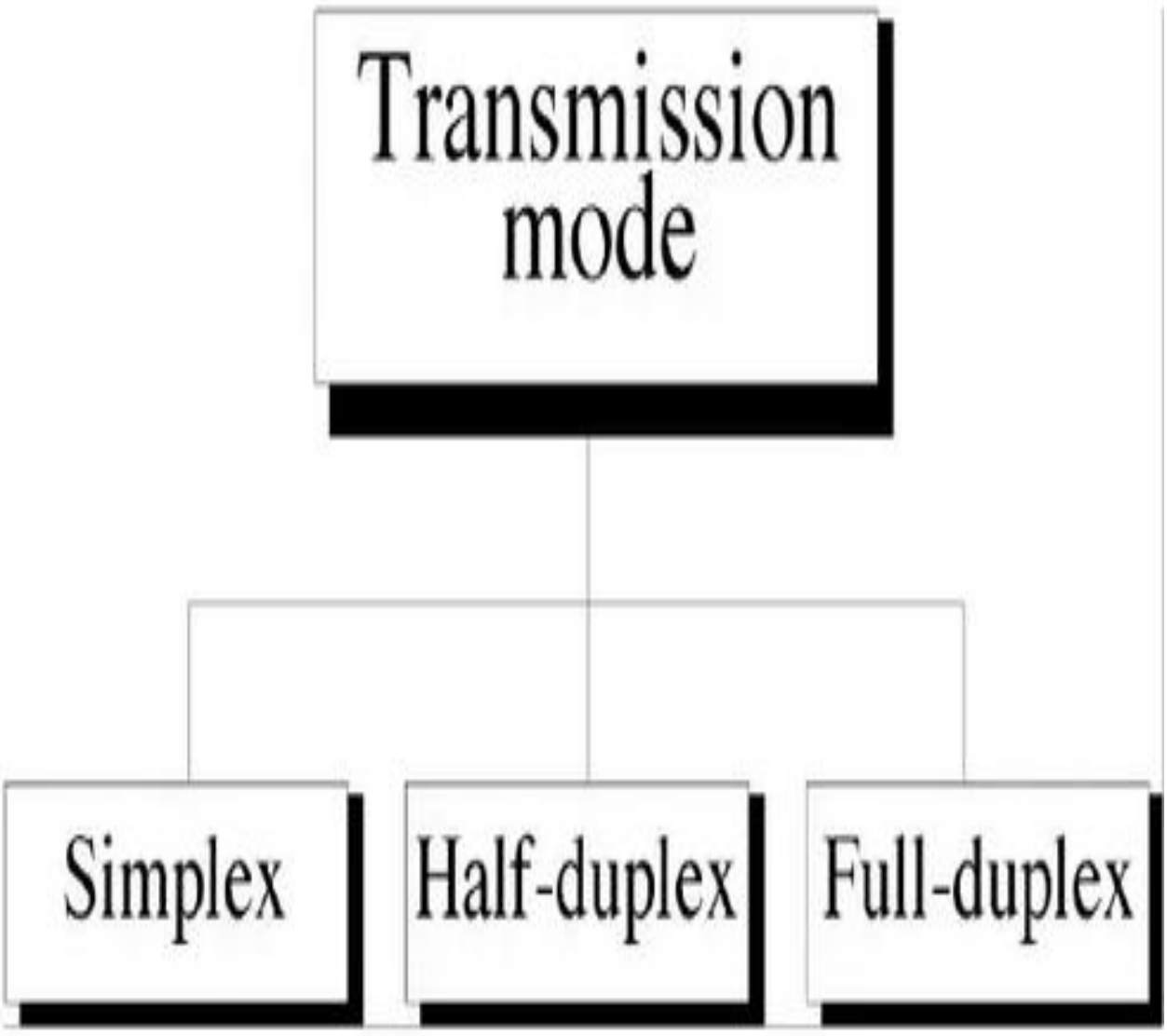


A hybrid topology: a star backbone with three bus networks

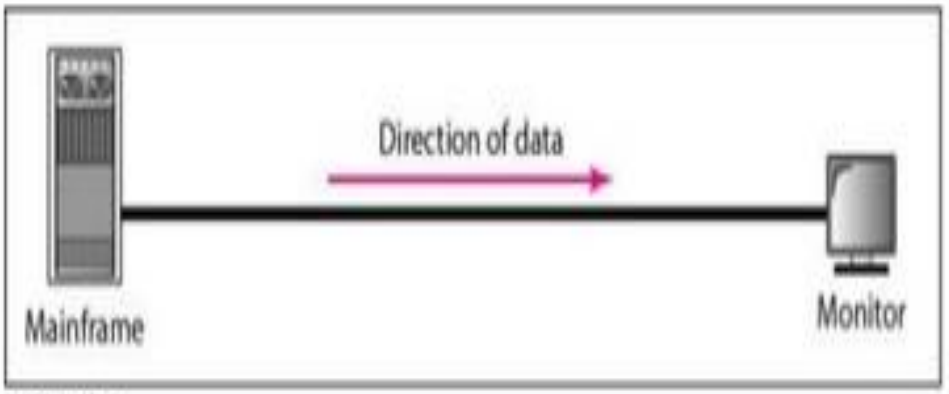


A tree Topology



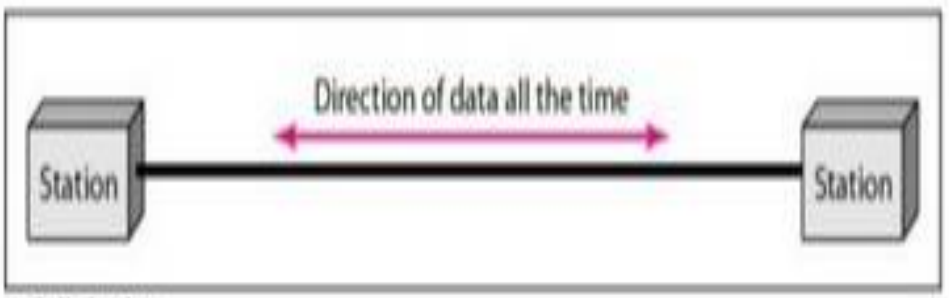

Transmission mode
Simplex
Half-duplex
Full-duplex

Data flow (simplex, half-duplex, and full-duplex)



a. Simplex

b. Half-duplex



c. Full-duplex

Simplex:

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

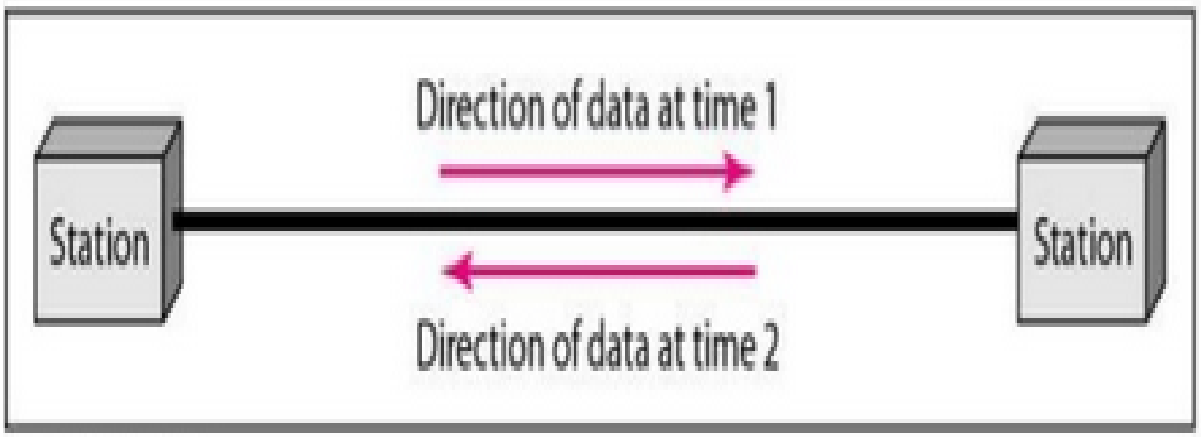
Examples:- Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

a. Simplex

Half-Duplex:

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

Examples:-When cars are traveling in one direction, cars going the other way must wait. 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 is half-duplex systems.



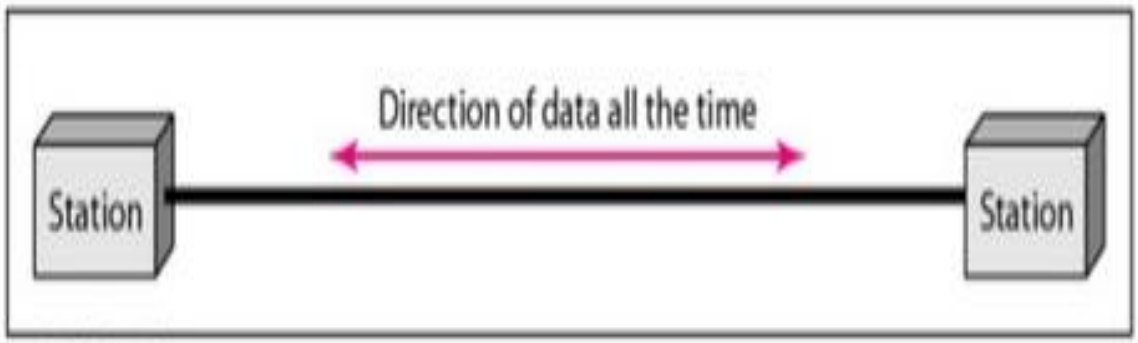
b. Half-duplex

MGMCOET

Full-Duplex:

In full-duplex both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction.

Example:- full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.



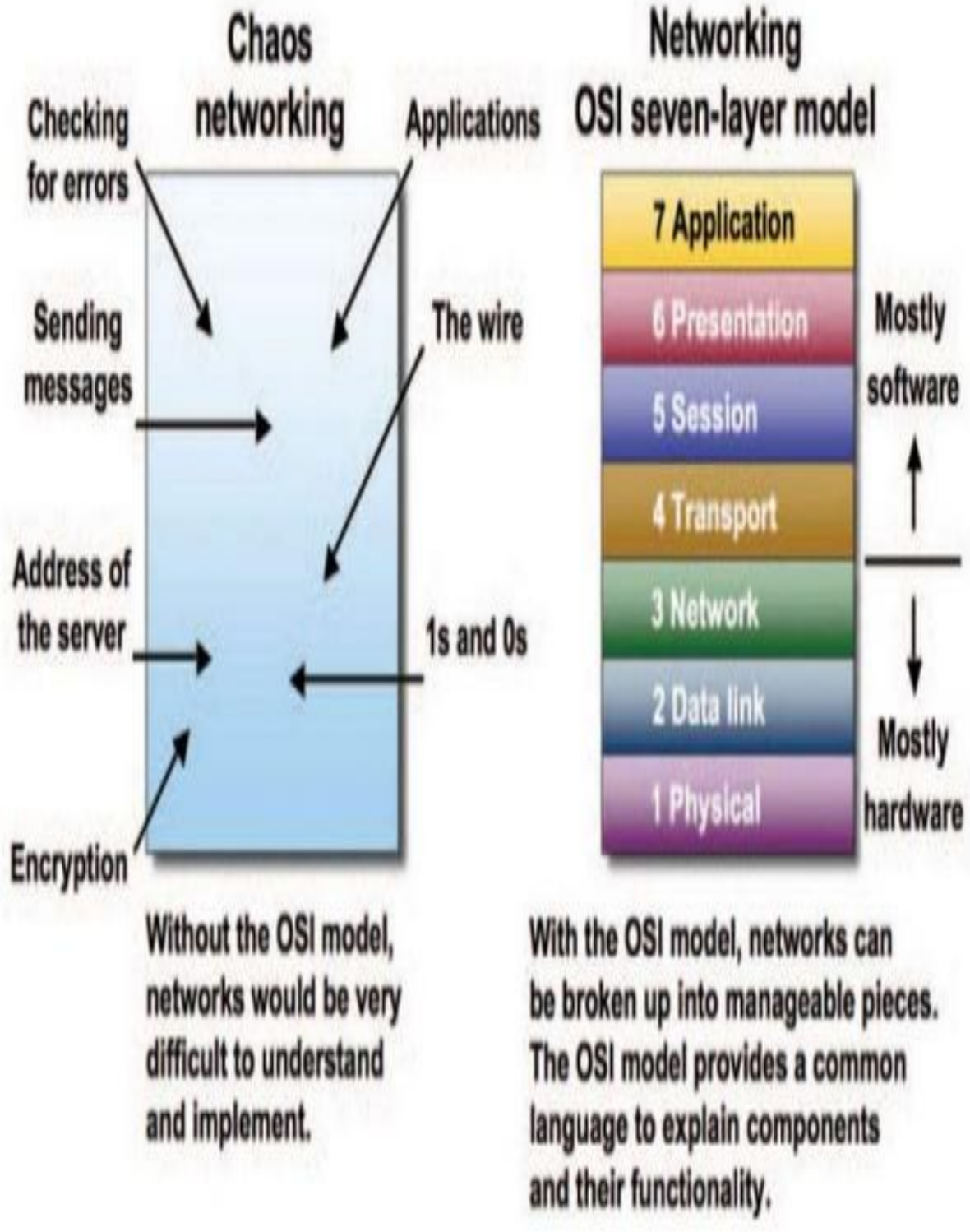
c. Full-duplex

The OSI Reference Model

- In 1947, the international standards organization(ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the **open systems interconnection** model.
- In late 1970s an open system is a set of protocols that allow any two different systems to communicate
- It divides the communications processes into seven layers.

ISO is the organization.
OSI is the model.

- The main concept of OSI is that the **process of communication** between two endpoints in a telecommunication network can be divided into seven distinct groups of related functions, or layers.
- Each communicating user or program is at a computer that can provide those seven layers of function.
- The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol).


Chaos networking
Checking for errors
Applications
Sending messages
The wire
Address of the server
1s and 0s
Encryption
Networking OSI seven-layer model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data link
1 Physical
Mostly software
Mostly hardware
Without the OSI model, networks would be very difficult to understand and implement.
With the OSI model, networks can be broken up into manageable pieces. The OSI model provides a common language to explain components and their functionality.

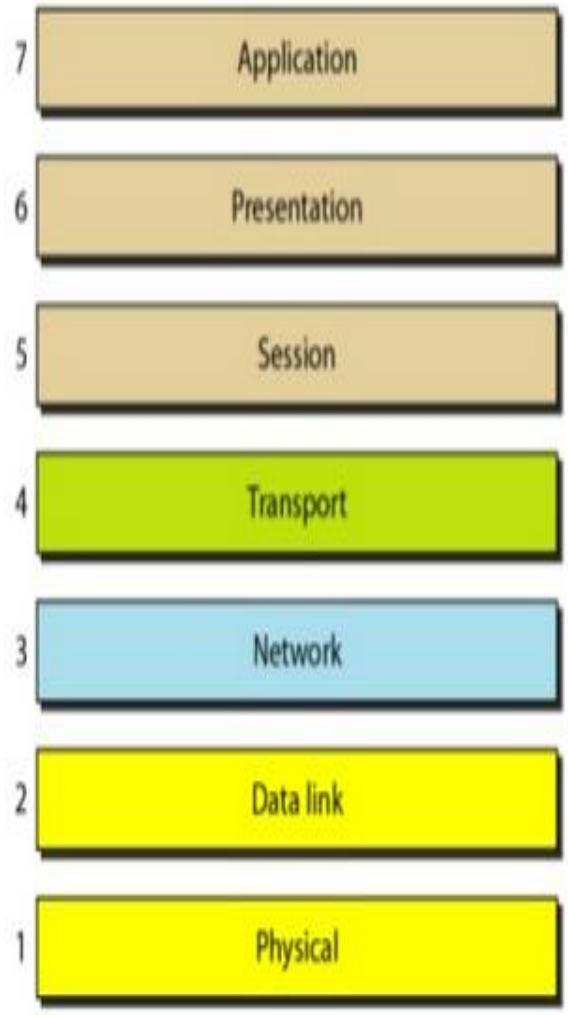
The OSI model has seven layers. The principles that were applied to arrive at the seven layers are:

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layers boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

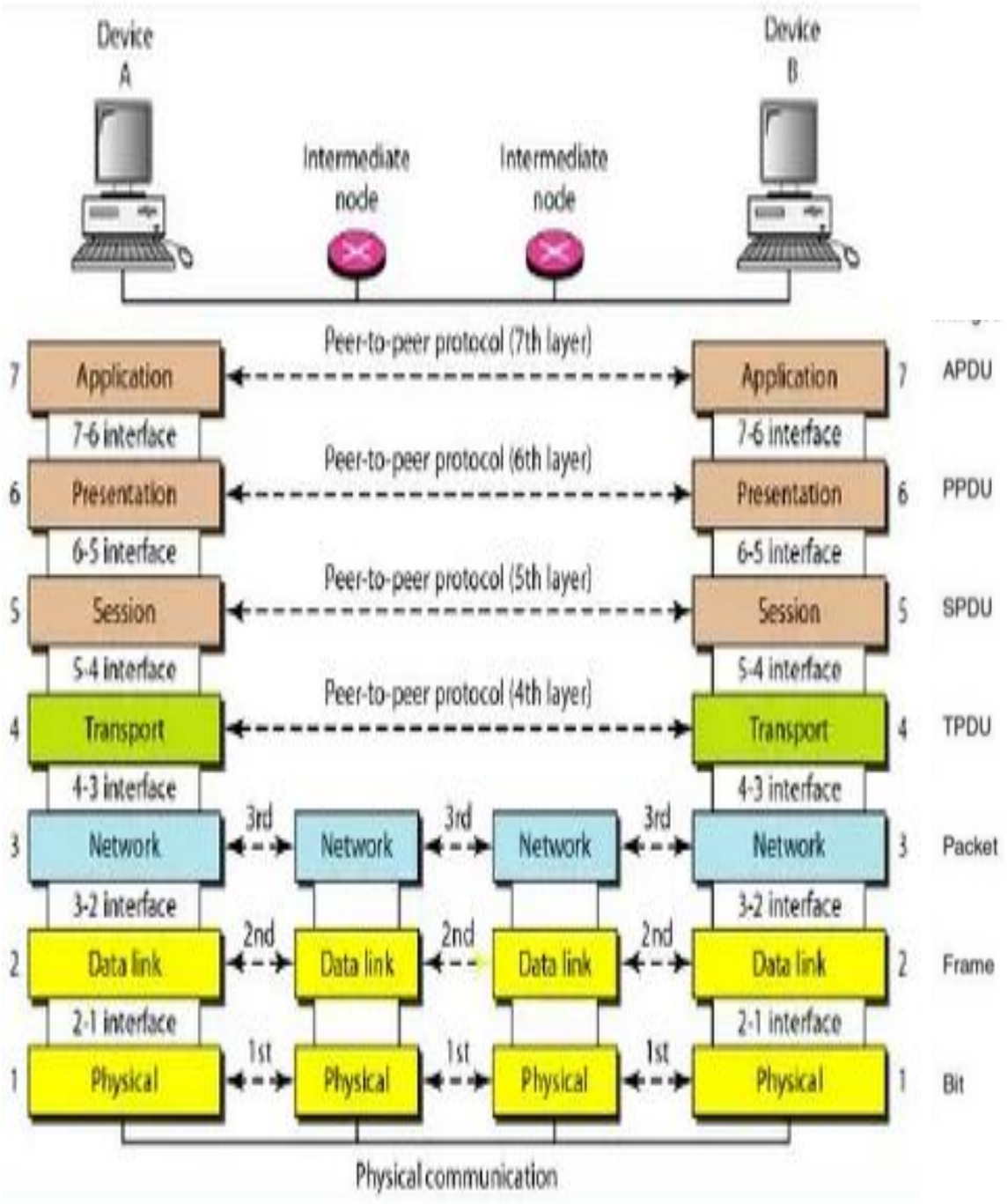
Learn 7 Layers

7 Application Layer
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data Link Layer
1. Physical Layer

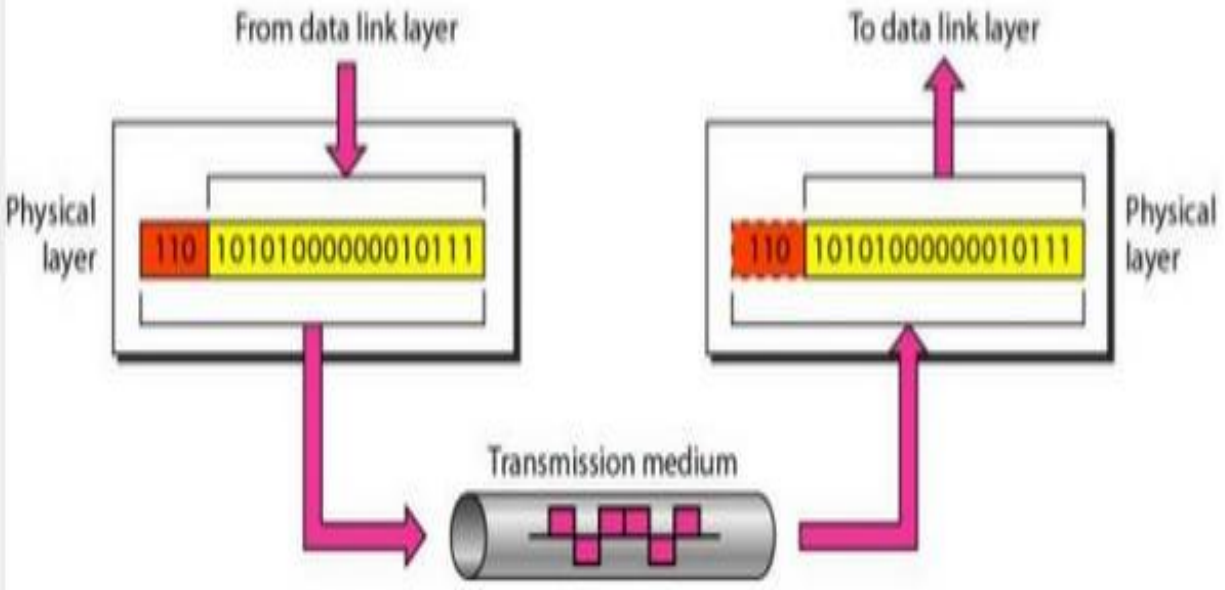
All People Seem To Need Data Processing



The interaction between layers in the OSI model



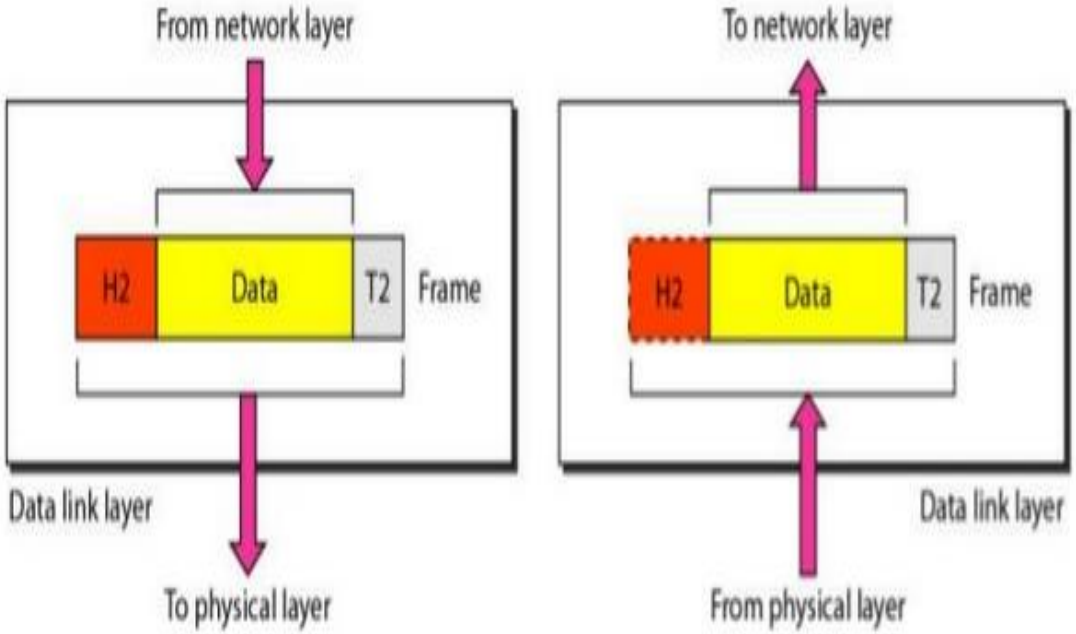
Physical Layer



- Converts **bits** into electronic signals for outgoing messages
- Converts electronic signals into bits for incoming messages
- The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.
- The design issues are
  - **Transmission medium**
  - **Synchronization of bits**
  - **Physical topology**
  - **Transmission mode**
- The bottom layer of the OSI model

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

Data Link Layer

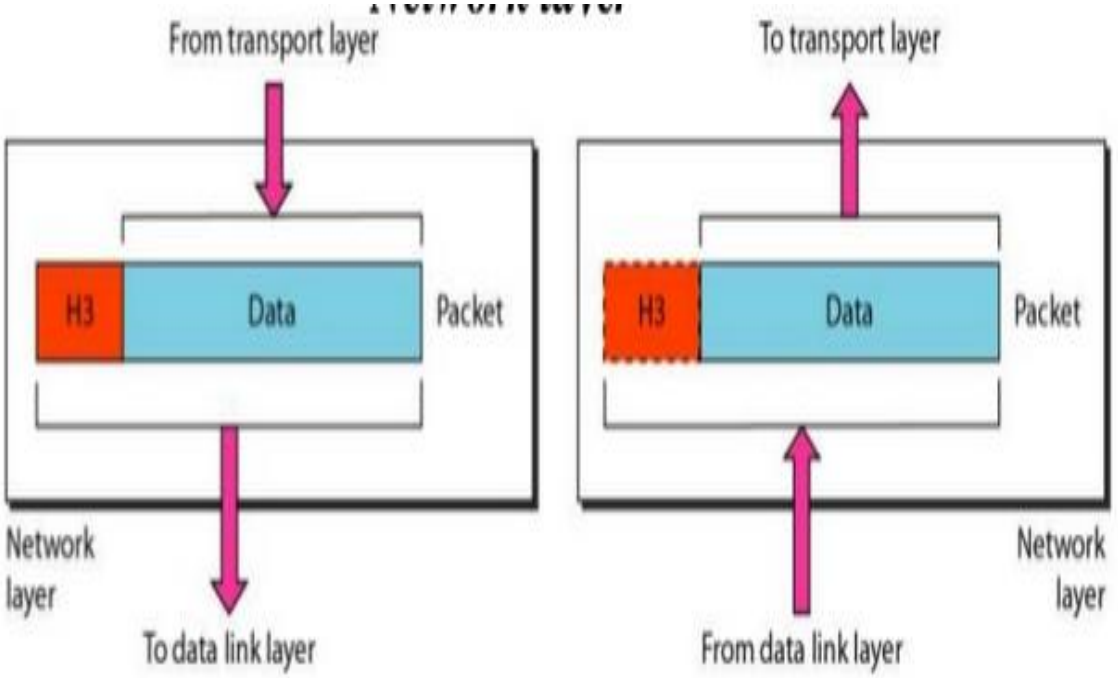


- The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission **errors** to the network layer.
- It accomplishes this task by having the sender break up the input data into data **frames** (typically a few hundred or a few thousand bytes) and transmits the frames sequentially.

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

- At the receiving end, this layer packages raw data from the physical layer into data frames for delivery to the Network layer
- At the sending end this layer handles conversion of data into raw formats that can be handled by the Physical Layer
- If the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement frame**
- The physical layer accepts and transmits stream of bits, the data link layer should create and recognize frame boundaries. This can be accomplished by attaching **special bit patterns to the beginning and ending of frame.**
- A duplicate frame could be sent if the acknowledgement frame from receiver back to the sender were lost.

Network Layer



- The network layer controls the operation of the **subnet**.

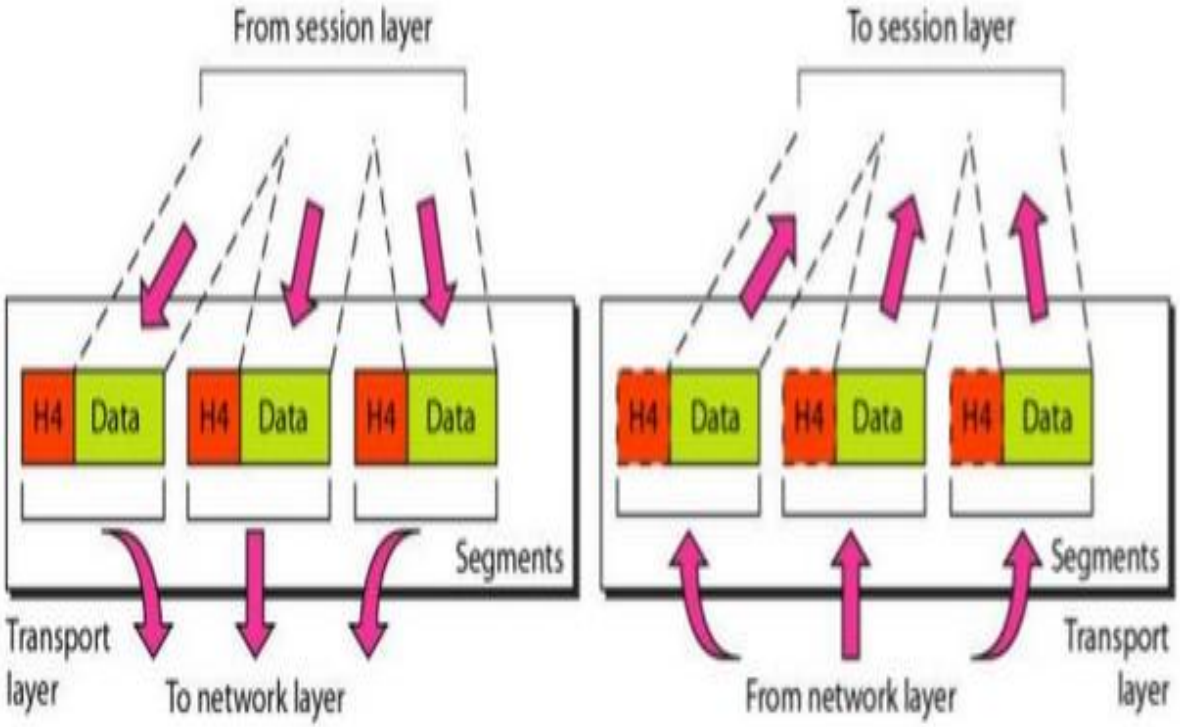
- The network layer is responsible for the delivery of individual **packets** from the source host to the destination host.

- The network layer controls the operation of the subnet. A key design issue is determining how **packets are routed from source to destination.**

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

- Routes can be based on **static tables** that are "wired into" the network and rarely changed. They can also be determined at the **start of each conversation.**
- If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The **control of such congestion** also belongs to the network layer.
- When a packet has to travel from one network to another to get to its destination, many problems can arise. The **addressing** used by the second network **may be different** from the first one. The second one may not accept the packet at all because it is **too large**. The **protocols may differ**, and so on. It is up to the network layer to overcome all these problems

Transport layer



- **Manages the transmission** of data across a network
- Manages the flow of data between parties by segmenting long data streams into smaller data chunks (based on allowed "packet" size for a given transmission medium)
- Reassembles chunks into their original sequence at the receiving end
- Provides **acknowledgements of successful transmissions** and requests **resends for packets** which arrive with **errors**

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

•The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.

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

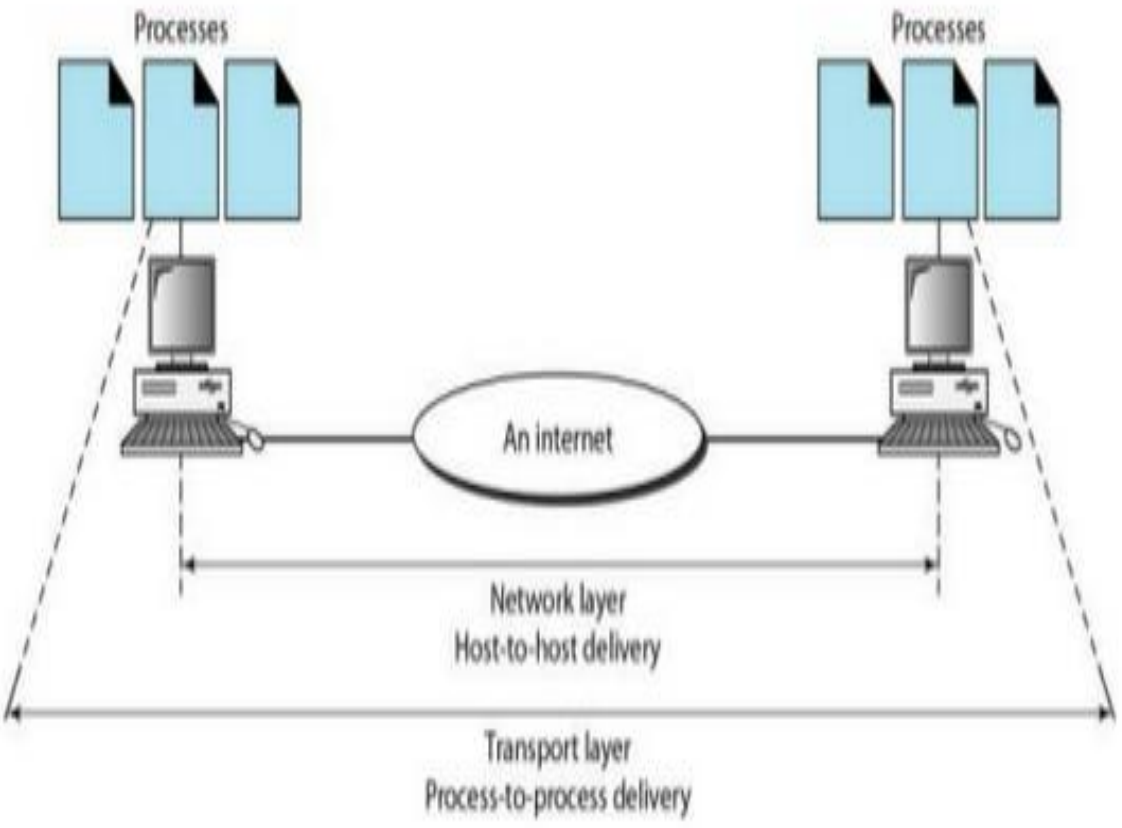
•**If** transport connection requires a high throughput, the transport layer might create multiple network connections.(if expensive multiple several transport connections onto the same network connection).

•The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an **error-free point-to-point channel** that delivers messages or bytes in the order in which they were sent. The type of service is determined when the **connection is established**.

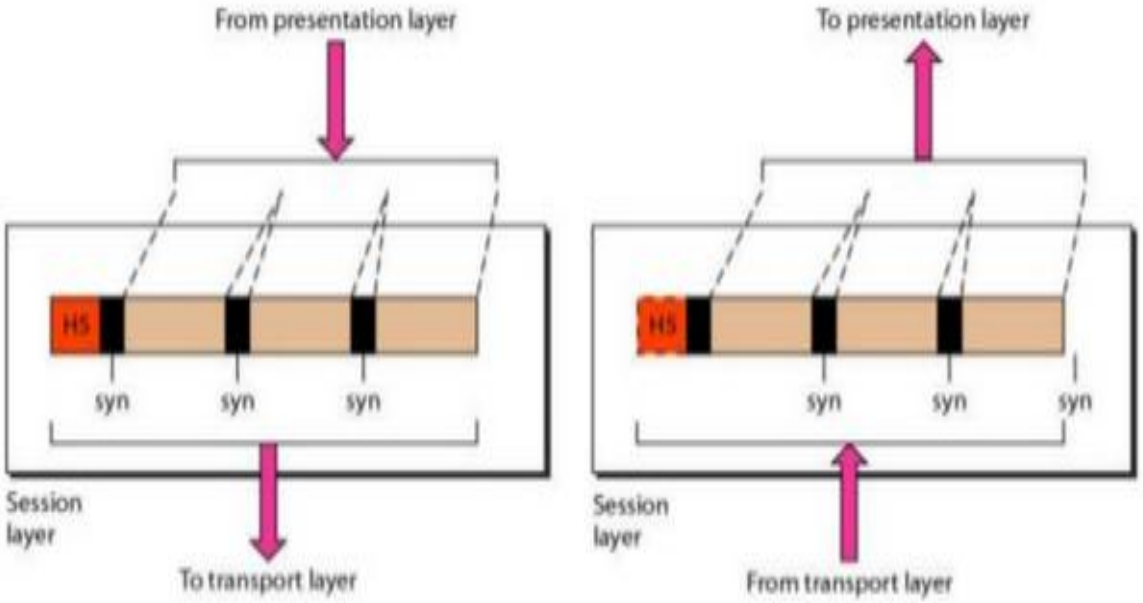
•The transport layer is a **true end-to-end layer**, all the way from the source to the destination.

•The difference between layer 1 through 3 , which are chained, and layer 4 through 7, which are end-to-end

Reliable process-to-process delivery of a message



Session layer

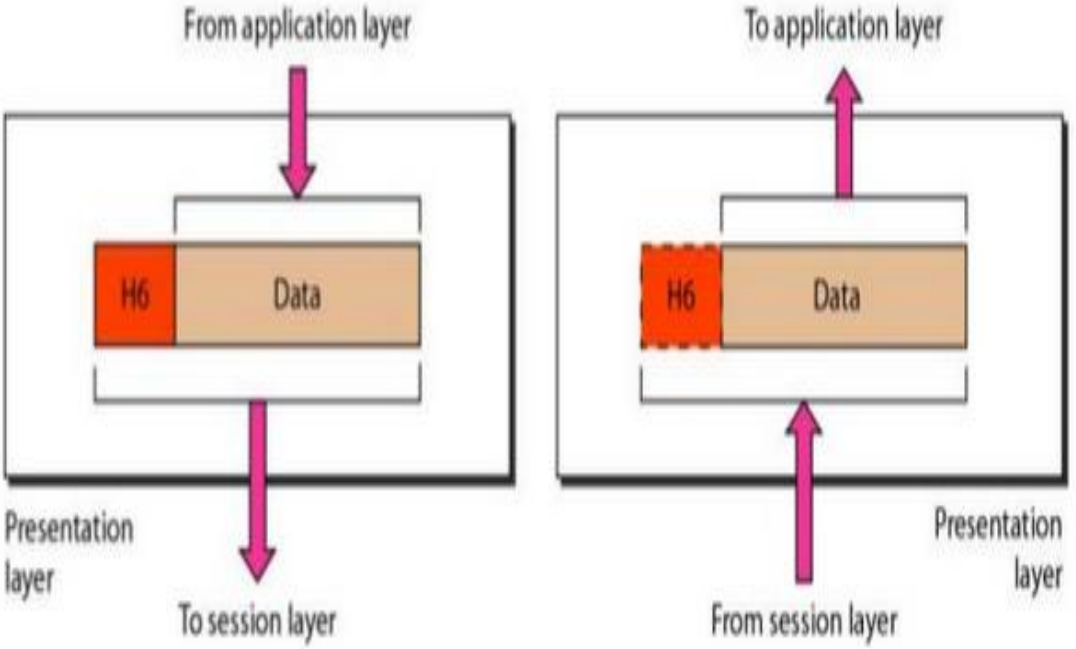


•The session layer allows users on different machines to establish sessions between them.

•Sessions offer various services, including **dialog control** (keeping track of whose turn it is to transmit), **token management** (preventing two parties from attempting the same critical operation at the same time), and **synchronization** (check pointing long transmissions to allow them to continue from where they were after a crash).

The session layer is responsible for dialog control and synchronization.

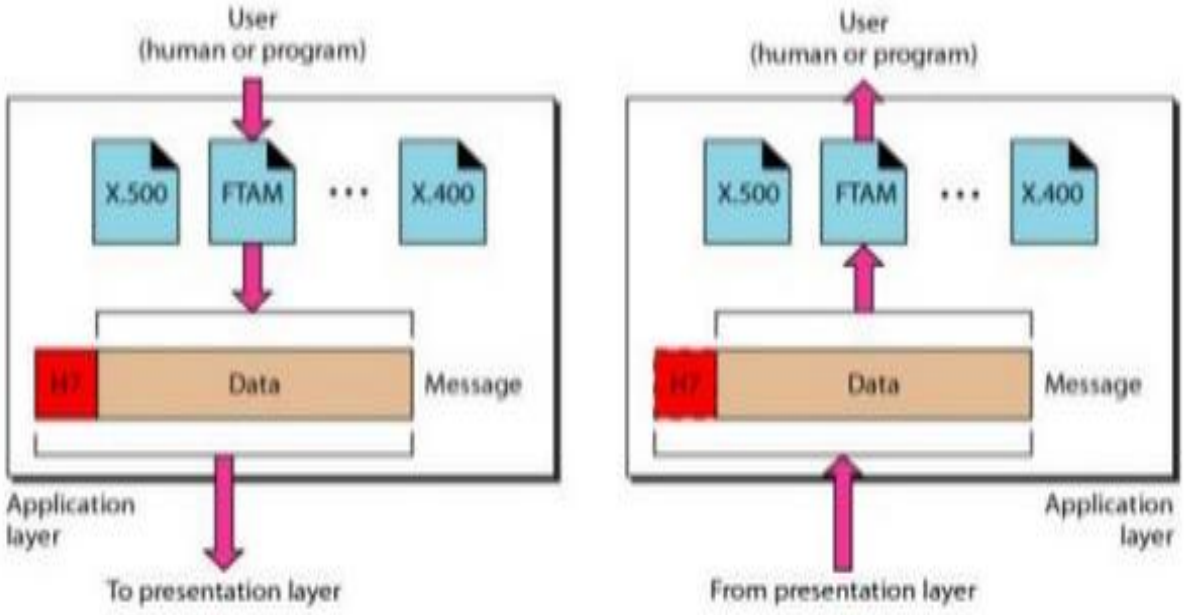
Presentation Layer



- The presentation layer is concerned with the **syntax** and **semantics** of the information transmitted.
- In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

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

Application layer



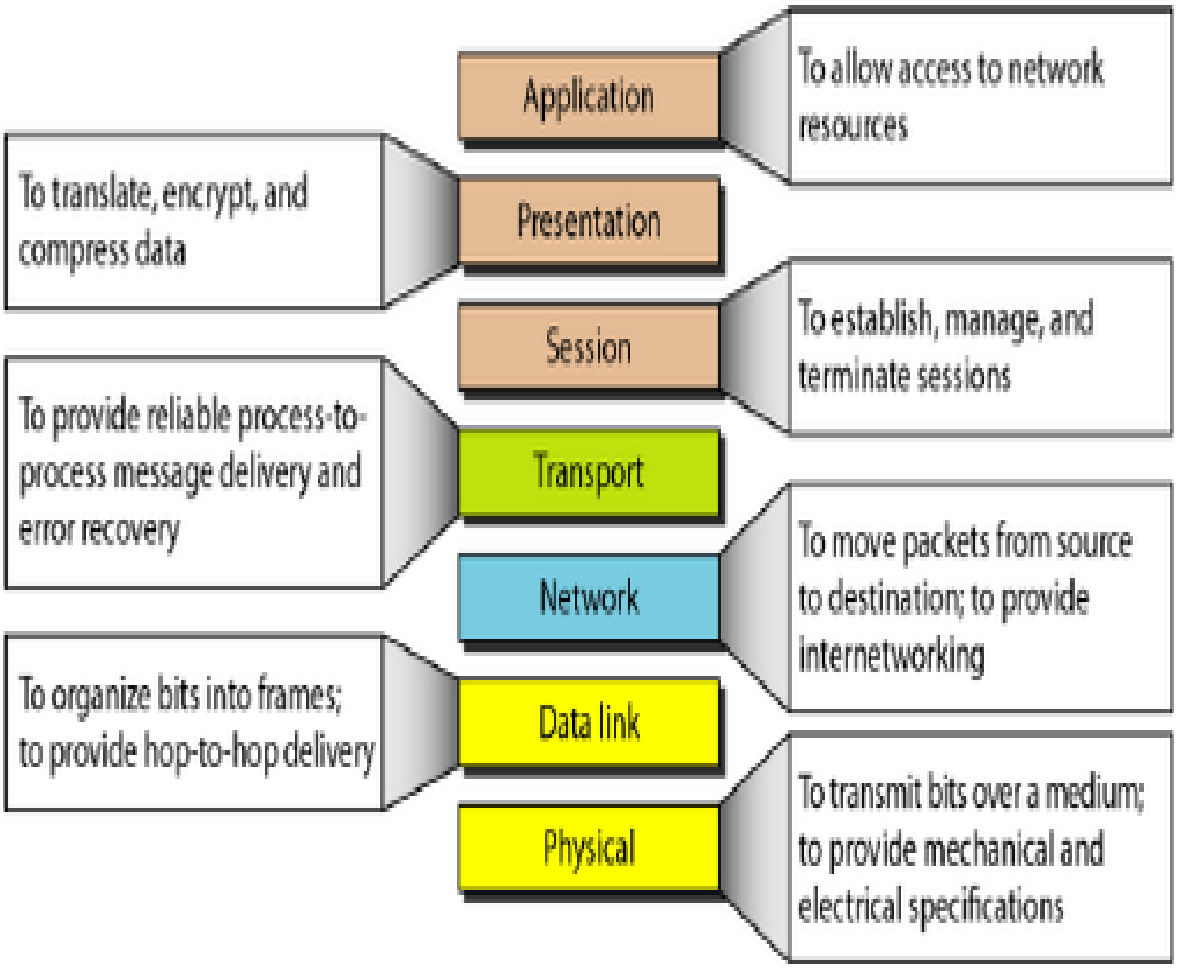
•The application layer is responsible for **providing services to the user**.

•The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

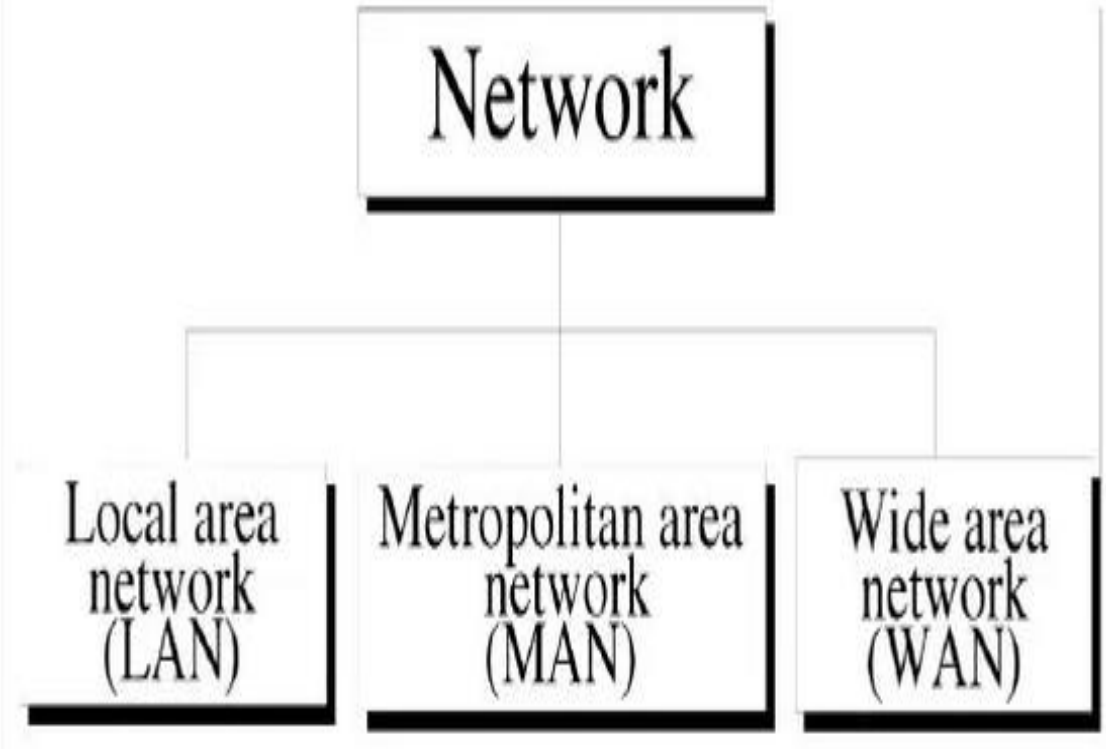
•Network virtual terminal

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

Figure 2.15 *Summary of layers*



Categories of Network



...also known as Back Bone Design

- Classification of interconnected processors by scale.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

•Personal area network is sending a message over a very short distance

•Computers that communicate by exchanging messages over longer cables. LAN MAN WAN

•The connection of two or more networks is called an internetwork.

Personal Area Network (PAN)

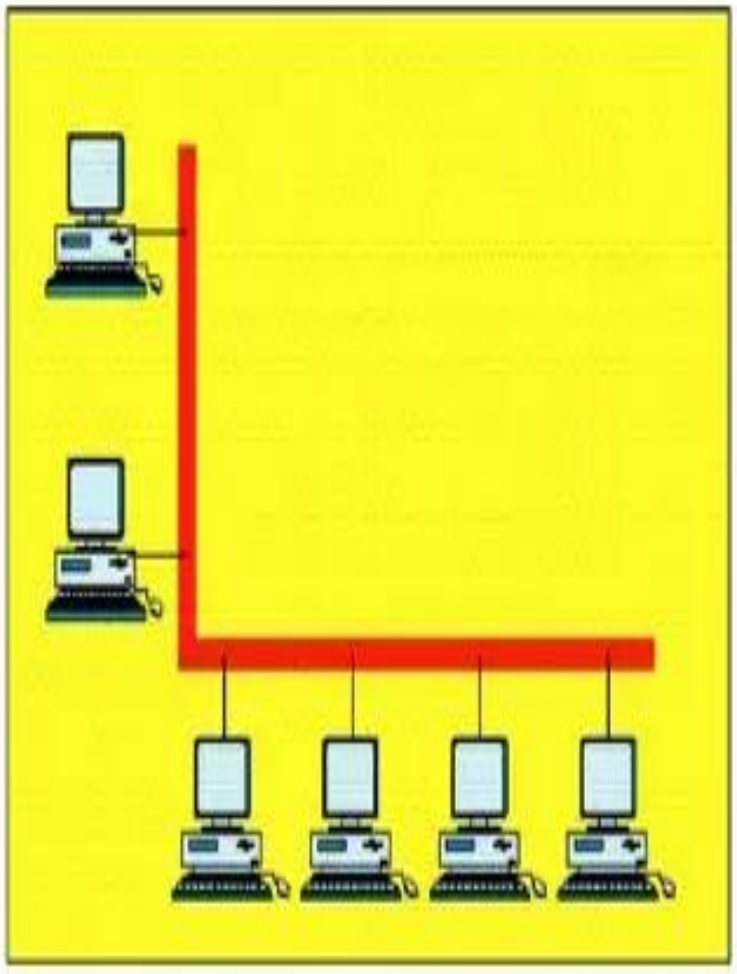
- PAN is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body.
- The devices may or may not belong to the person in question.
- The reach of a PAN is typically a few meters.

Personal Area Network (PAN)

Local Area Network (LAN)

- LAN is usually privately owned and links the devices in a single office, building or campus of up to few kilometers in size.
- LANs are distinguished from other kinds of networks by three categories: their size, transmission technology and topology.
- LANs are restricted in size
  - which means that their worst-case transmission time is bounded and known in advance. Hence is more reliable as compared to MAN and WAN. Knowing this bound makes it possible to use certain kinds of design that would not otherwise be possible. It also simplifies network management.
- LAN typically uses transmission technology consisting of single cable to which all machines are connected.
  - Traditional LANs run at speeds of 10 to 100 Mbps (but now much higher speeds can be achieved).
- The most common LAN topologies are bus, ring and star.

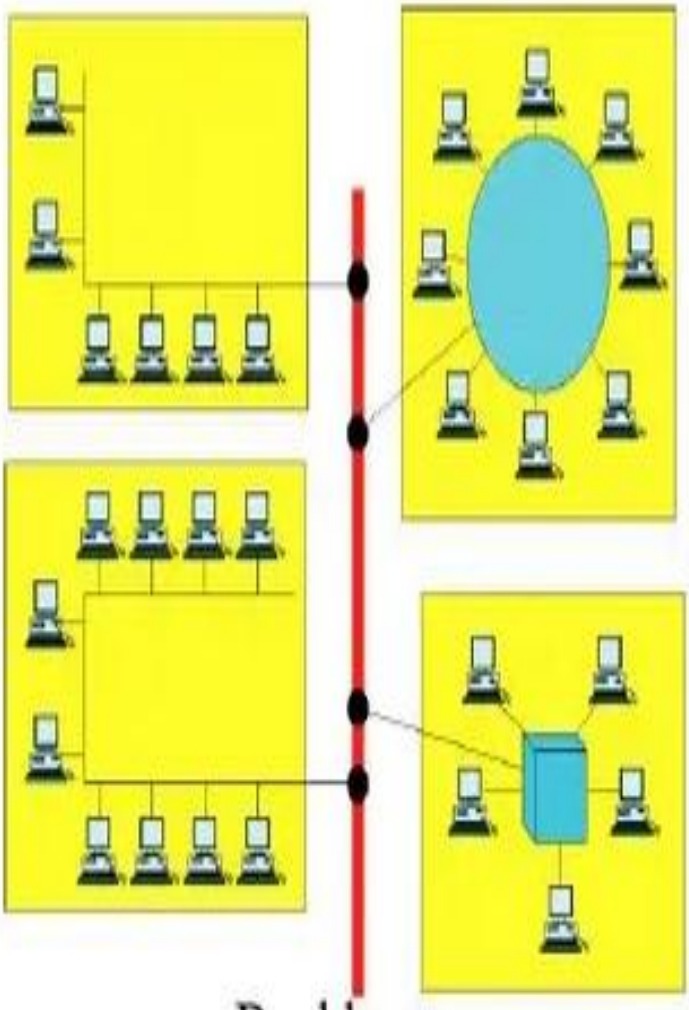
Local Area Network



Single building LAN

continued

Local Area Network



Multiple building LAN

Local Area Networks

Standardization Body

IEEE (Institute of Electric and Electronic Engineers) 802 group

For example:

802.3: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) (Ethernet is one of them.)

802.4: Token Bus

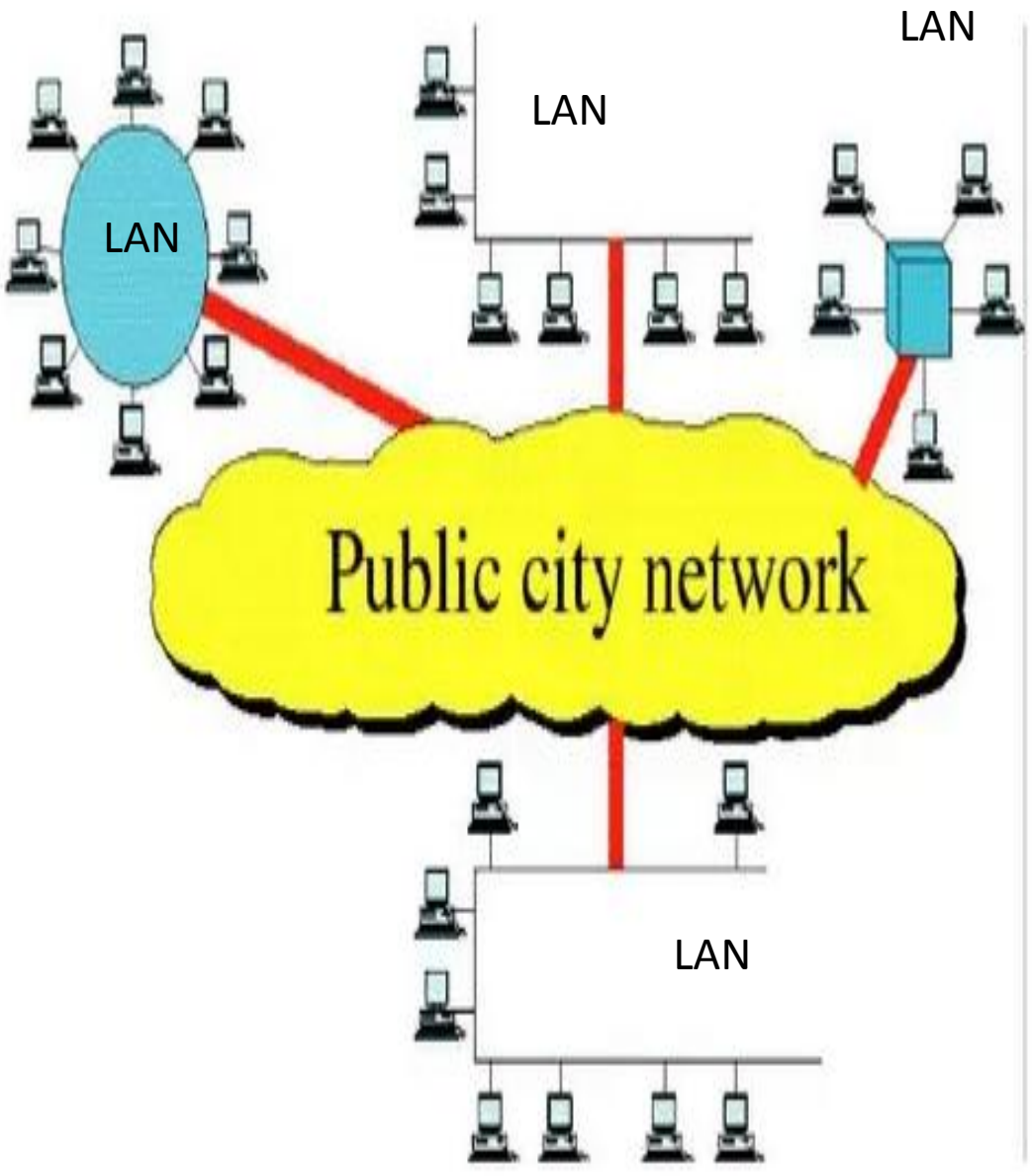
802.5: Token Ring

Metropolitan Area Networks (MAN)

- MAN is designed to extend over the entire city.
- It may be a single network as a cable TV network or it may be means of connecting a number of LANs into a larger network so that resources may be shared.
- MAN is wholly owned and operated by a private company or may be a service provided by a public company.

- The main reason for distinguishing MANs as a special category is that a standard has been adopted for them. It is DQDB (Distributed Queue Dual Bus) or IEEE 802.6.

Metropolitan Area Network (Example)



Metropolitan Area Networks

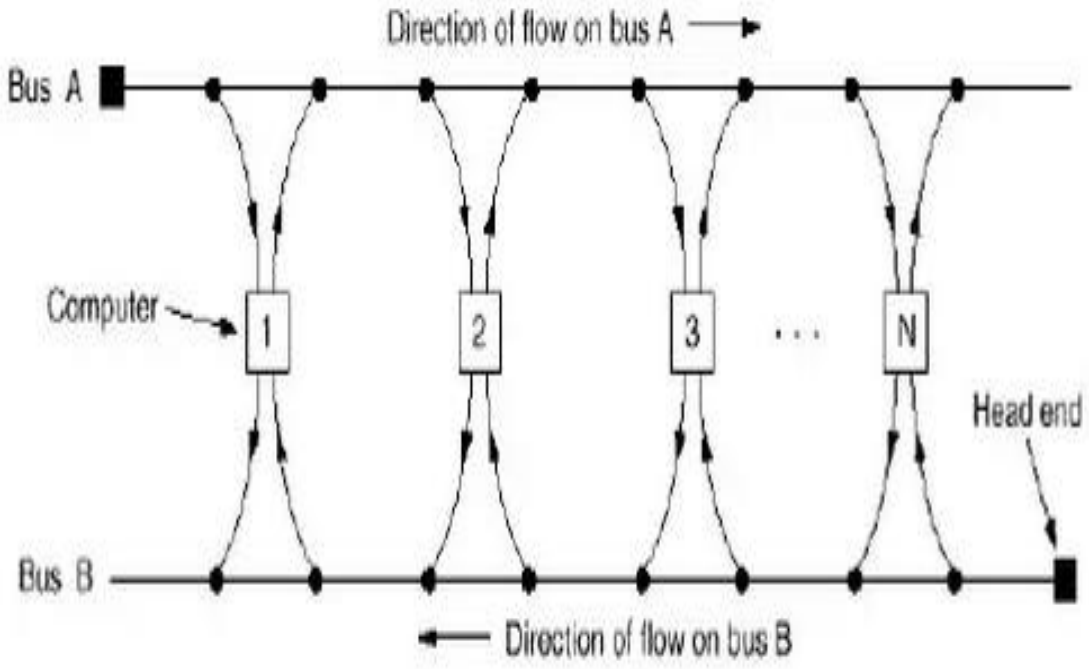


Fig. 1-4. Architecture of the DQDB metropolitan area network.

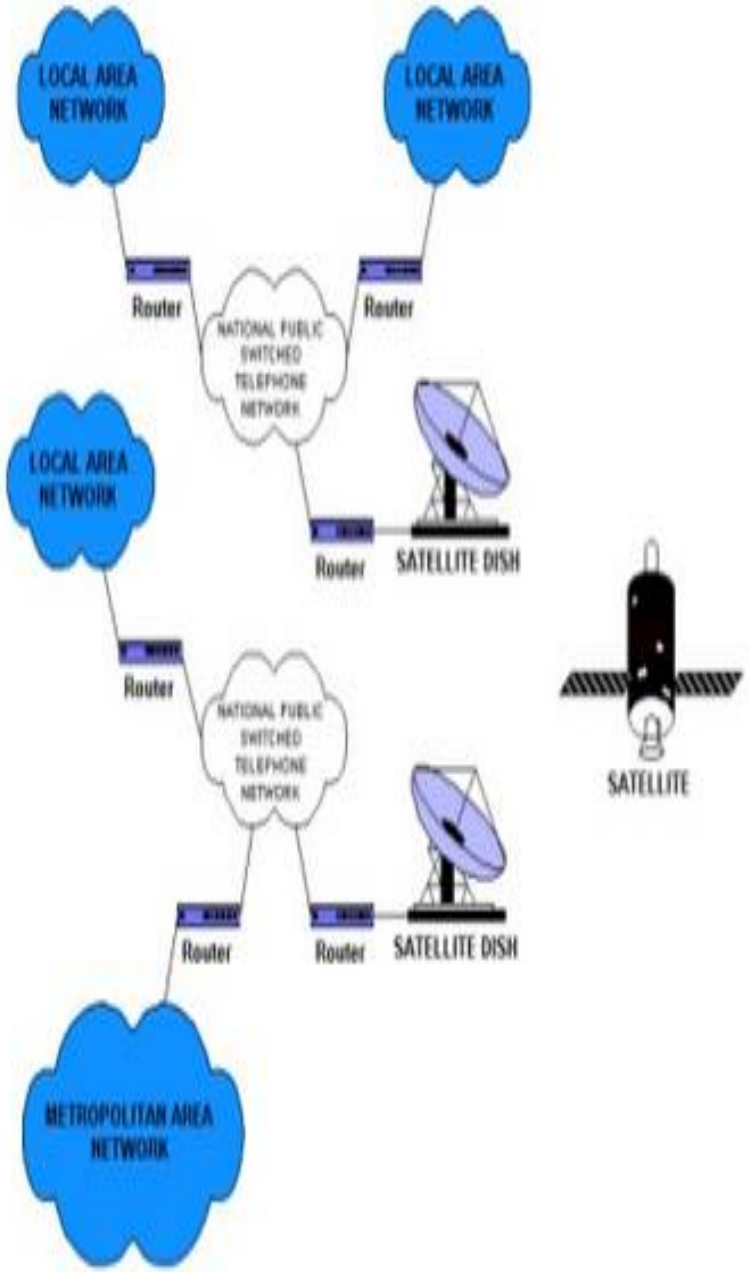
DQDB: Distributed Queue Dual Bus (IEEE 802.6 standard)

Wide Area Network (WAN)

- WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world.
- WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles.

- A WAN that is wholly owned and used by a single company is often referred to as *enterprise network.*

Wide Area Network (WAN)



Wide Area Networks

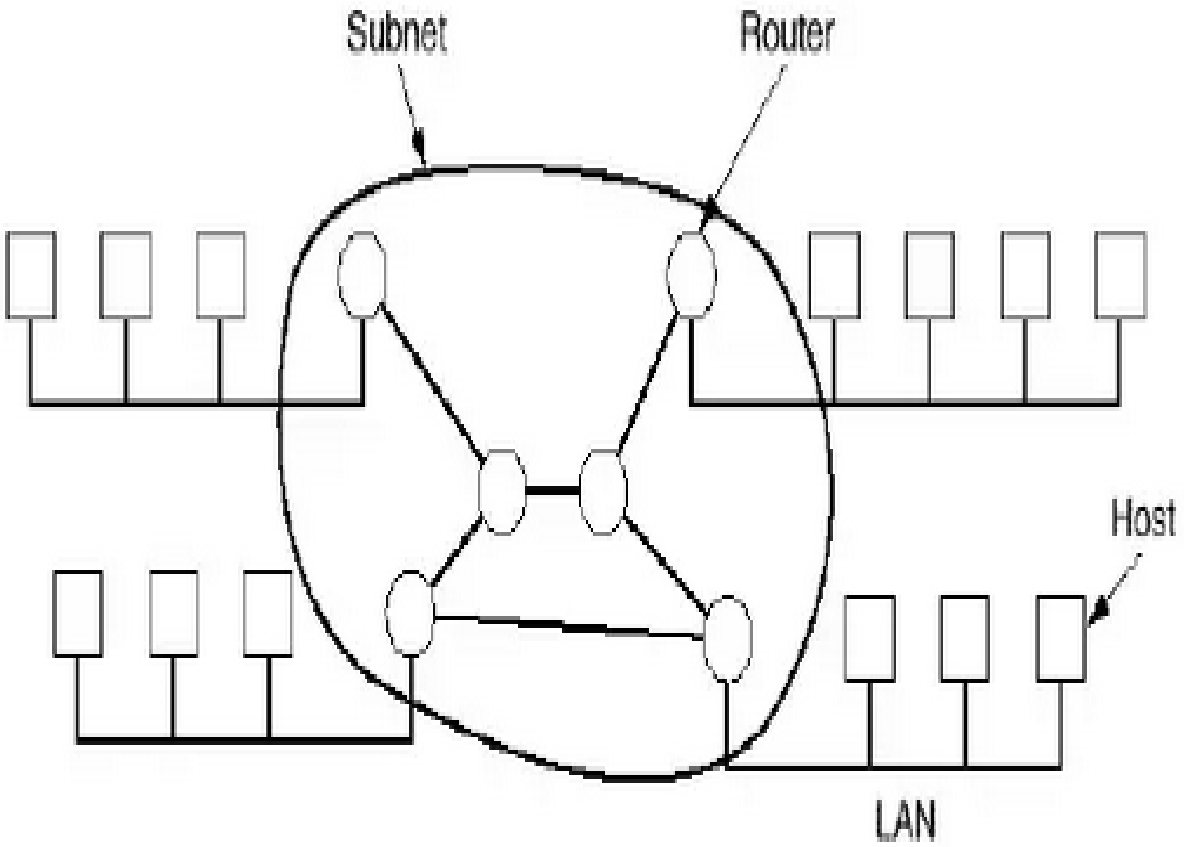
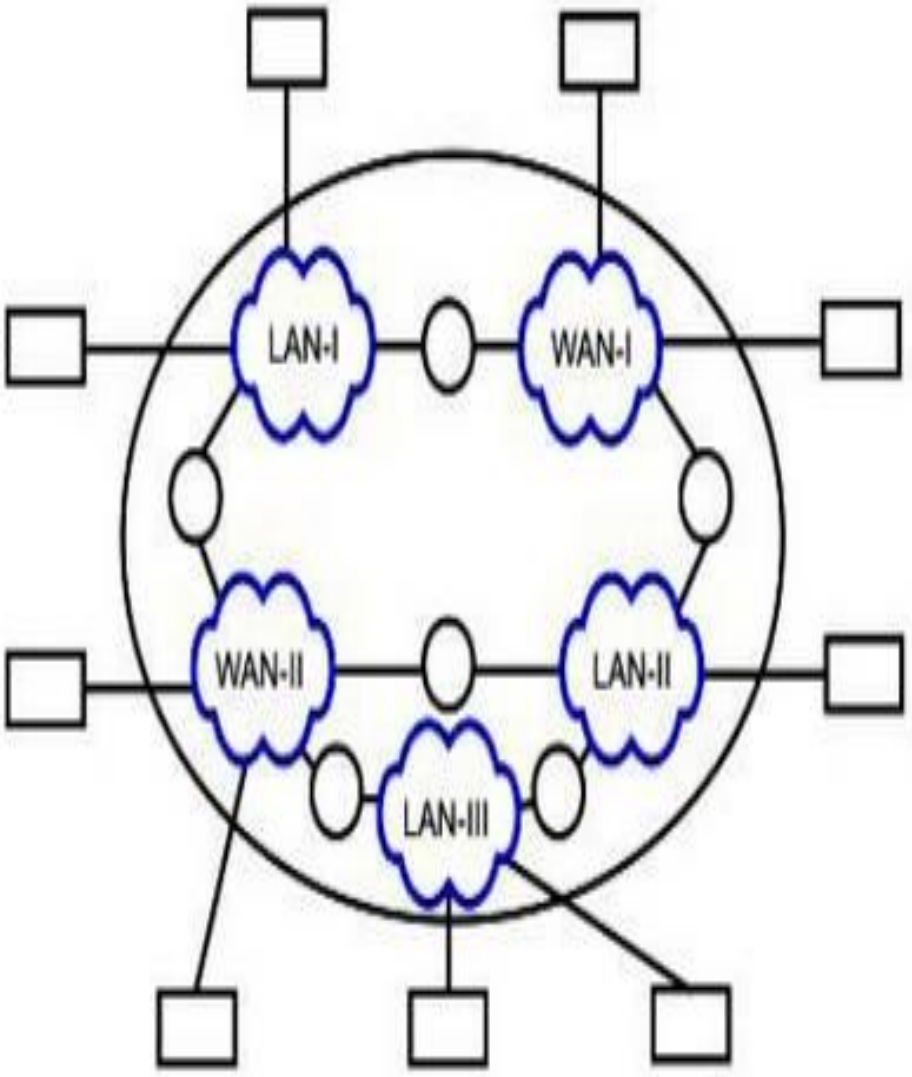


Fig. 1-5. Relation between hosts and the subnet.

Internet – network of networks

- Internet is a collection of networks or network of networks.
- The basic difference between WAN and Internet is that WAN is owned by a single organization while internet is not so.



Delay Analysis

1. Processing Delay(header)
2. Queuing Delay
3. Transmission Delay(1st come 1st serve)
4. Propagation Delay(physical medium)

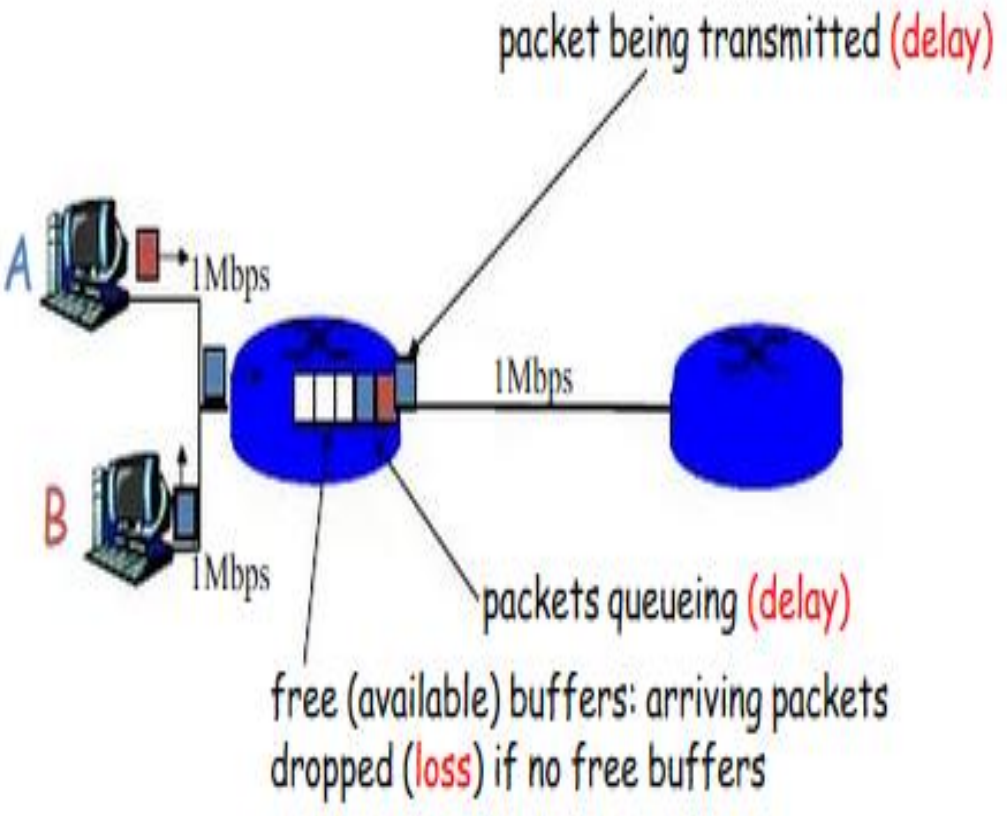
Packet losses

- Queue (buffer) preceding link in buffer has finite capacity
- When packet arrives to full queue, packet is dropped (lost)
- Lost packet may be retransmitted by previous node, by source end system, or not retransmitted at all, depending the protocols

How do loss and delay occur?

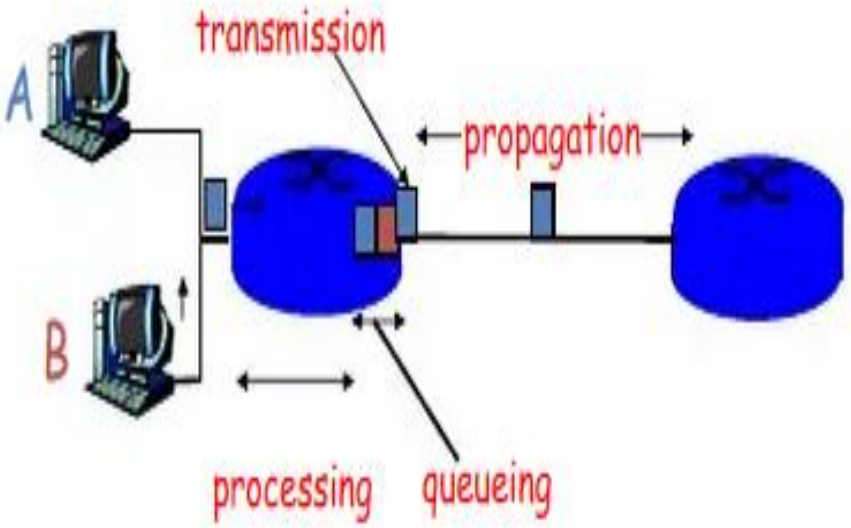
packets *queue* in router buffers

- packet arrival rate to link exceeds output link capacity
- packets queue, wait for turn



Delay: Four sources of delay

- 1. processing:
  - check bit errors
  - determine output link (routing table lookup)
  - Policies etc
- 2. queueing
  - time waiting at output link for transmission
  - depends on congestion level of router and queue size



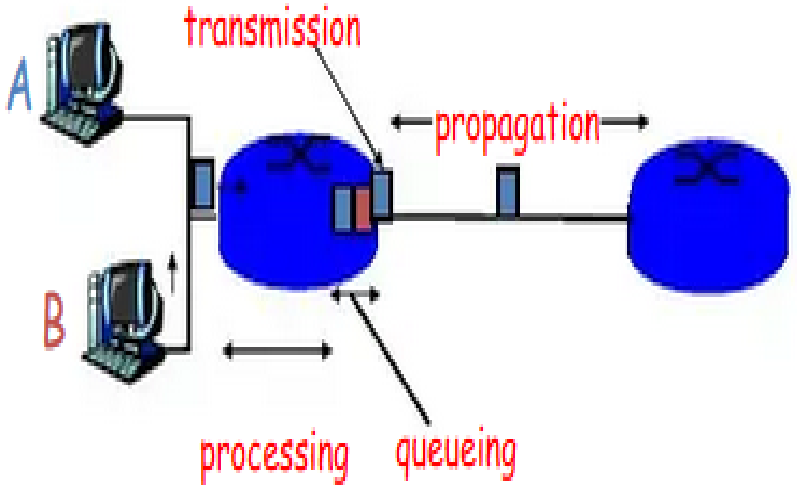
Four sources of packet delay

3. Transmission delay:

- R=link bandwidth (bps)
- L=packet length (bits)
- time to send bits into link = L/R

4. Propagation delay:

- d = length of physical link
- s = propagation speed in medium (~$2x10^8$ m/sec)
- propagation delay = d/s



Physical Layer Transmission Media

- The transmission medium can be defined as a pathway that can transmit information from a sender to a receiver.

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. We could say that transmission media belong to layer zero. Figure 1 shows the position of transmission media in relation to the physical layer.

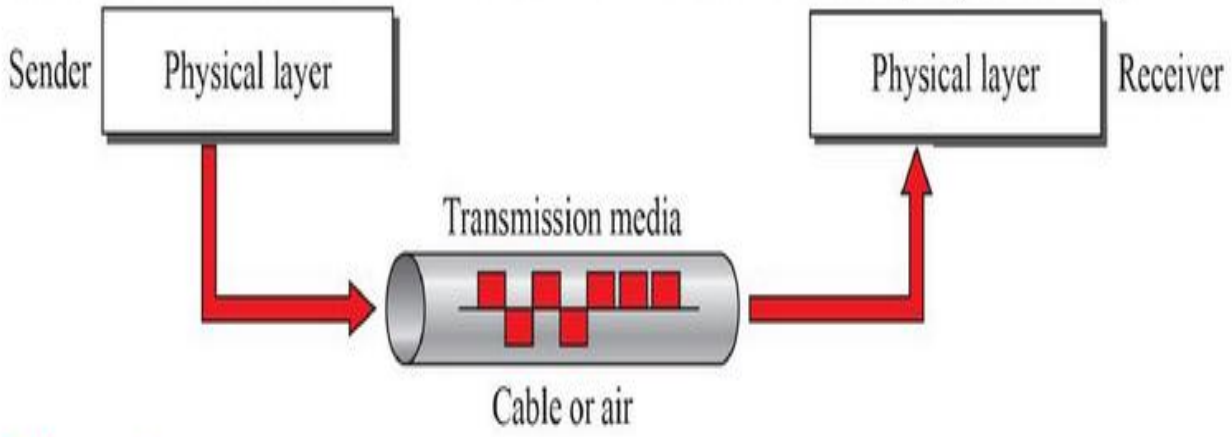


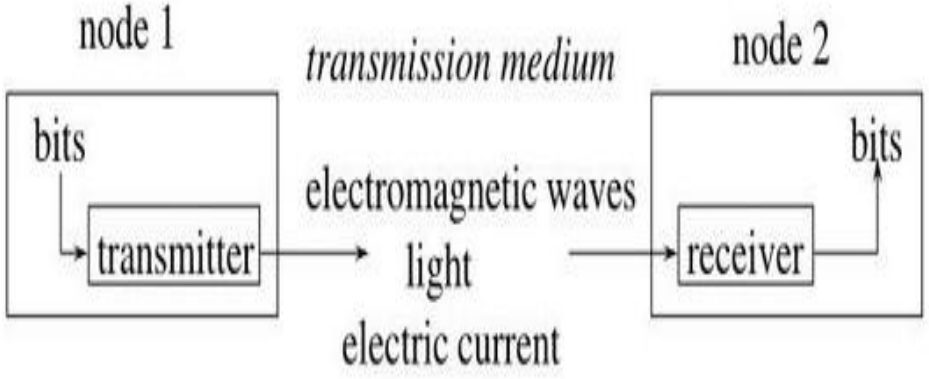
Figure 1: Transmission media and physical layer

Physical Layer Transmission Media

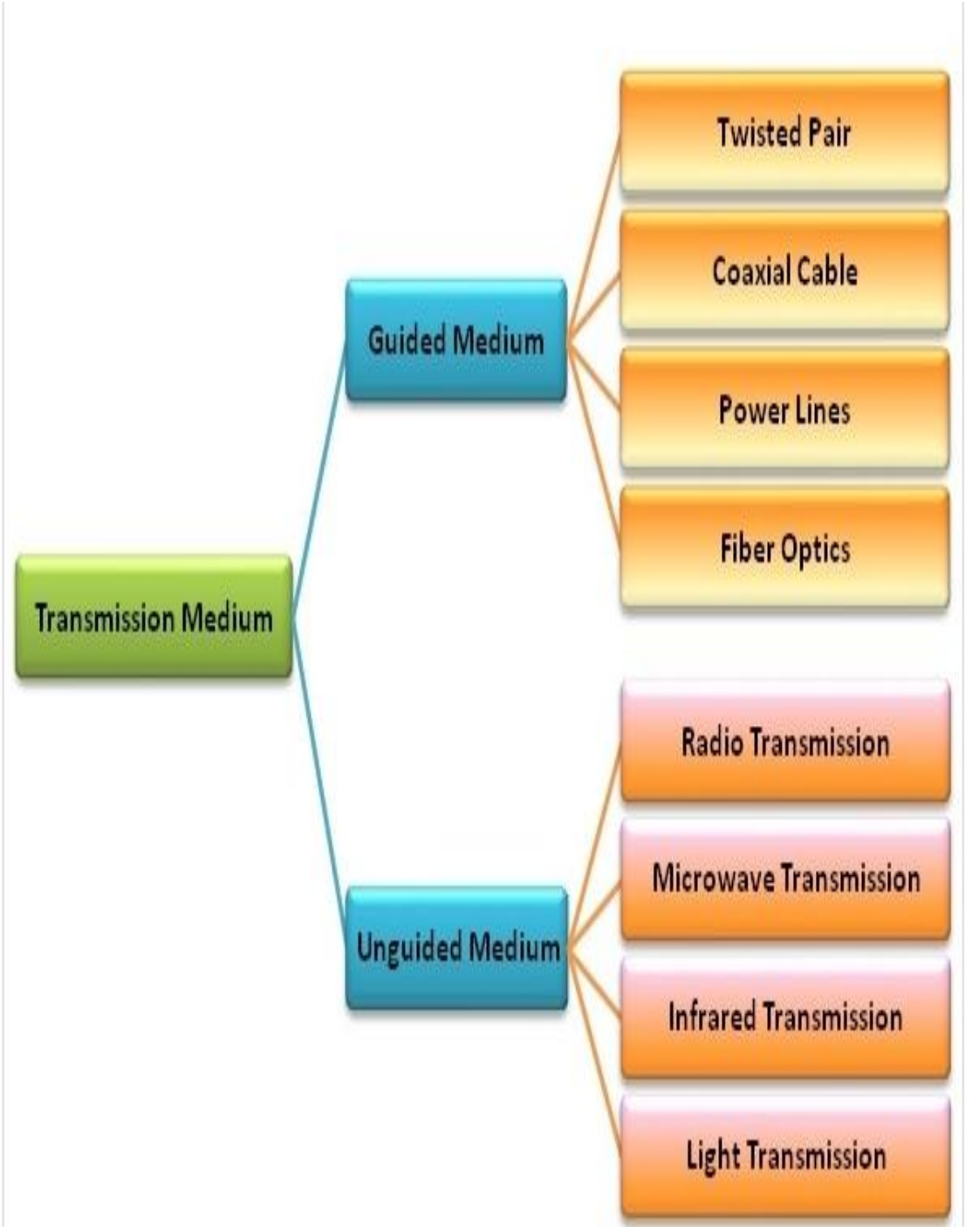
Transmission media are also called communication channels.

Transmission media are of two types –

- Guided Transmission Medium (wire)
- Unguided Transmission Medium



The following chart categorizes transmission media –



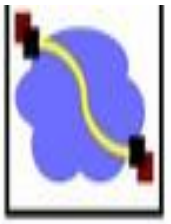
Guided Transmission Medium

Guided transmission media are also called **bounded media** or **wired media**. They comprise cables or wires through which data is transmitted. They are called guided since they provide a physical conduit from the sender device to the receiver device. The signal travelling through these media are bounded by the physical limits of the medium.

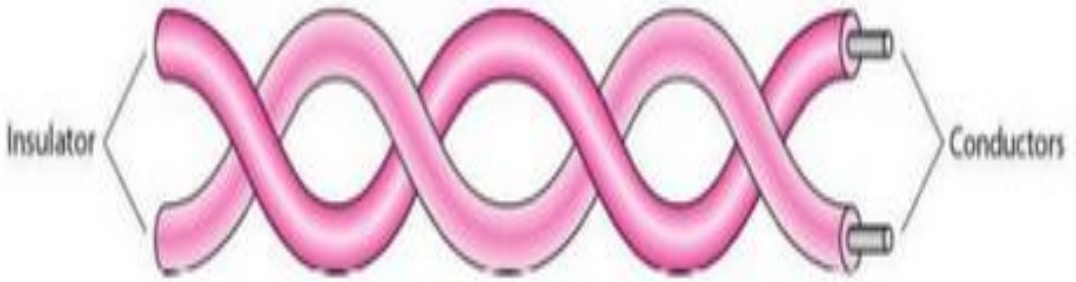
The most popular guided media are –

- Twisted pair cable
- Coaxial cable
- Power lines
- Fiber optics

Twisted Pair



- Twisted-pair is one of the oldest and still most common transmission media of cabling that is used for telephone communications and most modern Ethernet networks. Twisted pairs can be used for transmitting either analog or digital signals.
- The wires are twisted together in a helical form, just like a DNA molecule. Twisting is done because two parallel wires constitute a fine antenna. When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively..



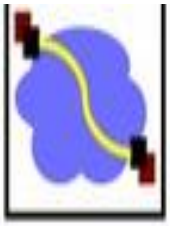
- There are two basic types, shielded twisted-pair (STP) and unshielded twisted-pair (UTP).

15

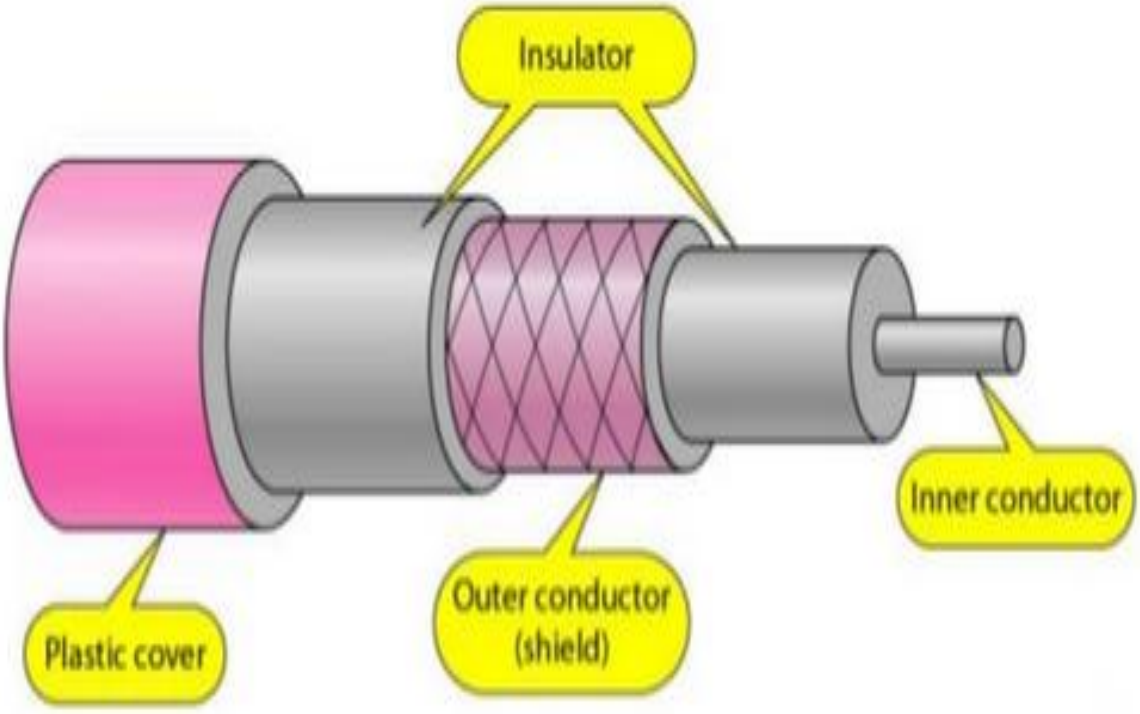
Twisted Pair - Applications

- **Most common medium**
- **Telephone network**
  - Between house and local exchange (subscriber loop)
- **Within buildings**
  - To private branch exchange (PBX)
- **For local area networks (LAN)**
  - 10Mbps or 100Mbps

Co-axial Cable



- A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh. The outer conductor is covered in a protective plastic sheath.



Coaxial Cable Applications

- **Most versatile medium**
- **Television distribution**
  - Ariel to TV
  - Cable TV
- Long distance telephone transmission
  - Can carry 10,000 voice calls simultaneously
  - Being replaced by fiber optic
- Short distance computer systems links
- Local area networks

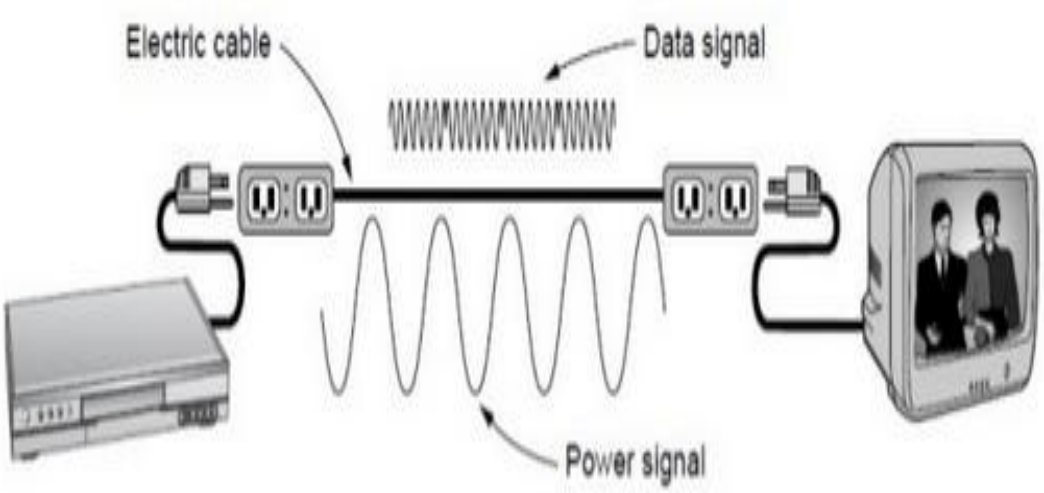
Power Lines

The difficulty with using household electrical wiring for a network is that it was designed to distribute power signals, a 50-60 Hz signal.

The wire attenuates the much higher frequency (MHz) signals needed for high-rate data communication.

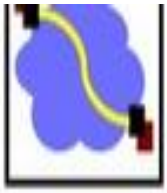
Noises when appliances are turned on or off

Under development and standardization



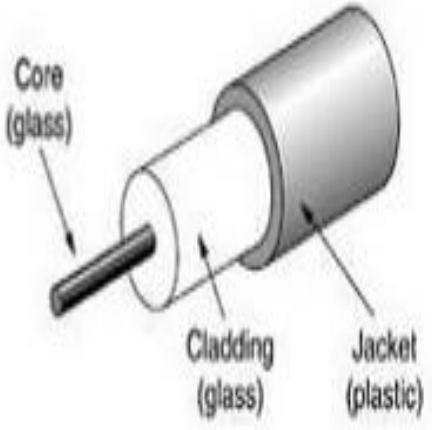
A network that uses household electrical wiring.

Optical Fiber

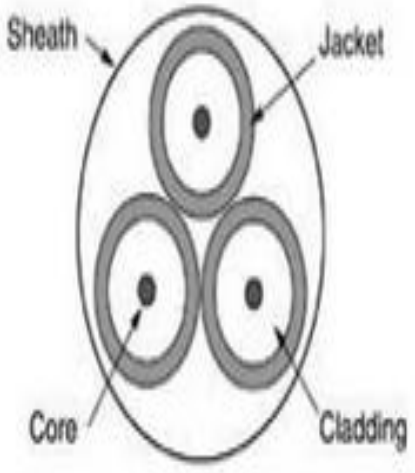


- Fiber-optic cable or optical fiber consists of thin glass fibers that can carry information in the form of visible light. The typical optical fiber consists of a very narrow strand of glass or plastic called the ***core***.

- Around the core is a concentric layer of less dense glass or plastic called the ***cladding***, whose refractive index is less than that of the core. The outer most layer of the cable is known as the jacket, which shields the cladding and the core from moisture, crushing and abrasion.



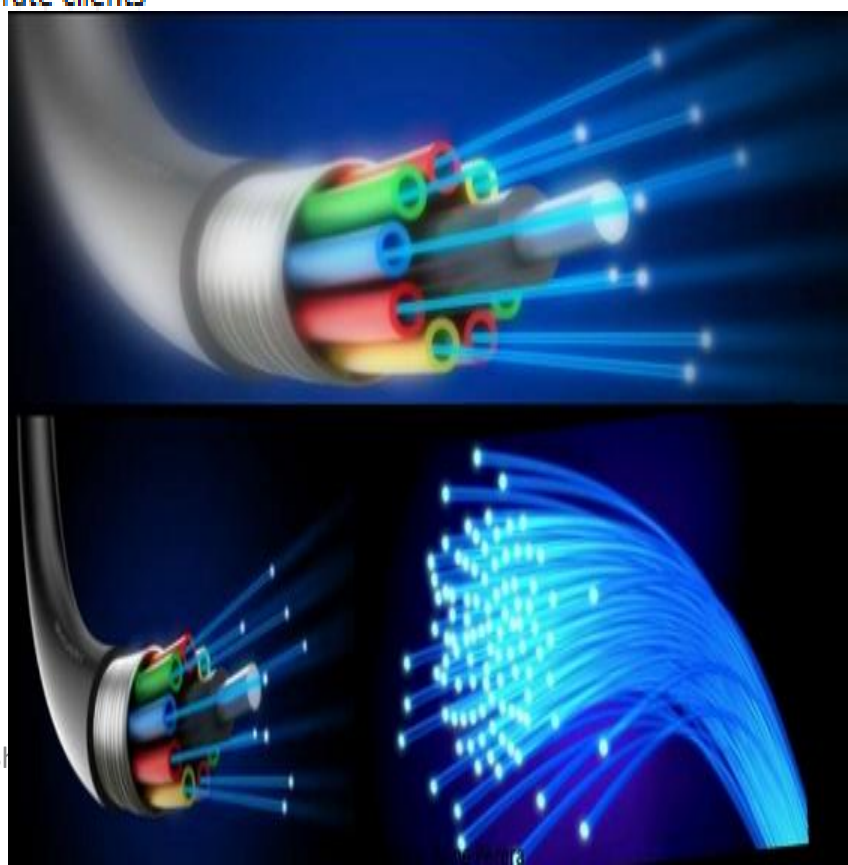
(a)



(b)

Optical Fiber - Applications

- Long-haul trunks
  - 1500km, 20 – 60k voice channels
- Metropolitan trunks
  - 12 km, 100k channels
- Rural exchange trunks
  - 40 – 160Km, 5k voice channels
- Subscriber loops
  - Voice data cables leased by corporate clients
- LANs
  - 100Mbps – 1 Ghz



Transmission Characteristics of Guided Media

	Frequency Range	Typical Attenuation	Typical Delay	Repeater Spacing
Twisted pair (with loading)	0 to 3.5 kHz	0.2 dB/km @ 1 kHz	50 μs/km	2 km
Twisted pairs (multi-pair cables)	0 to 1 MHz	0.7 dB/km @ 1 kHz	5 μs/km	2 km
Coaxial cable	0 to 500 MHz	7 dB/km @ 10 MHz	4 μs/km	1 to 9 km
Optical fiber	186 to 370 THz	0.2 to 0.5 dB/km	5 μs/km	40 km

A Comparison

Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

Unguided Transmission Medium

Unguided transmission media are also called wireless media. They transport data in the form of electromagnetic waves that do not require any cables for transmission. These media are bounded by geographical boundaries. These type of communication is commonly referred to as wireless communications.

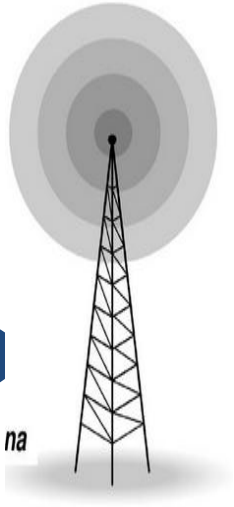
Unguided signals can travel in three ways −

- Ground propagation
- Sky propagation
- Line – of – sight propagation

The commonly used unguided transmissions are −

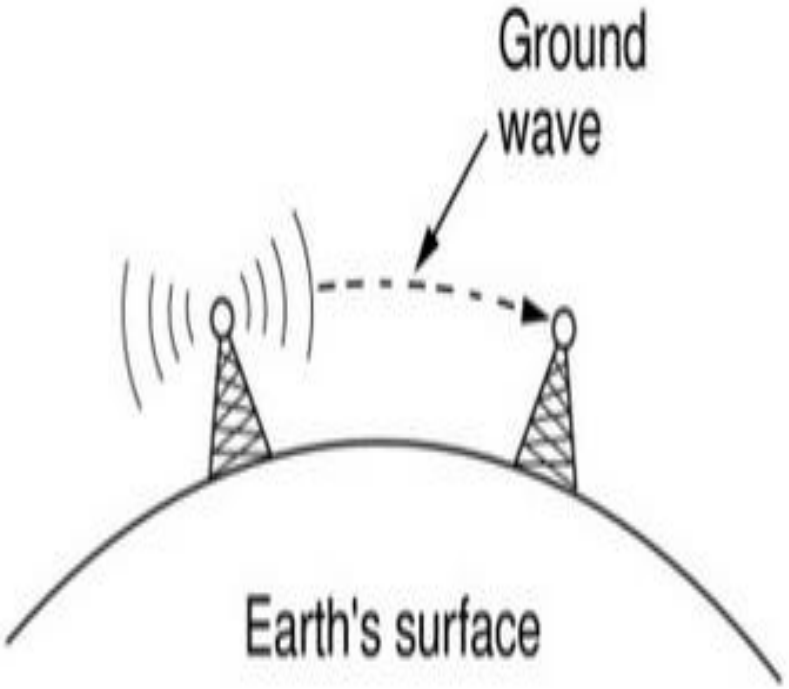
- Radio transmission
- Microwave transmission
- Infrared transmission
- Light transmission

Radio transmissio



- Radio Transmission Radio waves are **easy to generate**, can **travel long distance**, and penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
- Radio waves are also **omni directional**, meaning that they travel in all directions from the source, so that the transmitter and receiver do not have to be carefully aligned physically.
- Omni directional waves sometimes can have undesired side effects.
- The Transmitter and Receiver do not have to be in direct line of sight.
- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves;

Radio Transmission (1)

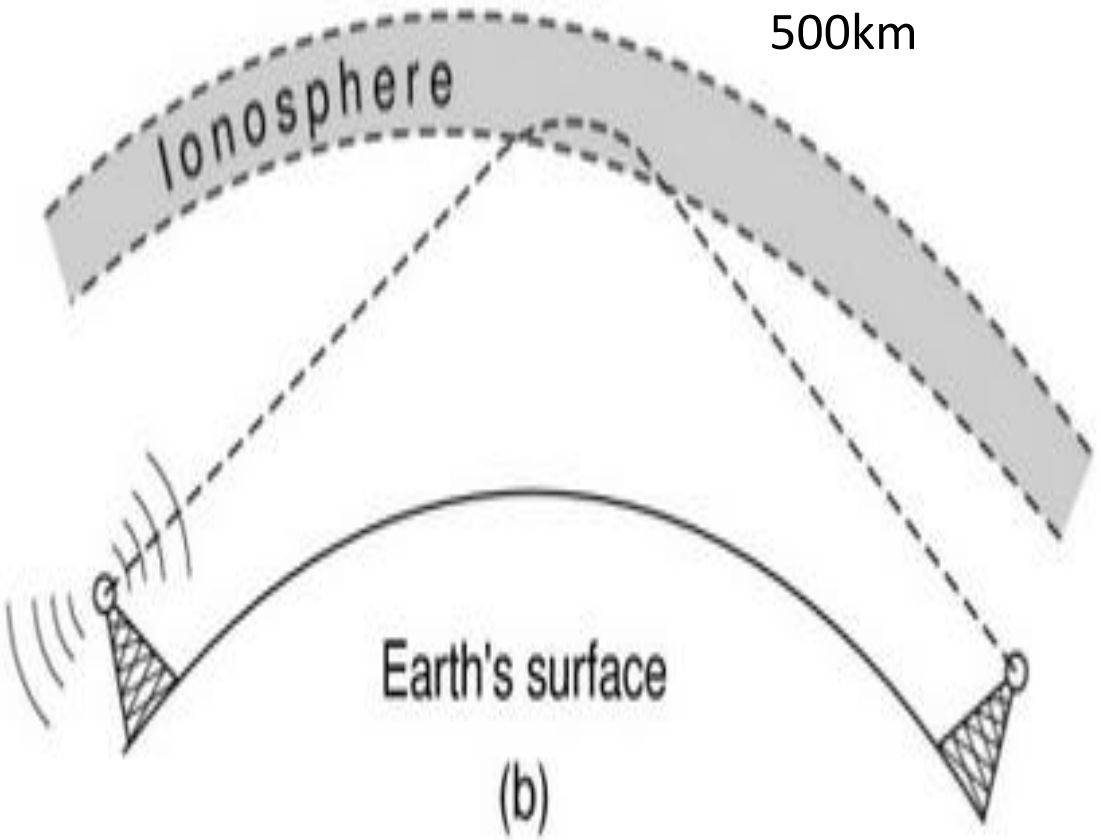


(a)

In the VLF, LF, and MF bands, radio waves follow the curvature of the earth

Radio Transmission (2)

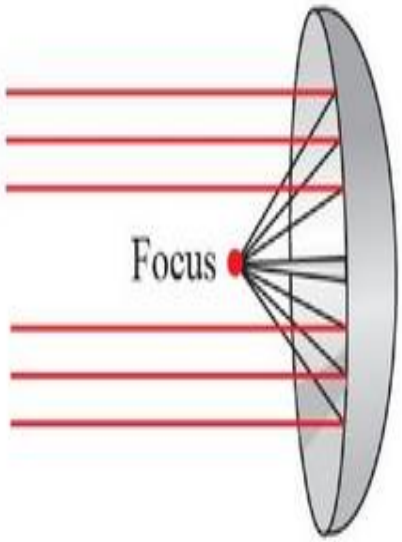
At height 100 to 500km



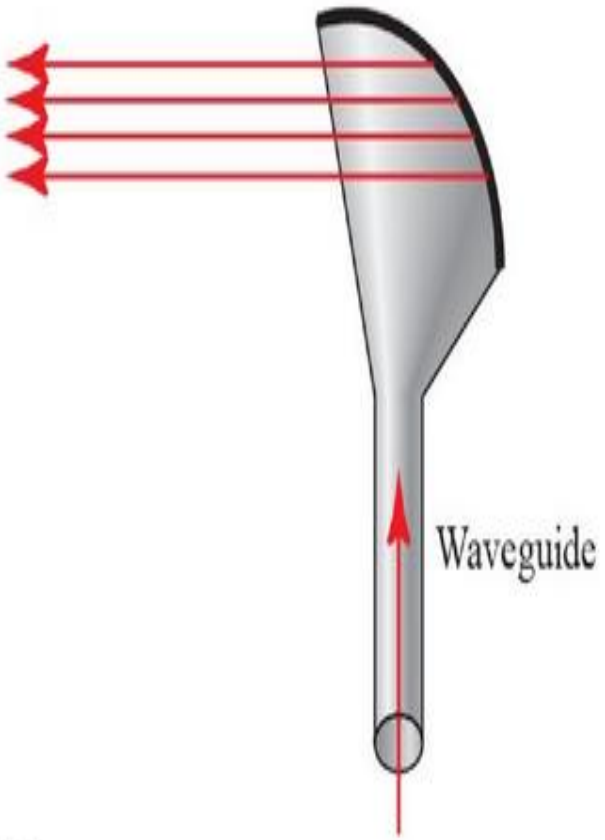
In the HF band, they bounce off the ionosphere.

Microwaves Transmission

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.



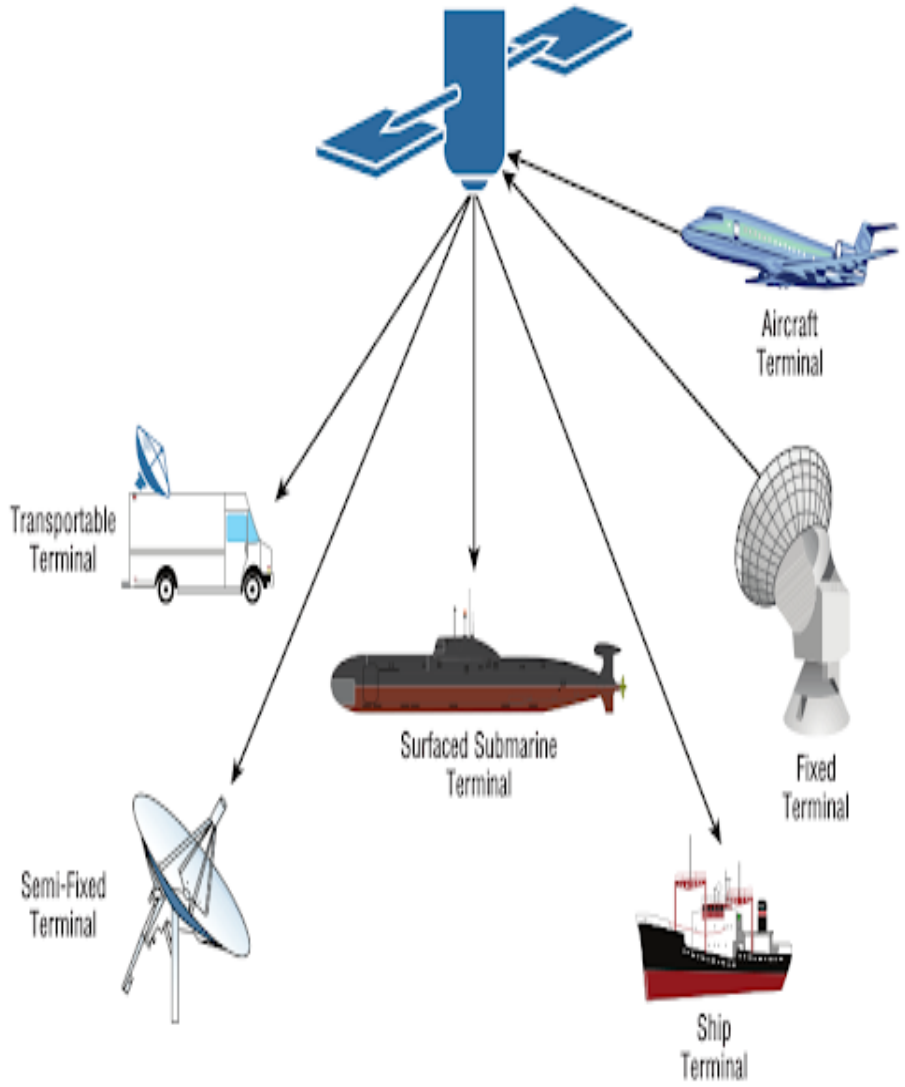
a. Parabolic dish antenna



b. Horn antenna

Figure 20: Unidirectional antenna

Microwaves



Picture: Microwave is used in satellite communication.

Infrared Transmission

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors.

- It has a very low frequency.
- These are largely used for data communication when wire- less keyboards, mouse and printers are used.

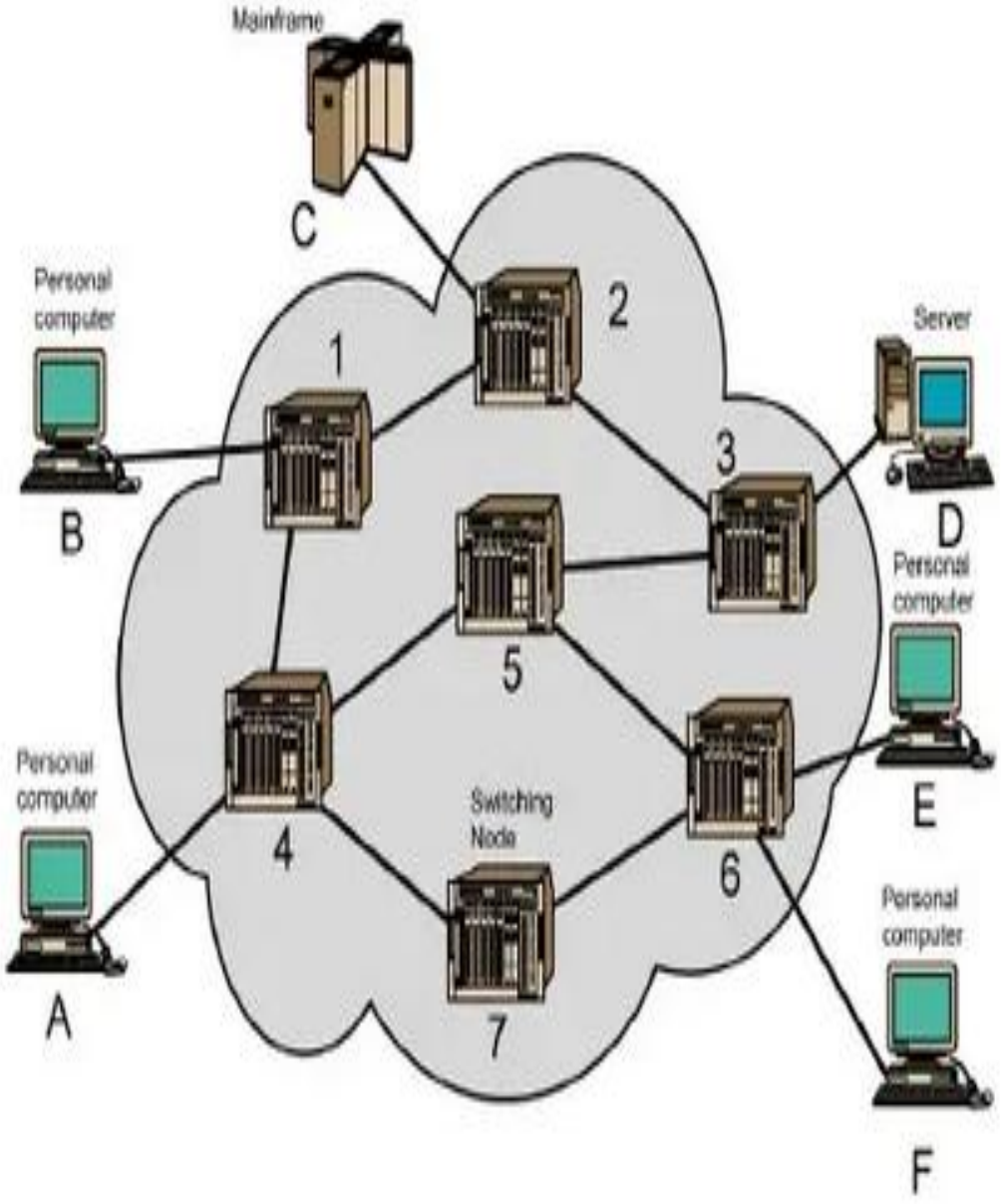
Switching Techniques

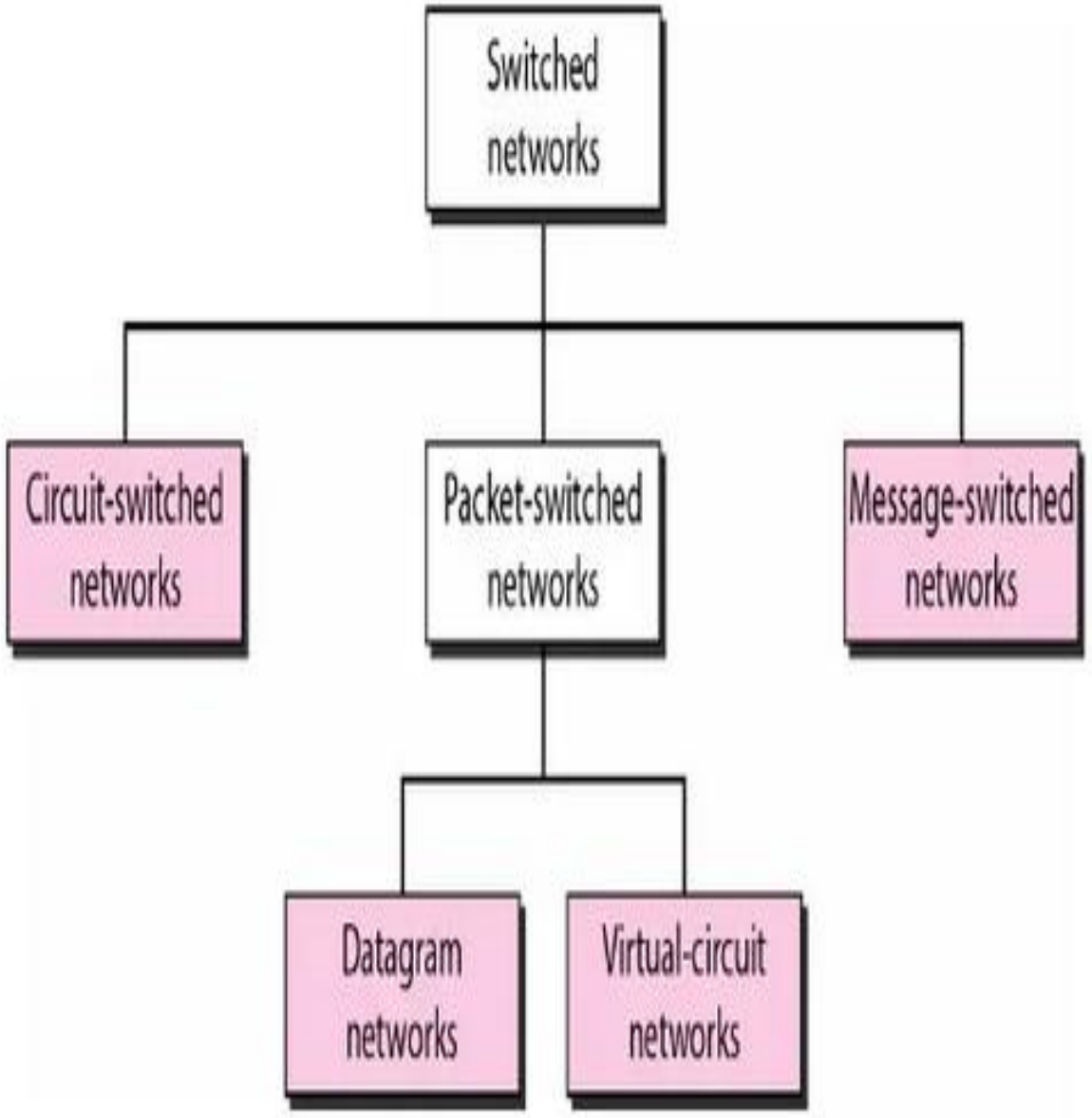
In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels. End devices are stations – Computer, terminal, Phone etc.

There are three typical switching techniques available for digital traffic.

- Circuit Switching
- Message Switching
- Packet Switching

Simple Switched Network



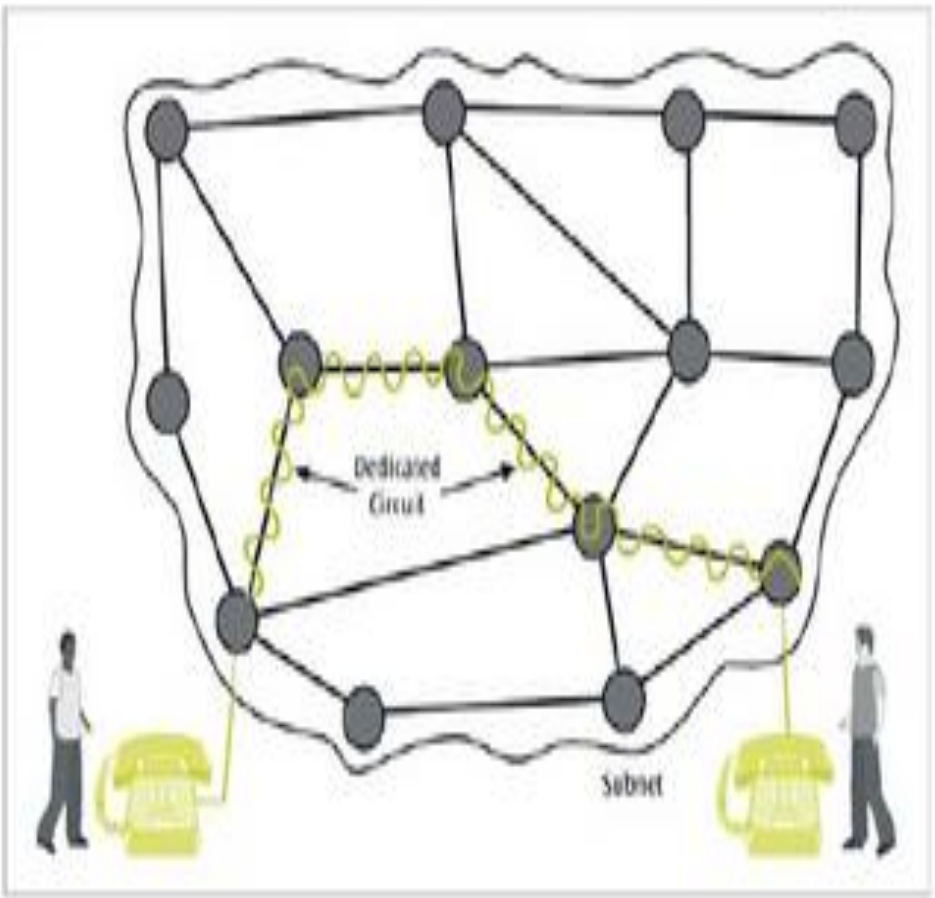

Switched networks
Circuit-switched networks
Packet-switched networks
Message-switched networks
Datagram networks
Virtual-circuit networks

Circuit Switching

- **Circuit switching** is a technique that directly connects the sender and the receiver in an unbroken path.
- **Circuit switching** networks operate almost the same way as the telephone system works.
- A complete end-to-end path must exist before communication can take place.
- The computer initiating the data transfer must ask for a connection to the destination.
- Before the establishment of the connection, the destination must send the acknowledge to the source node to indicate that it is ready and willing to send/receive data.

Circuit Switching

Figure 10-6
Two people carrying on a telephone conversation using a circuit-switched network



Circuit switching

Advantages:

- The communication channel (once established) is dedicated.

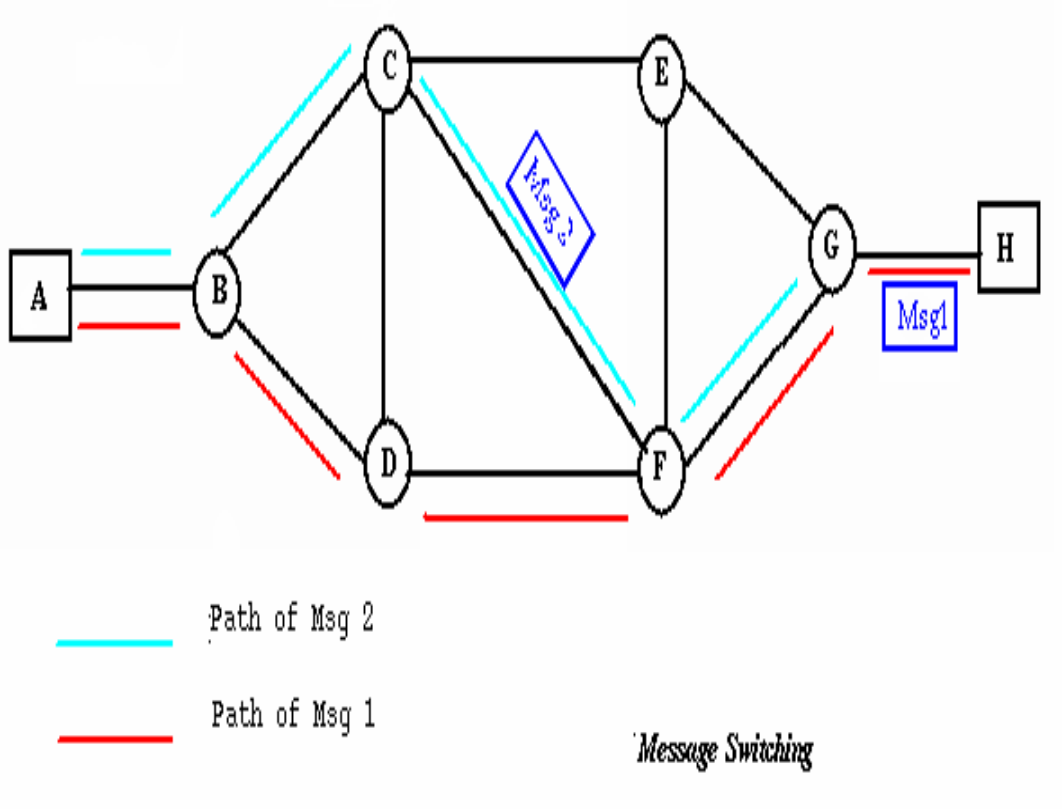
Disadvantages:

- Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.
- More expensive than any other switching techniques, because a dedicated path is required for each connection.
- Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Message Switching

- In message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- This type of network is called a store-and-forward network.

Message Switching



A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Message Switching

Advantages:

- Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
- Traffic congestion can be reduced, because messages may be temporarily stored in route.
- Message priorities can be established due to store-and-forward technique.
- Message broadcasting can be achieved with the use of broadcast address appended in the message.

Disadvantages

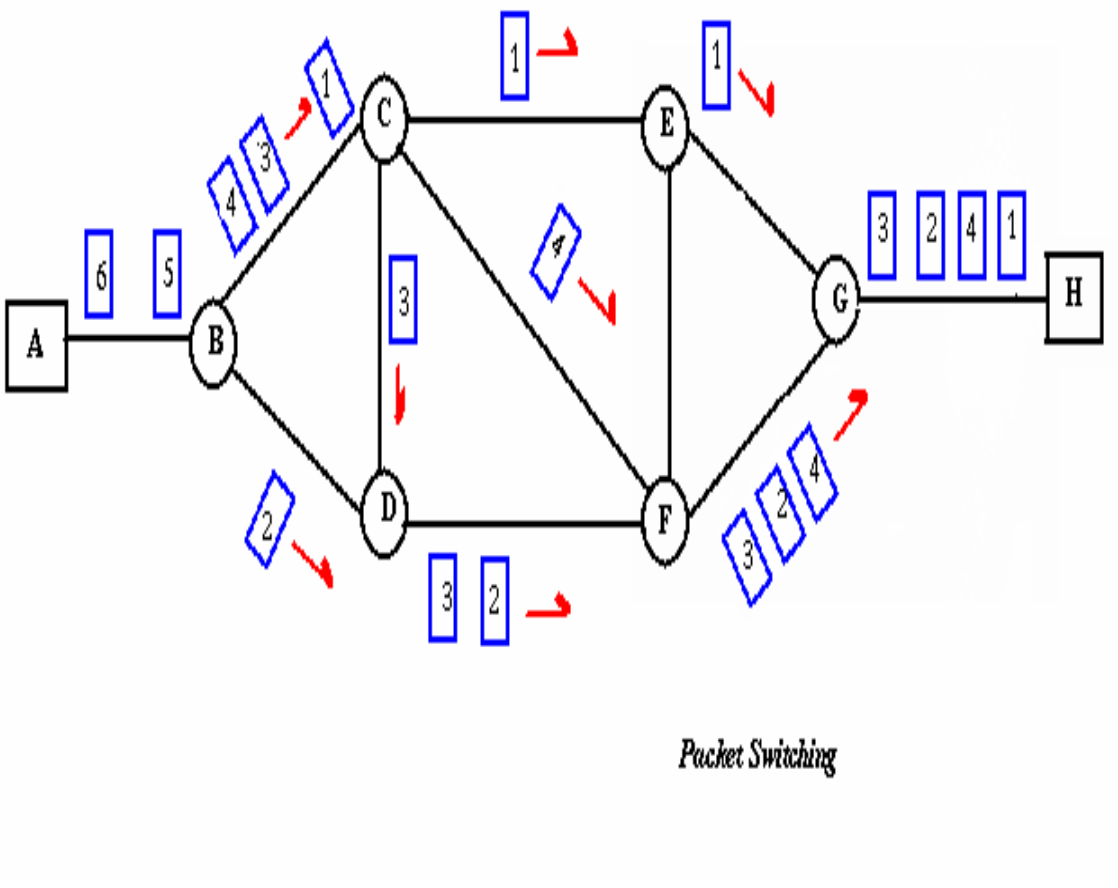
- Message switching is not compatible with interactive applications.
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages.

Packet Switching

- In both packet switching methods, a message is broken into small parts, called packets.
- Each packet is tagged with appropriate source and destination addresses.
- Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk, therefore access delay and cost are minimized.
- Also the transmission speeds, between nodes, are optimized.
- With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (“dropped").

Packet Switching

- *Packet switching* can be seen as a solution that tries to combine the
  advantages of message and circuit switching and to minimize the
  disadvantages of both.
- There are two methods of packet switching: Datagram
  and virtual circuit.



Packet Switching

Packet size

- The size of the packet can be:
  - 180 bits for the Datakit® virtual circuit switch designed by Bell Labs for communications and business applications.
  - 1,024 or 2,048 bits for the 1PSS® switch, also designed by Bell Labs for public data networking.
  - 53 bytes for ATM switching, such as Lucent Technologies' packet switches.

Packet Switching: Datagram

- Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
- This allows packets to take a variety of possible paths through the network.
- So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).
- Reordering is done at the destination point based on the sequence number of the packets.
- It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.

Packet Switching:Virtual Circuit

- In the virtual circuit approach, a preplanned route is established before any data packets are sent.
- A logical connection is established when
  - a sender send a "call request packet" to the receiver and
  - the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.
- The conversational parameters can be maximum packet sizes, path to be taken, and other variables necessary to establish and maintain the conversation.
- Virtual circuits imply acknowledgements, flow control, and error control, so virtual circuits are reliable.
- That is, they have the capability to inform upper-protocol layers if a transmission problem occurs.

Packet Switching:Virtual Circuit

- In virtual circuit, the route between stations does not mean that this is a dedicated path, as in circuit switching.
- A packet is still buffered at each node and queued for output over a line.
- The difference between virtual circuit and datagram approaches:

  - With virtual circuit, the node does not need to make a routing decision for each packet.
  - It is made only once for all packets using that virtual circuit.

Packet Switching: Virtual Circuit

VC guarantees that

- the packets arrive in the order they sent
- there are no duplicates or omissions.
- there are no errors (with high probability)

regardless of how they are implemented internally.

Advantages of packet switching

Advantages:

- Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
- Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
- Packet can be rerouted if there is any problem, such as, busy or disabled links.
- The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages of packet switching

Disadvantages:

- Protocols for packet switching are typically more complex.
- It can add some initial costs in implementation.
- If packet is lost, sender needs to retransmit the data.
- Another disadvantage is that packet-switched systems still
  can't deliver the same quality as dedicated circuits in
  applications requiring very little delay - like voice
  conversations or moving images.

Virtual Circuits vs. Datagram

- Virtual Circuits Approach
  - Network can provide sequencing and error control
  - Packets are forwarded more quickly
    - No routing decisions to make
  - Less reliable
    - Loss of a node looses all circuits through that node
- Datagram Approach
  - No call setup phase
    - Better if few packets
  - More flexible
    - Routing can be used to avoid congested parts of the network
  - More reliable
    - If a node fails, subsequent packets may find an alternate route that bypass that node

What is ISDN?

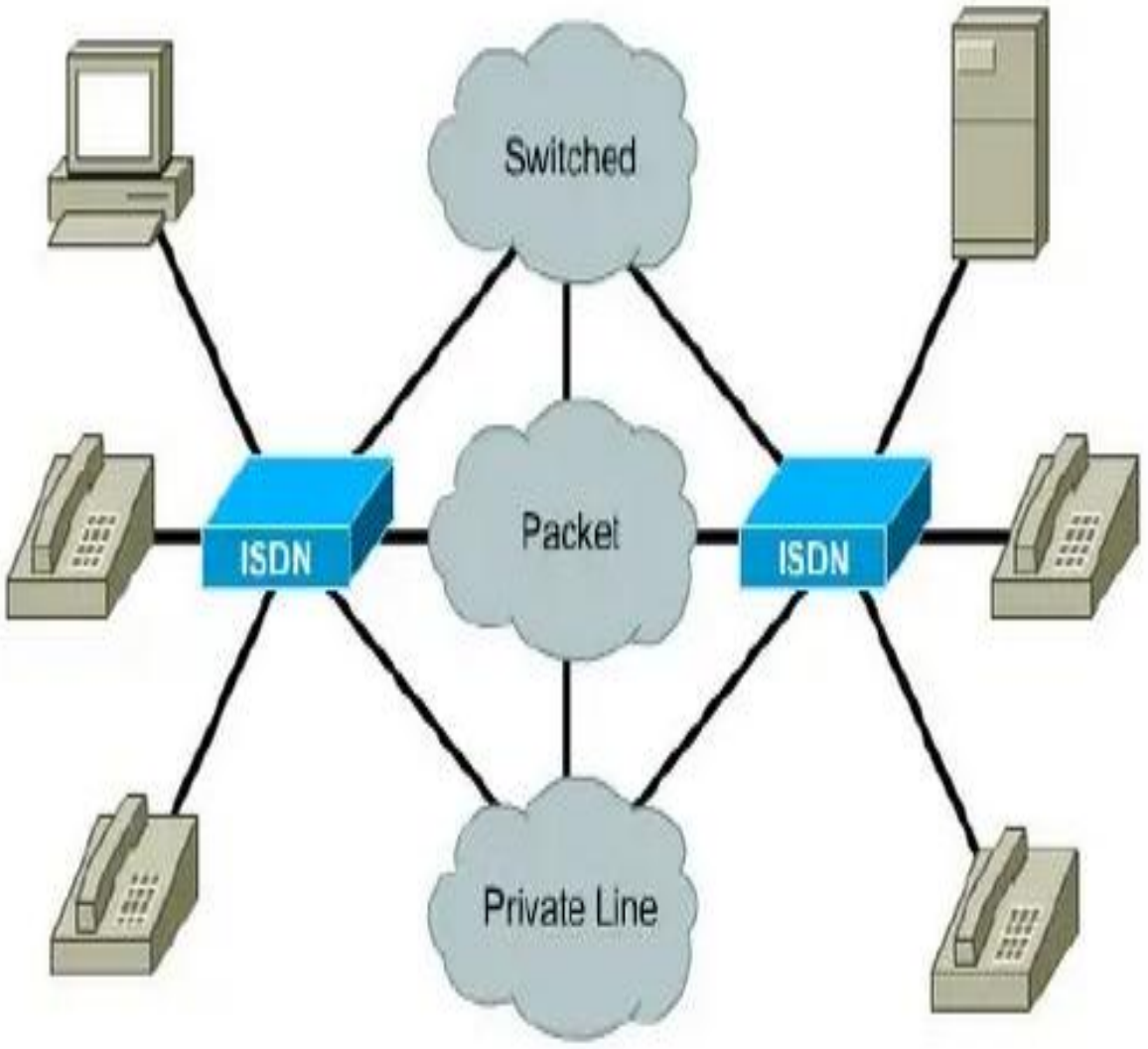
- Integrated Services Digital Network
- Carrier service offered by telephone companies and designed to transmit voice and non-voice communications simultaneously on the same network
- Used for voice, image and data
- Switched and non switched connections-circuit and packet switching and leased lines

ISDN protocols

- E- series for telephone network and ISDN
- I -series for ISDN concepts, aspects and interfaces
- Q-series for ISDN switching and signaling

which operates at three layers of OSI model.

ISDN network

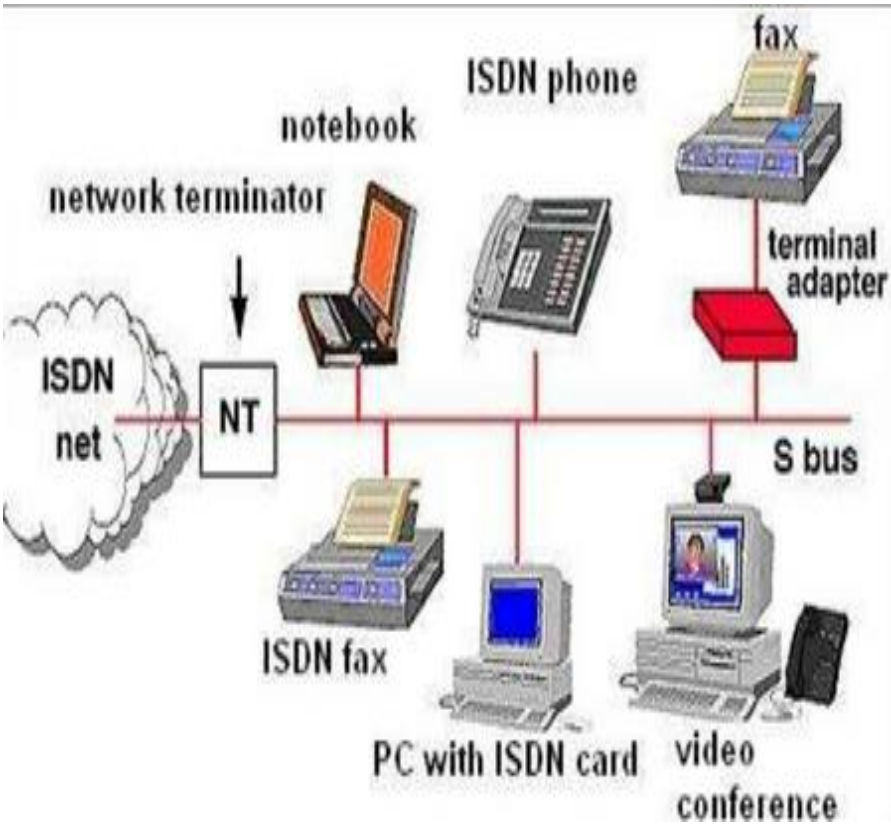


ISDN Benefits

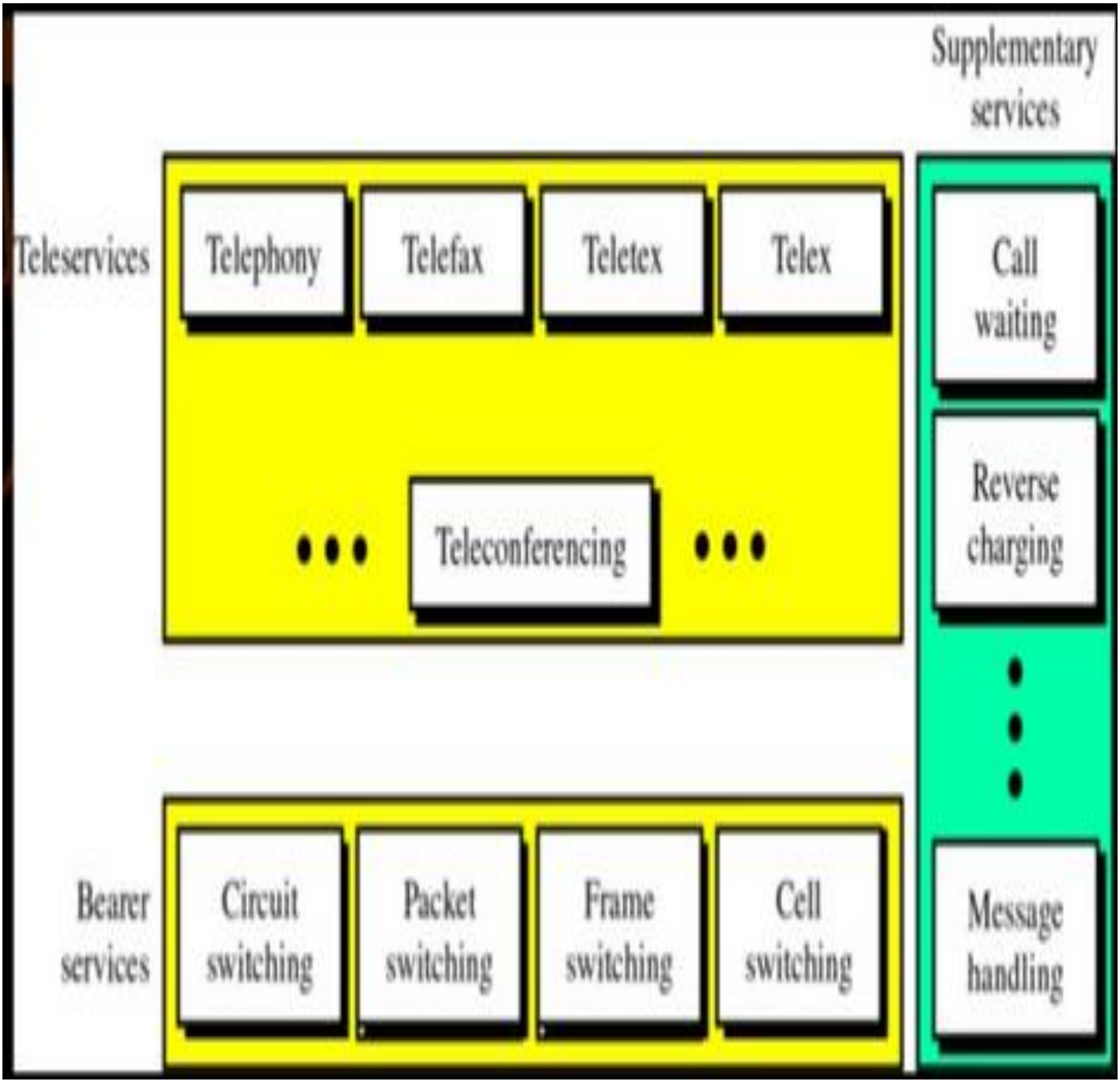
- End to end digital network for voice, text, data and video
- Separate connections are not needed for different transmissions
- Provide high data rate by using 64 or 128 kbps bearer channel (B-channel)
- Small offices and home offices can be supported with ISDN BRI services

ISDN Applications

- Telecommunications
- Video-Conferencing
- Internet Access
- Branch Office Communication
- Enhanced Voice Services



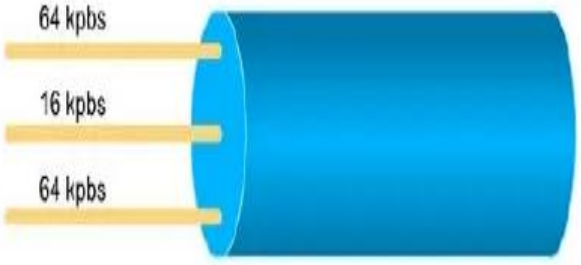
ISDN Services



ISDN Services – BRI

- **Basic Rate Interface (BRI)**
  - Two 64 Kbps B channels, one 16 Kbps D channel, and 48 Kbps worth of framing and synchronization.
  - **Available data bandwidth:** 128 Kbps (2 x 64 Kbps)
  - **User bandwidth:** 144 Kbps (128 Kbps + 16 Kbps D channel)
  - **Total line capacity:** 192 Kbps (144 Kbps + 48 Kbps framing)

- Each B channel can be used for separate applications, such as Internet and Voice



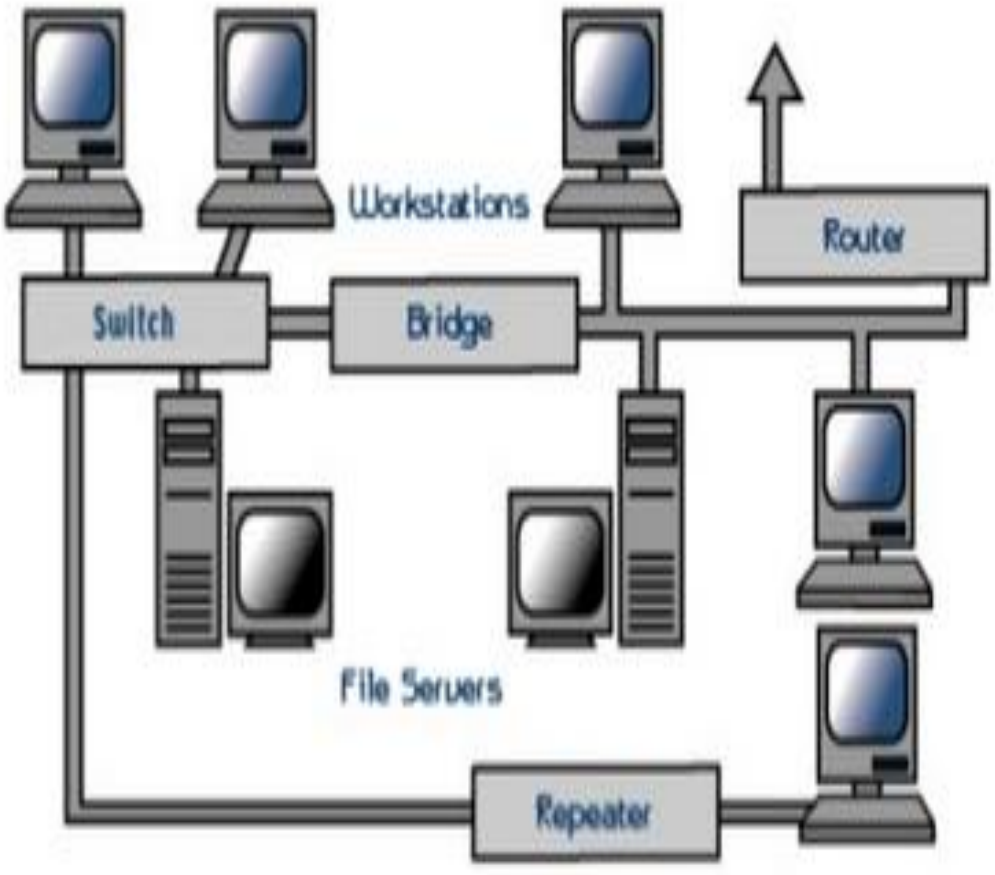
Three channels:
- Two 64 kbps bearer (B) channels
- One 16 kbps signaling (D) channel

ISDN Services – PRI

- **Primary Rate Interface (PRI)**
  - A PRI connection can assign various 64 Kbps channels to both ISDN and analog modem connections
  - North America and Japan – PRI service has 23 64 Kbps B channels, one 64 Kbps D channel, and 8 Kbps of synchronization and framing for a total bit rate of up to 1544 kbps
  - Europe, Australia, and other parts of the world – PRI service has 30 64 Kbps B channels, one 64 Kbps D channel, and 64 Kbps of framing and synchronization for a total bit rate of up to 2048 Kbps
  - Each B channel to be used for separate applications including voice, data and Internet
- Multiple B channels can be Multilinked together

What is Networking Hardware?

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network.



- Network Interface Card
- Hub
- Repeater
- Bridge
- Switch
- Gateway

Network Interface Cards

- Network interface cards, commonly referred to as NICs, are used to connect a PC to a network.
- The NIC provides a physical connection between the networking cable and the computer's internal bus.
- Different computers have different bus architectures; PCI bus master slots are most commonly found on 486/Pentium PCs and ISA expansion slots are commonly found on 386 and older PCs.
- NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable.

Hubs

- A hub joins multiple computers (or other network devices) together to form a single network.
- On this network, all computers can communicate directly with each other.
- The networking hub is a junction box with several ports in the back for receiving the Ethernet cables that are plugged into each computer on the LAN.

Hubs

- A *passive hub* serves simply as a passage for the data, enabling it to go from one device to another.
- *Intelligent hub* include additional features that enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.
- *Switching hub*, actually reads the destination address of each packet and then forwards the packet to the correct port.

Hubs

Repeater

- Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater.

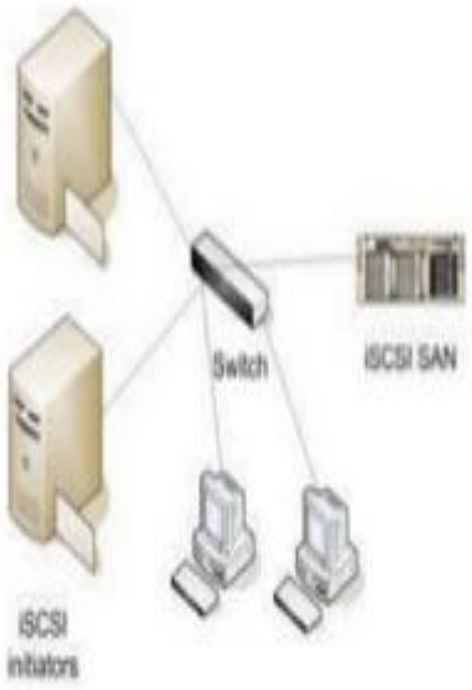
- A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level so that the signal can cover longer distances without degradation.

- A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling.

Switch

- A network switch is a small hardware device that joins multiple computers together within one local area network (LAN).
- Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence than a hub.
- Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately.
- Allow several users to send information over a network at the same time without slowing each other down.

Switch



Router

- A device to interconnect SIMILAR networks, e.g. similar protocols and workstations and servers.
- A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them.
- Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another.

Router

Bridge

- A bridge is a device that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

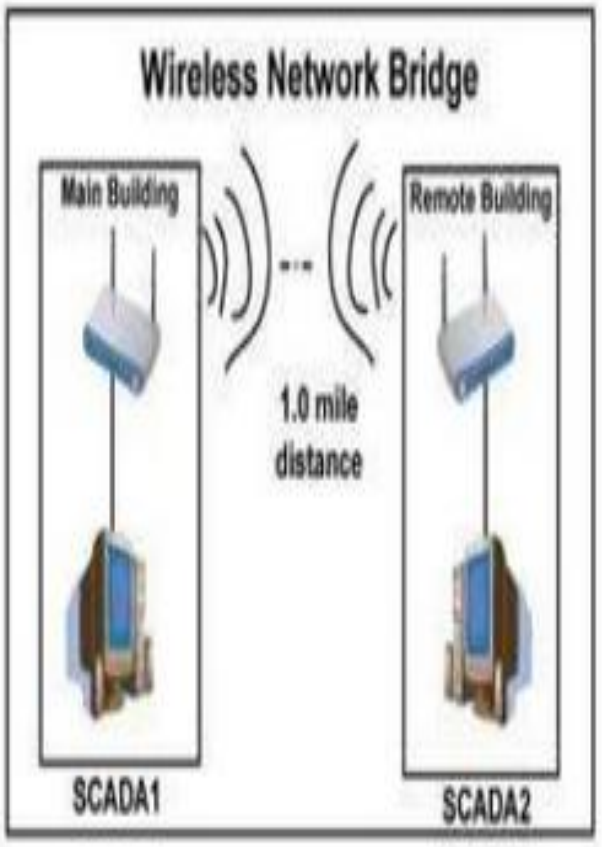
- The function of a bridge is to connect separate networks together. Bridges connect different networks types (such as Ethernet and Fast Ethernet) or networks of the same type.

- Bridges map the Ethernet addresses of the nodes residing on each network segment and allow only necessary traffic to pass through the bridge. When a packet is received by the bridge, the bridge determines the destination and source segments.

Types of Bridges

- Bridges come in three basic types:
- Local bridges: Directly connect local area networks (LANs)
- Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges have been replaced with routers.
- Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

Bridges

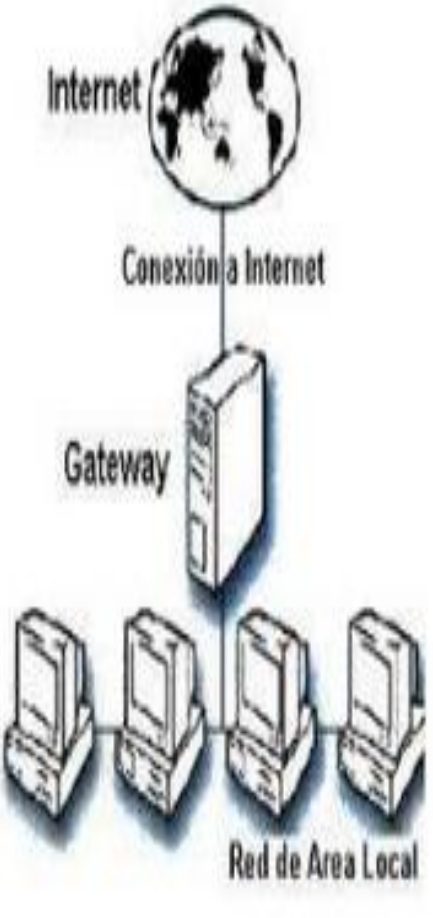

Wireless Network Bridge
Main Building
Remote Building
1.0 mile
distance
SCADA1
SCADA2

Gateway

- Gateways are used to interconnect two different networks having different protocols.
- Networks using different protocols use different addressing formats.
- A gateway is a network point that acts as an entrance to another network.
- Gateways are also called protocol converters.

Gateway


ICS
VoIP Gateway


Internet
Conexión a Internet
Gateway
Red de Area Local

What is the difference?

- Bridge: device to interconnect two LANs that use the SAME logical link control protocol but may use different medium access control protocols.
- Router: device to interconnect SIMILAR networks, e.g. similar protocols and workstations and servers.
- Gateway: device to interconnect DISSIMILAR protocols and servers, and Macintosh and IBM LANs and equipment