UNIT-1
Data Communications & Physical layers

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For Data Communication to occur, the communicating devices must be a part of a communication system made up of a combination of hardware and software.

The effectiveness of a data communication system depends on four fundamental characteristics:
1. Delivery
2. Accuracy
3. Timeliness
4. Jitter

There are five components of data communication as shown in Fig. below:

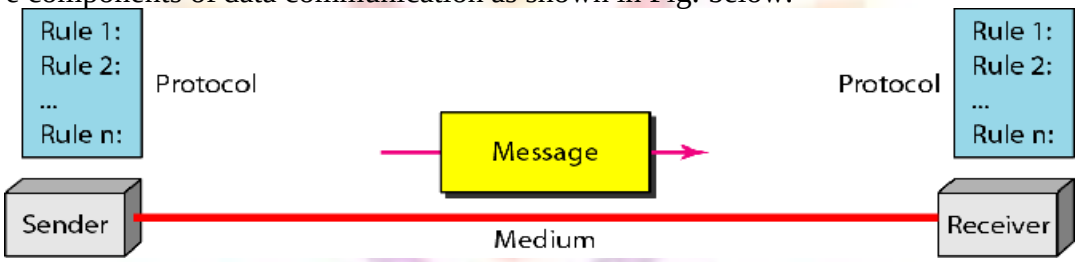


Fig: Components of Data Communication

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

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.

1. Networks

A network is a set of devices (nodes) connected by communication links. In this definition, a device can be a host such as a large computer, desktop, laptop, workstation, cellular phone, or security system.

❖ Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance: Performance can be measured in many ways, including transit time and response time. *Transit time* is the amount of time required for a message to travel from one device to another. *Response time* is the elapsed time between an inquiry and a response.
The performance of a network depends on a *number of factors*, including
The number of users,
The type of transmission medium,
The capabilities of the connected hardware,
The efficiency of the software.

Reliability: In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure.

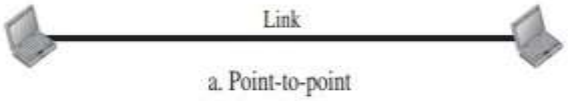
Security: Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

❖ Physical Structures

- **Type of Connection**

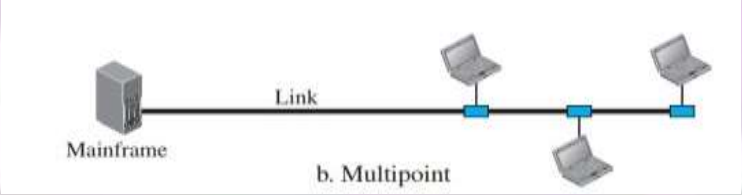
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points.

There are *two possible types of connections*: point-to-point and multipoint.
Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.
For ex: When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.



a. Point-to-point

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



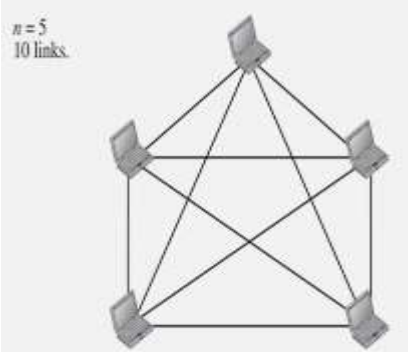
b. Multipoint

In a multipoint environment, the capacity of the channel is shared temporally.

- **Physical Topology or network 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.
Two or more devices connect to a link; two or more links form a topology. The physical layout of the network is called as topology.
There are *four basic topologies* possible: mesh, star, bus, and ring.

1. ***Mesh Topology:*** In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.



To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n – 1 nodes, node 2 must be connected to n – 1 nodes. We need n (n – 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we need n (n – 1) / 2 duplex-mode links.

Fig: mesh topology

Advantages:

i) Dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.

ii) A mesh topology is robust. If one link becomes unusable, it does not harm the entire system.

iii) Privacy or security.

iv) Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

i) The amount of cabling and the number of I/O ports required.

ii) Installation and reconnection are difficult.

iii) The hardware required to connect each link (I/O ports and cable) can be expensive.

2. ***Star Topology:*** In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. a star topology does not allow direct traffic between devices.

The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controllers, which then transmit the data to the other connected device.

Advantages:

A star topology is less expensive than a mesh topology.

i) Easy to install and reconfigure.

ii) Robustness, if one link fails; only that link is affected. All other links remain active.

iii) Easy fault identification and fault isolation.

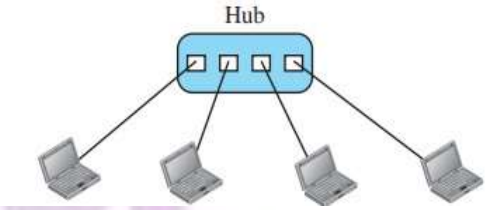


Fig: star topology

Disadvantages:

Whole topology depends on one single point, the hub. If the hub goes down, the whole system is dead.

3. ***Bus Topology*****:** A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps. A *drop line* is a connection running between the device and the main cable. A *tap* is a connector that link into the main cable to create a contact with the metallic core.

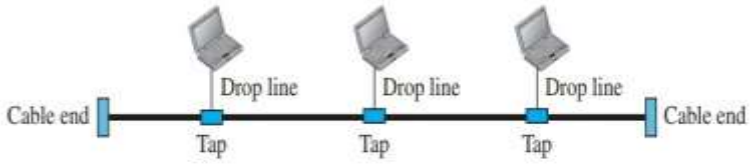


Fig: bus topology

Advantages:

i) Ease of installation.
ii) A bus uses less cabling than mesh or star topologies.
iii) Redundancy is eliminated. Only the backbone cable stretches through the entire facility.

Disadvantages:
i) Difficult reconnection and fault isolation.
ii) Difficult to add new devices. Adding new devices may therefore require modification or replacement of the backbone.
iii) Heavy network traffic.

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

Advantages:
i) Easy to install and reconfigure.
ii) Fault isolation is simplified.

Disadvantages:
i) Unidirectional traffic can be a disadvantage.
ii) A break in the ring (such as a disabled station) can disable the entire network.

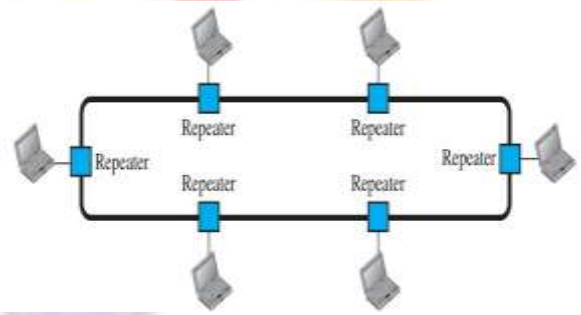


Fig: ring topology

2. Network Types

The criteria of distinguishing one type of network from another are difficult and sometimes confusing. We use a few criteria such as size, geographical coverage.
There are three types of networks:

1. ***LAN(Local Area Network)***
2. ***MAN(Metropolitan Area Networks)***
3. ***WAN(Wide Area Network)***

1. LAN (Local Area Network): A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.
LAN covers small area. LAN size is limited to a few kilometers.
Each host in a LAN has an identifier, an address that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.
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.

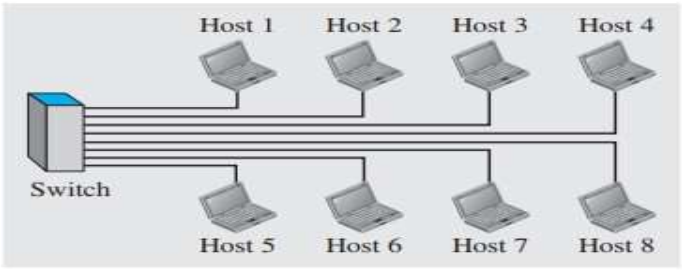


Fig: LAN with a switch

2. MAN (Metropolitan Area Network): 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.

3. WAN (Wide Area Network): 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 LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.
There are two distinct examples of WANs today: point-to-point WANs and switched WANs.

Point-to-Point WAN: A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

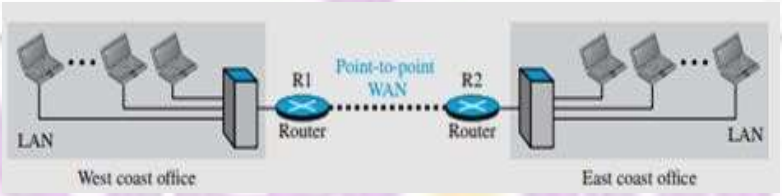


Fig: point-to-point WAN

Switched WAN: A switched WAN is a network with more than two ends. We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches.

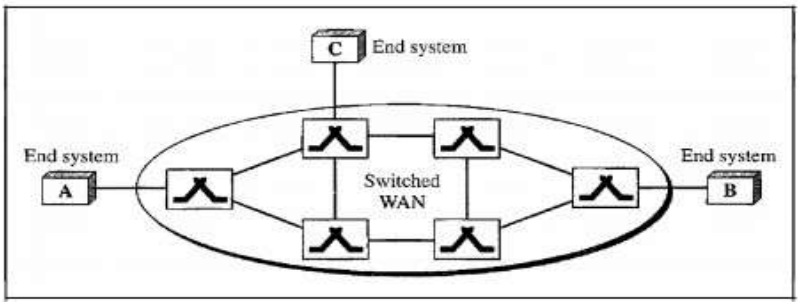


Fig: switched WAN

Interconnection of Networks: When two or more networks are connected, they become an internetwork, or internet.

3. Protocols and Standards

protocol means rule and standards are agreed-upon rules.

- **Protocols:** A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated.

The key elements of a protocol are syntax, semantics, and timing.

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

Timing: The term timing refers to two characteristics: when data should be sent and how fast they can be sent.

- **Standards Organizations**

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 communications.

Standards Organizations Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees:

International Organization for Standardization (ISO). The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

International Telecommunication Union-Telecommunication Standards Sector (ITU-T). 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

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.

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, and electronics.

Electronic Industries Association (EIA). Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns.

4. The OSI Model

The OSI model is based on a proposal developed by the International Standards Organization (ISO). The model is called the ISO OSI (Open Systems Interconnection), which allows different systems to communicate.

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.

It consists of ***seven layers***: 1. Physical Layer, 2. Data link Layer, 3. Network Layer, 4.transport Layer, 5. Session Layer, 6. Presentation layer, 7. Application Layer.

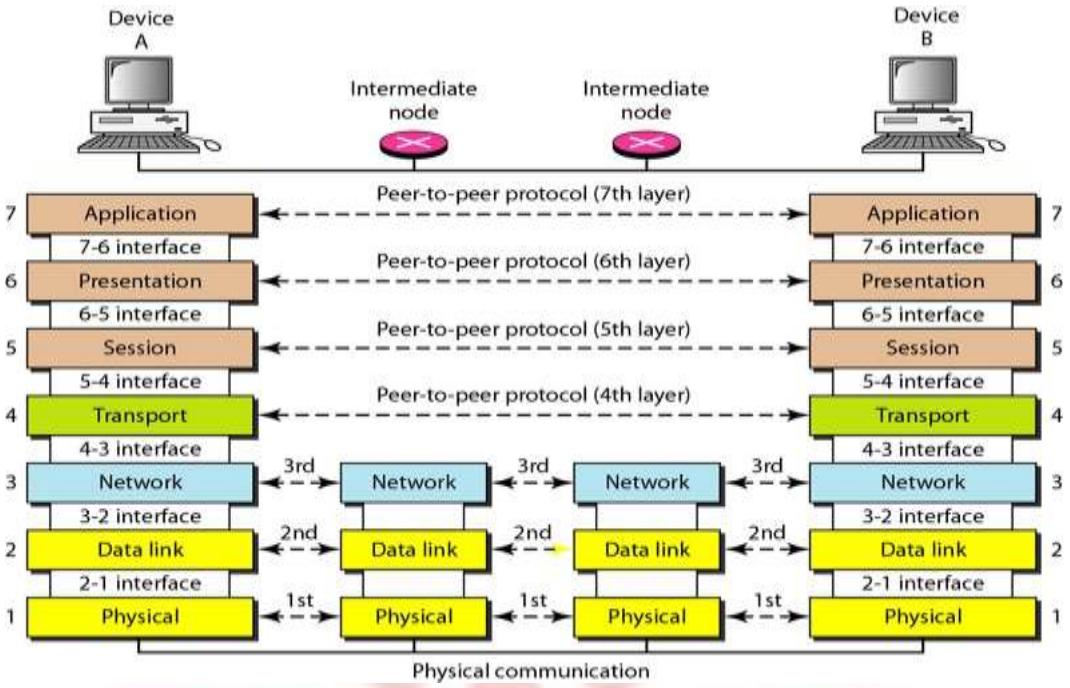


Fig: The interaction between layers in the OSI model

i) Physical layer: the physical layer is responsible for movement of individual bits from one node to the next.

- The physical layer required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.

Responsibilities of physical layer:

Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
Physical topology: The physical topology defines how devices are connected to make a network.
Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

ii) Data Link Layer: The data link layer is responsible for moving frames from one node to the next.Frame: Frame is a series of bits that form a unit of data.

Responsibilities of the data link layer:

Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
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.
Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
Error control: The data link layer adding a mechanism to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames.
Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

iii) Network Layer: The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

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

Responsibilities of the network layer

Logical addressing: Addressing system to help to differentiate the source and destination systems. The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.

Routing: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

iv) Transport Layer: The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.

Responsibilities of the transport layer:

Service-point addressing: Source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header includes a type of address called a service-point address (or port address).

Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination.

Connection control: The transport layer can be either connectionless or connection oriented. A **connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A **connection-oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

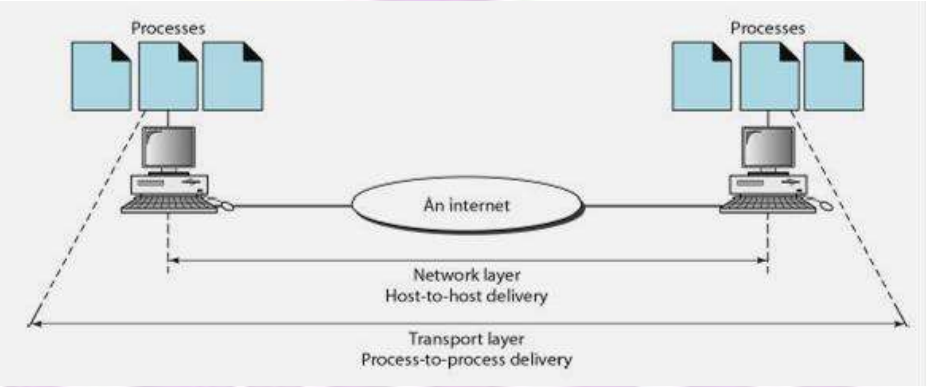


Fig: process-to-process delivery of a message

v) Session Layer: The session layer is responsible for dialog control and synchronization. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems

Responsibilities of the session layer:

Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash

happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

vi) Presentation Layer: The presentation layer is responsible for translation, compression, and encryption. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Responsibilities of the presentation layer:

Translation: The presentation layer at the sender machine changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

vii) Application Layer: The application layer is responsible for providing services to the user.

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

Services provided by the application layer:

Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

File transfer, access, and management: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Mail services: This application provides the basis for e-mail forwarding and storage.

Directory services: This application provides distributed database sources and access for global information about various objects and services.

Transmission Media

Introduction

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 shows the position of transmission media in relation to the physical layer.

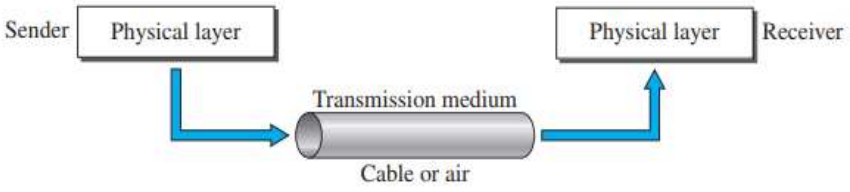


Fig: Transmission medium and physical layer

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. It is also called physical medium.

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.

In telecommunications, transmission media can be divided into **two broad categories**: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

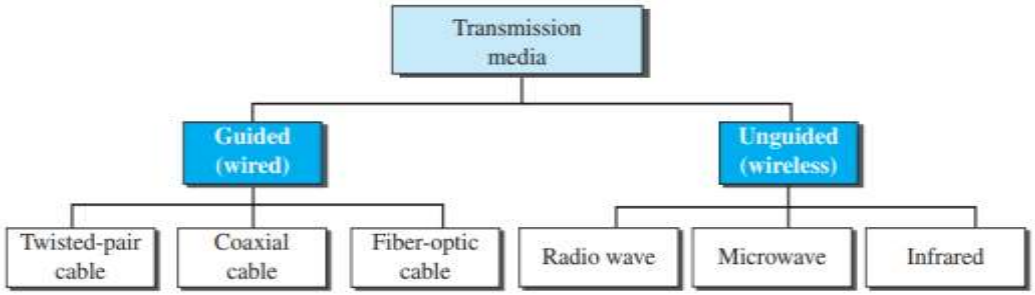


Fig: Classes of transmission media

1. Guided Media

Guided media, which are those that provide a channel from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

❖ **Twisted-Pair Cable:** A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure

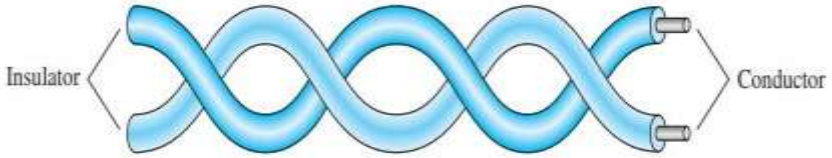


Fig: Twisted-pair cable

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. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Unshielded Versus Shielded Twisted-Pair Cable: The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP).

IBM has also produced a version of twisted-pair cable for its use, called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

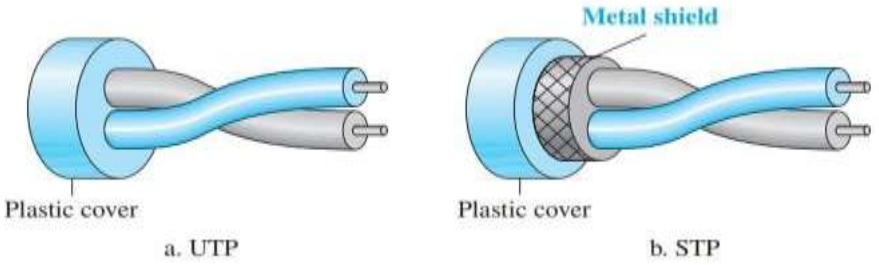


Fig: UTP and STP cables

Performance: One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies.

Applications: Twisted-pair cables are used in telephone lines to provide voice and data channels.

- Local-area networks also use twisted-pair cables.

❖ **Coaxial Cable:** Coaxial cable (or coax) 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.

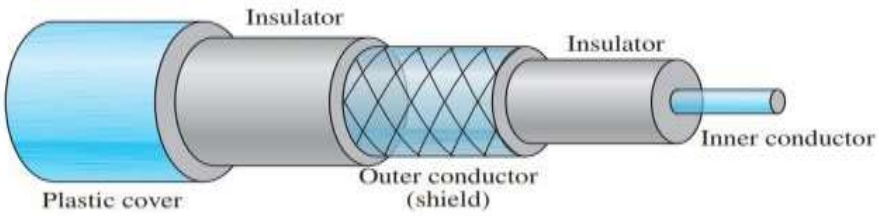


Fig: Coaxial cable

Performance we measure the performance of a coaxial cable. The attenuation is much higher in coaxial cable than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications 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.
- Cable TV networks also use coaxial cables. Later, however, cable TV providers replaced most of the media with fiber-optic cable.
- Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.

❖ **Fiber-Optic Cable:** A fiber-optic cable is made of glass or plastic and transmits signals in the form 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 (density), the ray changes direction.

- Figure shows how a ray of light changes direction when going from a more dense to a less dense substance. As the figure shows, if the angle of incidence I is less than the critical angle, the ray refracts and moves closer to the surface.
- If the angle of incidence is equal to the critical angle, the light bends along the interface.
- If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance.

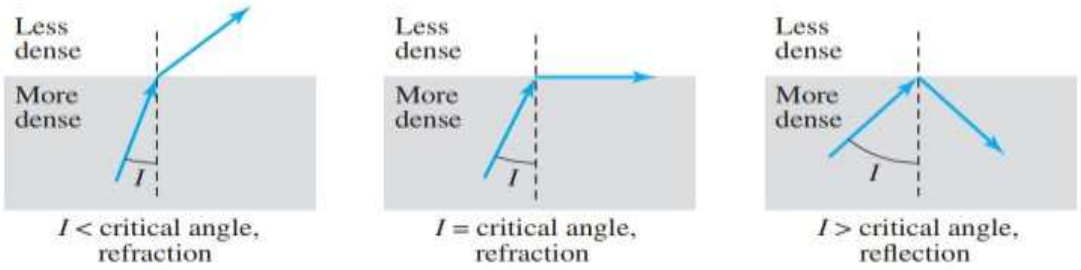


Fig: Bending of light ray

Optical fibers use reflection to guide light through a channel. A glass or **plastic core** is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the **cladding** instead of being refracted into it.

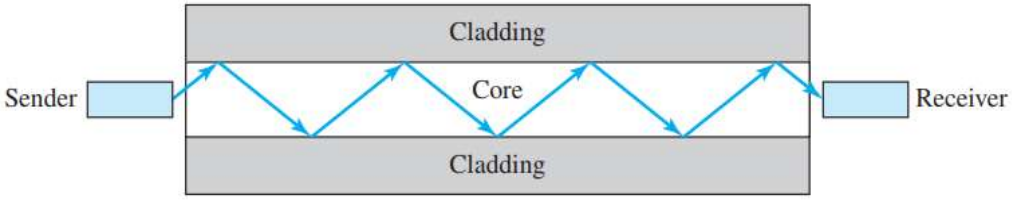


Fig: Optical fiber

Cable Composition: Figure shows the composition of a typical fiber-optic cable. The outer jacket is made of Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

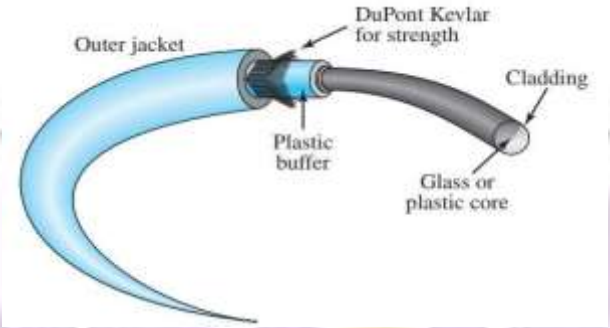


Fig: Fiber construction

Performance: Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer repeaters when we use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber:

Advantages: Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- Higher bandwidth.
- Less signal attenuation..
- Immunity to electromagnetic interference.
- Resistance to corrosive materials.
- Light weight.

.

Disadvantages There are some disadvantages in the use of optical fiber.

- Installation and maintenance.

- Unidirectional light propagation.
- Cost.

Switching

Introduction

Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

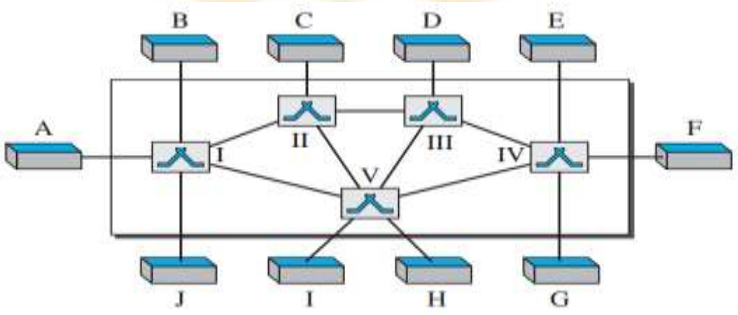


Fig: Switched network

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

Three Methods of Switching: Traditionally, three methods of switching have been discussed: circuit switching, packet switching, and message switching.

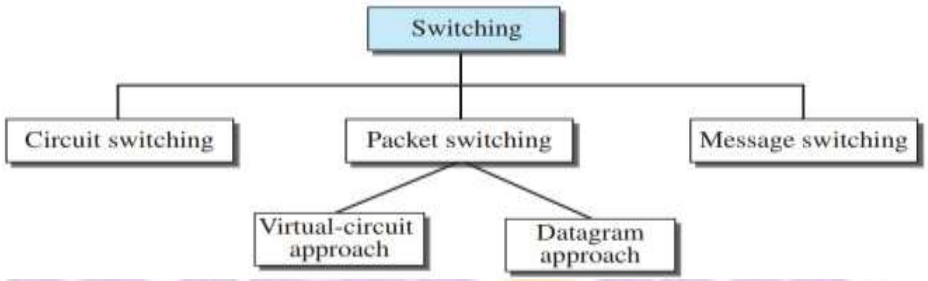


Fig: Taxonomy of switched networks

❖ **Switching and TCP/IP Layers:** Switching can happen at several layers of the TCP/IP protocol suite.

Switching at Physical Layer At the physical layer, we can have only circuit switching. There are no packets exchanged at the physical layer. The switches at the physical layer allow signals to travel in one path or another.

Switching at Data-Link Layer At the data-link layer, we can have packet switching. However, the term packet in this case means frames or cells. Packet switching at the data-link layer is normally done using a virtual-circuit approach.

Switching at Network Layer At the network layer, we can have packet switching. In this case, either a virtual-circuit approach or a datagram approach can be used. Currently the Internet uses a datagram approach.

Switching at Application Layer At the application layer, we can have only message switching. The communication at the application layer occurs by exchanging messages.

2. Circuit-Switched Networks

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

Figure shows a trivial circuit-switched network with four switches and four links. Each link is divided into n (n is 3 in the figure) channels by using FDM or TDM.

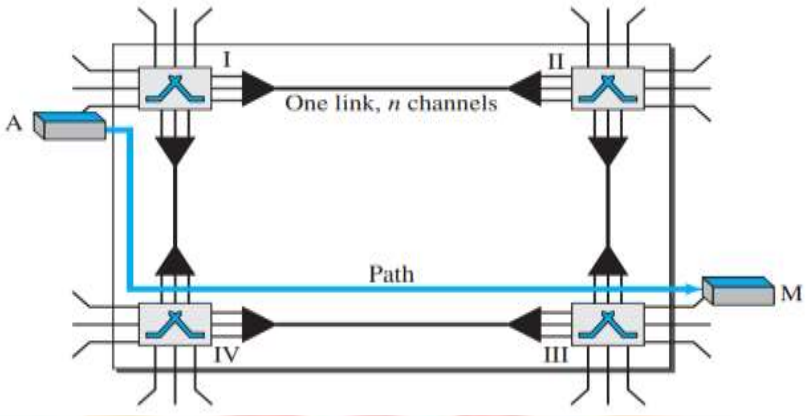


Fig: A trivial circuit-switched network

❖ **Three phases:** A circuit-switched network consists of ***3 phases***: 1) Setup phase (establish),2) Data transfer phase (transfer), 3) Tear down phase (disconnect).

Setup Phase: Before the two parties can communicate, a dedicated circuit needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data-Transfer Phase: After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase: When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

For example: When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the ***setup phase***; after the dedicated path made of connected circuits (channels) is established, the ***data-transfer*** phase can take place. After all data have been transferred, the circuits are **tearing down.**

In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.

Efficiency: It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Delay: Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

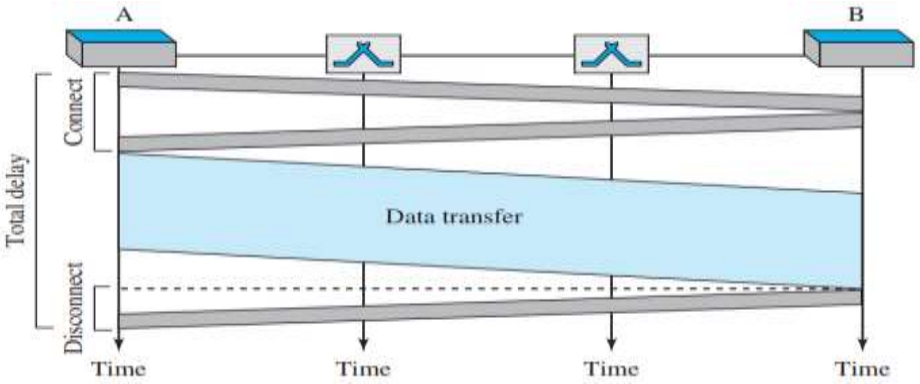


Fig: Delay in a circuit-switched network

3. Packet Switching

In this network data is transferred by dividing the data into individual packets. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size.

In a packet-switched network, there is no resource reservation; resources are allocated on demand. The allocation is done on a first come first served basis.

We can have two types of packet-switched networks: datagram networks and virtual circuit networks.

❖ **Datagram Networks:** In a datagram network; each packet is treated independently of all others. Even if a packet is part of a multi packet transmission, the network treats it as though it existed alone.

Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer. Packets contains header with full information about the destination. The datagram networks are sometimes referred to as connectionless networks.

Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.

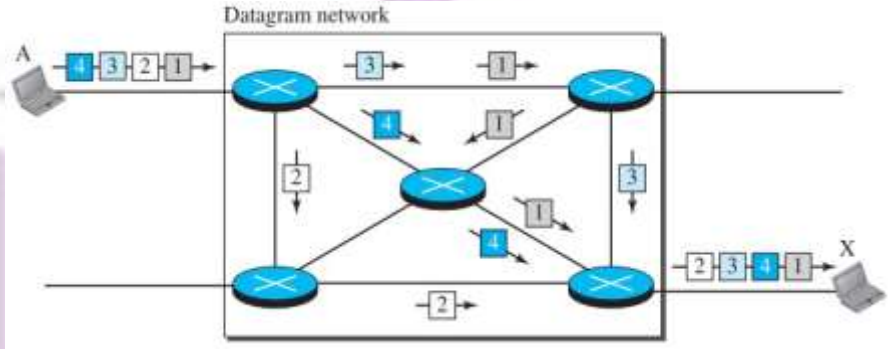


Fig: A datagram network with four switches (routers)

Routing Table: A switch in a datagram network uses a routing table that is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables.

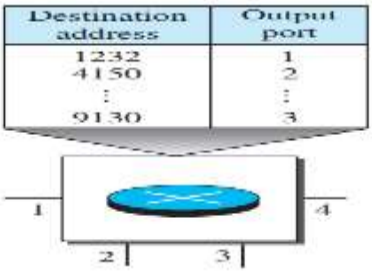


Fig: Routing table in a datagram network

Destination Address: Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet.

Efficiency: The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

Delay: There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded.

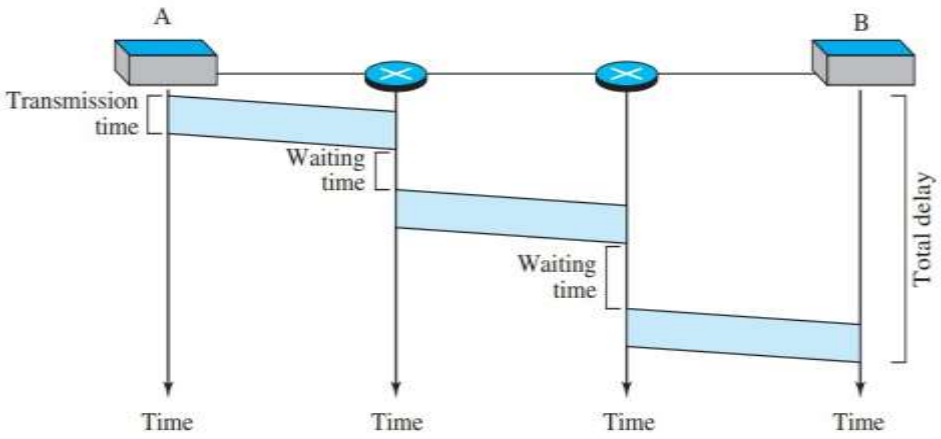


Fig: Delay in a datagram network

❖ **Virtual-Circuit Networks:** A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data-link layer.

Figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations.

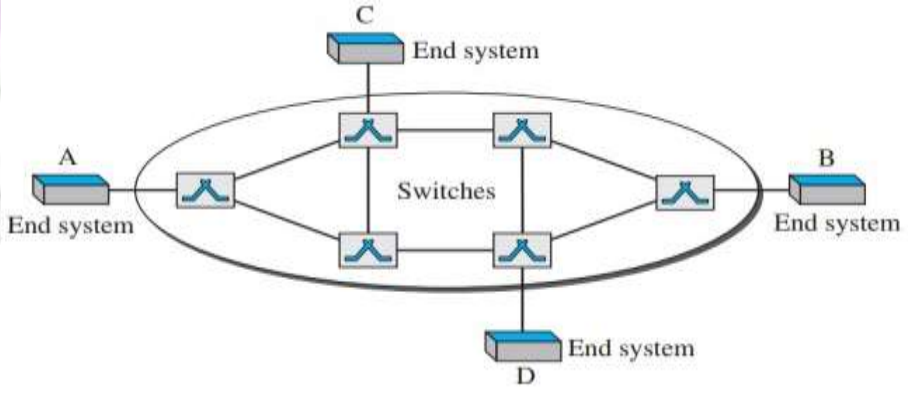


Fig: Virtual-circuit network

❖ **Three phases:** A circuit-switched network consists of ***3 phases***: 1) Setup phase (establish),2) Data transfer phase (transfer), 3) Tear down phase (disconnect).

Setup Phase: Before the two parties can communicate, a dedicated circuit needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.
Data-Transfer Phase: After the establishment of the dedicated circuit (channels), the two parties can transfer data.
Teardown Phase: When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.
In virtual-circuit switching, all packets belonging to the same source and destination travel the same path, but the packets may arrive at the destination with different delays if resource allocation is on demand.

Delay in Virtual-Circuit: Networks In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets.

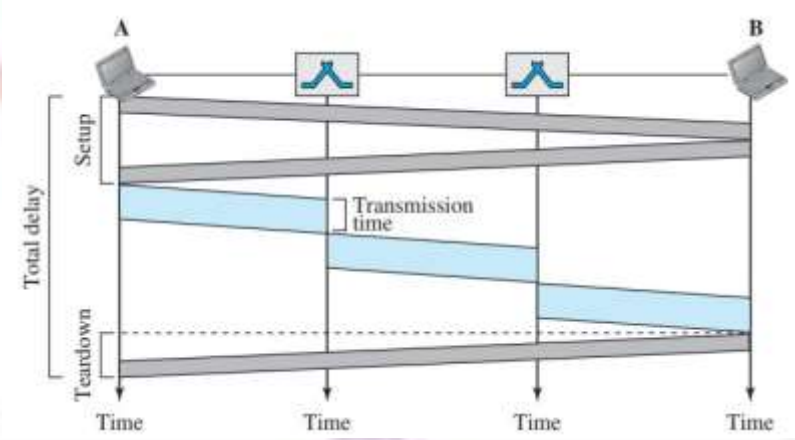


Fig: Delay in a virtual-circuit network

4. Structure of a Switch

We use switches in circuit-switched and packet-switched networks.

❖ Structure of Circuit Switches

Circuit switching today can use either of two technologies: the ***space-division*** switch or the ***time-division*** switch.

- ***Space-Division Switch***

In **space-division switching,** 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. It has evolved through a long history of many designs.

Crossbar Switch

A **crossbar switch** connects *n* inputs to *m* outputs in a grid, using electronic micro switches (transistors) at each **cross point**. The major limitation of this design is the number of cross points required. To connect *n* inputs to *m* outputs using a crossbar switch requires *n* **m* cross points. For example, to connect 1000 inputs to 1000 outputs requires a switch with 1,000,000 cross points.

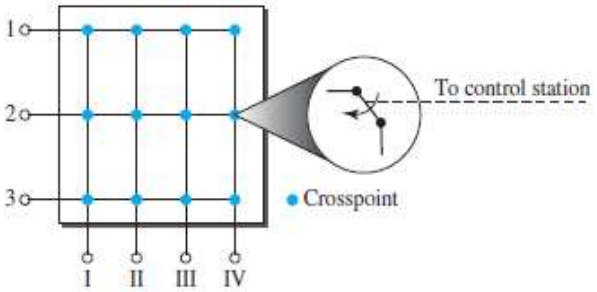


Fig: ***Crossbar switch with three inputs and four outputs***

Multistage Switch

The solution to the limitations of the crossbar switch is the **multistage switch,** which combines crossbar switches in several (normally three) stages, as shown in Figure.

In a single crossbar switch, only one row or column (one path) is active for any connection. So we need *N *N* crosspoints.

If we can allow multiple paths inside the switch, we can decrease the number of crosspoints. Each crosspoint in the middle stage can be accessed by multiple crosspoints in the first or third stage.

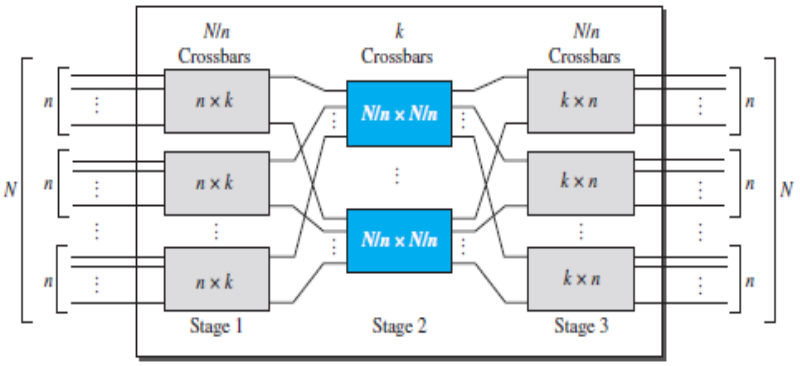


Fig:Multistage switch

To design a three-stage switch, we follow these steps:

1. We divide the *N* input lines into groups, each of *n* lines. For each group, we use one crossbar of size *n *k*, where *k* is the number of crossbars in the middle stage. In other words, the first stage has *N*/*n* crossbars of *n*k* crosspoints.
2. We use *k* crossbars, each of size (*N*/*n*) *(*N*/*n*) in the middle stage.
3. We use *N*/*n* crossbars, each of size *k *n* at the third stage.

We can calculate the total number of crosspoints as follows:

$$\frac{N}{n}(n \times k) + k\left(\frac{N}{n} \times \frac{N}{n}\right) + \frac{N}{n}(k \times n) = 2kN + k\left(\frac{N}{n}\right)^2$$

In a three-stage switch, the total number of crosspoints is

$$2kN + k\left(\frac{N}{n}\right)^2$$

which is much smaller than the number of crosspoints in a single-stage switch (N^2).

- ***Time-Division Switch***

Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the **time-slot interchange (TSI).**

Time-Slot Interchange

Figure shows a system connecting four input lines to four output lines. Imagine that each input line wants to send data to an output line according to the following pattern: (1→ 3), (2 → 4), (3 → 1), and (4 →2), in which the arrow means "to."

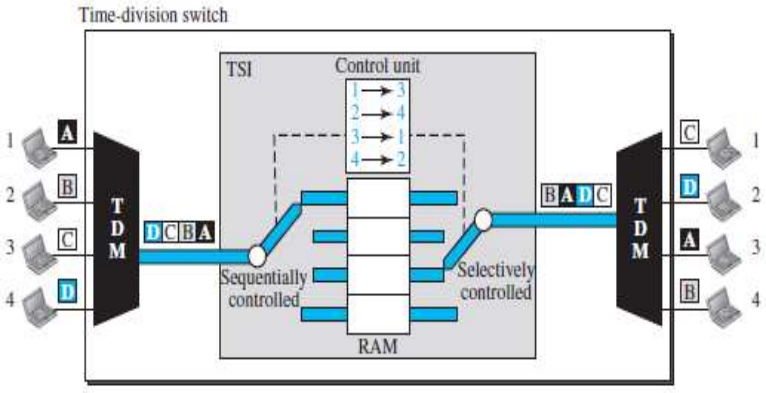


Fig: Time-slot interchange

❖ Structure of Packet Switches

A switch used in a packet-switched network has a different structure from a switch used in a circuit-switched network. We can say that a packet switch has four components: **input ports, output ports,** the **routing processor,** and the **switching fabric,** as shown in Figure.

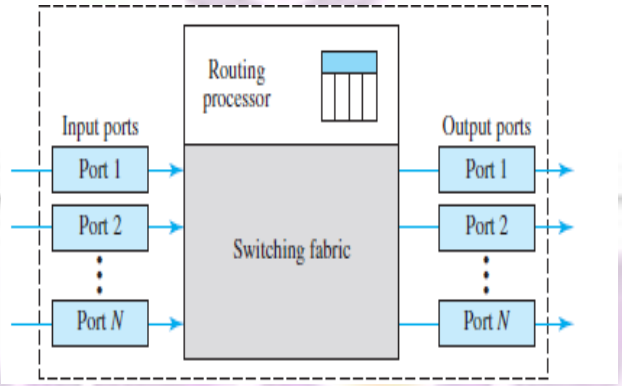


Fig: Packet switch components

Banyan Switch

A more realistic approach than the crossbar switch is the **banyan switch** (named after the banyan tree). A banyan switch is a multistage switch with microswitches at each stage that route the packets based on the output port represented as a binary string.

For *n* inputs and *n* outputs, we have ***log2 n stages*** with **n/2 microswitches** at each stage. The first stage routes the packet based on the high-order bit of the binary string. The second stage routes the packet based on the second high-order bit, and so on.

Fig shows a banyan switch with eight inputs and eight outputs. The number of stages is log2(8) = 3.