Data Communication and Computer Networks

Module – I

Overview of Data Communications and Networking:

Introduction:

Data communications and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the decision makers require immediate access to accurate information.

A revolution is occurring in data communications and networking. Technological advances are making it possible for communications links to carry more and faster signals. As a result, services are evolving to allow use of this expanded capacity.

Data Communications:

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

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

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.
4. **Jitter:** Jitter refers to the variation in the packet arrival time.

Components:

A data communications system has five components as follows;

1. **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Data Representation:

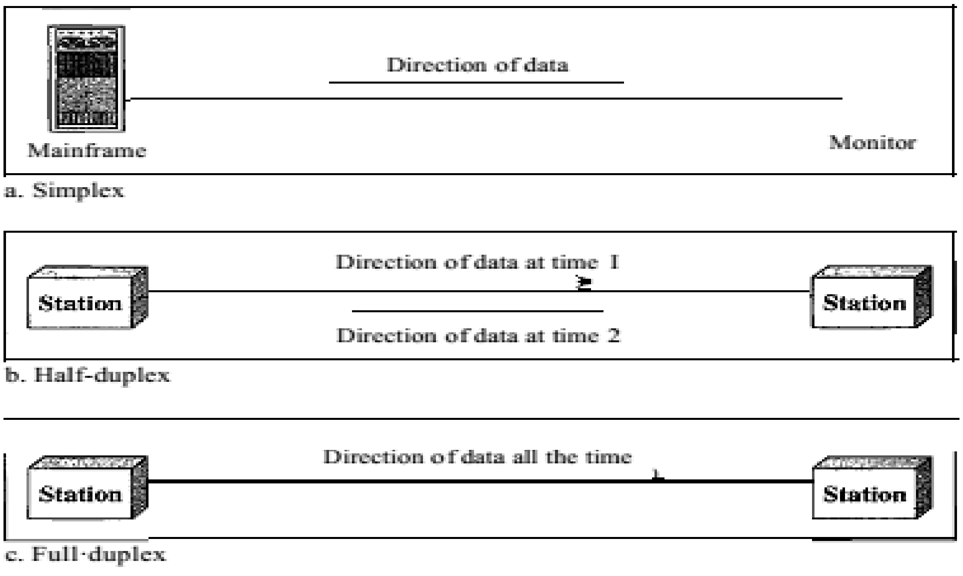
Information today comes in different forms such as text, numbers, images, audio, and video.

1. **Text:** In data communications, text is represented as a bit pattern, a sequence of bits (0s or Is).
2. **Numbers:** Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.
3. **Images:** Images are also represented by bit patterns. In its simplest form, an image is composed of matrix of pixels (picture elements), where each pixel is a small dot.
4. **Audio:** Audio refers to the recording or broadcasting of sound or music.
5. **Video:** Video refers to the recording or broadcasting of a picture or movie.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex.

- **Simplex:** In simplex mode, the communication is unidirectional, as on a one-way street.
- **Half-Duplex:** In half-duplex mode, each station can both transmit and receive, but not at the same time.


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

- **Full-Duplex**: In full-duplex mode both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time.

NETWORKS:

A network is a set of devices 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.

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.
- **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, and the network's robustness in a catastrophe.
- **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. There are two possible types of connections: point-to-point and multipoint.

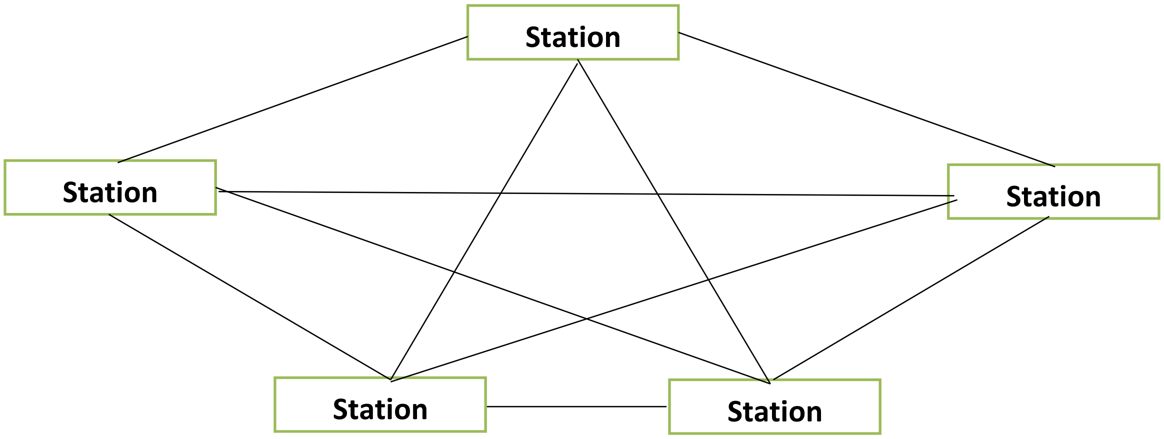
1. **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices.
2. **Multipoint:** A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link.

Physical Topology

- The term physical topology refers to the way in which a network is laid out physically.
- In a network 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 to one another. There are four basic topologies possible: mesh, star, bus, and ring.

Mesh:

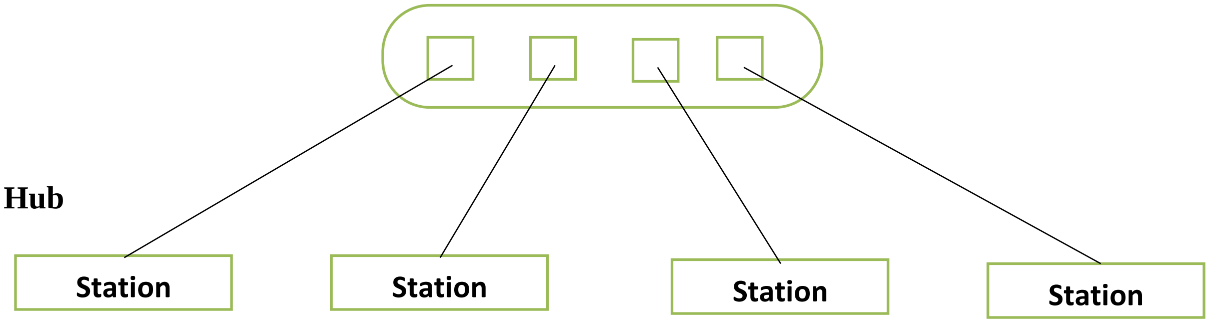
- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term *dedicated* means that the link carries traffic only between the two devices it connects.
- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. We need n*(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n -1) /2.



- **Advantages**
  - The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
  - A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.
- **Disadvantages**
  - The main of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult.
  - The sheer bulk of the wiring can be greater than the available space can accommodate. Finally, the hardware required to connect each link can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion.

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.
- Unlike a mesh topology, 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 controller, which then relays the data to the other connected device.
- **Advantages**
    - A star topology is less expensive than a mesh topology.
    - In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
    - Robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

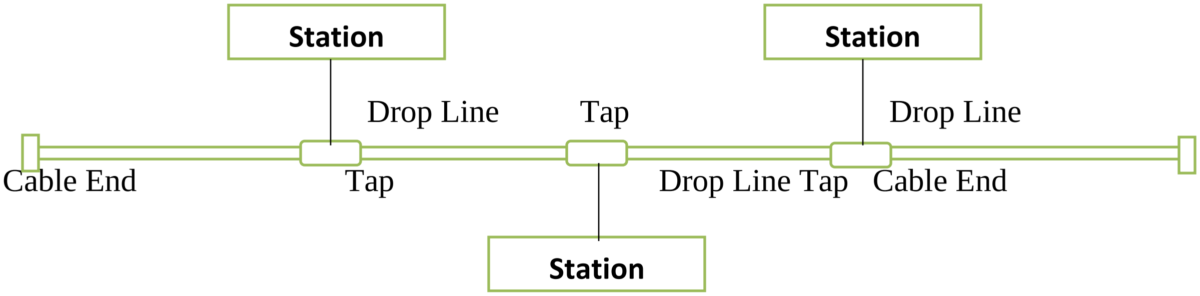


- **Disadvantage: T**he whole topology is dependent on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

Bus Topology:

- The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.

- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

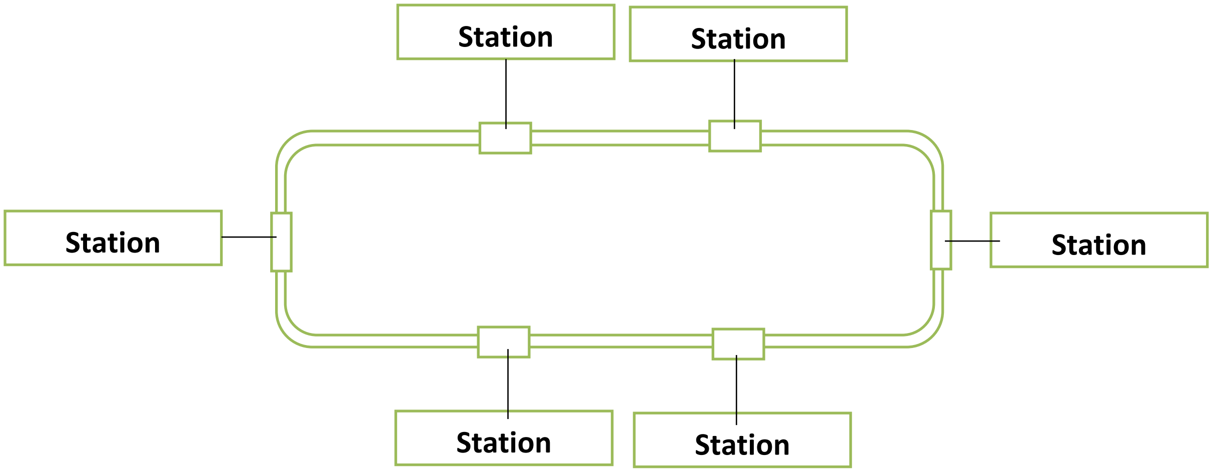


- **Advantages :** A bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.
- **Disadvantages**:
  - Include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
  - In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

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.

- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors.
- To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations. In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.



- However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

1. **Hardware or Network device:**

- **Hub:**
  - It is uses to connect systems or nodes or networks.
  - It has direct connection to a node (point to point connection).
  - It suffers from high collision of data, results to data loss.
  - A hub takes data from input port and retransmits the input data on output port.

- **Repeater:**
  - A repeater is a device which regenerates or amplifies the data or signal so that it can be travel to the other segment of cable.
  - It is use to connect two networks that uses same technology and protocol.
  - It does not filter or translate any data.
  - Work in physical layer.

- **Bridge:**
  - **I**t is used to connect two networks.
  - It divides the collision domain based on number of ports or interface present in a bridge.
  - It uses the packet switches that forward and filter the frames using LAN destination address.
  - Bridge examines the destination address of frame and forwards it to the interface or port which leads to the destination.
  - It uses the routing table for routing frame from one node to other using MAC address.
  - It works in Data Link Layer.

- **Switch :**
  - It is similar to bridge. It has more number of interfaces as compared to bridge.
  - It allows direct communication between the nodes.
  - It work in Data Link Layer.
  - It uses MAC address for data transfer in a network.

- **Router:**
  - It is used to connect different types of network (types- architecture/ Protocol).
  - It work similar to bridge but it uses IP address for routing data.
  - Router can't be used for connecting Systems.
  - It work in Network Layer.

- **Gateways:** Gateways make communication possible between systems that use different communication protocols, data formatting structures, languages and architectures. Gateways repackage data going from one system to another. Gateways are usually dedicated servers on a network and are task-specific.

Categories of Networks:

Today when we speak of networks, we are generally referring to two primary categories: local-area networks and wide-area networks. The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 mi; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

Local Area Network:

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office;

or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

- LANs are designed to allow resources to be shared between personal computers or workstations. In addition to size, 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.

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 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. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider. This type of WAN is often used to provide Internet access.

Metropolitan Area Networks:

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.

THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use. The Internet is a structured, organized system. We begin with a brief history of the Internet. We follow with a description of the Internet today.

PROTOCOLS AND STANDARDS:

In this section, we define two widely used terms: protocols and standards. First, we define protocol, which is synonymous with rule. Then we discuss standards, which 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:** It refers to the structure or format of the data. This refers the order in which the data are presented.

Example :

- The first 8 bits of data to be the address of the sender.
- The second 8 bits to be the address of the receiver.
- The rest of the stream may be the message itself

- **Semantics:** It refers to the meaning of each section of bits. How a particular pattern to be interpreted. What action is to be taken based on that interpretation

  Example

  An address specifies the route to be taken or the final destination of the message.

- **Timing:** It refers to two characteristics. When data should be sent and how fast they can be sent.

  Example

  If a sender produces data at 100 Mbps and the receiver process data at only 1 Mbps, it will overload the receiver and data will be lost.

Standards:

Why do we need standards?

- To create and maintain an open and competitive market for equipment manufacturers
- To guarantee national and international interoperability of data, telecommunication technology and process
- To give a fixed quality and product to the customer
- To allow the same product to be re used again elsewhere
- To aid the design and implementation of ideas
- To provide guidelines to manufacturers, vendors, government agencies and other service providers to ensure kind of interconnectivity.

Data communication standards are divided into two categories

De facto (from the fact):

- Standards that have not been approved by an organized body.
- It has been adopted as standards through widespread use.

- This is often established originally by manufacturers to define the functionality of a new product or technology.

De jure (by law):

- Those that have been legislated by an officially recognized body.

Standards organizations

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

Standards Creation Committees

ITU, International Telecommunications Union formerly the (CCITT):

- It a standard for telecommunication in general and data systems in particular.

ISO, International Standards Organization:

- It is active in developing cooperation in the realms of scientific, technological and economic activity.

ANSI, American National Standards Institute:

- It is a private nonprofit corporation and affiliated with the U.S federal government.

IEEE, Institute of Electrical and Electronics Engineers:

- It aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics radio and in all related branches of Engineering.
- It oversees the development and adoption of international standards for computing and communications. See http://standards.ieee.org/

EIA, Electronic Industries Association:

- It 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.
- It also made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

Forums

- It work with universities and users to test, evaluate, and standardize new technologies.
- The forums are able to speed acceptance and use of those technologies in the telecommunications community.
- It present their conclusions to standard bodies.

Regulatory Agencies:

- Its purpose is to protect the public interest by regulating radio, television and wire cable communications.
- It has authority over interstate and international commerce as it relates to communication.

Internet Standards

- It is a thoroughly tested specification that is useful to and adhered to by those who work with the internet.
- It is a formalized regulation that must be followed.
- A specification begins as an internet draft and attains Internet standard status.
- An Internet draft is a working document and it may be published as Request for Comment (RFC).RFC is edited, assigned a number, and made available to all interested parties.

OSI Reference Model

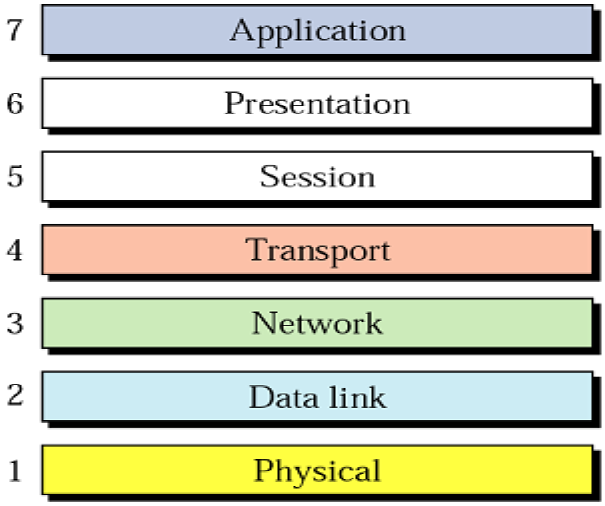


Figure 1 OSI Model

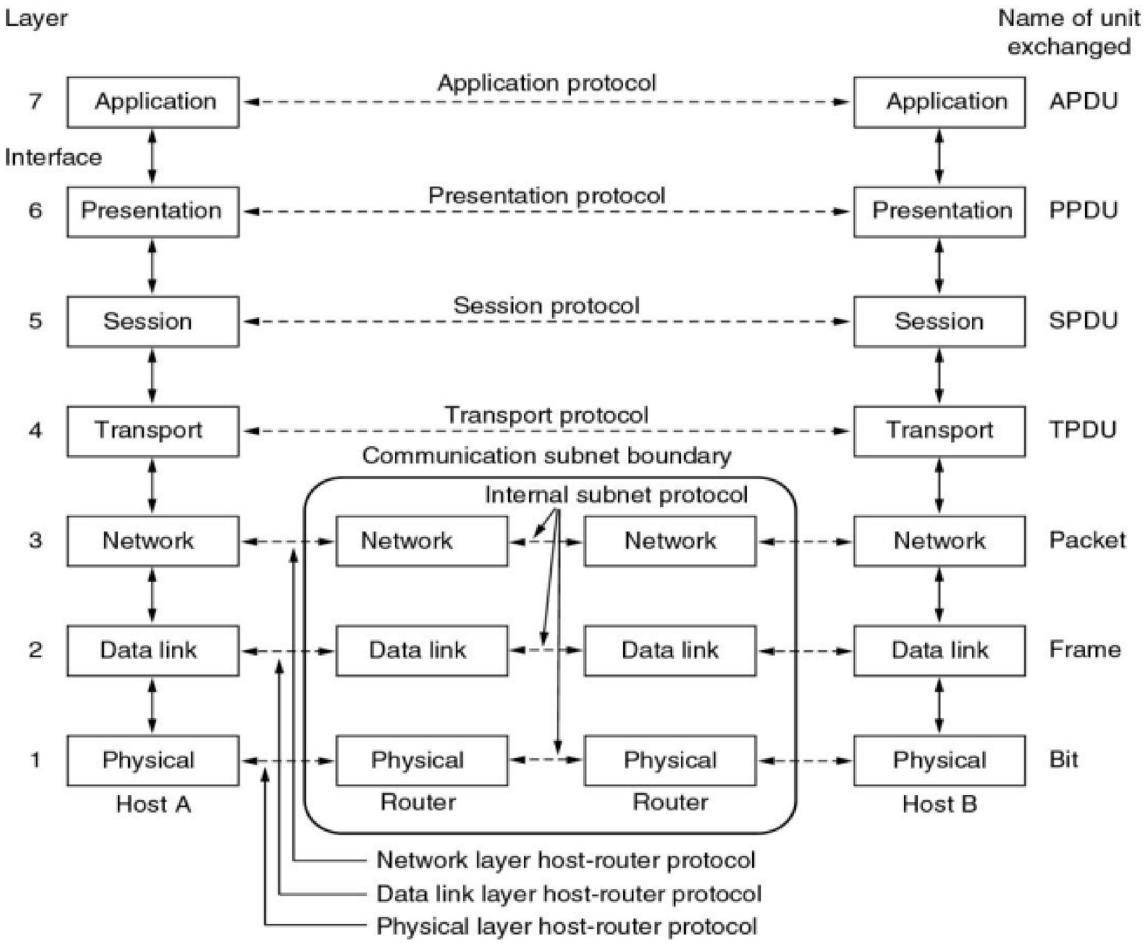
- The OSI model shown in figure 1 is based on the proposal developed by the International Standards Organization (ISO) as a first step towards international standardization of the protocols used in the various layers.
- The model is called the OSI (Open System Interconnection) reference model because it deals with connecting open systems, i.e., systems that are open for communication with other systems.
- 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 not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable.
- 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 separate but related layers, each of which defines a part of the process of moving information across a network. The principles that were applied to arrive at the seven layers are as follows:
- A layer should be created where a different level of abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Layered Architecture:

The OSI model is composed of seven layers: Physical, Data link, Network, Transport, Session, Presentation, Application layers. Fig (iii) shows the layers involved when a message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes involve only the first 3 layers of the OSI model.

Within a single machine, each layer calls upon the services of the layer just below it, layer 3 for ex. Uses the services provided by layer 2 & provides services for layer 4. Between machines, layer X on one machine communicates with layer X on another machine. This communication is governed by an agreed upon series of rules & Conventions called protocols. The processes on each machine that communicate at a given layer are called peer – to – peer processes.

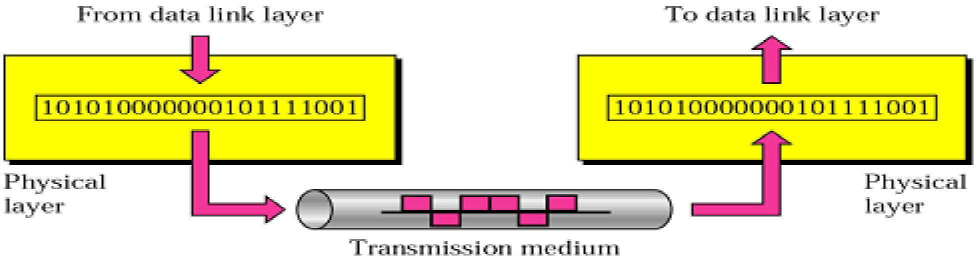
Communication between machines is therefore a peer – to –peer process using the protocols appropriate to a given layer.



Layers in the OSI model:

1. Physical Layer:

Physical Layer is responsible for movements of individual bits from one node to the next node.

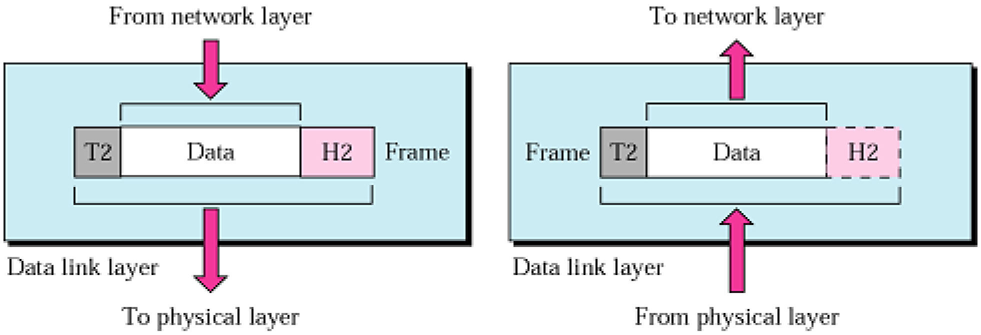


- Physical characteristics of interfaces & medium, type of transmission medium.
- Representation of bits: Bits encoded to signals: electrical or optical
- Data rate: no.of bits sent each second
- Synchronization of bits: sender and receiver clocks are synchronized.

- Line configuration: point-to point or multipoint
- Physical topology – Mesh, Star, Ring, Bus, Hybrid.
- Transmission mode – Simplex, Half -duplex, Full-duplex.

2. Data Link Layer:

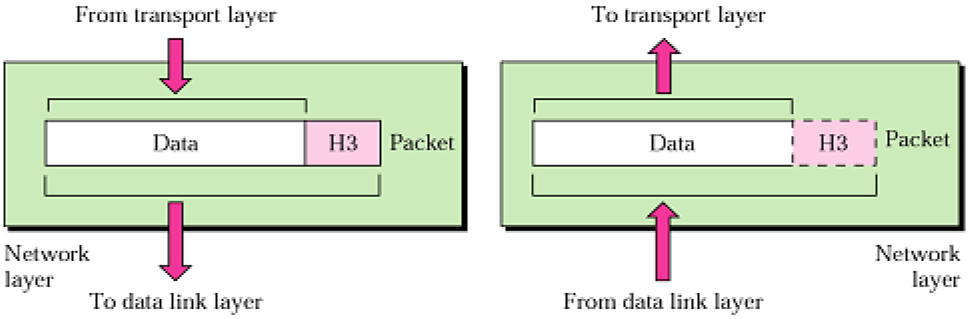
Data link layer is responsible for moving frames from one node to the next.



- Framing: divides the stream of bits into manageable data units called frames.
- Physical addressing: adds a header to frame to define the sender/receiver within a network.
- Flow control: data rate of sender and receiver should match.
- Error control: adds mechanism to detect and retransmit damaged or lost frames. Achieved through a trailer added to the end of frame.
- Access control: when more devices are connected to same link, it determines which device has control over the link at any given time.

3. Network Layer:

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

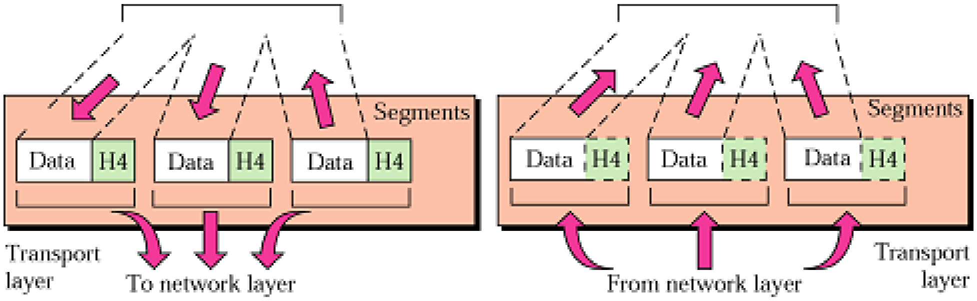


- Logical addressing : Adds a header including logical address for communication in different network.

- Routing: uses physical devices routers.

4. Transport Layer:

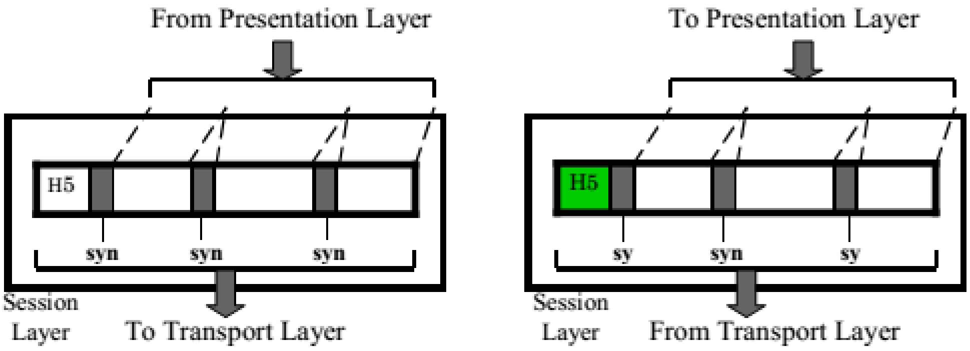
- Transport layer is responsible for the delivery of a message from one process to another.
- A process is an application program running on a host.



- Service-point addressing: Adds the port address(service-point) to deliver the entire message to the correct process on that computer.
- Segmentation and reassembly: Divide into transmittable segments with a sequence number at sender side; reassembled correctly at receiver side.
- Connection control: Connection less or connection-oriented
- Flow control: flow control is from end to end rather than across a single link.
- Error control: performed process to process rather than a single link.

5. Session Layer:

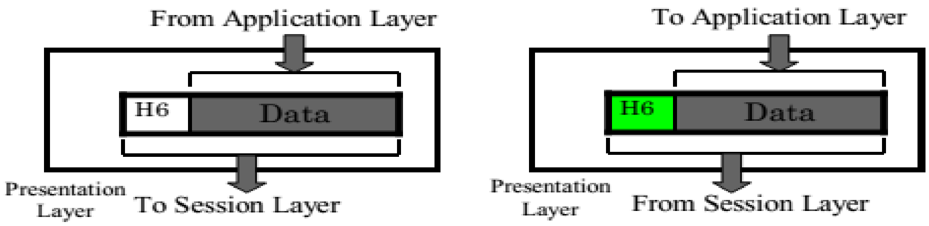
The session layer is responsible for dialog control and synchronization.



- Dialog control: communication between two processes : half-duplex or full-duplex
- Synchronization: add synchronization points (checkpoints) to a stream of data.

6. Presentation Layer:

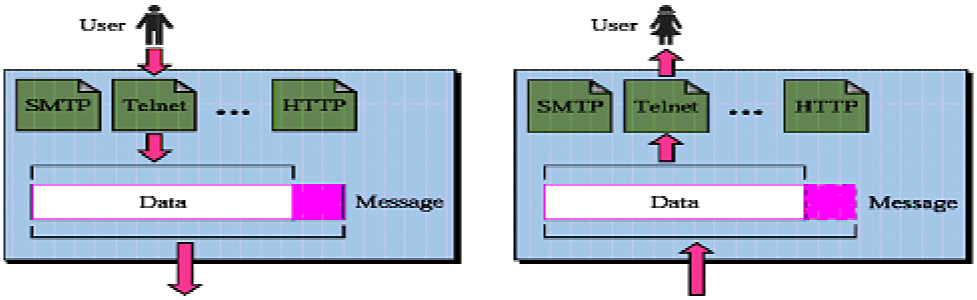
The Presentation layer is responsible for translation, compression, and encryption.



- Concerned with syntax and semantics of the information.
- Translation: different datatypes changed to bit streams.
- Encryption: enhances security for sensitive information.
- Compression: reduces the number of bits contained in the information. Applicable for text, audio and video.

7. Application Layer:

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



- Network virtual terminal: a software version of physical terminal, that allows user to log on to remote host.
- File transfer, access, and management.
- Mail services: basis for e-mail forwarding and storage.
- Directory services: provides distributed database sources and access for global information about various objects and services.

TCP/IP Protocol suite:

The TCP/IP protocol suite has four layers: Host – to – Network, Internet, Transport and Application. Comparing TCP/IP to OSI model: the Host – to – Network layer is equivalent to the combination of physical and data link layers, the Internet layer is equivalent to the network layer, the Transport layer in TCP/IP taking care of part of the duties of the session layer, and the application layer is roughly doing the job of the session, presentation, & application layers.

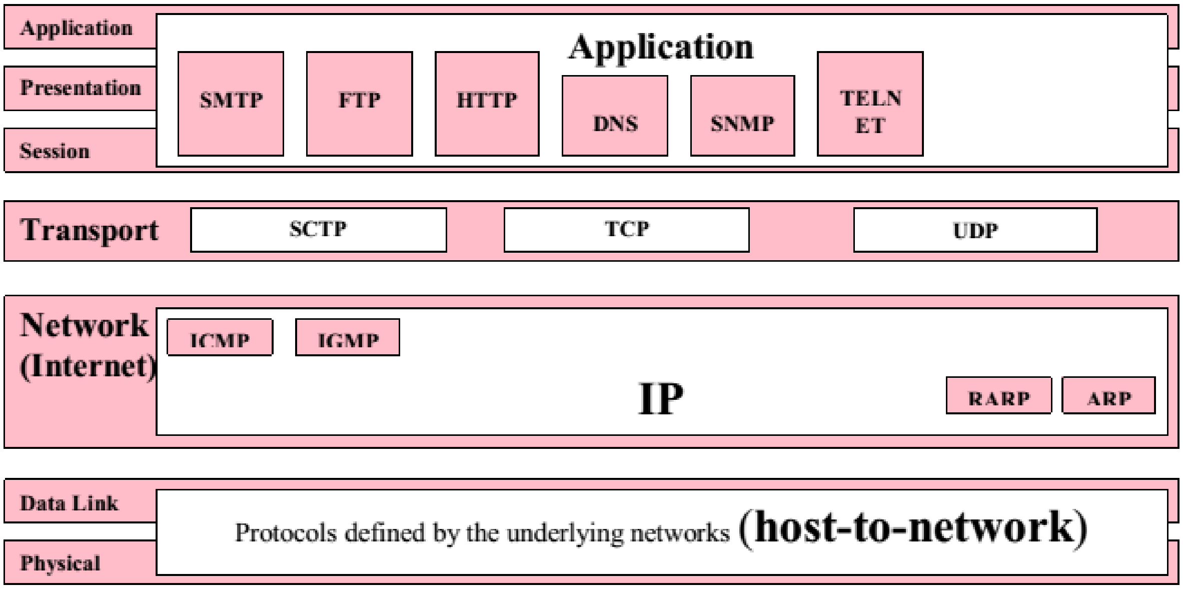


Figure 2 TCP/IP Protocol suite

Physical and Datalink layer: Do not define any specific protocol. It supports all the standard protocols.

Network Layer: supports Internetworking Protocol(IP).
IP: Unreliable and connectionless protocol. Provides no error checking or tracking. Transports data in packets called *datagrams*. Uses four protocols:

a. ARP: *Address Resolution Protocol*: used to associate a logical address with a physical address.
b. RARP: *Reverse Address Resolution Protocol:* allows a host to discover its Internet address when it knows only its physical address.
c. ICMP: *Internet Control Message Protocol*: used by hosts and gateways to send notification of datagram problems back to the sender.
d. IGMP: *Internet Group Message Protocol*: used to facilitate the simultaneous transmission of a message to a group of recipients

Transport Layer: represented by two protocols: TCP and UDP. A new protocol SCTP has been devised to meet the needs of some newer applications.

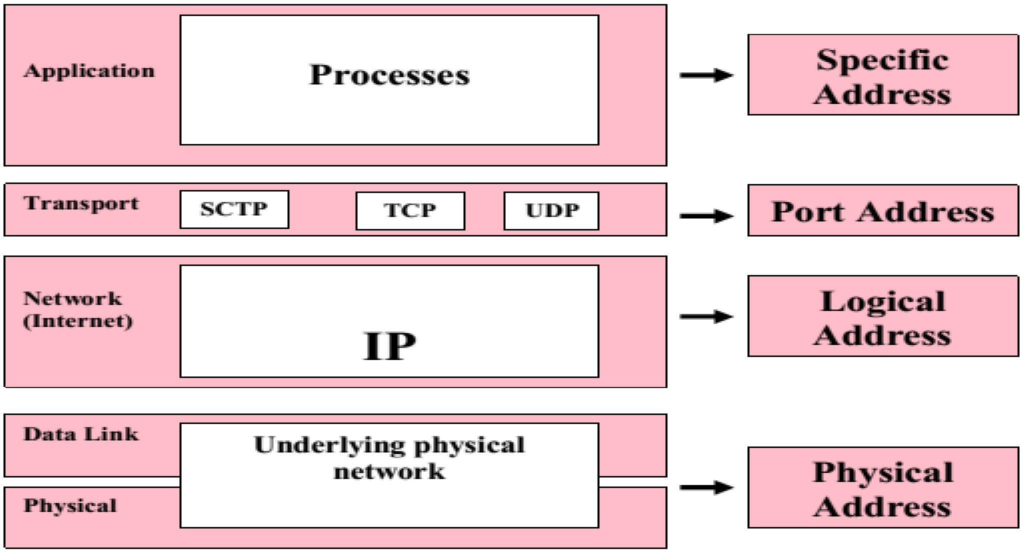
1. *UDP: User datagram Protocol:* It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
2. *TCP: Transmission Control Protocol:* provides full transport layer services. It is connection-oriented. Divides a stream of data into smaller units called segments.
3. *SCTP: Stream Control Transmission Protocol:* supports newer applications such as voice over internet. It combines the best features of UDP and TCP.

Application Layer: Equivalent to the combined session, presentation and application layers in the OSI model. Many protocols are defined at this layer.

Addressing:

Four levels of addresses are used in an internet employing the TCP/IP Protocols:

1. **Physical addresses:** Also known as link address, is the address of a node as defined by its LAN or WAN. Included in the frame by the datalink layer. It is the lowest level address. The size and format vary depending upon the network. Ex: Ethernet uses 6-byte(48bit) NIC (Network Interface Card).
2. **Logical addresses:** necessary in an internetwork environment where different networks have different address formats. It is 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. The physical addresses will change from hop to hop, but the logical addresses usually remain the same.
3. **Port addresses:** The port address is used for communication between process. It is 16 bits in length. Ex: CompA communicate with CompC using TELNET, and with CompB by using FTP.
4. **Specific addresses:** Some applications have user-friendly addresses that are designed for that specific address. Ex: e-mail address, URL(Universal Resource Locator)



Physical Layer

We start the discussion of the Internet model with the bottom-most layer, the physical layer. It is the layer that actually interacts with the transmission media, the physical part of the network that connects network components together. This layer is involved in physically carrying information from one node in the network to the next.

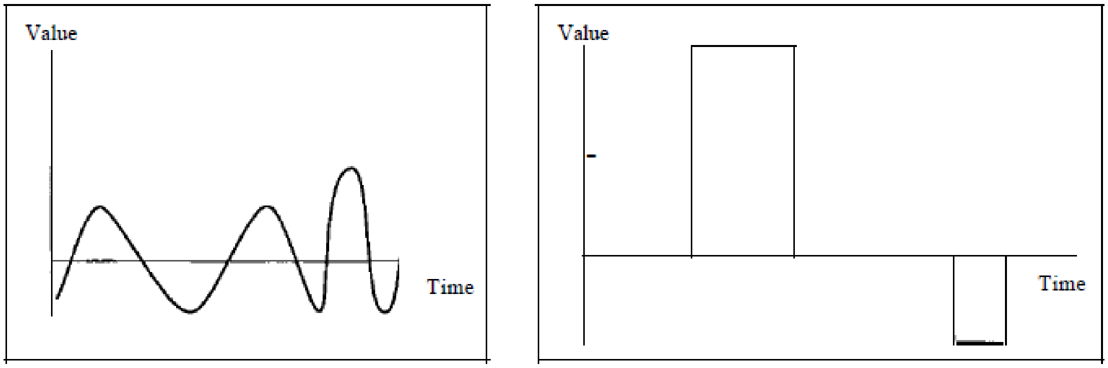
The physical layer has complex tasks to perform. One major task is to provide services for the data link layer. The data in the data link layer consists of 0s and 1s organized into frames that are ready to be sent across the transmission medium. This stream of 0s and 1s must first be converted into another entity: signals. One of the services provided by the physical layer is to create a signal that represents this stream of bits.

The physical layer must also take care of the physical network, the transmission medium. The transmission medium is a passive entity; it has no internal program or logic for control like other layers. The transmission medium must be controlled by the physical layer. The physical layer decides on the directions of data flow. The physical layer decides on the number of logical channels for transporting data coming from different sources.

Analog and Digital:

Both data and the signals that represent them can be either **analog or digital** in form. Data can be analog or digital. The term **analog data** refers to information that is continuous; **digital data** refers to information that has discrete states.

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.



a. Analog signal

b. Digital signal

Periodic and Nonperiodic Signals:

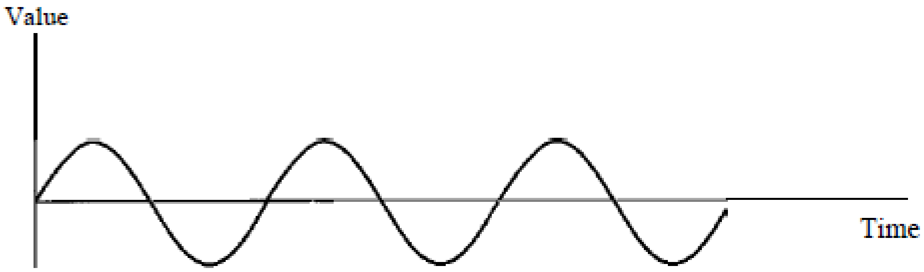
Both analog and digital signals can take one of two forms: periodic or nonperiodic. In data communications, we commonly use periodic analog signals

Periodic Analog Signals:

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.

The sine wave is the most fundamental form of a periodic analog signal.

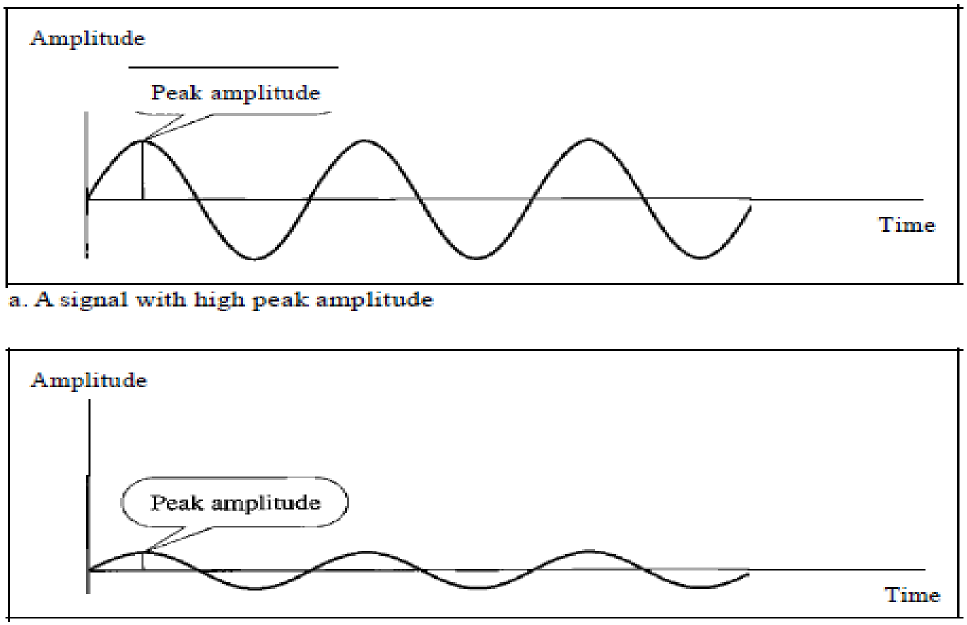
A sine wave



Peak Amplitude:

The peak amplitude of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in volts.

Two signals with the same phase andfrequency, but different amplitudes



a. A signal with high peak amplitude

b. A signal with low peak amplitude

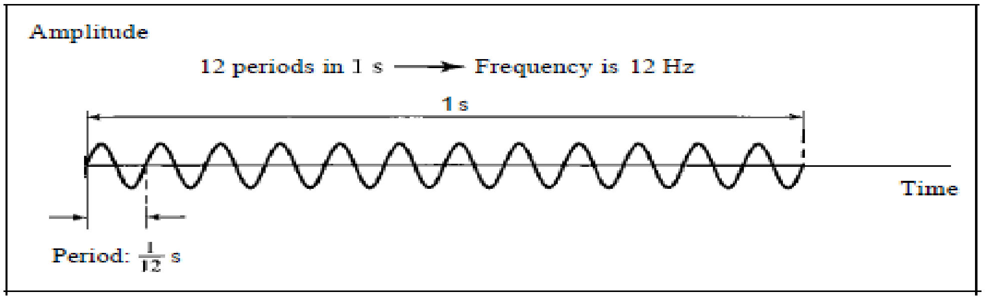
<u>Period and Frequency:</u>

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle. Frequency refers to the number of periods in I s. Note that period and frequency are just one characteristic defined in two ways. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

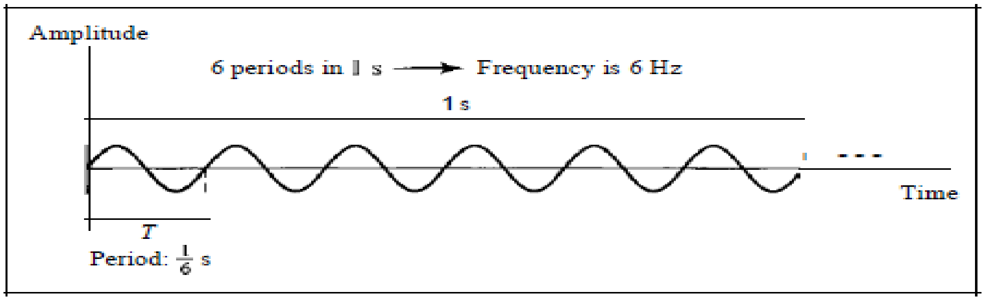
$$f = \left(\frac{1}{T}\right) \text{ And } T = \left(\frac{1}{f}\right)$$

Frequency and period are the inverse of each other.

Two signals with the same amplitude and phase, but different frequencies



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

Units of period and frequency

Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (μs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

Question: The period of a signal is 100 ms. What is its frequency in kilohertz?

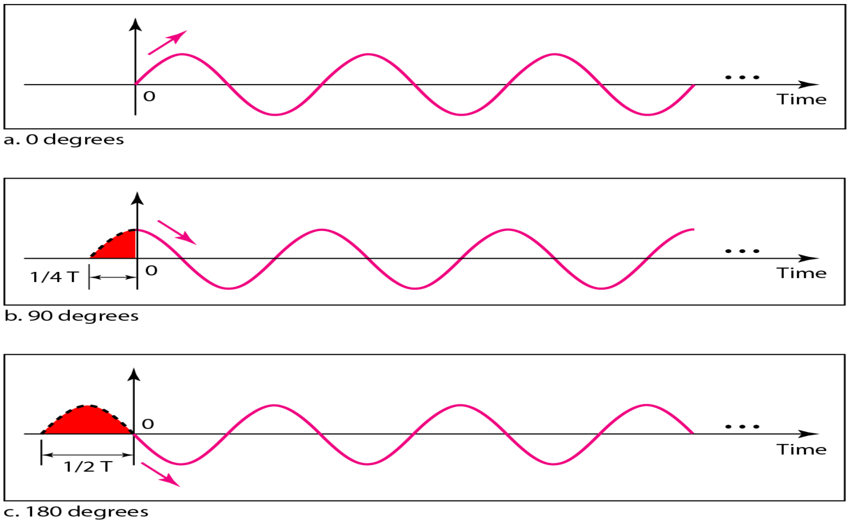
Solution: *First we change 100 ms to seconds, and then we calculate the frequency from the period (1 Hz = 10^{-3} kHz).*

$$100 \text{ ms} = 100 \times 10^{-3} \text{ s} = 10^{-1} \text{ s}$$

$$f = \frac{1}{T} = \frac{1}{10^{-1}} \text{ Hz} = 10 \text{ Hz} = 10 \times 10^{-3} \text{ kHz} = 10^{-2} \text{ kHz}$$

Phase:

The term phase describes the position of the waveform relative to time O. If we think of the wave as something that can be shifted backward or forward along the time axis, phase describes the amount of that shift. Phase is measured in degrees or radians.



a. 0 degrees

b. 90 degrees

c. 180 degrees

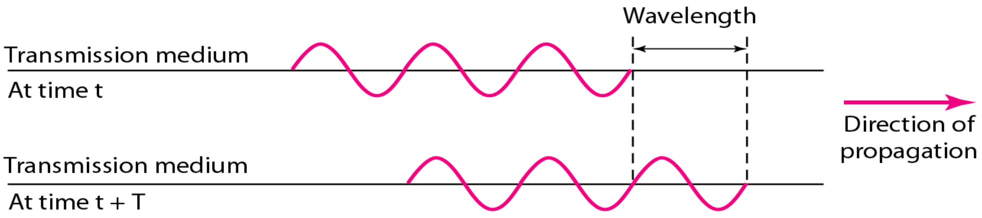
Question: A sine wave is offset 1/6 cycle with respect to time 0. What is its phase in degrees and radians?

Solution: *We know that 1 complete cycle is 360°. Therefore, 1/6 cycle is*

$$\boxed{\frac{1}{6} \times 360 = 60^\circ = 60 \times \frac{2\pi}{360}\ \text{rad} = \frac{\pi}{3}\ \text{rad} = 1.046\ \text{rad}}$$

Wavelength:

Wavelength is another characteristic of a signal traveling through a transmission medium. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium.



Wavelength = propagation speed x period = propagation speed/frequency

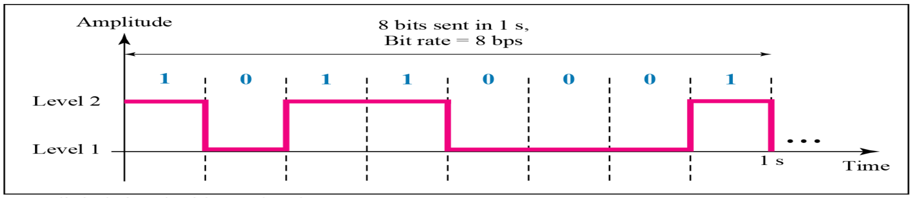
$\lambda = c/f$ c=speed of light = 3×10^8 m/s

Digital Signals:

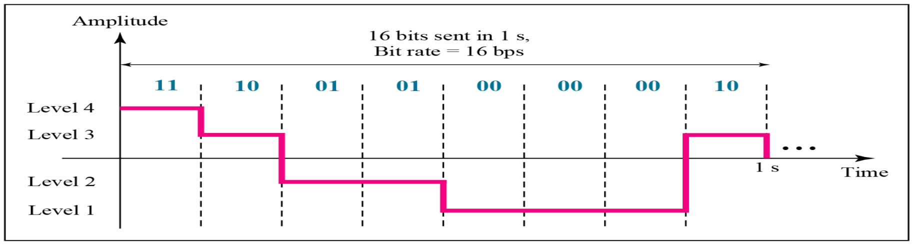
A digital signal can have more than two levels. We can send more than 1 bit for each level.

Bit Rate:

Most digital signals are non periodic, and thus period and frequency are not appropriate characteristics. Another term bit rate (instead frequency) is used to describe digital signals. The bit rate is the number of bits sent in 1s, expressed in bits per second (bps).



a. A digital signal with two levels



b. A digital signal with four levels

***Question:** Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel?*

Solution: A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

$$\boxed{100 \times 24 \times 80 \times 8 = 1{,}636{,}000 \text{ bps} = 1.636 \text{ Mbps}}$$

***Question:** A digitized voice channel, as we will see in Chapter 4, is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?*

Solution: The bit rate can be calculated as

$$\boxed{2 \times 4000 \times 8 = 64{,}000 \text{ bps} = 64 \text{ kbps}}$$

Bit Length:

The distance one cycle occupies on the transmission medium. We can define something similar for a digital signal: the bit length. The bit length is the distance one bit occupies on the transmission medium.

Bit length =propagation speed x bit duration

TRANSMISSION MEDIA

A **transmission medium** (plural *transmission media*) is a material substance (solid, liquid, gas, or plasma) which can propagate energy waves. For example, the transmission medium for sound received by the ears is usually air, but solids and liquids may also act as transmission media for sound.

Transmission media are the physical pathways that connect computers, other devices, and people on a network.

A transmission medium can be classified as a:

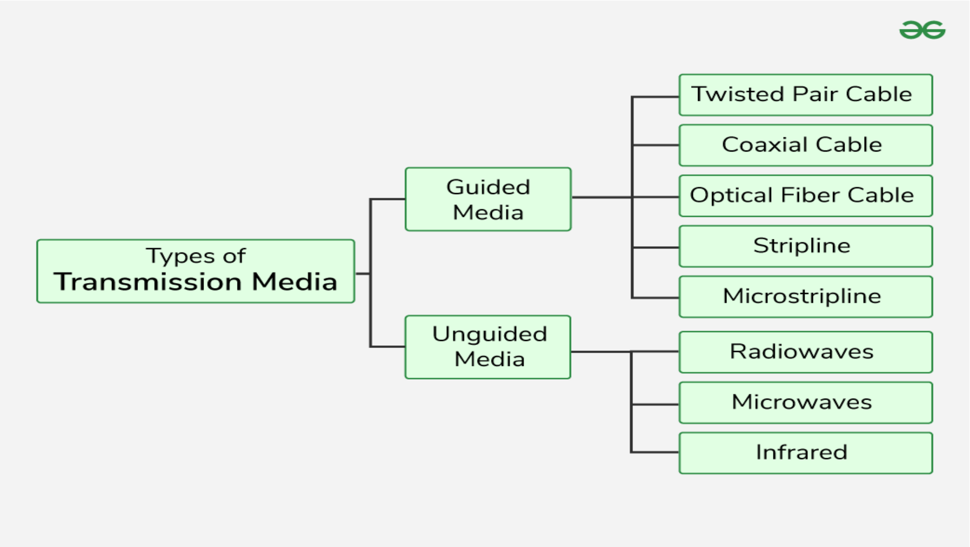
- ***Linear medium***, if different waves at any particular point in the medium can be superposed;
- ***Bounded medium***, if it is finite in extent, otherwise *unbounded medium*;
- ***Uniform medium*** or ***homogeneous medium***, if its physical properties are unchanged at different points;
- ***Isotropic medium***, if its physical properties are the same in different directions.

Types of Transmission media:

The means through which data is transformed from one place to another is called transmission or communication media.

There are two categories of transmission media used in computer communications.

- GUIDED MEDIA
- UNGUIDED MEDIA



1. GUIDED MEDIA:

Bounded media are the physical links through which signals are confined to narrow path. These are also called guide media. Bounded media are made up o a external conductor (Usually Copper) bounded by jacket material. Bounded media are great for LABS because they offer high speed, good security and low cast. However, some time they cannot be used due distance communication.

Three common types of bounded media are used these are :

- Coaxial Cable.
- Twisted pair cable.
- Fiber optics

COAXIAL CABLE:

Coaxial cable is very common & widely used commutation media. For example TV wire is usually coaxial. Coaxial cable gets its name because it contains two conductors that are parallel to each other.

- Coaxial cable has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.
- The coaxial cable transmits information in two modes: *Baseband mode*(dedicated cable bandwidth) and Broadband mode (cable bandwidth is split into separate ranges).

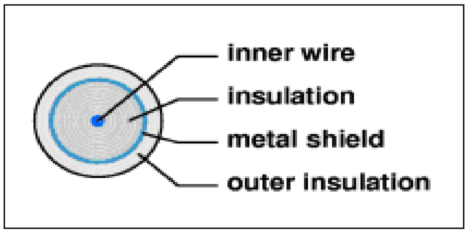
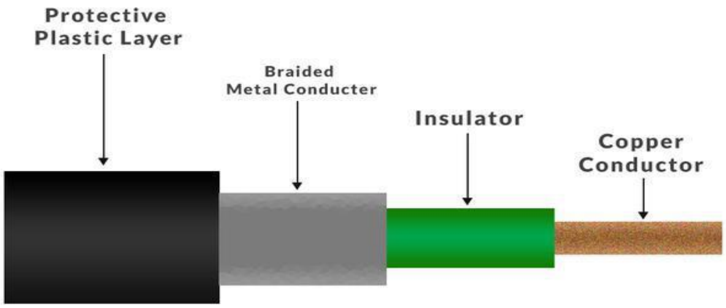


Fig.: Cross-section of a coaxial cable



ADVANTAGES :

- Coaxial cables have high bandwidth
- Inexpensive
- Easy to wire
- Moderate level of Electro Magnetic Inference immunity
- Coaxial cables support multiple channels

DISADVANTAGE :

- Single cable failure can take down an entire network.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.
- There is a chance of breaking the coaxial cable and attaching a "t-joint" by hackers, this compromises the security of the data.

TWISTED PAIR CABLE :

The most popular network cabling is Twisted pair. It is light weight, easy to install, inexpensive and support many different types of network. It also supports the speed of **100 mps.** Twisted pair cabling is made of pairs of solid or stranded copper twisted along each other.

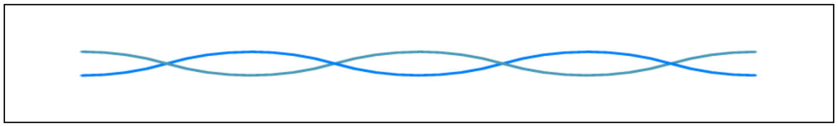


Fig.: Twisted pair wire

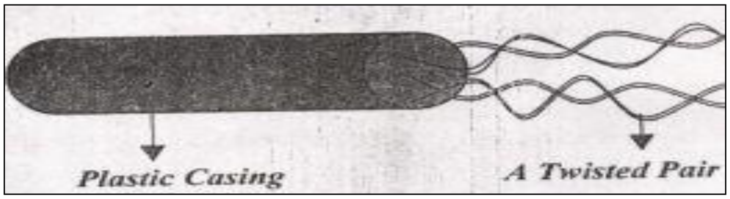
There are two types of twisted pairs cabling

1. Unshielded twisted pair (UTP)

2. Shielded twisted pair (STP)

Unshielded twisted pair (UTP)

UTP is more common. It can be either voice grade or data grade depending on the condition. UTP cable normally has an impedance of 100 ohm. UTP cost less than STP and easily available. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Advantages of Unshielded Twisted Pair

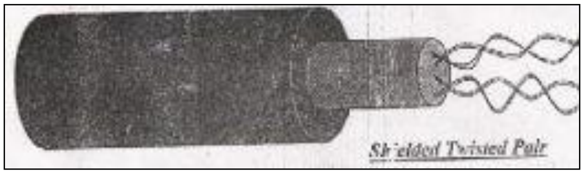
- Least expensive
- Easy to install
- High-speed capacity

Disadvantages of Unshielded Twisted Pair

- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation

Shielded twisted pair (STP)

It is similar to UTP but has a mesh shielding that's protects it from EMI which allows for higher transmission rate. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Advantages of Shielded Twisted Pair

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

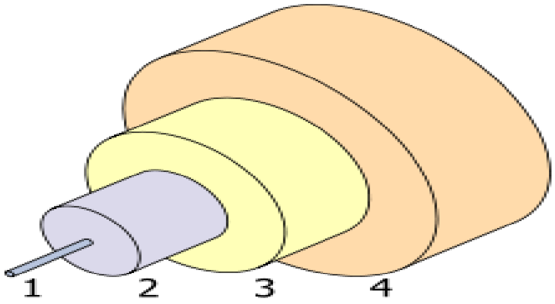
Disadvantages of Shielded Twisted Pair

- Comparatively difficult to install and manufacture
- More expensive
- Bulky

FIBER OPTICS:

Fiber optic cable uses electrical signals to transmit data. It uses light. In fiber optic cable light only moves in one direction for two-way communication to take place a second connection must be made between the two devices. It is actually two stands of cable.

Optical Fiber Cable uses the concept *total internal reflection of light* through a core made up of glass. The core is surrounded by a less dense glass or plastic covering called the coating. It is used for the transmission of large volumes of data.



1. Core: 8 µm diameter.
2. Cladding: 125 µm diameter.
3. Buffer: 250 µm diameter.
4. Jacket: 400 µm diameter.

Structure of fibre optic cable

Advantages of Optical Fibre Cable

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages of Optical Fibre Cable

- Difficult to install and maintain
- High cost

Applications of Optical Fibre Cable

- Medical Purpose: Used in several types of medical instruments.
- Defence Purpose: Used in transmission of data in aerospace.
- For Communication: This is largely used in formation of internet cables.
- Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

Stripline

- Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s.
- Stripline is the earliest form of the planar transmission line.
- It uses a conducting material to transmit high-frequency waves it is also called a waveguide.
- This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

Microstripline

- A **microstripline** is a type of transmission media used to carry high-frequency signals, commonly found in microwave and radio frequency circuits.
- It consists of a flat, narrow conducting strip (usually made of metal) placed on top of a dielectric material (an insulating layer), with a metal ground plane on the other side.

2. UNGUIDED MEDIA

Unguided/Unbounded transmission media are methods that allow the transmission of data without the use of physical means to define the path it takes. Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum and seawater.

Examples of Unguided media are:

- microwave
- radio waves
- infrared waves
- Satellites

Microwave: Microwave transmission is usually point-to-point using directional antennae with a clear path between transmitter and receiver. It is a line-of-sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. **Micro waves** are majorly used for mobile phone communication and television distribution.

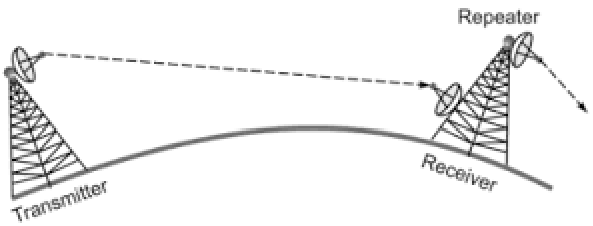
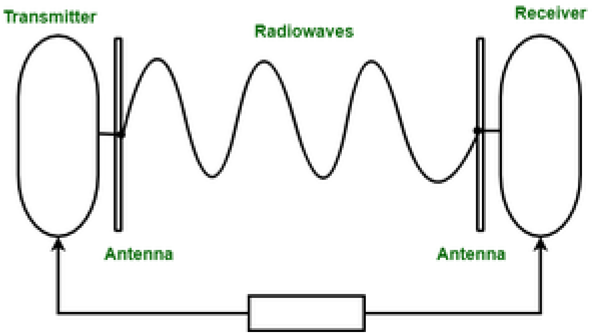


Fig: Microwave Transmission

Radio waves: Radio waves is the transmission of signals by modulation of electromagnetic waves with frequencies below those of visible light. Radio waves are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

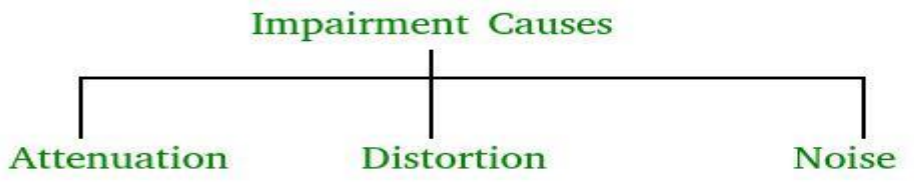


Infrared: Infrared (IR) light is electromagnetic radiation with a wavelength between 0.7 and 300 micrometers, which equates to a frequency range between approximately 1 and 430 THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Satellites: `When used for communications, a satellite acts as a repeater. Its height above the Earth means that signals can be transmitted over distances that are very much greater than the line of sight.

Causes of Transmission Impairment

Transmission impairment refers to the loss or distortion of signals during data transmission, leading to errors or reduced quality in communication. Common causes include signal distortion, attenuation, and noise all of which can affect the clarity and reliability of transmitted data.



Transmission Impairment

- **Attenuation:** It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.

- **Distortion:** It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And that’s why it delays in arriving at the final destination Every component arrives at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at sender’s end.

- **Noise:** The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

Factors Considered for Designing the Transmission Media

- **Bandwidth:** Assuming all other conditions remain constant, the greater a medium's bandwidth, the faster a signal's data transmission rate.

- **Transmission Impairment :** Transmission Impairment occurs when the received signal differs from the transmitted signal. Signal quality will be impacted as a result of transmission impairment.

- **Interference:** Interference is defined as the process of disturbing a signal as it travels over a communication medium with the addition of an undesired signal.

SWITCHING NETWORKS

A network is a collection of inter-connected system. In a network, we have one to one communication. To resolves this, one of the solutions is to make point to point connection between each pair of system (using mesh topology) or connecting centralized system to every other system (using star topology). But still, this is not a cost effective as the number of systems grows. Also, it is limited to small distance between inter connected system.

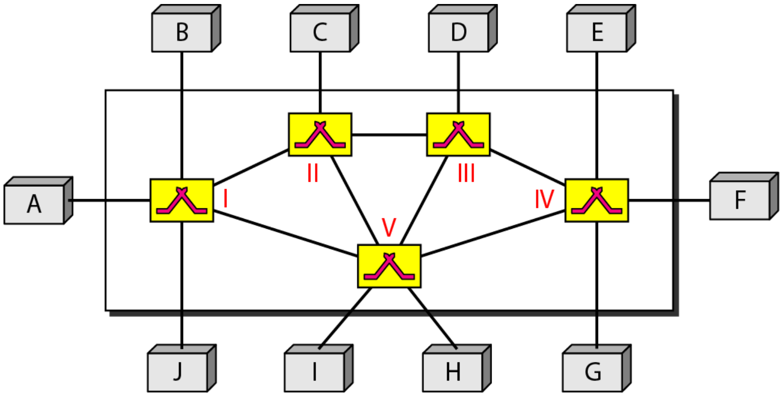


Figure 3 Switched Network

A solution to the above problem is switching. A switched network consists of a series of interlinked device called switches. It is a device which can create a temporary connection between two or more system linked to the switch. In switched network some of the nodes are system and other are used for routing.

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.

There are three methods of switching:

1. Circuit Switched Networks
2. Packet Switched Networks
   A. Datagram Networks
   B. Virtual- circuit Networks
3. Message Switched Networks

1. <u>Circuit Switched Network:</u>

- In circuit-switched networks, a dedicated path is needed for communication between the end systems, are reserved for the duration of the session.
- Each connection uses only one dedicated channel on each link.
- Each link is divided into n channels by using FDM (frequency division Multiplexing) or TDM (Time Division multiplexing).

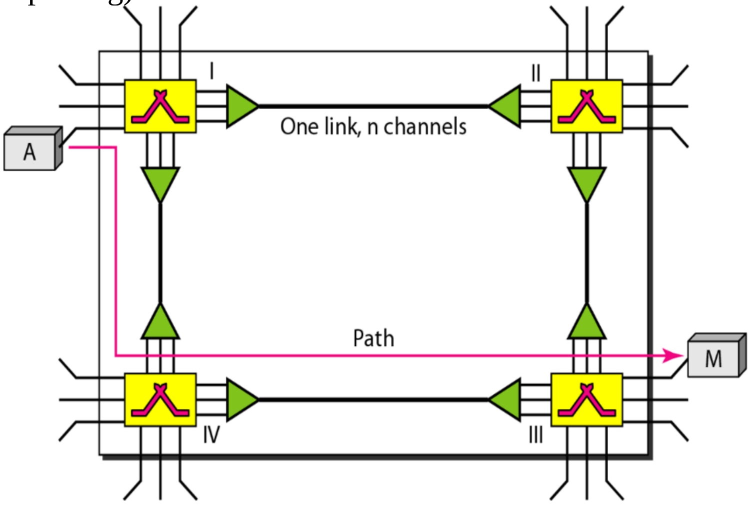


Figure 4 A trivial circuit-switched network

In the above figure one link is divided into n channel (here n=3). A circuit switched network requires following three phase during the session.

1. **Setup Phase:** First of all two system needs to create dedicated circuit or path for communication. For example, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch II that can be dedicated for this purpose. Switch I then sends the request to switch II, which finds a dedicated channel between itself and switch III. Switch III informs system M of about system A.

   To establish a path system M must send an acknowledgement for the request of A. Only after system A receives this acknowledgement the connection is established. Only end to end addressing is required for establishing connection between two end systems.

2. **Data Transfer Phase**
   After the establishment of the dedicated path (channels), the two systems can transfer data.
3. **Teardown Phase**
   When one of the systems needs to disconnect, a signal is sent to each switch to release the resources.

Not efficient coz the link is reserved and can’t be used by other system during the connection.
Minimum delay in data transfer.

Example: Let us consider how long it takes to send a file of 640 Kbits from host A to host B over a circuit-switched network. Suppose that all links in the network use TDM with 24 slots and have bit rate 1.536 Mbps. Also suppose that it takes 500 msec to establish an end-to-end circuit before A can begin to transmit the file. How long does it take to send the file?

Each circuit has a transmission rate of (1.536 Mbps)/24 = 64 Kbps, so it takes (640 Kbits)/(64 Kbps) = 10 seconds to transmit the file. To this 10 second, we add the circuit establishment time, giving 10.5 seconds to send the file. Note that the transmission time is independent of the number links: the transmission time would be 10 seconds if the end-to-end circuit passes through one link or one-hundred links.

2. Packet Switched Networks

2. A. Datagram Networks

- In packet switched network message is divided into number of packets. Each packet is of fixed size defined by network or protocol.
- **Datagram switched network is also known as Connectionless packet switching**
- There is no dedicated link between source and destination.
- No dedicated Resources are allocated for packet. Resources are allocated on demand and it follows first come first basis. When a switch receives a packet, irrespective of the source or destination, the packet must wait if the other packets being processed.
- A single message is divided into number of packets. During the transfer of packets from source to destination, each packet is treated independently. Destination can receive unordered packets and later packet can be ordered and combine the packets to extract the message.
- Packets are referred as datagrams in this type of switching. Datagram switching is normally done at the network layer.
- The datagram networks are referred to as connectionless networks. Connectionless means switches have no connection state information.
- There is no setup and teardown phase. So a routing table is required in every switch to route packet from source to destination. A Routing table is based on the destination address. The routing table updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over. Figure below shows the routing table for a switch.

Destination address	Output Port
1234	1
4444	2
6666	3
…..	.

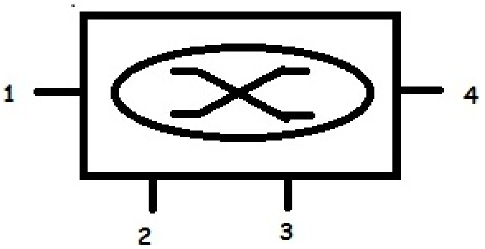
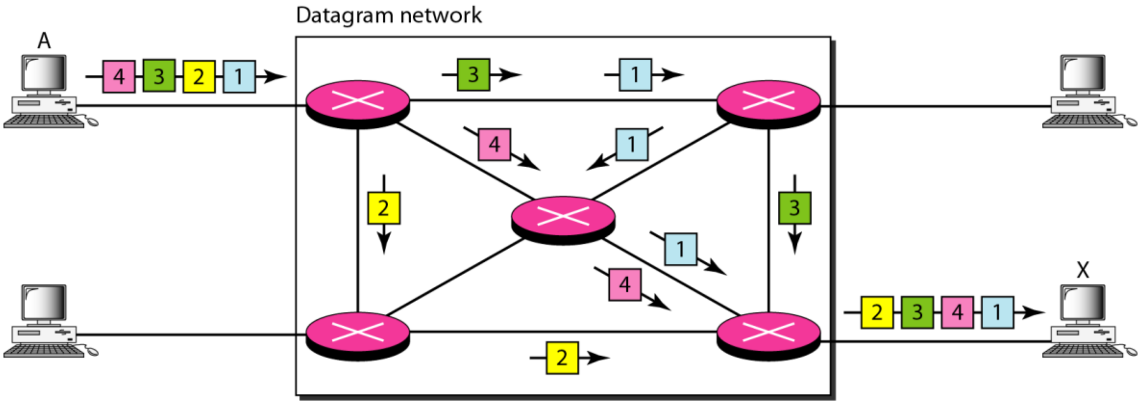


Figure 5 Routing table for a switch



Destination Address

Every packet in a datagram network carries a header that contains information of the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

NOTE: The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

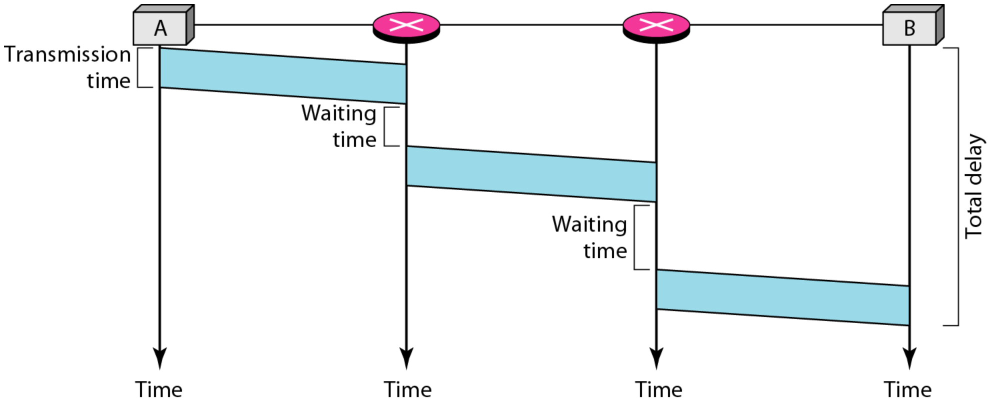
Efficiency

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. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

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. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

Switching in the Internet is done by using the datagram approach to packet switching at the network layer.



The packet travels through two switches. There are three transmission times (3T), three propagation delays (slope of the lines: 3ꞇ), and two waiting times ($w_1 + w_2$). Ignoring the processing time in each switch, total delay = 3T + 3 ꞇ + $w_1 + w_2$

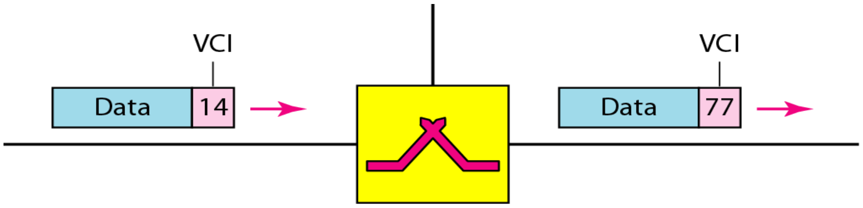
2.B. <u>Virtual –Circuit Networks:</u>

A virtual-circuit network uses the characteristics of both the circuit switched network and the datagram network. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. Virtual-circuit network is also known as <u>Connection-oriented packet switching.</u>

Addressing

Two types of addressing are used in virtual-circuit network

- <u>Global Addressing:</u> It is an address which can uniquely identify the systems (source or destination) in a network or internet. This address is used to create virtual circuit identifier only.
- <u>Virtual Circuit Identifier:</u> The identifier that is actually used for data transfer is known as virtual circuit identifier (VCI). It is a small number which is used by a frame between two switches. This VCI changes from one switch to another. Every switch uses a fixed range of values for VCI.
-

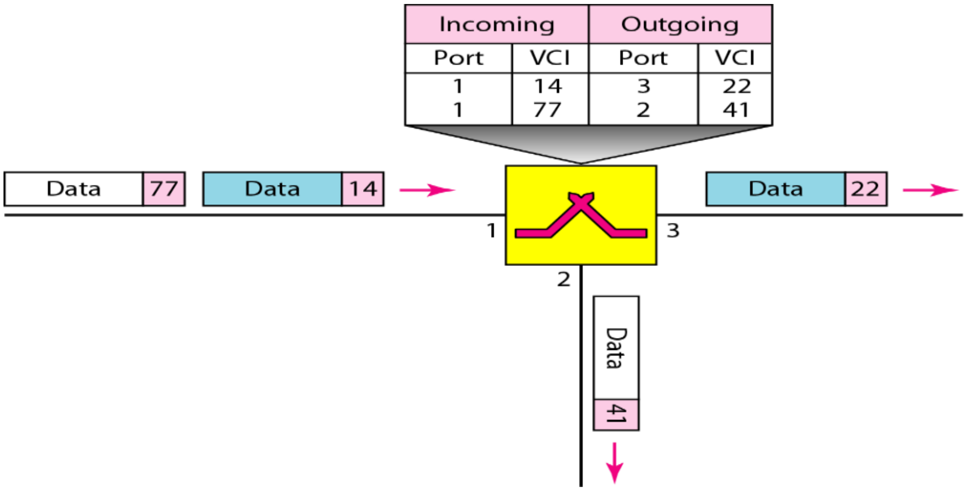


Three phases of Virtual –Circuit Networks:

1. **Data Transfer Phase**

   To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already setup. Figure 13 shows such a switch and its corresponding table. Figure below shows a frame arriving at port 1with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41

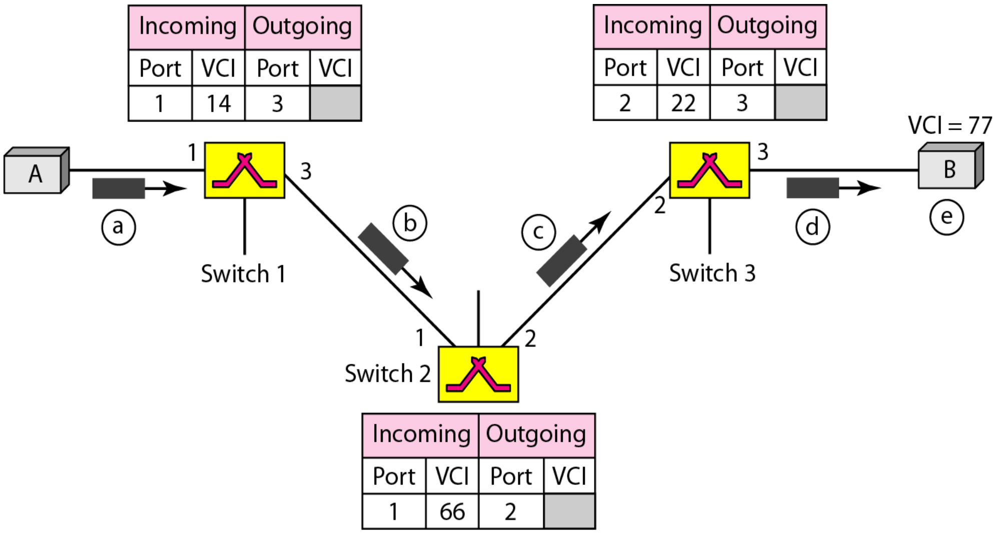
Switch and tables in a virtual-circuit network

2. **Setup Phase**

In the setup phase, a switch creates an entry for a virtual circuit. For example, suppose source A needs to create a virtual circuit to B.

Two steps are required:

a. Setup request
b. Acknowledgment.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	

Setup request in a virtual-circuit network

2.1. Setup Request: A setup request frame is sent from the source to the destination. Figure above shows the process.

a. Source A sends a setup frame to switch 1.

b. Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3.The switch, in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table. For the moment, assume that it knows the output port. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port3 to switch 2.

c. Switch 2 receives the setup request frames. The same events happen here as at switch1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).

d. Switch 3 receives the setup request frame. Again, three columns are completed: Incoming port (2), incoming VCI (22), and outgoing port (3).

e. Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not from other sources.

2.2. Acknowledgment: A special frame, called the acknowledgment frame, completes the entries in the switching tables. Figure below shows the process.

a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from

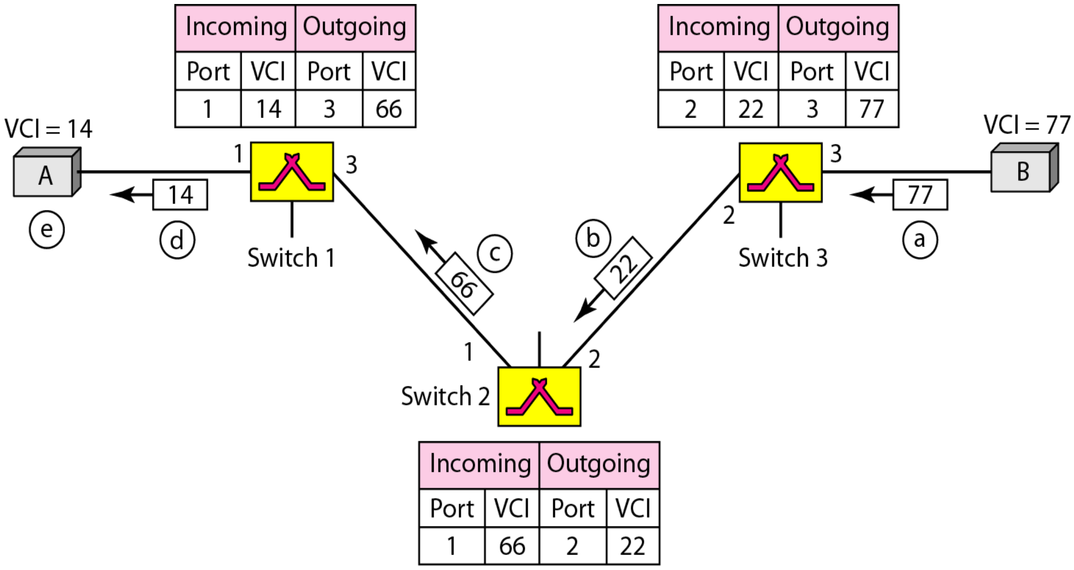
A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.

b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.

c. Switch 2 sends an acknowledgment to switch 1that contains its incoming VCI in the table, chosen in the previous step. Switch 1uses this as the outgoing VCI in the table.

d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.

e. The source uses this as the outgoing VCI for the data frames to be sent to destination B.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

Setup acknowledgment in a virtual-circuit network

3. Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request*. Destination B responds with a teardown *confirmation frame*. All switches delete the corresponding entry from their tables.

Note: ***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.***

Efficiency of Virtual-Circuit Networks:

Virtual-Circuit Networks uses the resources efficiently and it reduces the waiting time of data frame.

Delay in Virtual-Circuit Networks:

In a virtual-circuit network, there is a delay for setup and for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. Figure 16 shows the delay for a packet traveling through two switches in a virtual-circuit network.

The packet is traveling through two switches (routers). There are three transmission times (3T), three propagation times (3 ȶ), data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a teardown delay (which includes transmission and propagation in one direction).
We ignore the processing time in each switch. The total delay time is

Total delay=3T+3 ȶ +setup delay + tear down delay

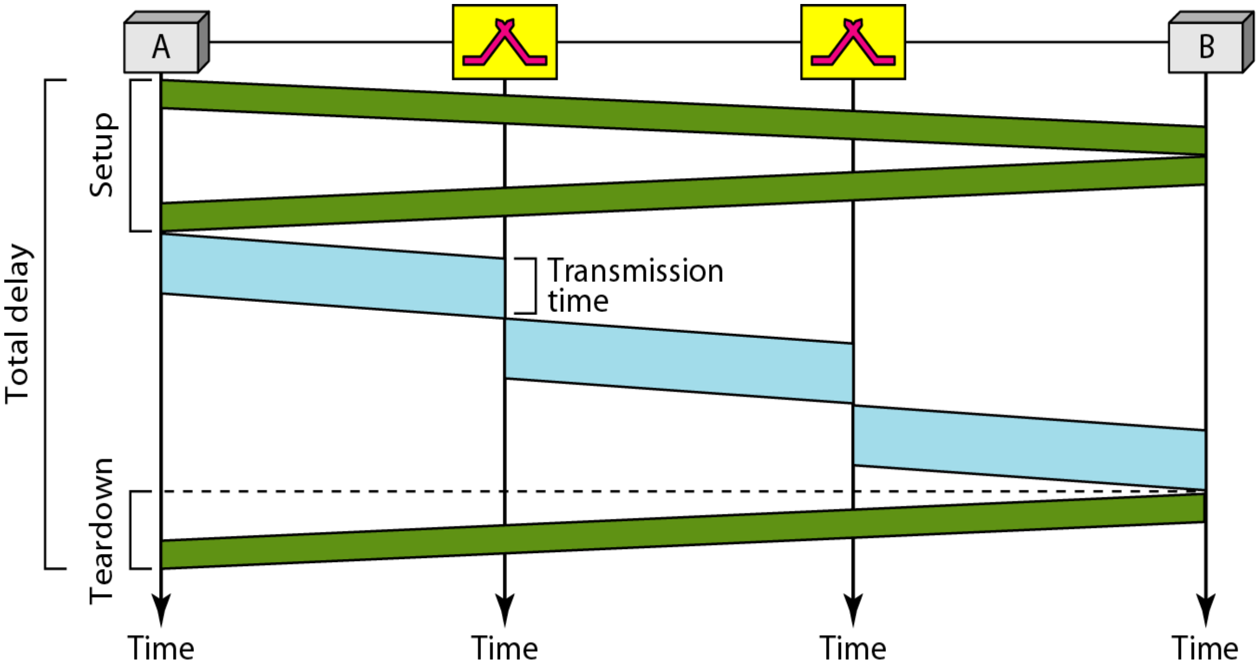


Figure 6 Delay in a virtual-circuit network