NOTES

ON

SUBJECT: COMPUTER NETWORKS

SUBJECT CODE: ECS-510

BRANCH: CSE

SEM:7th

SESSION: 2024-25

Evaluation Scheme:

Subject Code	Name of Subject	Periods			Evaluation Scheme				Subject Total	Credit
		L	T	P	CT	TA	TOTAL	ESC		
ECS-510	Computer Networks	3	0	0						

Prof. Ashok Kumar
CCSIT,TMU,
Moradabad

UNIT I: NETWORKS

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

"Computer network'' to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms, as we will see later. They are usually connected together to make larger networks, with the **Internet** being the most well-known example of a network of networks.

There is difference between a **computer network** and a **distributed system**. The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called **middleware**, is responsible for implementing this model. A well-known example of a distributed system is the **World Wide Web**. It runs on top of the Internet and presents a model in which everything looks like a document (Web page).

USES OF COMPUTER NETWORKS

1. Business Applications

- to distribute information throughout the company (**resource sharing).** sharing physical resources such as printers, and tape backup systems, is sharing information
- **client-server model**. It is widely used and forms the basis of much network usage.
- **communication medium** among employees.**email** (**electronic mail**), which employees generally use for a great deal of daily communication.
- Telephone calls between employees may be carried by the computer network instead of by the phone company. This technology is called **IP telephony** or **Voice over IP** (**VoIP**) when Internet technology is used.
- **Desktop sharing** lets remote workers see and interact with a graphical computer screen
- doing business electronically, especially with customers and suppliers. This new model is called **e-commerce** (**electronic commerce**) and it has grown rapidly in recent years.

2. Home Applications

- **peer-to-peer** communication
- person-to-person communication
- electronic commerce
- entertainment. (game playing,)

3. Mobile Users

- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce

- NFC (Near Field Communication)

4. Social Issues

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

THE CHARACTERISTICS OF A DATA COMMUNICATION SYSTEM:

1. **Delivery-**The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy-**The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

THERE ARE FIVE COMPONENTS OF DATA COMMUNICATION:

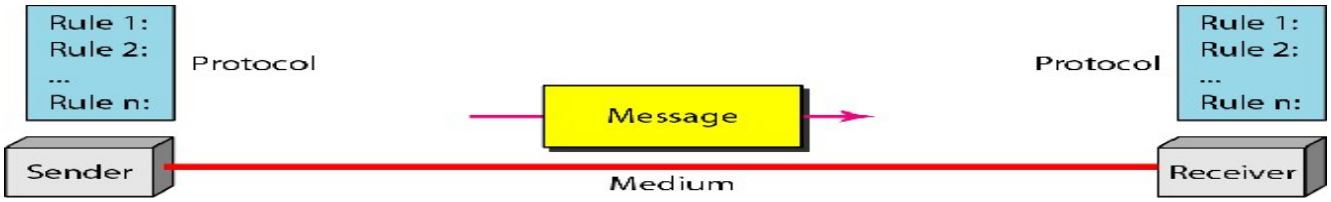


Fig 1.1 Components of Data Communication

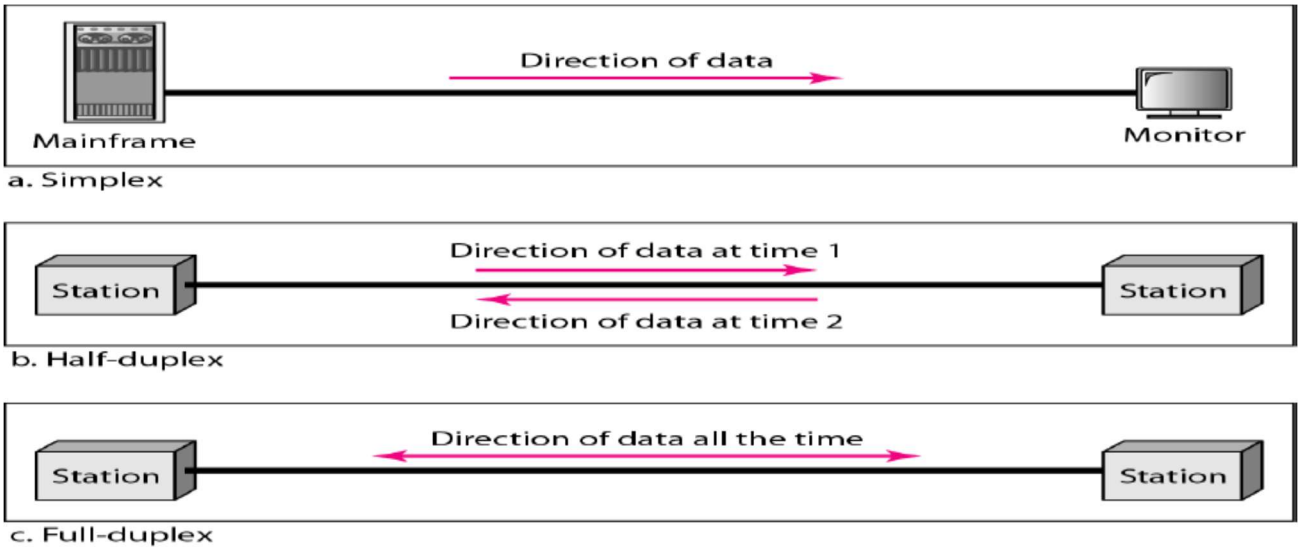
1. **Sender:** is the device that sends the data message.
2. **Message**: is the information (data) to be communicated. Eg: text, numbers etc.
3. **Transmission Medium**: is the physical path by which a message travels from sender to receiver. Eg: twisted pair cable, fiber-optic cable etc.
4. **Receiver**: is the device that receives the message.
5. **Protocols**: is a set of rules that govern the data communication. It represents anagreement between the communicating devices.

Moreover, Data can flow in three different ways namely Simplex, Half- Duplex and Full Duplex. 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. In half-duplex mode, each station can both transmit and receive, but not at the same time. i.e. When one device is sending, the other can only receive, and vice versa. Whereas, in full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

DIRECTION OF DATA FLOW:

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



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 (Figure a). Keyboards and traditional monitors are examples of simplex devices.

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 (Figure b). Walkie-talkies and CB (citizens band) radios are both half duplex systems.

Full-Duplex

In full-duplex, both stations can transmit and receive simultaneously (Figure c). One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.

A NETWORK MUST BE ABLE TO MEET THESE THREE CRITERIA'S:

1. **Performance:** can be measured using Transit time and Response time:
   (a) **Transit Time:** is the time required for a message to travel from one device to another.
   (b) **Response Time:** is the elapsed time between an inquiry and a response.
2. **Reliability:** is measured by the frequency of failure i.e the time it takes a link to recover from a failure.
3. **Security:** issues include protecting data from unauthorized access and losses.

TYPES OF CONNECTION:

1. Point -to-Point:Connection provides a dedicated link between two devices.
2. Multi-Point: Connectionis one in which more than two devices share a single link.

NETWORK CATEGORIES: The category into which a network falls is determined by its size. Network can be categorized as: LAN, WAN, MAN, Wireless Network and Internetwork.

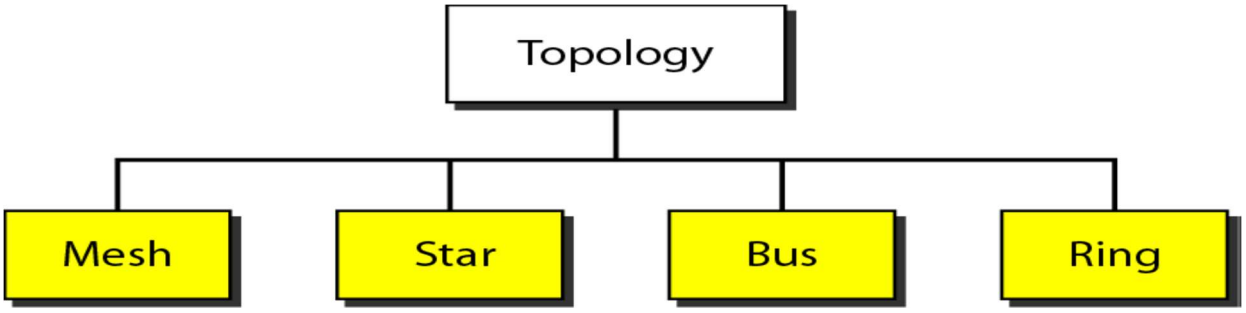
1. **LANs** are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps

2. **A wide area network (WAN)** provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from atelephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.

3. **A metropolitan area network (MAN)** is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

TOPOLOGIES:

The term *physical topology* refers to the way in which a network is laid out physically.Two 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:

A mesh topology is the one where every node is connected to every other node in the network. A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**.

In a *full mesh topology*, every computer in the network has a connection to each of the other computers in that network. The number of connections in thisnetwork can be calculated using the following formula (***n*** is the number of computers in the network): **n(n-1)/2** In a *partially connected mesh topology*, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.

Advantages of a mesh topology

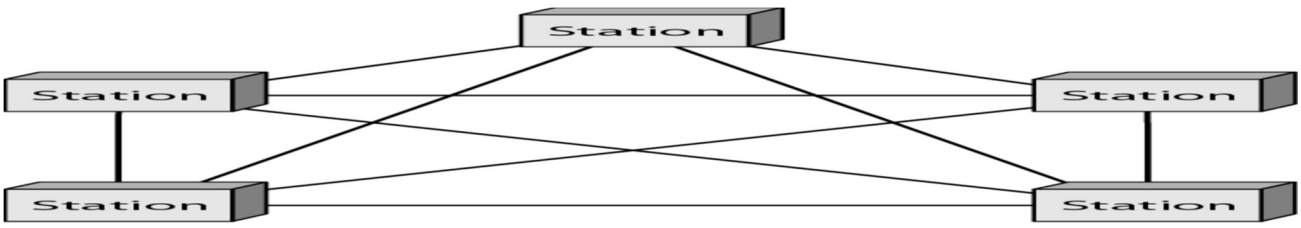
- Can handle high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it a

less desirable option.

- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.



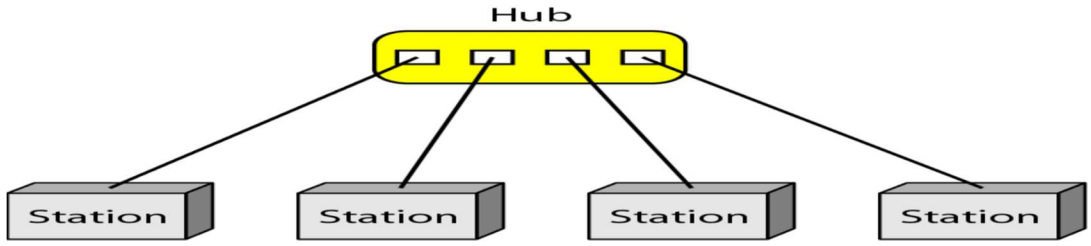
Star topology is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or a RJ-45 network cable is used to connect computers together.

Advantages of star topology

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.
- The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

Disadvantages of star topology

- Can have a higher cost to implement, especially when using a switch or router as the central network device.
- The central network device determines the performance and number of nodes the network can handle.
- If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network.



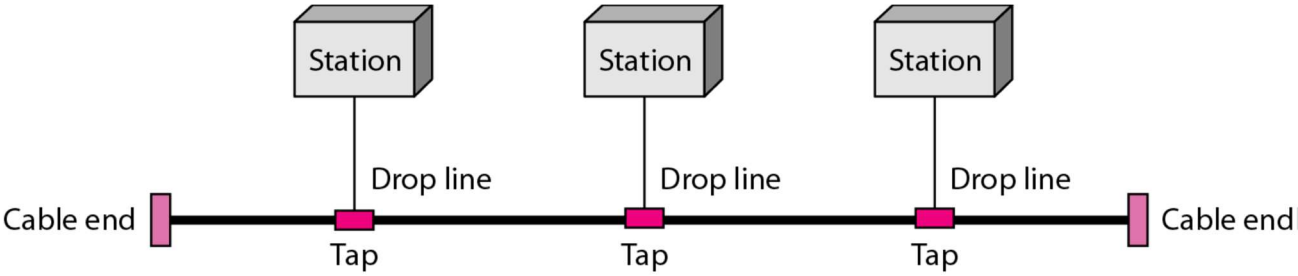
BUS: a **line topology**, a **bus topology** is a network setup in which each computer and network device are connected to a single cable or backbone.

Advantages of bus topology

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.



A **Ring topology** is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.

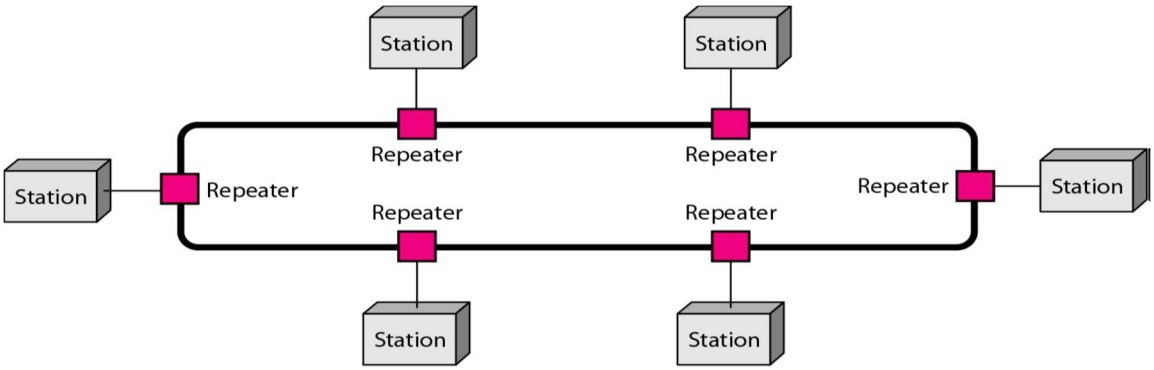
The major disadvantage of a ring topology is that if any individual connection in the ring is broken, the entire network is affected. Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).

Advantages of ring topology

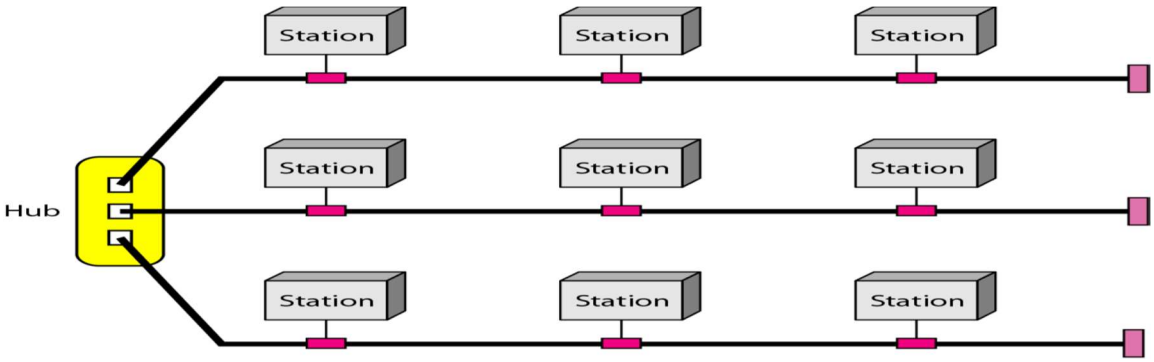
- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages of ring topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.



Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure


Station
Station
Station
Station
Station
Station
Station
Station
Station
Hub

PROTOCOLS & STANDARDS

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. Thus, for communication to occur, the entities must agree on a protocol. Therefore, a protocol is a set of rules that govern data communications. A protocol defines: what is communicated, how it is communicated, & when it is communicated.

There are three elements of a protocol:

- **Syntax:** The term syntax refers to the structure or format of the data, meaning the order in which they are presented.
- **Semantics:** The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- **Timing:** The term timing refers to two characteristics: when data should be sent and how fast they can be sent.

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communication. Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies. The various standard creation committees are:

- **International Organization for Standardization (ISO):** The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- **International Telecommunication Union-Telecommunication StandardsSector (ITU-T):** By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).
- **American National Standards Institute (ANSI):** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
- **Institute of Electrical and Electronics Engineers (IEEE):** The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity,

and product quality in the fields of electrical engineering, electronics, and radio aswell as in all related branches of engineering.

- **Electronic Industries Association (EIA):** Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development.

LAYERED TASKS: OSI MODEL

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office. Figure 1.3 below shows tasks involved in sending a letter:

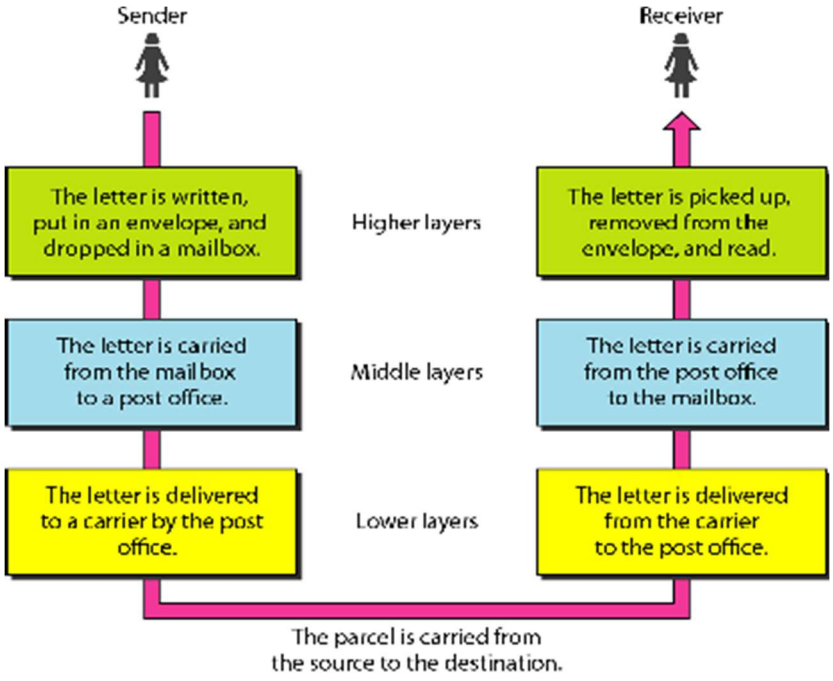


Fig 1.3 Layered Tasks

Thus from above figure it is clearly understood that layer architecture simplifies the network design. It is easy to debug network applications in a layered architecture network. There are two layered Models namely OSI Model and TCP/IP Model.

OSI MODEL: OPEN SYSTEM FOR INTERCONNECTION

International Standard Organization (ISO) established a committee in 1977 to develop architecture for computer communication. Open Systems Interconnection (OSI) reference model is the result of this effort.

In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture. Term “open” denotes the ability to

connect any two systems which conform to the reference model and associated standards. The purpose of OSI Model is to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is now considered the primary Architectural model for inter-computer communications. The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network. The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems. This separation into smaller more manageable functions is known as layering. Figure below shows interaction between layers in the OSI model:

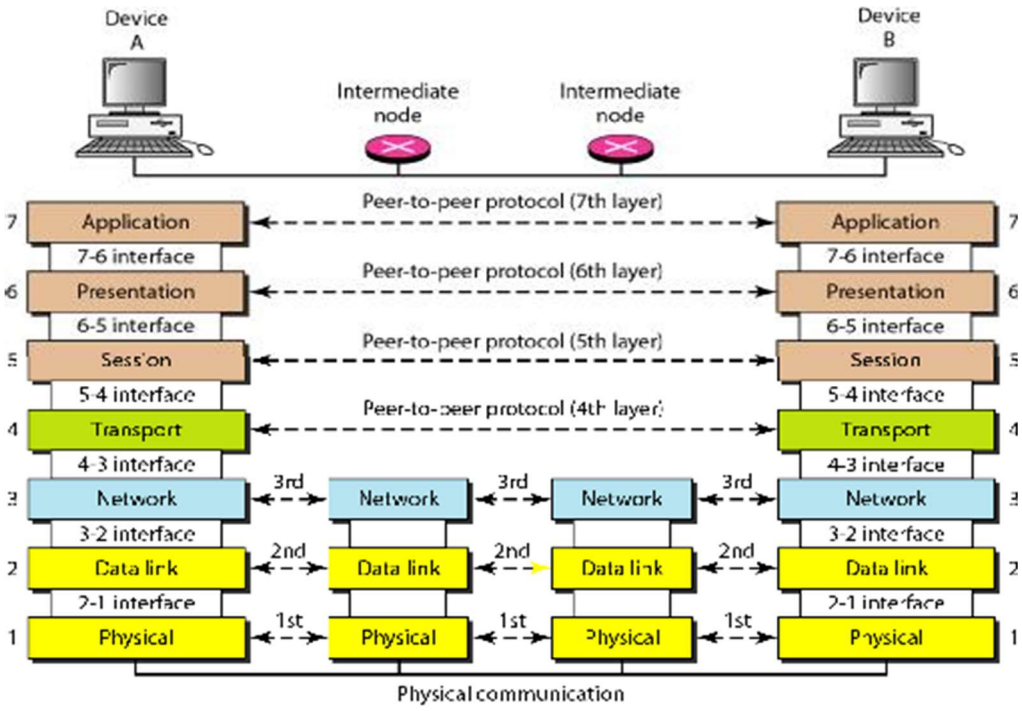


Fig 1.4 OSI Model

The process of breaking up the functions or tasks of networking into layers reduces complexity. Each layer provides a service to the layer above it in the protocol specification. Each layer communicates with the same layer's software or hardware on other computers. The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network. The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications. Data is encapsulated with the necessary protocol information as it moves down the layers before network transit. A message begins at the top application layer and moves down the OSI layers to the bottom physical layer. As the message descends, each successive OSI model layer adds a header to it. A header is layer-specific information that basically explains what functions the layer carried out. Conversely, at the receiving end, headers are striped from the message as it travels up the corresponding layers as shown in Fig.1.5.

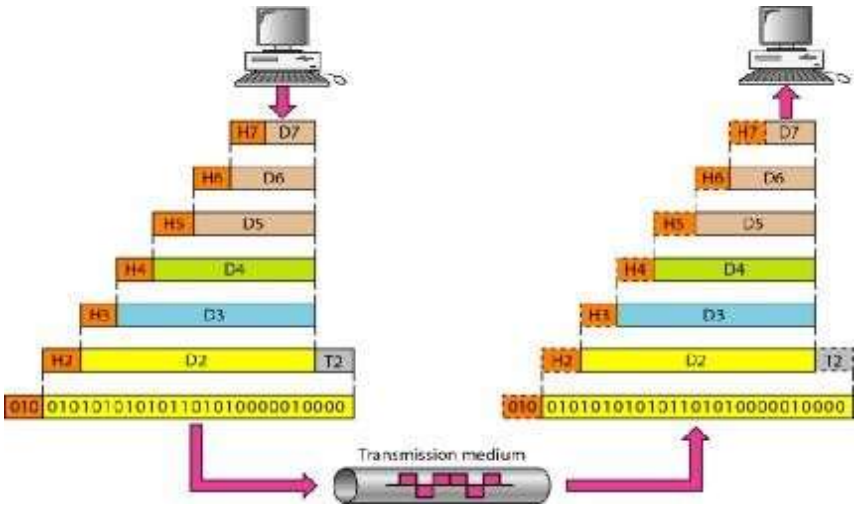


Fig 1.5 Working Principle

A) PHYSICAL LAYER

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

B) DATA LINK LAYER

- Data link layer attempts to provide reliable communication over the physical layer interface.
- Breaks the outgoing data into frames and reassemble the received frames.
- Create and detect frame boundaries.
- Handle errors by implementing an acknowledgement and retransmission scheme.
- Implement flow control.
- Responsible for Error Control.
- Supports points-to-point as well as broadcast communication.
- Supports simplex, half-duplex or full-duplex communication.

C) NETWORK LAYER

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination.
- Defines logical addressing so that any endpoint can be identified.

- Handles congestion in the network.
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

D) TRANSPORT LAYER

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

E) SESSION LAYER

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

F) PRESENTATION LAYER

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

G) APPLICATION LAYER

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

Fig. 1.6 below shows summary of all layers of OSI Model:

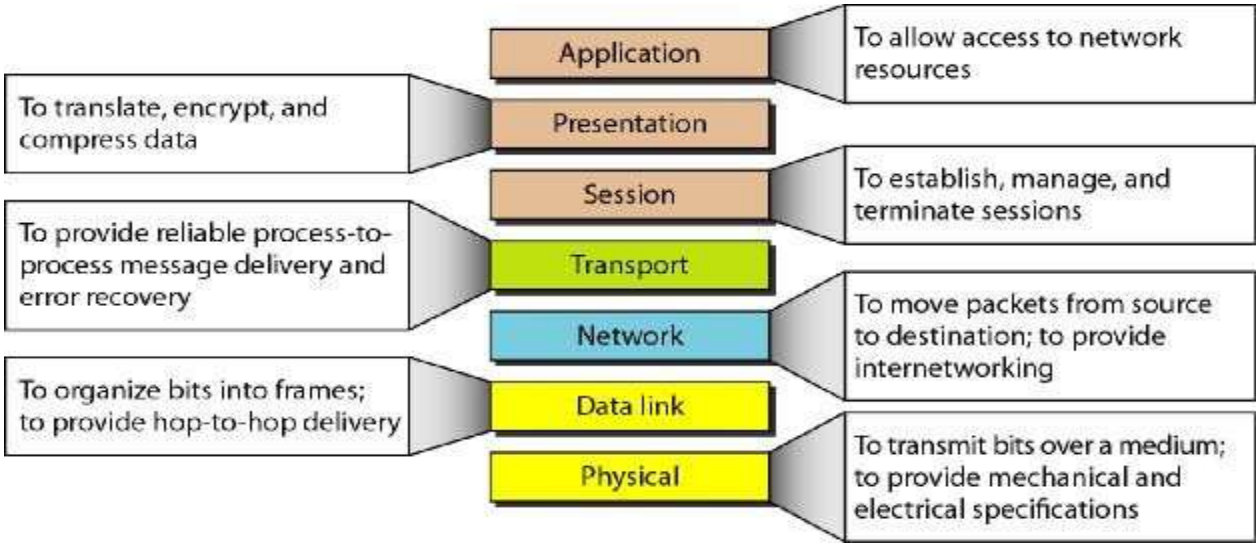


Fig 1.6 Summary of OSI Model

TCP/IP MODEL:(TRANSMISSION CONTROLPROTOCOL / INTERNETPROTOCOL)

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. Fig. 1.7 below shows TCP/IP layers in comparison to OSI Model:

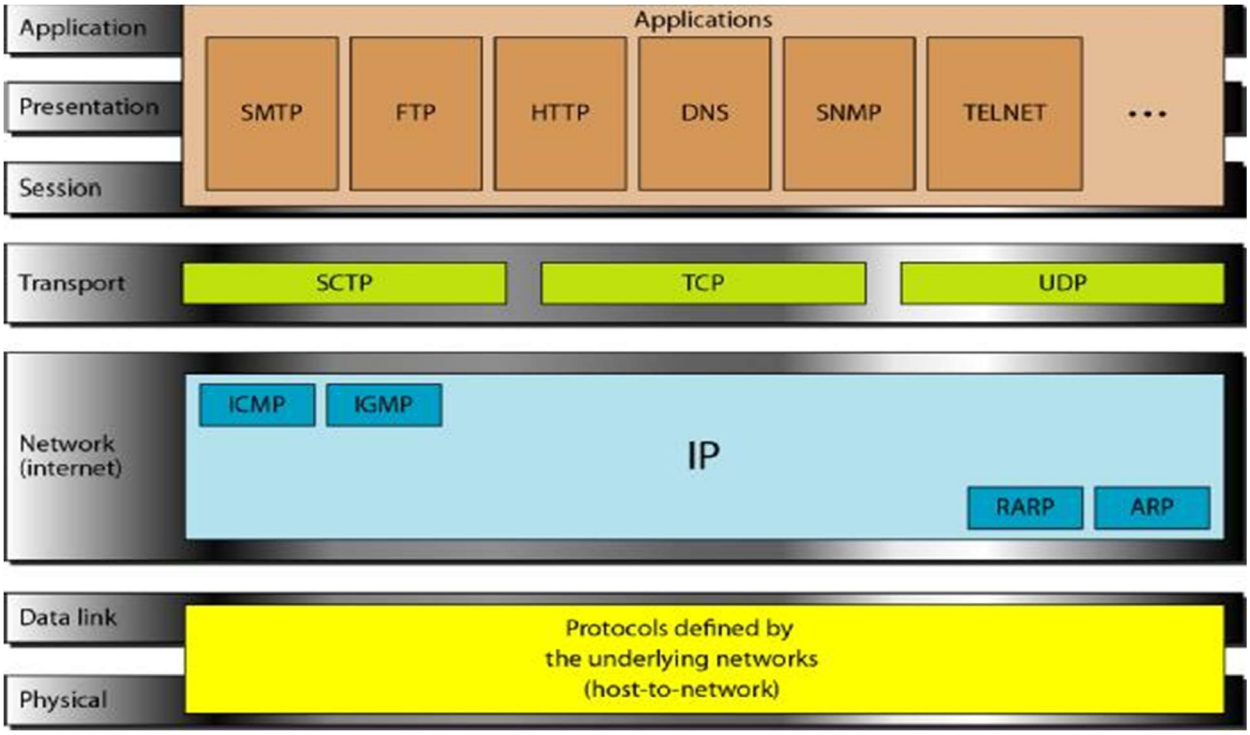


Fig 1.7 TCP/IP Model Vs OSI Model

A) APPLICATION LAYER

Application layer protocols define the rules when implementing specific network applications. It relies on the underlying layers to provide accurate and efficient data delivery. Typical protocols are:

- FTP – File Transfer Protocol: For file transfer
- Telnet – Remote terminal protocol: For remote login on any other computer on the network
- SMTP – Simple Mail Transfer Protocol: For mail transfer
- HTTP – Hypertext Transfer Protocol: For Web browsing

B) TRANSPORT LAYER

Transport Layer protocols define the rules of dividing a chunk of data into segments and then reassemble segments into the original chunk. Typical protocols are:TCP – Transmission Control Protocol: Provide functions such as reordering and data resend.

- UDP – User Datagram Service: Use when the message to be sent fit exactly into a datagram and Use also when a more simplified data format is required.
- SCTP - Stream Control Transmission Protocol: The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet.

C) NETWORK LAYER

Network layer protocols define the rules of how to find the routes for a packet to the destination It only gives best effort delivery. Packets can be delayed, corrupted, lost, duplicated, out-of-order.

- IP – Internet Protocol: Provide packet delivery
- ARP – Address Resolution Protocol: Define the procedures of network address / MAC address translation i.e The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known.
- RARP – Reverse Address Resolution Protocol: The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.
- ICMP – Internet Control Message Protocol: The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- IGMP – Internet Control Message Protocol: The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

D) PHYSICAL AND DATA LINK LAYER

At the physical and data link layers, TCP-IP does not define any specific protocol. Rather, it supports all the standard protocols.

1.2 ADDRESSING

There are four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific. Figure 1.8 below shows relationship of layers and addresses in TCP/IP:

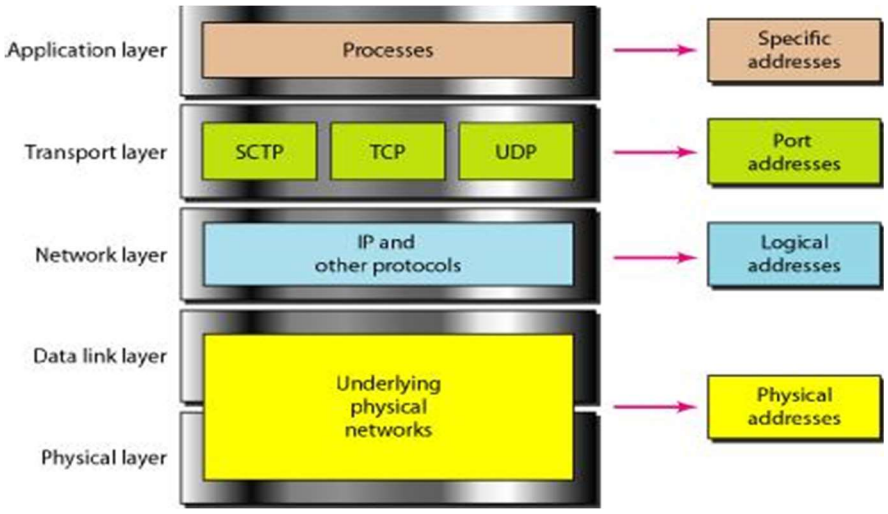


Fig 1.8 TCP/IP Addressing

A) PHYSICAL ADDRESSING:

The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. Example of Physical Addressing: A node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure 1.9 shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

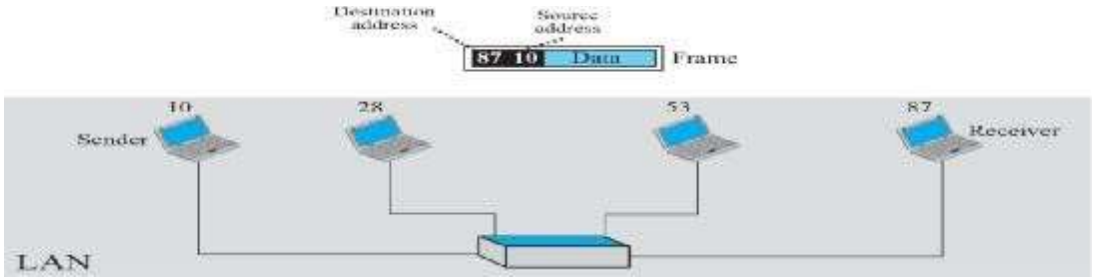


Fig 1.9 Example of Physical Addressing

B) LOGICAL ADDRESSING

Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address. Example of Logical addressing: Figure 1.10 shows a part of an internet with two routers connecting three LANs.

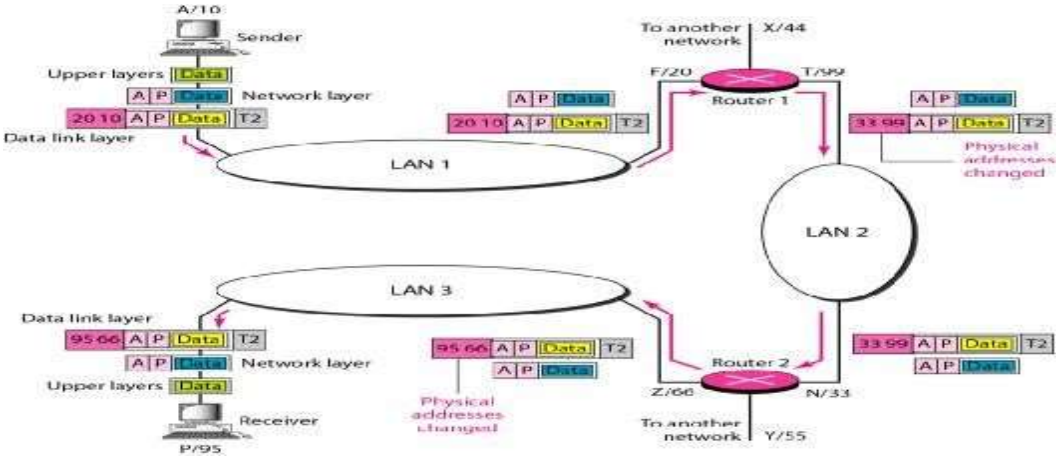


Fig 1.10 Example of Logical Addressing

C) PORT ADDRESSING:

The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete. Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCPIIP architecture, the label assigned to a process is called a port address. A port address in TCPIIP is 16 bits in length. Example of Port addressing: Figure 1.11 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.

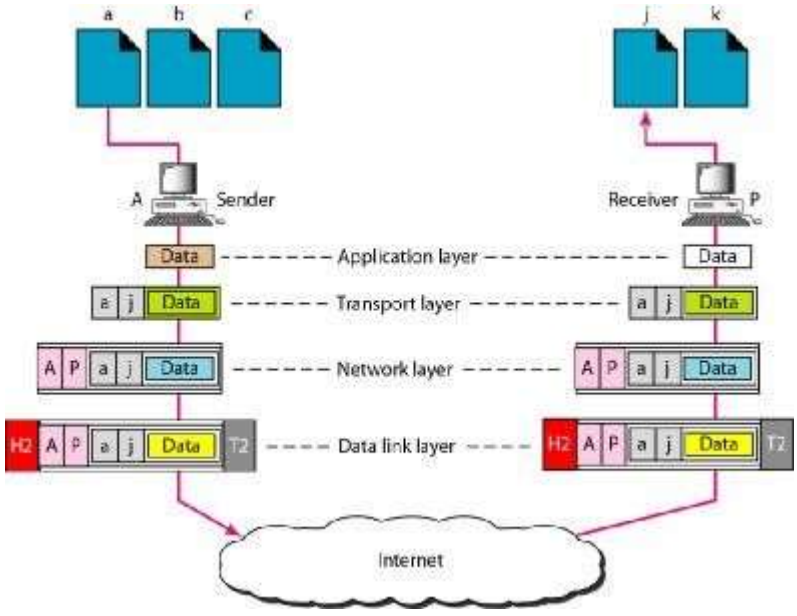


Fig 1.11 Example of Port Addressing

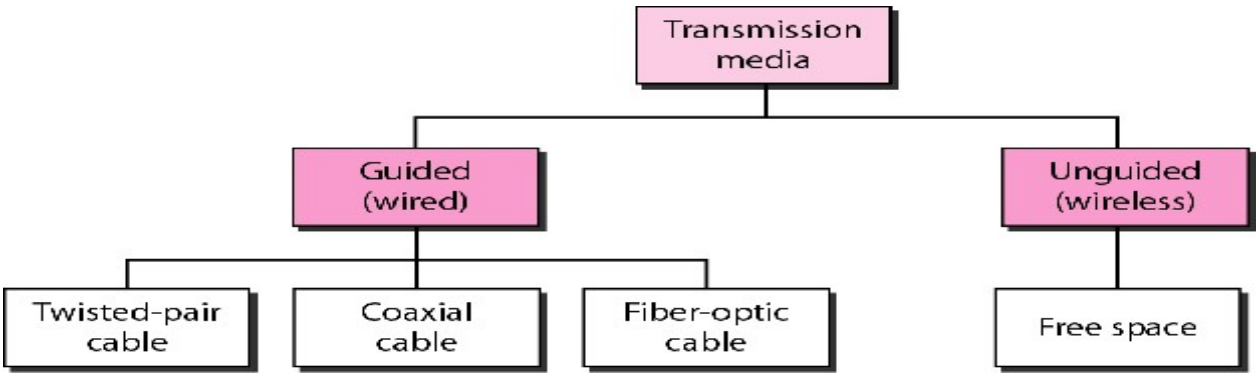
D) SPECIFIC ADDRESSING:

Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address (for example, forouzan@fhda.edu): defines the recipient of an e-mail and the Universal Resource Locator (URL) (for example, www.mhhe.com): used to

find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

TRANSMISSION MEDIA

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane. In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form. It can be classified as:



Guided Media:

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

Twisted Pair Cable: A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Twisted pair Cable is shown below in Fig. 1.19:

Fig 1.19 Twisted Pair Cable

Coaxial Cable: Coaxial cable (or coax) as shown in Fig1.20 carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover as shown in figure below:

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single

coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable

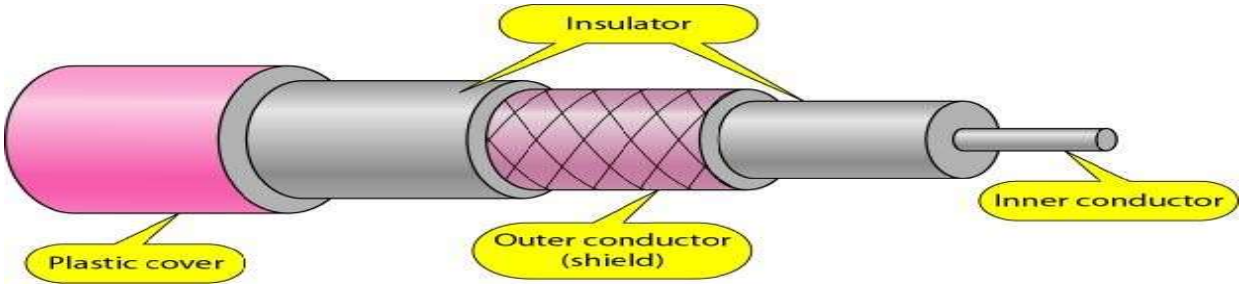


Fig 1.20 Coaxial Cable

.

Fiber Optic Cable: A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction as shown in Fig.1.21.

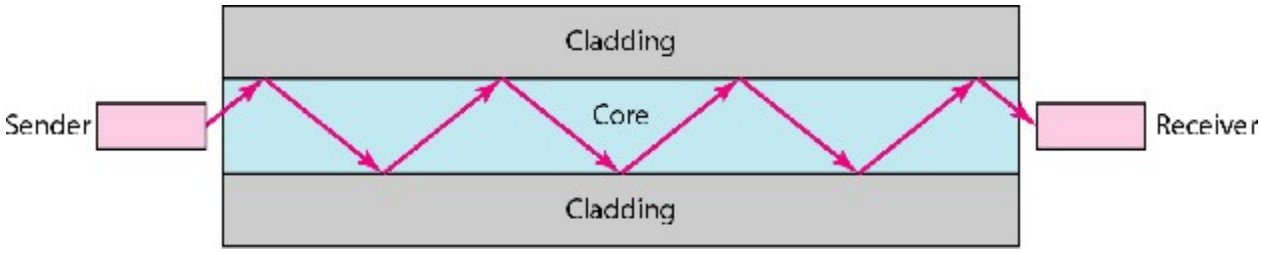


Fig 1.21 Fiber Optic Cable

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps.

Unguided Media

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation. Wireless transmission is of three types as shown below in Fig 1.22:

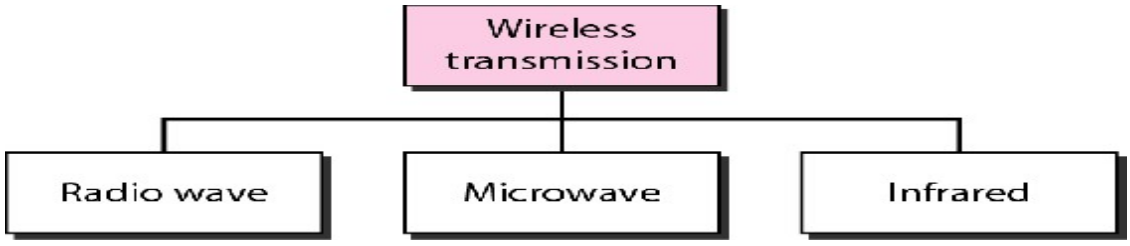


Fig 1.22 Wireless Transmission

Radio Waves: Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than the frequencies, is a better criterion for classification. Radio waves use omni-directional antennas that send out signals in all directions. The omni-directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio,television, cordless phones, and paging are examples of multicasting.

Microwaves: Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, 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. Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellites and wireless LANs.

Infrared: 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. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication. The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. The standard originally defined a data rate of 75 kbps for a distance up to 8 m. The recent standard defines a data rate of 4 Mbps.

SWITCHING

In large networks we need some means to allow one-to-one communication between any two nodes. In LANs this is achieved using one of three methods:

- Direct point-to-point connection (mesh)
- Via central controller (star)
- Connection to common bus in a multipoint configuration (bus/hup)

None of the previous works in larger networks with large physical separation or consisting of a large number of computers because it requires too much infrastructure and majority of those links would be idle for most of the time. Thus, better solution is a switching network. It consists of a series of interlinked nodes called switched. Switches are capable to create temporary connections between two or more devices. Some of these nodes are connected to the end system and others are used only for routing. End systems can be computers or telephones. Switching network has been shown in Figure 2.1

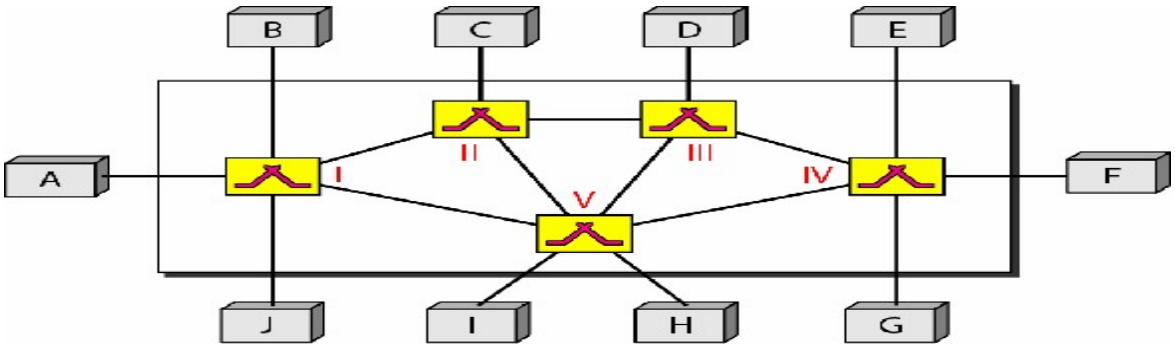


Fig 2.1 Switching Network

There are three types of Switched Network namely Circuit Switched Network, Packet Switched Network and Message Switched Network as shown in Fig 2.2

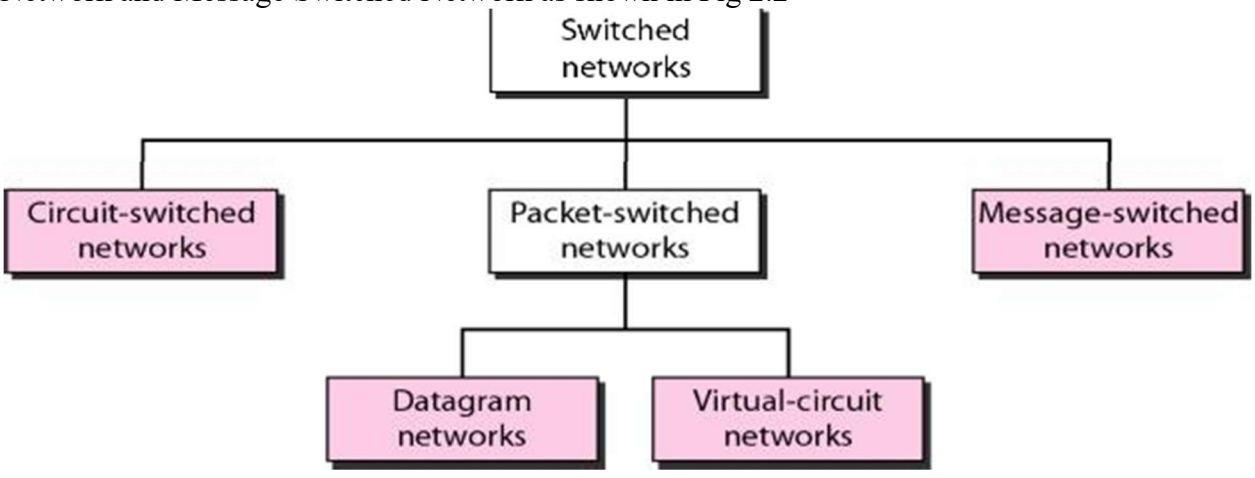


Fig 2.2 Types of Circuit Switching

A) CIRCUIT SWITCHING

A circuit-switched network (as shown in Fig 2.3) consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. Each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM. The link can be permanent (leased line) or temporary (telephone).

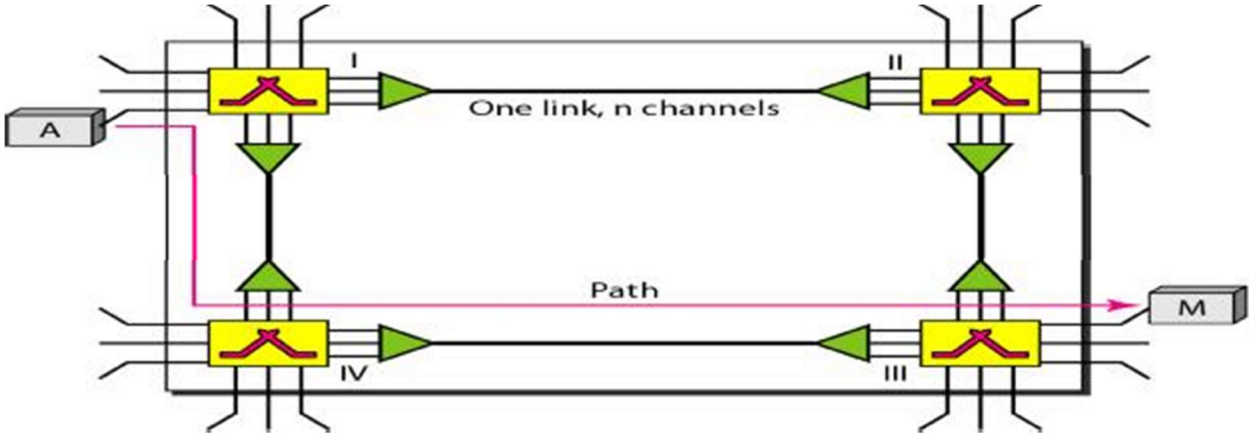


Fig 2.3 Circuit Switching

Switching takes place at physical layer. Resources can be bandwidth in FDM and time slot in TDM, switch buffer, switch processing time or switch I/O ports. Data transferred are not packetized, but it is a continuous flow. No addressing involved during data transfer. There are three transmission phases in circuit switching namely Setup phase, data transfer phase and tear down phase.

It can be argued that circuit-switched networks are not as efficient as the other two types of networks resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation. However, in computer networks, a computer can be connected to another computer even if there is no activity for a long time. In this case, allowing resources to be dedicated means that other connections are deprived. The total delay in this circuit switching is shown in Fig 2.4

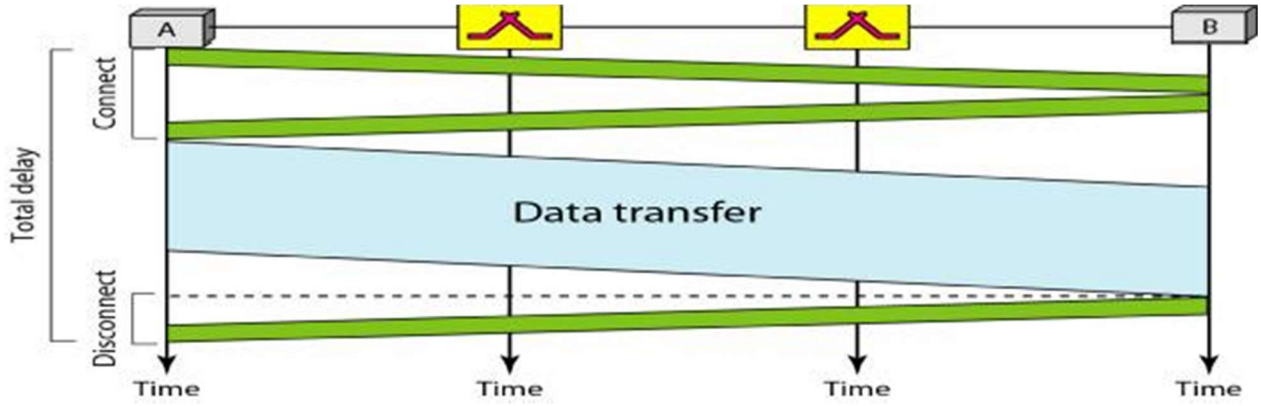


Fig 2.4 Delay in Circuit Switching

B) PACKET SWITCHING

In packet Switching, flow of data is not continuous rather it flows in the form of packets. The size of the packet is determined by the network and the governing protocol. This type of switching further classify into datagram networks and virtual circuit networks.

2.1.1 Datagram Networks

Data are transmitted in discrete units called packets. Size of the packet depends on the protocol and network. Packets switched networks are connectionless, hence no resource allocation. Connectionless means the switch does not keep information about the connection state. Datagram switching is done at network layer as shown in Fig 2.5

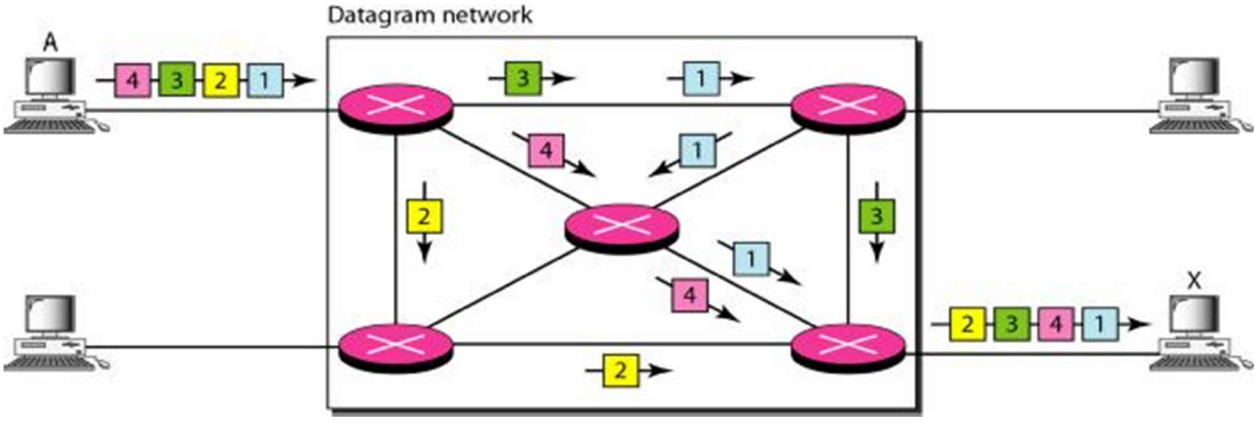


Fig 2.5 Datagram Networks

A switch in a datagram network uses a routing table that is based on the destination address. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet. The total delay is shown in Fig 2.6

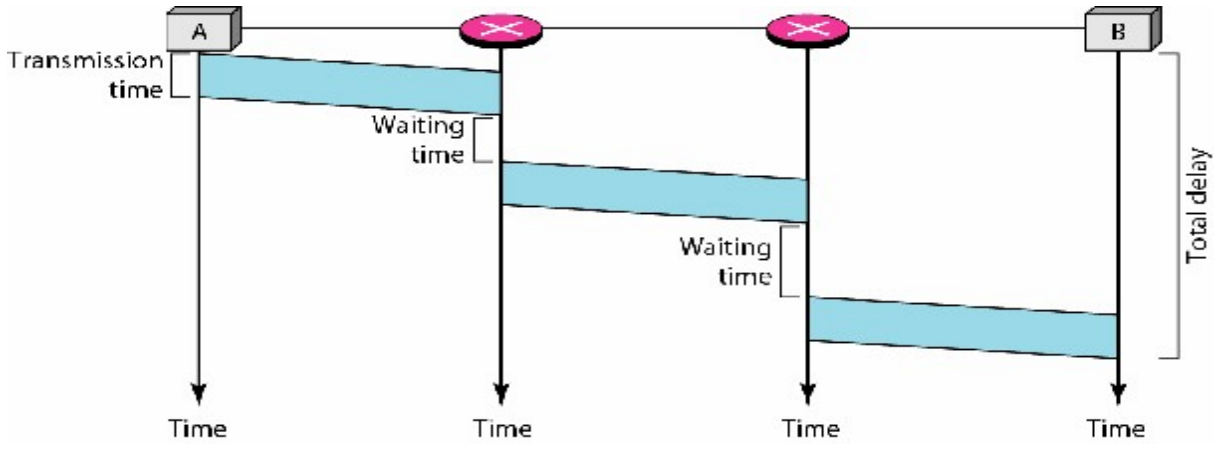


Fig 2.6 Delay in Datagram Networks

2.1.2 Virtual Circuit Networks

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. The virtual-circuit shares characteristics of both. Packets form a single message travel along the same path. Following are the characteristics of virtual circuit networks:

- Three phases to transfer data
- Resources can be allocated during setup phase
- Data are packetized and each packet carries an address in the header
- All packets follow the same path
- Implemented in data link layer

A virtual-circuit network uses a series of special temporary addresses known as virtual circuit identifiers (VCI). The VCI at each switch is used to advance the frame towards its final destination. The switch has a table with 4 columns as shown in Fig 2.7 i.e. Inputs half: Input Port Number and Input VCI and Outputs half: Output Port Number and Output VCI.

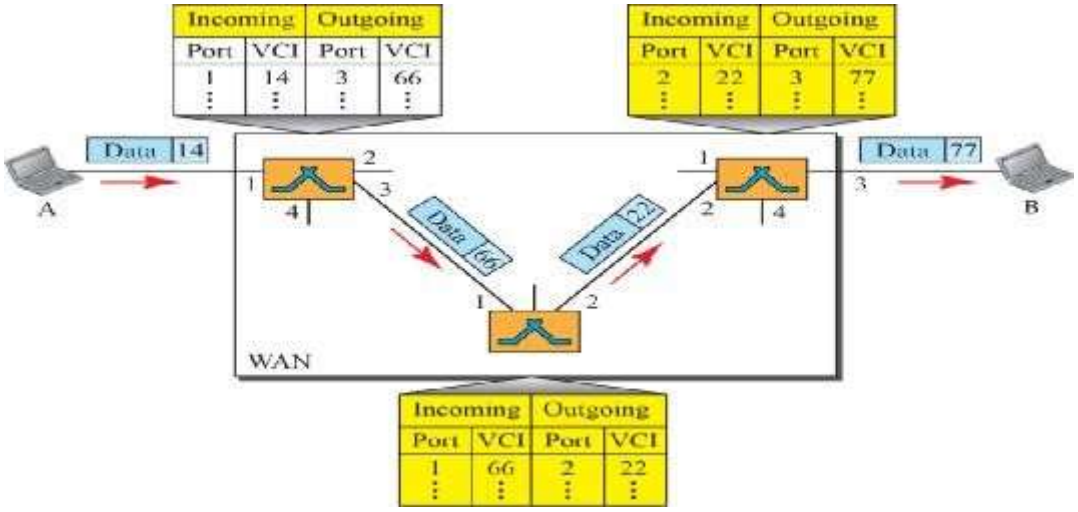


Fig 2.7 Virtual Circuit Identifier

The VCN behaves like a circuit switched net because there is a setup phase to establish the VCI entries in the switch table. There is also a data transfer phase and teardown phase. The total delay in virtual circuit network is shown in Fig 2.8

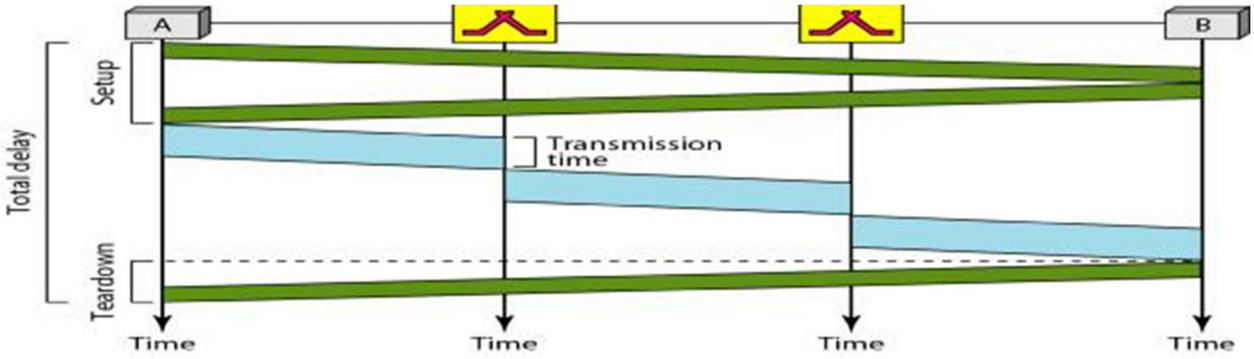


Fig 2.8 Delay in Virtual Circuit Identifier

2.1.3 Structure of a Switch

We use switches in circuit-switched and packet-switched networks. There are two structures of a switch named as space division switch and time division switch.

In space-division switching as shown in Fig 2.9, the paths in the circuit are separated from one another spatially. This technology was originally designed for use in analog networks but is used currently in both analog and digital networks.

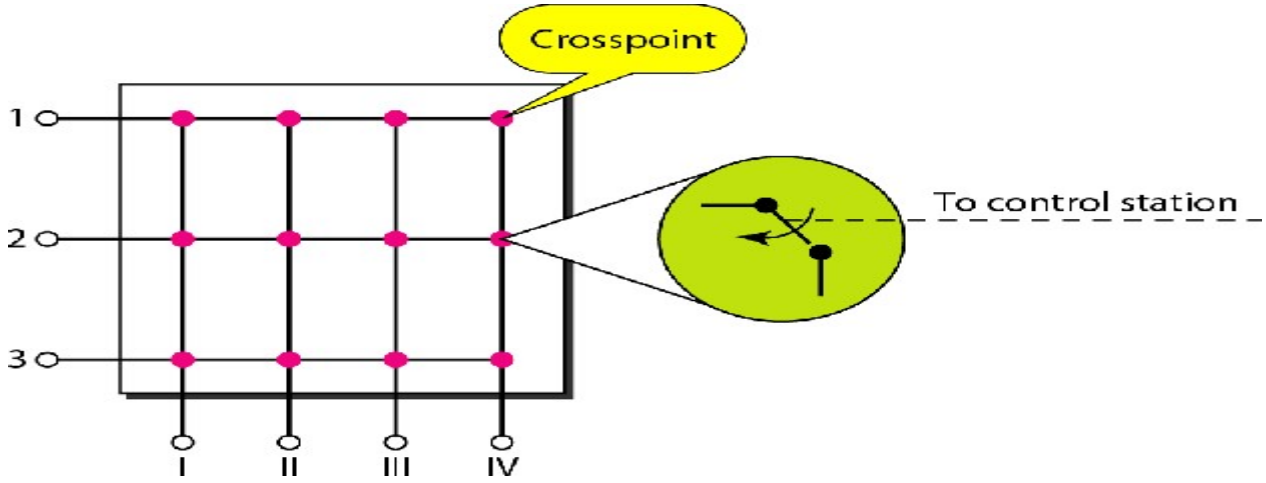


Fig 2.9 Space Division Switching: Crossbar Switch

Time Division Switching as shown in Fig 2.10 consists of a TDM Multiplexer, a TDM Demultiplexer, and a TSI consisting of random access memory (RAM) with several memory locations. The size of each location is the same as the size of a single time slot. The number of locations is the same as the number of inputs (in most cases, the numbers of inputs and outputs

are equal). The RAM fills up with incoming data from time slots in the order received. Slots are then sent out in an order based on the decisions of a control unit.

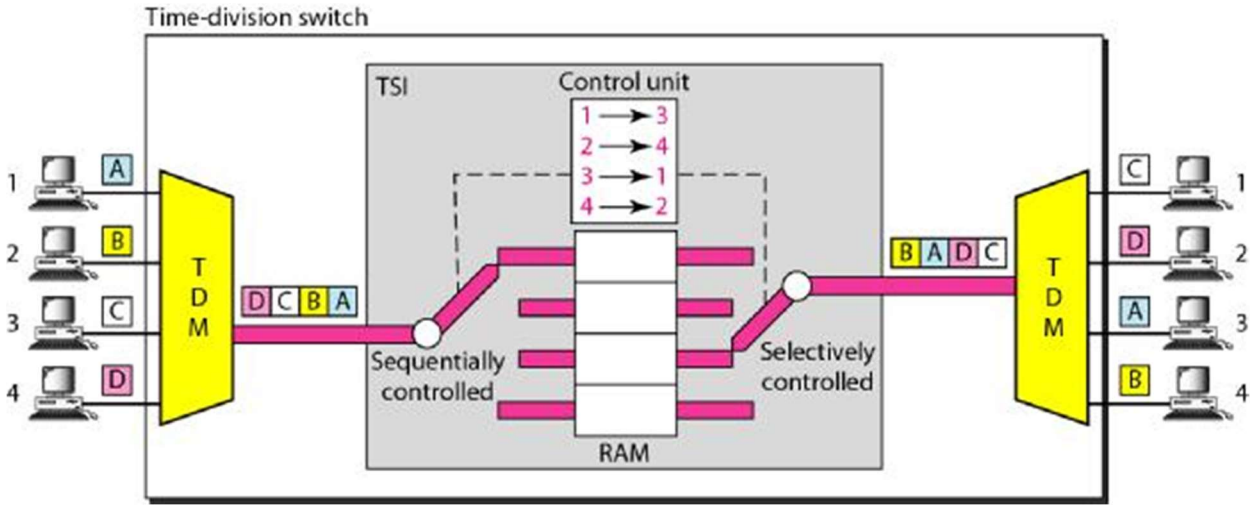


Fig 2.10 Time Division Switching

2.1.4 Ethernet Physical Layer

Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, which is referred to as the plain old telephone system (POTS), was originally an analog system using analog signals to transmit voice. There are three major components of telephone system namely local loops, trunks and switching offices as shown in Fig 2.11.

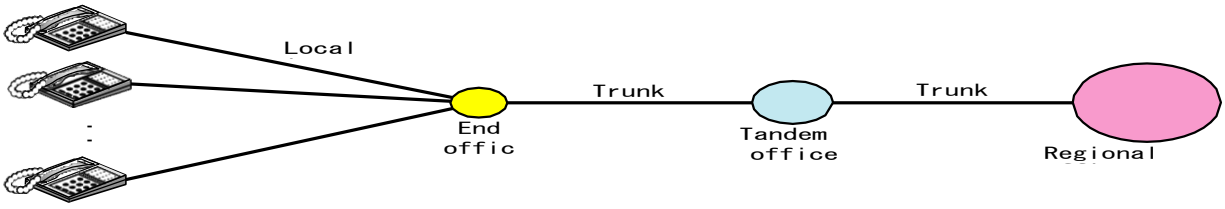


Fig 2.11 Telephone Network

Local Loops: One component of the telephone network is the local loop, a twisted-pair cable that connects the subscriber telephone to the nearest end office or local central office. Trunks: Trunks are transmission media that handle the communication between offices. A trunk normally handles hundreds or thousands of connections through multiplexing. Switching Offices: To avoid having a permanent physical link between any two subscribers, the telephone company has switches located in a switching office. A switch connects several local loops or trunks and allows a connection between different subscribers. The telephone network has several levels of switching offices such as end offices, tandem offices, and regional offices.

Signaling can be defined as the information exchange concerning the establishment and control of a telecommunication circuit and the management of the network. There are two types: In-Band and Out-Band. In in-band signaling, the same circuit can be used for both signaling and voice communication. In out-of-band signaling, a portion of the voice channel bandwidth was used for signaling; the voice bandwidth and the signaling bandwidth were separate. The signaling system was required to perform other tasks such as: providing dial tone, ring tone, and busy tone, transferring telephone numbers between offices, and providing other functions such as caller ID, voice mail etc. These complex tasks resulted in the provision of a separate network for signaling. This means that a telephone network today can be thought of as two networks: a signaling network and a data transfer network. The protocol that is used in signaling network is SS7 (Signaling System Seven) as shown in Fig 2.12.

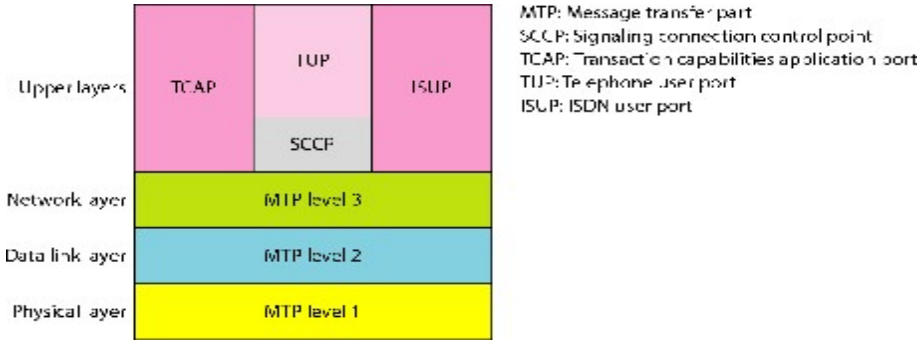


Fig 2.12 SS7 (Signaling System Seven)