Syllabus:

Introduction to Networks, Data and signals-analog and digital, periodic analog signals, digital signals, bit rate, baud rate, bandwidth. Transmission impairments- attenuation, distortion and noise. Data communication protocols and standards, Network models - OSI model-layers and their functions. TCP/IP protocol suite.

1.NEED OF NETWORK:

A set of devices often mentioned as nodes connected by media link is called a **Network**.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

A network must be able to meet certain criteria, these are mentioned below:

1) Performance: It can be measured in the following ways:

- **Transit time:** It is the time taken to travel a message from one device to another.
- **Response time:** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are:

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

2) Reliability: It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

3) Security

It refers to the protection of data from any unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Bandwidth (in digital systems) between two given nodes is the maximal amount of data per unit time that can be transmitted from one node to the other. **Throughput** defines how much useful data can be transmitted per unit time.

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.
2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:** Authorized users are allowed to share the files on the network.

Computer networks help users on the network to share the resources and in communication. We cannot imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet.

File sharing: Networking of computers helps the network users to share data files.

Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.

Application sharing: Applications can be shared over the network, and this allows to implement client/server applications.

User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.

Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

Voice over IP (VoIP): Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

Basic Communication Model

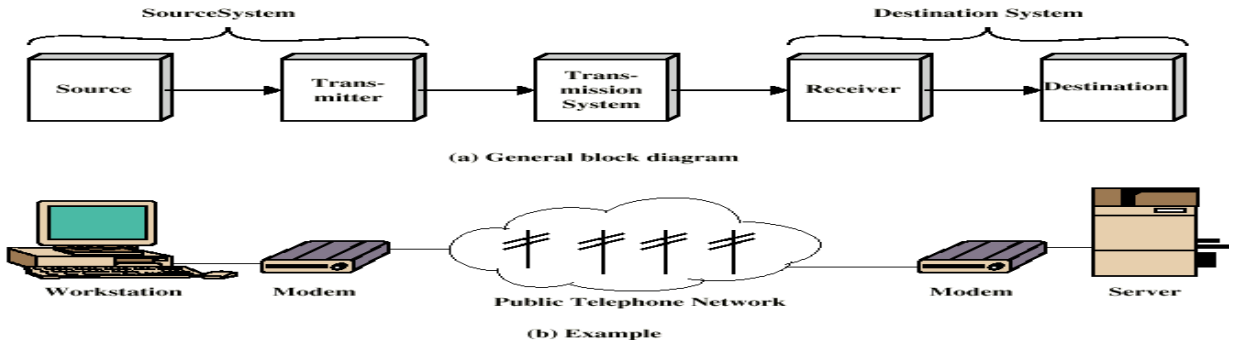


Figure 1.1 Simplified Communications Model

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter

The data generated by the source system is not directly transmitted in the form it's generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Destination

Destination receives the incoming data from the receiver.

Protocol

Defines what is communicated when and how is communicated.

Data Communication

The exchange of data between two devices through a transmission medium is called **Data Communication**. The data is exchanged in the form of **0's** and **1's**. The transmission medium used is wire cable. For data communication to occur, the communication device must be a part of a communication system. Data Communication has two types - **Local** and **Remote** which are discussed below:

Data Communication: Local

Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

Data Communication: Remote

Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features :

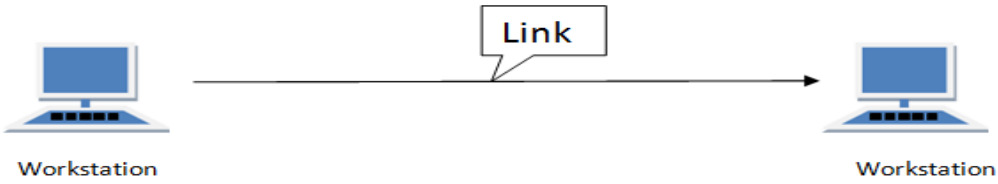
1. **Delivery**: Delivery should be done to the correct destination.
2. **Timeliness**: Delivery should be on time.
3. **Accuracy**: Data delivered should be accurate.

There are two possible ways of connection.

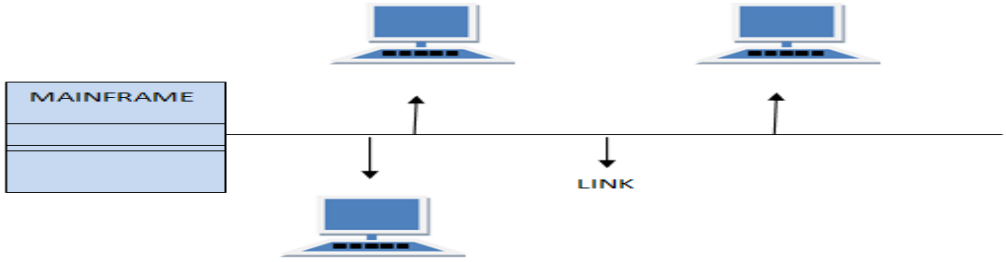
a)Point-to-Point

b)Multipoint

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. Ex;when you change the television channels by infrared remote control, you are establishing a point-to-point connection between television and the remote control.



Multipoint connection is also called as multidrop connection in which more than two specific devices share a same link. In this environment the capacity of the channel is shared spatially or temporally. If several devices use the same link simultaneously. It is a Spatially shared connection. If the user must take turns it is a timeshared connection Physical topology refers to the way in which a network is laid out physically.



Topology

Topology of a network is the geometric representation of the relationship of all the links and linking devices (nodes) to another.

There are 4 basic topologies:-

1)Mesh Topology

2)Star Topology

3)Bus Topology

4)Ring Topology

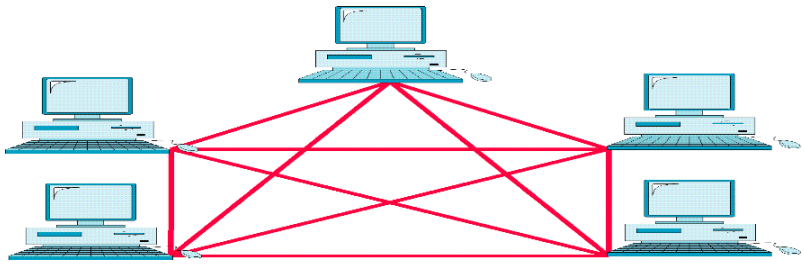
1)Mesh Topology ,

every device has a dedicated point to point link to every other device. Link carries traffic between the two devices it connects.

Ex: telephone regional office, connect to other regional offices

Advantages

-The use of dedicate link guarantees the connection can carry its own data, thus can avoid traffic problem.



-it is Robust, one link is unusable, it does not affect the system.

-privacy and security, physical boundaries prevent unauthorized access.

Disadvantage :

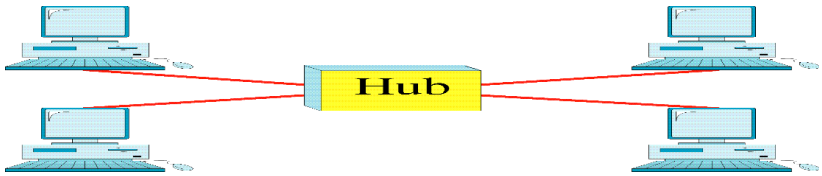
-Amount of cabling required is for installation is difficult

-every device is connected to each other, so installation is difficult

-bulk of wiring is required.

-hardware required to connect is expensive

2)Star Topology



Advantages:

-Dedicated point to point link

-only a central controller is their called, Hub

-device is not directly linked to another.

-each device send and receive data through the central controller.

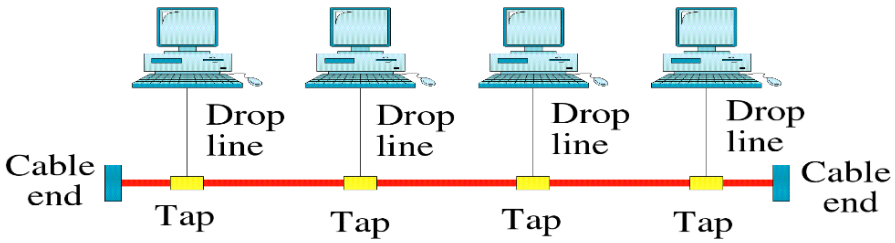
-less expensive, each device have an I/O port, and thus it is easy to configure.

-robustness is an advantage, if one link is dead, it won't affect the system.

Disadvantage :

-if hub goes down, system is dead.

3)Bus Topology



-nodes are connected to bus cable by drop line and taps. Bus topology was the 1st topology used in LAN. -Tap is connector to split the main cable to create contact with metallic core.

Disadvantage:

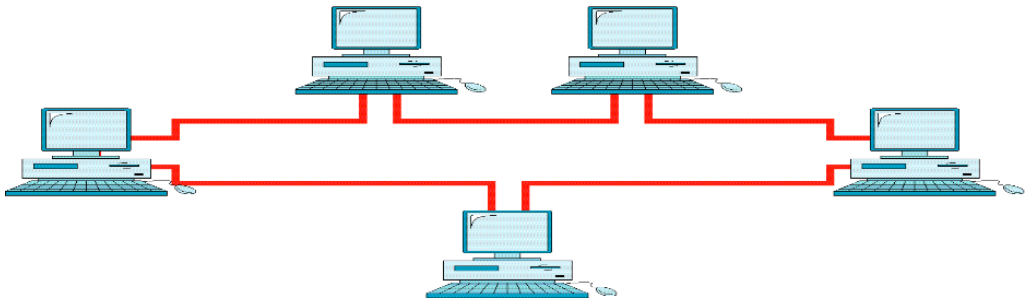
-Signal travel ,through the backbone, some energy is transformed to heat, thus it become weak., so bus support limited number of taps.

- Difficult reconnection, fault isolation, signals reflection cause degradation in quality.

-degradation can be controlled by the limiting the devices and spacing between devices.

-

4)Ring Topology



Advantages:

-easy to install and re-configure.

-each device, linked to intermediate neighbors.

-signal is circuiting all times, if one device does not received the signal in specific period it will issue an alarm, thus make the network operator alert.

Disadvantages:

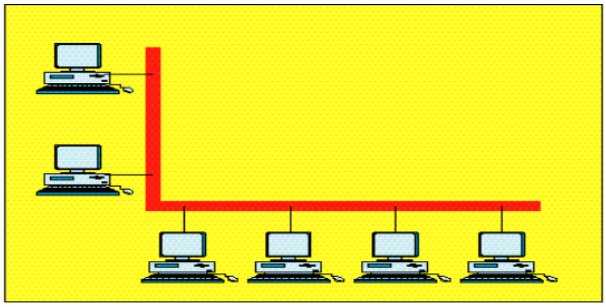
-not Robust - break in ring will disable the entire network.

-this can be solved by dual-ring or switch capable of closing break.

NETWORK CLASSIFICATION

Computer networks are created by different entities. Networks are classified by its size. MaInly into LAN, MAN, WAN

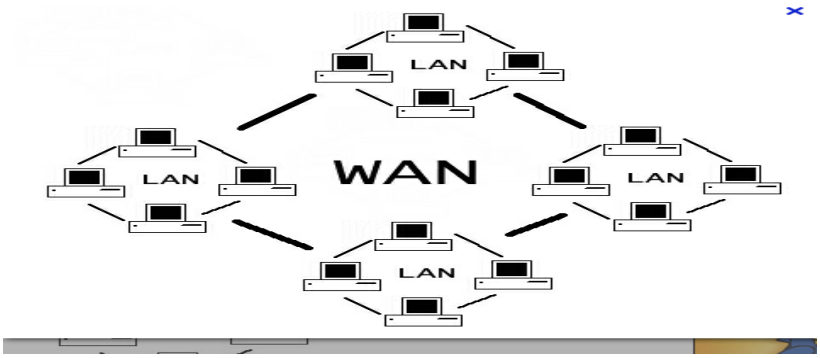
LOCAL AREA NETWORK



Single building LAN

A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. A LAN is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of the 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 PC or workstations. The resources to be shared can include hardware , software or data. A common egs of a LAN, found in many business environments , links a workgroup of task related computers, for eg. engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group.

Wide Area Network



A Wide Area Network (WAN) covers a significantly larger geographic area than LANs or MANs. WAN can range from 100krn to 1000krn and the speed between cities can vary from l.5 Mbps to 2.4 Gbps. typically, a WAN consists of two or more local-area networks (LANs) or MANs. They can connect networks across cities, states or even countries. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

A WAN provides long distance transmission of data, image, audio, and video information over large geographic areas that may compromise a country, a continent or the entire 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

Switched WAN

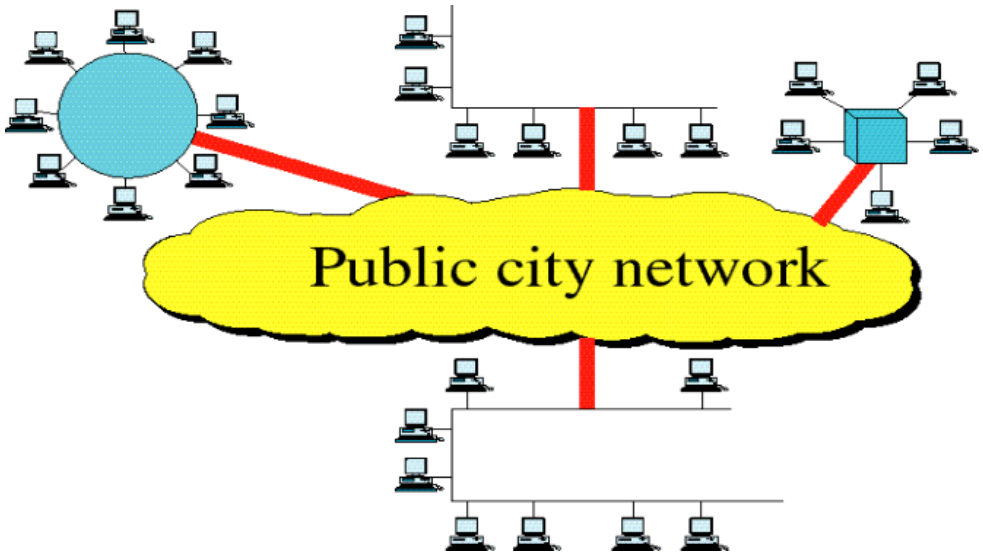
It connect the end systems, which usually comprise a router that connects to another LAN or WAN

Point-point WAN

It is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an ISP(Internet service provider). This type of WAN is often used to provide internet access.

MAN

A MAN is a network with a size between a LAN and a Wan. It normally covers the area inside a town or city. It is designed for customers who need high speed connectivity, normally to the internet, and have endpoints spread over a city or part of city. A good egs of a MAN is the part of the telephone company network that can provide a high speed DSL line to the customer.



WIRELESS NETWORKS

Wireless network refer to any type of computer network that is not connected by cables of any kind. It is a method by which telecommunications networks and enterprise (business), installations avoid the costly process of introducing cables into to a building, or as a connection between various equipment locations.[1] Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves.

Types of wireless connections

Wireless PAN: Wireless Personal Area Networks (WPANs) interconnect devices within a relatively small area, generally within a person's reach. For example, both Bluetooth radio and invisible Infrared light provides a WPAN for interconnecting a headset to a laptop.

Wireless LAN: A wireless local area network (WLAN) links two or more devices using a wireless distribution method, providing a connection through an access point to the wider internet.

- Wi-Fi: "Wi-Fi" is a term used to describe 802.11 WLANs, although it is technically a declared standard of interoperability between 802.11 devices.
- Fixed Wireless Data: This implements point to point links between computers or networks at two distant locations, often using dedicated microwave or modulated laser light beams over line of sight paths. It is often used in cities to connect networks in two or more buildings without installing a wired link.

Wireless MAN:-Wireless Metropolitan Area Networks are a type of wireless network that connects several Wireless LANs. WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard.

Wireless WAN:-Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2.4 GHz band, rather than omnidirectional antennas used with smaller networks.

Mobile devices networks:-With the development of smart phones, cellular telephone networks routinely carry data in addition to telephone conversations:-Global System for Mobile Communications (GSM): The GSM network is divided into three major systems: the switching system, the base station system, and the operation and support system. The cell phone connects to the base system station which then connects to the operation and support station; it then connects to the switching station where the call is transferred to where it needs to go. GSM is the most common standard and is used for a majority of cell phones.

INTERNET

A network is a group of connected devices such as computers and printers. Private individuals as well as various organizations such as gov, agencies schools, research facilities, corporations, and libraries in more than 100 countries use the internet. Millions of people are users. The extraordinary c/m system only comes into being in 1969.

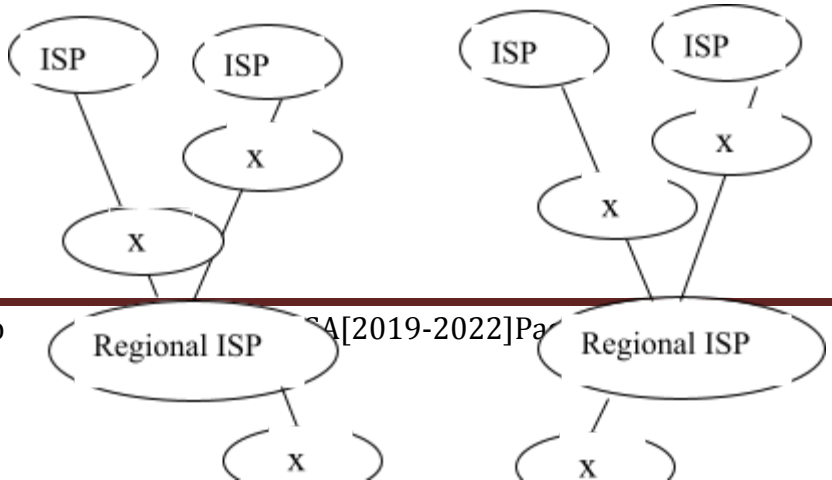
Internet Today

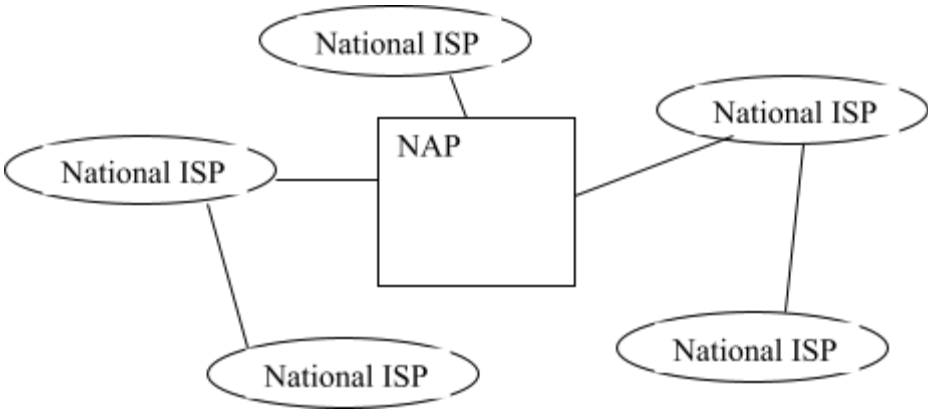
Internet today is not a simple hierarchical structure. It is made up of many LAN, WAN joined by connecting devices and switching stations. And the architecture is continually changing. Today most end users who want internet services of internet connection use the service of “internet service provider (ISP)”

There are international internet service provider, national internet service provider, regional internet service provider and local internet service provider. The internet toady is running by private companies.

International internet service provider : The International internet service provider Connect Nations together.

National internet service provider : National internet service providers are the backbone networks created and maintained by specialized companies. There are many national ISP’s operating in north America. **a)Structure of National ISP**





b)Interconnection of national ISP's

Regional internet service provider: Smaller ISP's, connected to one or more national ISP's.

Local internet service provider: Provide direct service to the end users. The local service providers can directly connect to the regional ISP's or National ISP's. Most end users are connected to the local ISP's.

DATA and SIGNALS

DATA

We define data as entities that convey meaning or information. Data can be analog or digital.

ANALOG AND DIGITAL

The term analog data refers to the information that is continuous; digital data refers to information that has discrete values.

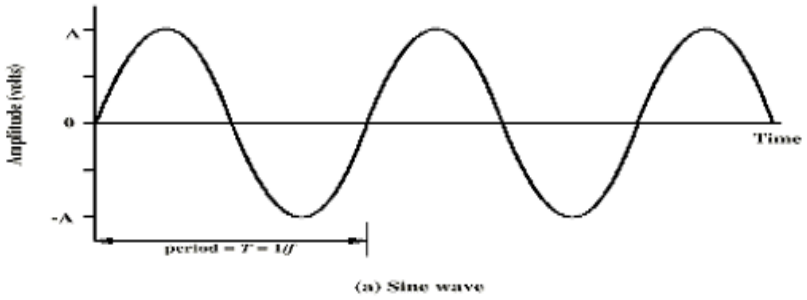
Analog data take noncontiguous values in some interval Example: Voice and video are continuously varying patterns of intensity. The most familiar example of analog data is audio, which is in the form of acoustic sound waves, can be perceived by human beings; video.

The most familiar example of digital data is data stored on computers (0,1).

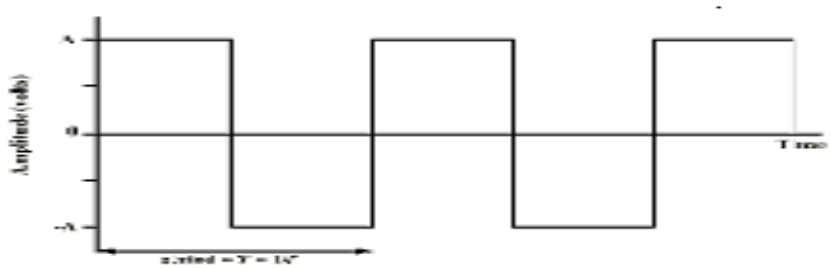
SIGNALS

Signals are electric or electromagnetic representations of data. Signaling are the physical propagation of the signal along a suitable medium. Transmission is the communication of data by the propagation and processing of signals

Analog signals can have an infinite number of values in a range; **digital signals** can have only a limited number of values



(a) Sine wave



Periodic and Non periodic signals

Both analog and digital signal can take one of two forms, 'periodic' and 'nonperiodic' or 'aperiodic'

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 full pattern is called a **cycle.**

A **non periodic signal** changes without exhibiting a pattern or cycle that repeats over a time.**In data communications, we commonly use periodic analog signals and non periodic digital signals**

Periodic analog signals

Periodic analog signals can be classified as simple or composite. a simple periodic signal 'a sine wave' cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

Sine waves

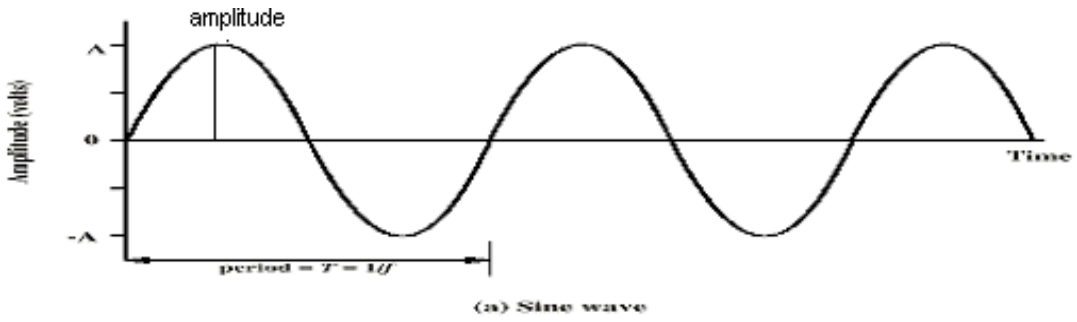
- fundamental form of a periodic analog signal

- visualize it as a simple oscillating curve
- sine wave can be represented by 3 parameters.

1.peak amplitude

2.frequency

3.phase



(a) Sine wave

Peak amplitude: The absolute value of its highest intensity, proportional to the energy it carries. For electric signals it is measured in volts.

Periods : Amount of time in seconds a signal need to complete one cycle. Period refers in seconds. T=1/f

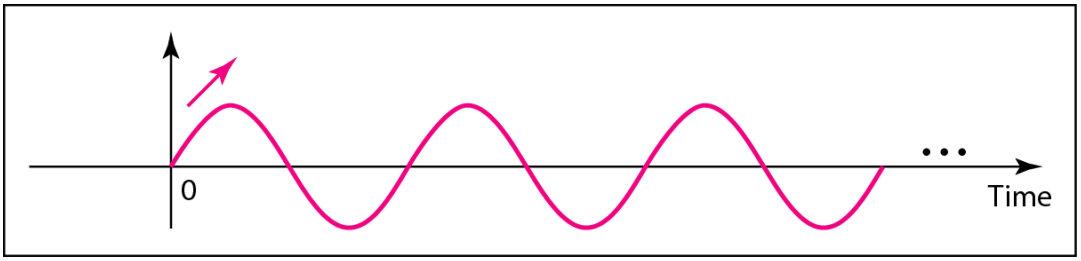
Frequency : Number of periods in 1s.frequency refers in Hertz (Hz) f=1/T

Phase: phase describes the position of the waveform relative to time 0

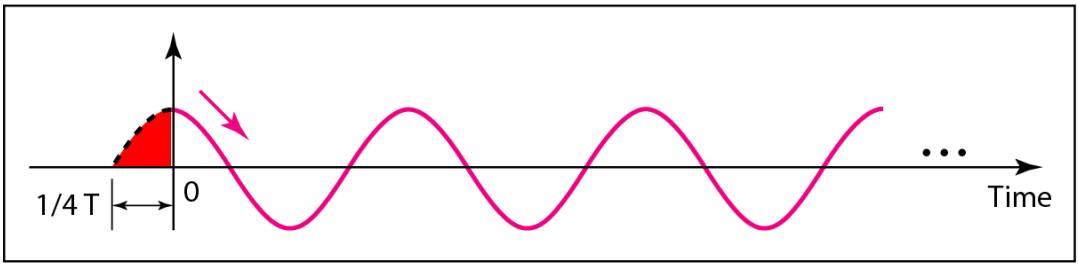
If a signal does not change at all, its frequency is zero.

*If a signal changes instantaneously, its frequency is infinite***.**

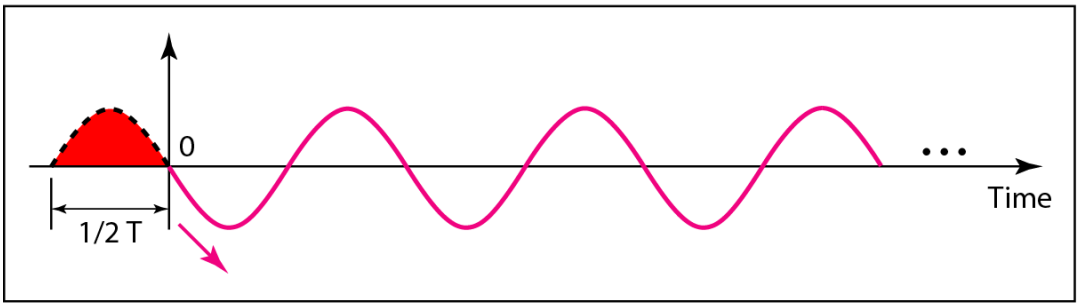
Three sine waves with the same amplitude and frequency, but different phases



a. 0 degrees



b. 90 degrees



c. 180 degrees

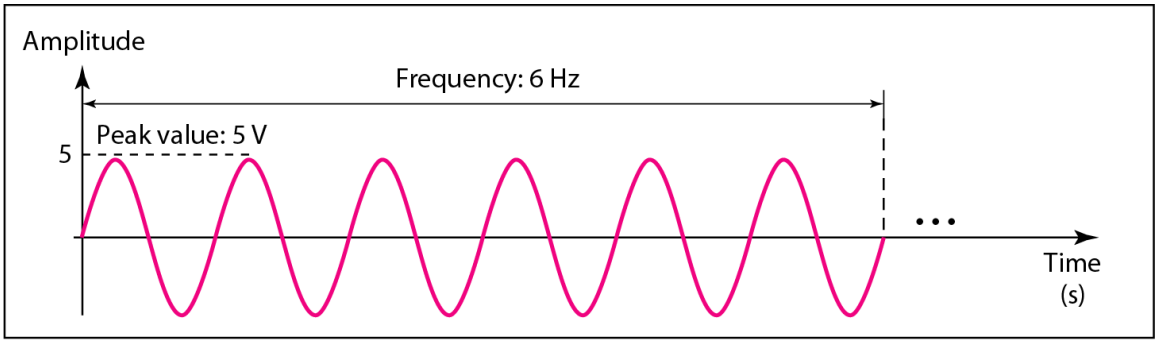
Wavelength(λ)

Wavelength binds the period or frequency of a simple sine wave to the propagation speed of medium.

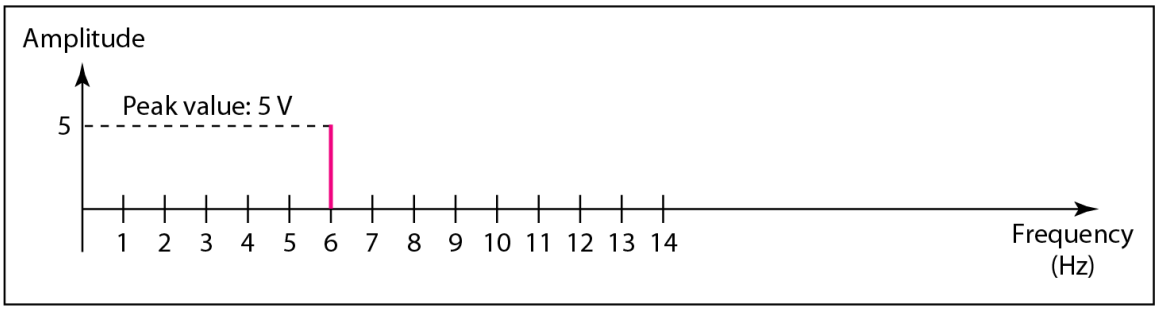
Frequency of signal is independent of the medium. The wavelength depends on both the frequency and medium. Wavelength is the property of any type of signal. The wavelength is the distance that a single sine wave can travel in 1 period.

$$\text{Wavelength} = \text{propagation speed} * \text{period} = \frac{\text{propagation speed}}{\text{frequency}}$$

The time-domain and frequency-domain plots of a sine wave



a. A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)



b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

A complete sine wave in the time domain can be represented by one single spike in the frequency domain.

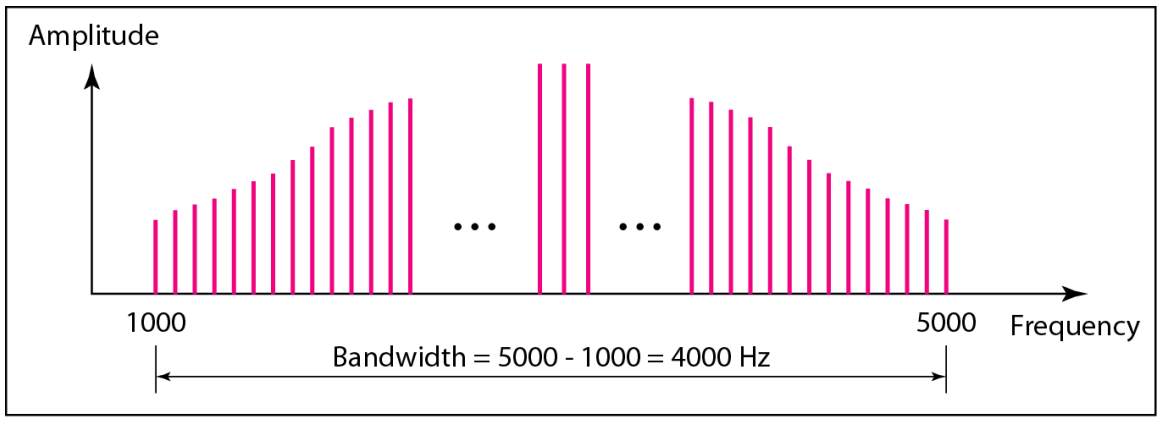
A single-frequency sine wave is not useful in data communications; we need to send a composite signal, a signal made of many simple sine waves.

According to Fourier analysis, any **composite signal** is a combination of simple sine waves with different frequencies, amplitudes, and phases.

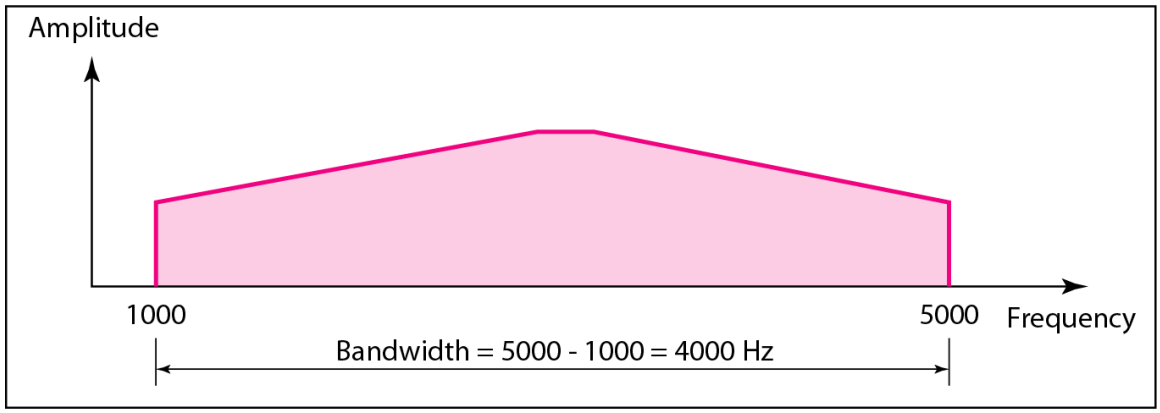
If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is non periodic, the decomposition gives a combination of sine waves with continuous frequencies.

BANDWIDTH

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.



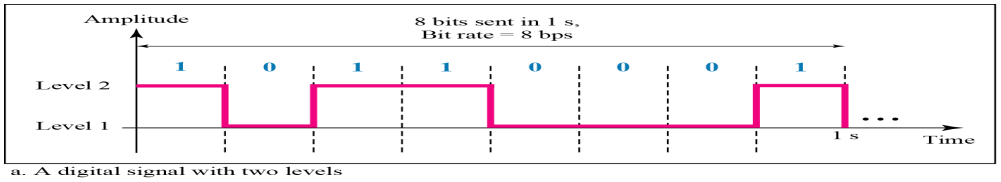
a. Bandwidth of a periodic signal



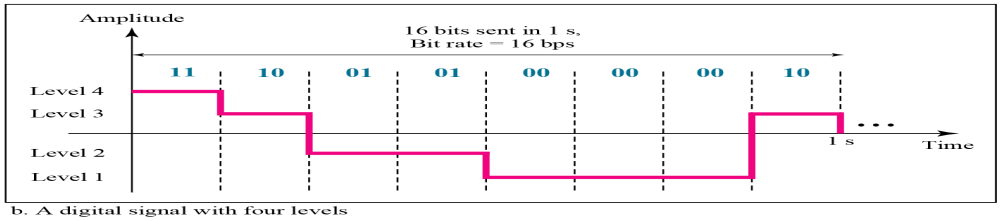
b. Bandwidth of a nonperiodic signal

DIGITAL SIGNAL

A digital signal is a sequence of voltage pulses that may be transmitted over a wire medium; for example, a constant positive voltage level may represent binary 0and a constant negative voltage may represent binary 1. A digital signal can have more than two levels. In this case, we can send more than 1 bit for each level.



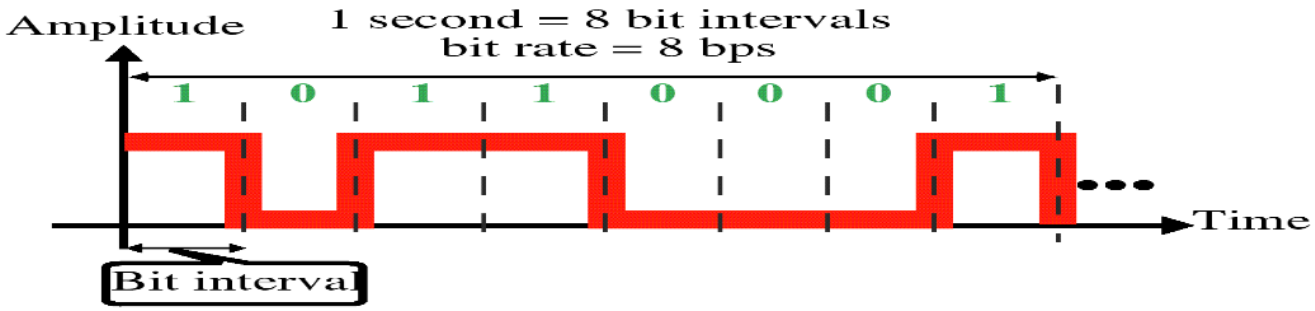
a. A digital signal with two levels



b. A digital signal with four levels

Bit rate

Most digital signals are non periodic, and thus period and frequency are not appropriate characteristics. Bit rate is used to represent digital signals. The bit rate is the number of bit sent in 1s, expressed in bits per second (bps). A bit rate of 2,400 bits per second (bps) for example, would mean 2,400 zeros and ones are transmitted each second.



Bit length

We know the wavelength for an analog signal: the distance one cycle occupies on the transmission medium. The bit length is the distance one bit occupies on the transmission medium.

Bit length=propagation speed *bit duration

1. **Baud rate**

Baud rate represents the number of times per second a signal (changing from zero to one or one to zero) or symbol (the connection's voltage, frequency or phase) in a communications channel changes state or varies. For example, a 2,400 baud rate means the channel is changing states up to 2,400 times per second. The baud rate is therefore equal to the bit rate only if each signal element represents one bit of information.

2. Bandwidth

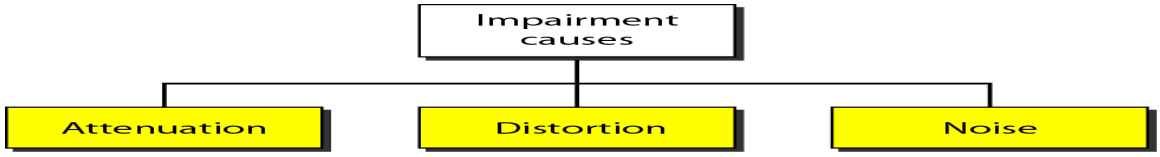
Bandwidth *is defined as* a range within a band of frequencies or wavelengths. *Bandwidth is also* the amount of *data* that can be transmitted in a fixed amount of time.
For digital devices, the bandwidth is usually expressed in bits per second(bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz*).*

DIGITAL SIGNALS

A digital signal is a composite analog signal with an infinite bandwidth. We can transmit a digital signal by two methods: BASEBAND OR BROADBAND TRANSMISSION.

5. TRANSMISSION IMPAIRMENTS

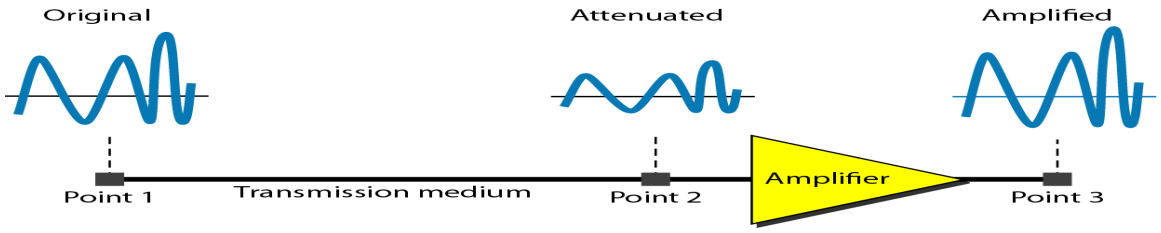
Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are **attenuation, distortion, and noise.**



Attenuation

- Means loss of energy -> weaker signal
- When a signal travels through a medium it loses energy overcoming the resistance of the medium

- A wire carrying electric signal gets warm after sometime i.e., some of the energy is converted to heat.
- Amplifiers are used to compensate for this loss of energy by amplifying the signal.



Measurement of Attenuation : To show the loss or gain of energy the unit "decibel" is used.

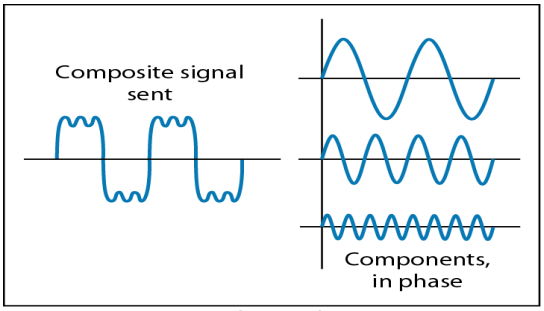
$$dB = 10\log_{10}P_2/P_1$$

P_1 - input signal P_2 - output signal

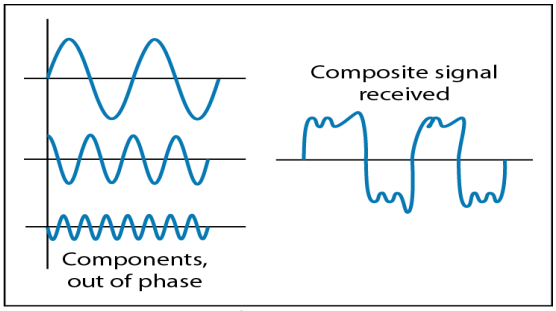
Decibel measures the relative strength of two signals or one signal at two different points. It is negative if signal is attenuated and positive when signal is amplified.

Distortion

- Means that the signal changes its form or shape
- Distortion occurs in composite signals made of different frequencies
- Each signal component has its own propagation speed traveling through a medium.
- The different components therefore arrive with different delays at the receiver.
- That means that the signals have different phases at the receiver than they did at the source.



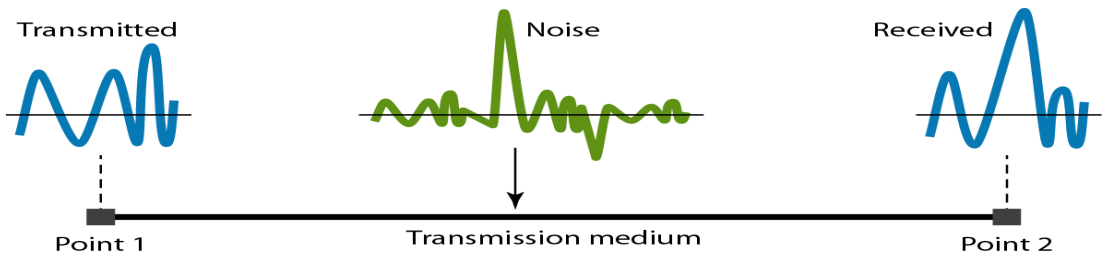
At the sender



At the receiver

Noise

- There are different types of noise
  - Thermal - random noise of electrons in the wire creates an extra signal
  - Induced - from motors and appliances, devices act are transmitter antenna and medium as receiving antenna.
  - Crosstalk – is the effect of one wire over another wires. One wire acts as sending antenna and other wire as receiving antenna
  - Impulse – Spikes (signals with high energy in a very short time) that result from power lines, lightning, etc.



Signal to Noise Ratio (SNR)

- To measure the quality of a system the SNR is often used. It indicates the strength of the signal w.r.t the noise power in the system.
- It shows what is wanted (signal) to what is not wanted (noise).
- SNR = $\frac{\text{Average signal power}}{\text{Average noise power}}$
- It is usually given in dB and referred to as $SNR_{dB.}$

- If SNR is high signal is less corrupted by noise.

6. DATA COMMUNICATION PROTOCOLS and STANDARDS

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.

Protocols

A protocol is synonymous with rule. It consists of a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing

Elements of a Protocol

- Syntax
  - Structure or format of the data
  - Indicates how to read the bits - field delineation
- Semantics
  - Interprets the meaning of the bits
  - Knows which fields define what action
- Timing
  - When data should be sent and what
  - Speed at which data should be sent or speed at which it is being received.

STANDARDS

A common set of rules. Provides guidelines to vendors' agencies, governments and other service providers.

Two categories are there:

De facto: They are not approved by an organized body but adopted as standards through widespread use. Standards established by manufactures who seek to define the functionality of a new product or technology.

De Jure: standards legislated by an officially recognized body.

Standards Organization

1) International Organization for Standardization (ISO)-
2) International Telecommunication Union-Telecommunication Standards Sector-(ITU-T)
3) American National Standards Institute (ANSI)-
4) Institute of Electrical and Electronics Engineers (IEEE)
5) Electronic Industries Association (EIA)-

7. NETWORK MODELS

OSI MODEL

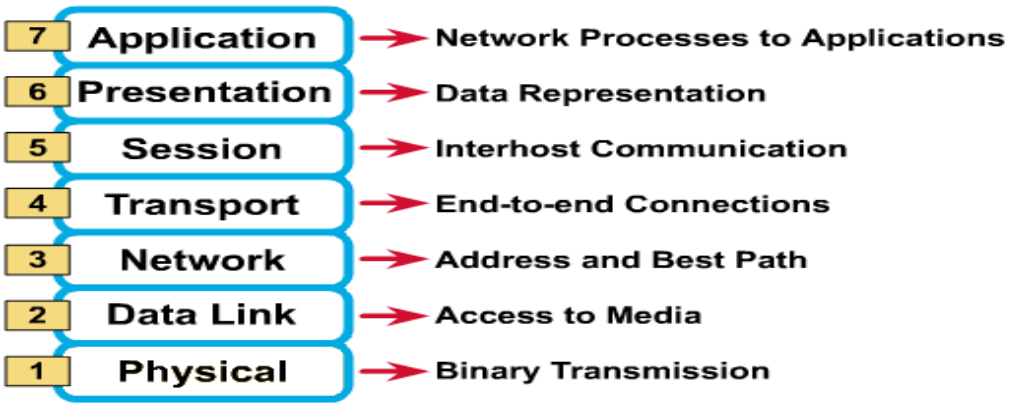
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s***. ISO is the organization. OSI is the model.***

Layered Architecture

Peer-to-Peer Processes

Encapsulation

Layered Architecture



- Layer architecture simplifies the network design, reduces complexity
- It is easy to debug network applications in a layered architecture network.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems.
- This separation into smaller more manageable functions is known as **layering.**
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper four layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.

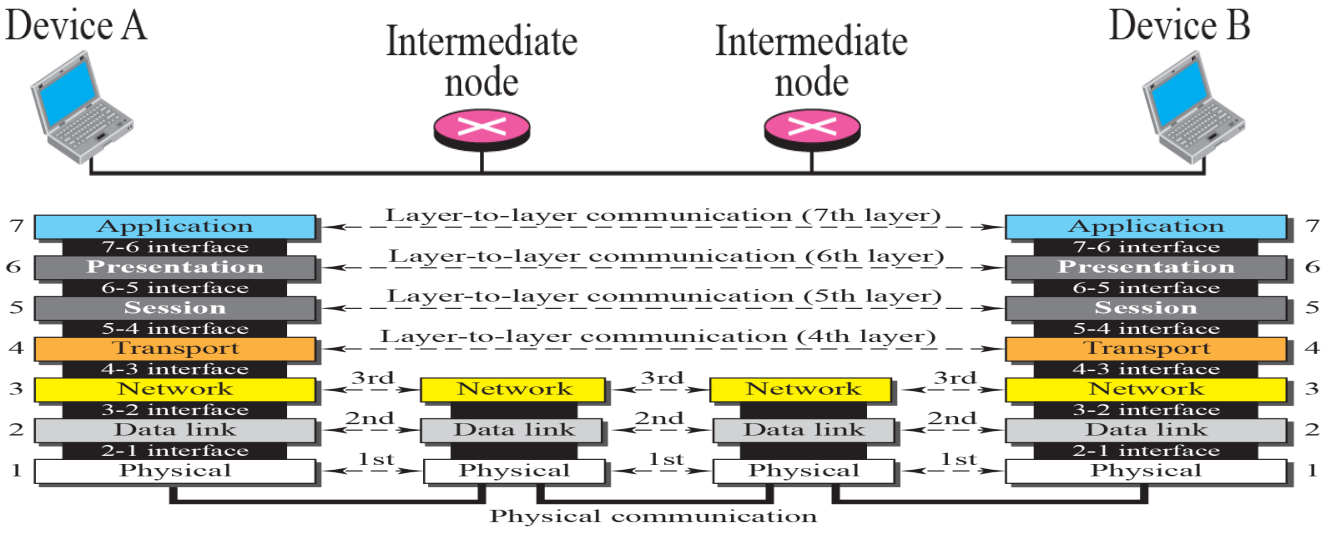
- The processes on each machine that communicate at a given layer are called **peer to peer processes.**

  - At the physical layer communication is direct.

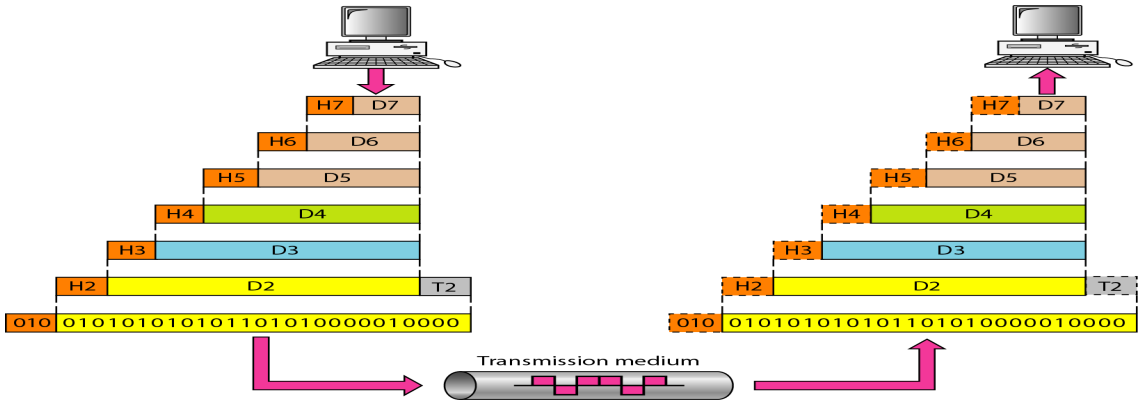
- At the higher layers communication moves down through the layers on device A to device B and then back up through the layers.
- Each layer in the sender adds its own information to the message it receives from the layer above it and passes the whole to layers below.
- At layer 1 the entire message is converted to a form that can be transmitted to receiver.
- At the receiver the message is unwrapped layer by layer with each process receiving and removing the data meant for it.
- The passing of data between layers is done by **an interface which provides** services and information to layers above it.
- At each layer a header and trailer is added to data unit.

- Data is **encapsulated** with the necessary protocol information as it moves down the layers before network transit.
  - The data portion of a packet at level (N-1) carries the whole packet from level N. It is called encapsulation.
  - Level N-1 is mot aware of which part of the encapsulated packet is data and which part is header or trailer.

LAYERS IN OSI MODEL

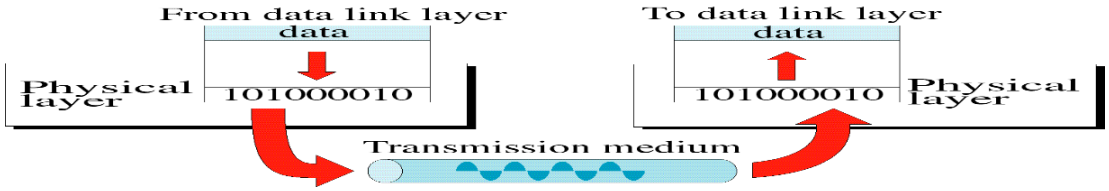


Exchange using the OSI Model



1) PHYSICAL LAYER

The physical layer concerned with the transmitting of the raw bits over a communication channel. When one side sends a 1 bit, it is received by other side as 1 bit, note as 0 bit. The physical layer coordinates the function required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specification of the interface and transmission medium.



The physical layer concerned with the following:

Physical characteristics and medium: defines the characteristics of the interface between the devices and the transmission medium, and type of transmission medium.

Representation of bits:- the physical layer data consists of stream of bit (0s or 1s) with no representation. To be transmitted bits must be encoded into signals-electrical or optical. The physical layer defines the type of encoding.

Data Rate : The transmission rate-the number of bits sent second –is also defined by the physical layer. It defines the duration of a bit i.e., how long it lasts.

Synchronization of bits: The sender and receiver must use the same bit rate and synchronized at the bit level .ie, the sender and receiver clock must be synchronized.

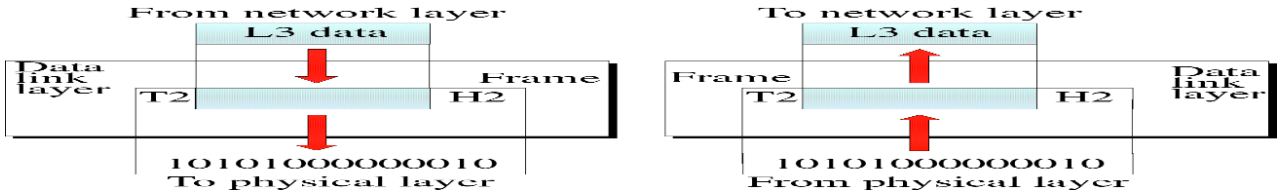
Line configuration: the physical layer is concerned with the connecting device to the media. In point-point device the 2 devices will connect through a dedicated link. In multipoint the link is shared.

Physical topology: Physical topology means how devices are connected to make a network, devices can be connected using, mesh topology, star topology, ring topology, bus topology, or it can be hybrid topology

Transmission Mode: the physical layer defines the direction of transmission between 2 devices. Simplex(only one device can send, the other can receive),half-duplex(two devices can send and receive, but not at the same time),full duplex(2 devices can send and receive at the same time).

2)DATA LINK LAYER

This layer transforms the physical layer, a raw transmission facility to reliable link. It makes the physical layer error free to the upper layer (network layer). It is responsible for moving frames from one hop (node) to the next.



Responsibilities of data link layer.

Framing: Data link layer divide the stream of bits received from the network layer to manageable data units called **frames.**

Physical addressing: It adds a header to define the sender or receiver of the frame. each node has its unique address.

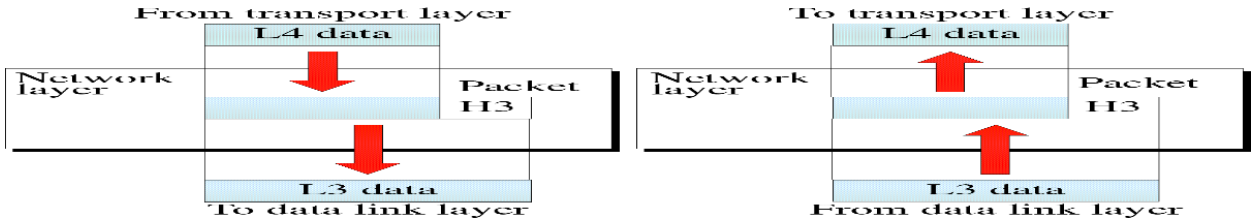
Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produces is the sender, the data link layer gives the flow of control mechanism to avoid overwhelming the receiver.

Error Control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It uses the mechanisms to recognize duplicate frames. Error control is normally achieved through a trailer added to the end frame.

Access control: When 2 or more devices are connected to the same link data link protocols will define which device has the control over the link at the given time.

3)NETWORK LAYER

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

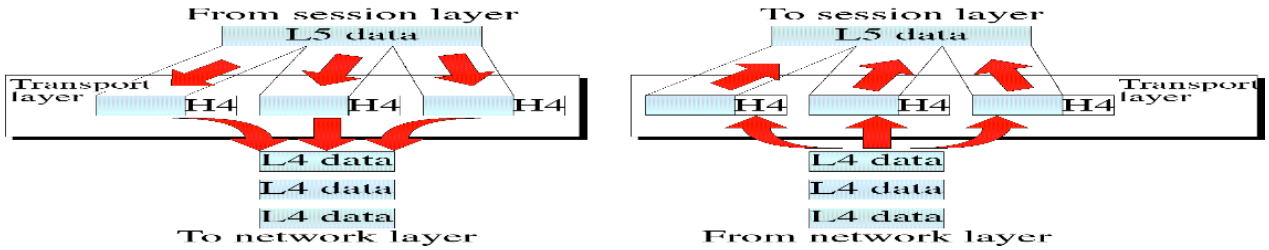


Responsibilities of Network layer:

Logical Addressing: physical addressing by the data link layer handle the addressing problem locally. If the packet passes the network boundary we need another addressing system to distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that among others things include the logical address of the sender and receiver.

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

4)TRANSPORT LAYER



It is responsible for the process to process delivery of the entire message. A process is an application program running in the host. The network layer oversees source to destination delivery of individual packets, does not recognize the relationship of the packet, it treats each one independently, because each piece belongs to separate message. The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source to destination level.

Responsibilities of Transport layer:

Service point addressing: source to destination delivery means delivery not only from 1 computer to the next but also from the specific processes (running program)on 1 computer to specific processes (running program)on other. the transport layer header must add a type of address called a service point address (port address)

Segmentation and reassembly: a message is divided into transmitable segments, with each segment containing a sequence number. These number's enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Connection Control: the transport layer can be either connection oriented or connection less .A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at destination. A connection oriented transport layer makes connection with the transport layer at the destination machine first before delivering the packets.

Flow control: Transport layer is responsible for flow of control like the data link layer. Flow of control at this layer is performed end to end rather than across a single link.

Error control: Error control is performed process to processes rather than across a single link. the sending transport layer makes sure that entire message arrives at the

receiving transport layer without error. Error correction is usually done through retransmission.

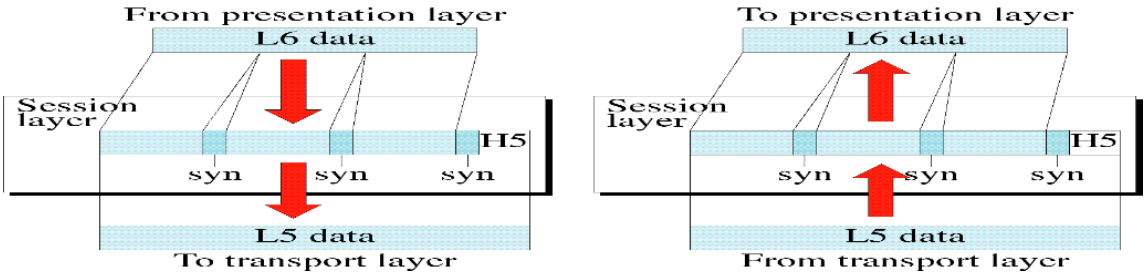
5)SESSION LAYER

The session layer is responsible for dialog control and synchronization. Session layer is the network "dialog controller". It establishes, maintaines, and synchronizes the interaction among communication systems.

Responsibilities of the session layer

Dialog control: allows 2 systems to enter into a dialog. It allows the communication between 2 processes to take place in either half duplex or full duplex mode.

Synchronization: the session layer add check points, or synchronization points, to stream of data.ex: if a system sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that 100 page unit is received and acknowledged independently.



6)PRESENTATION LAYER

Presentation layer is concerned with the syntax and semantics of the information. The presentation layer is responsible for translation, compression, and encryption

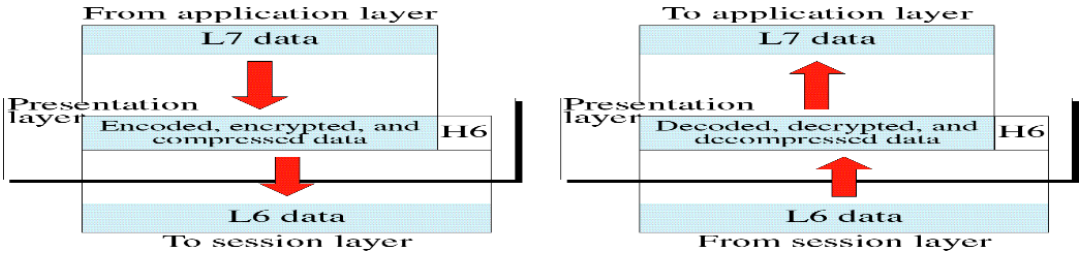
Responsibilities of a Presentation Layer:

Translation: the processes (running programs)in two systems are usually exchanging information in the form of character string, numbers and so on. The information must be changed into bit stream before being transmitted. Because different systems have

different encoding systems. This layer transform the sender dependent format to a common format and this layer at receiving side re transform to receiver dependent format.

Encryption: means the sender transforms the original information to another form and sends the resulting message over the network. Decryption reverses the original processes to transform the message back to the original form.

Compression: It is the reducing the number of bits contained in the information to be sent. This plays vital role in the transmission of information in form of audio, video, images, etc.



7)APPLICATION LAYER

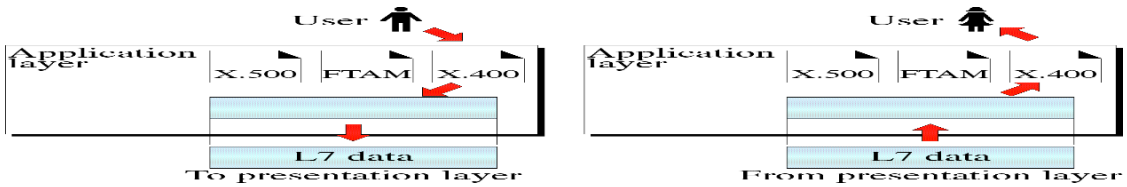
Application layer enables the user (human, software.) to access the internet. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information systems.

Network virtual Terminal: software version of a physical terminal and it allows the user to log on to a remote host..

File transfer, access and mangement: 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 local machine, and to manage the remote computer locally

Mail services: used for email stoarge and forwarding.

Directory services: provides distributed data sources and accesses for global information about various objects and service.



Summary of layers.

Application :To allow access to network

Presentation :-To translate encrypt and compress data

Session:- To establish manage and terminate sessions.

Transport:-To provide reliable process-to-process delivery and error recovery.

Network:-To move packets from source to destination to provide networking.

Data link:-To organize bits into frames to provide hop to hop delivery

Physical:-To transmit bits over a medium to provide mechanical and electrical specification

TCP/IP PROTOCOL SUITE

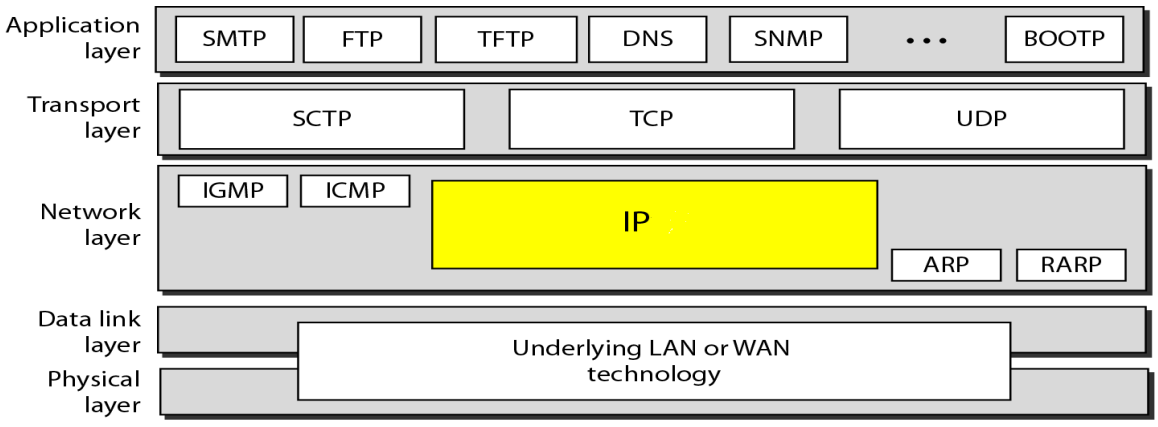
TCP/IP protocol suite was developed prior to OSI model. The layers in the TCP/IP protocol suite do not exactly match those to OSI model. The original TCP/IP protocol suite Designed has 4 layers:

Host to Network.

Internet

Transport

Application



The host to network is equivalent to the combination of physical and data link layers. The internet layer is equivalent to network layer, and application layers is doing the job of session, presentation and application layers with the transport layer in TCP/IP taking care of part of duties of session layer.

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means each upper level protocol is supported by one or more low-level protocols.

At transport layer TCP/IP defines 3 protocols. Transmission control protocol (TCP), User Datagram Protocol (UDP), stream control Transmission Protocol (SCTP)

At network layer the main protocol defined by TCP/IP is the internetworking protocol (IP),some other protocols are also supporting this layer.

1. PHYSICAL AND DATALINK LAYER

At this layers TCP/IP does not define any specific protocol. It supports all standard and proprietary Protocols. A network in TCP/IP internetwork can be LAN or WAN.

2. NETWORK LAYER.

TCP/IP supports the internetworking protocols. IP uses 4 protocols: ARP, RARP, ICMP, and IGMP.

Internetworking protocol (IP)

It is a transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol- a best effort delivery service. (IP provides no error checking and tracking.) IP transfers data in the form of packets called datagram, each of which is transported separately. Datagram can travel through different routes and can arrive out of sequence or may be duplicated. IP does not track routes and has no facility to reorder the datagrams once they reach destination.

Address Resolution Protocol (ARP)

Used to associate the logical address with physical address ARP is used to find the physical addresses of the node when its internet address is known.

Reverse Address Resolution Protocol (RARP)

Allows a host to discover it internet addresses when it knows its physical address. It is used when computer is connected to network for first time or when diskless computer is booted.

Internet control message protocol (ICMP)

A mechanism used by the host and gateways to send notification of datagram problems back to the sender. ICMP send query and error reporting messages.

Internet Group Message Protocol (IGMP)

It is used to facilitate the simultaneous transmission of messages to a group of recipients.

TRANSPORT LAYER: Transport layer was represented in TCP/IP by 2 protocols. TCP and UDP.IP is a host to host protocol meaning that it can deliver packet from one physical device to another. UDP, TCP are transport level protocols, responsible for the delivery of message from a process to another processes.

User datagram Protocol (UDP)

It is the simpler of two standard TCP/IP transport protocols. It is a process to process protocol that adds only port address, checksum, error control and length information to the data from upper layer.

Transmission control Protocol (TCP)

TCP provides full transport-layer services to applications.TCP is reliable stream transport protocol. Stream means, connection oriented.(connection must be established before message transmission)

At the sending end of each transmission TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for recording after receipt

together with an acknowledgment number for the segment received. Segments are carried across the internet inside of IP datagram. At receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Stream control Transmission Protocol

Provides support for newer applications such as voice over internet. It is a transport level protocol that combines best feature of UDP and TCP.

3. APPLICATION LAYER

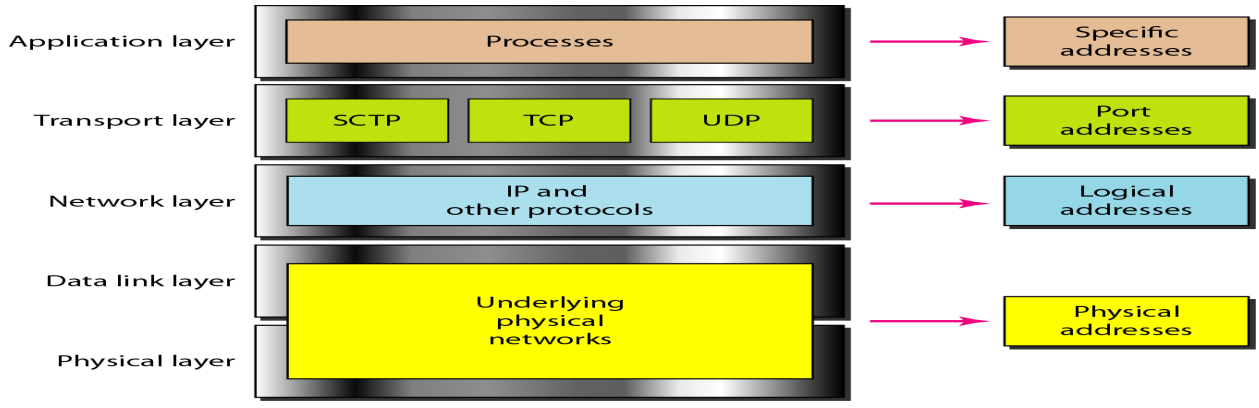
Application layer in TCP/IP is equivalent to the combined session, presentation and application layers in the OSI model. Many protocols are defined at this layer.

ADDRESSING

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

- ✔ Physical address (link): Ex. Ethernet address, machine address
- ✔ Logical address : IP address
- ✔ Port number
- ✔ Specific : URL, Email address, domain name

Relationship of layers and addresses in TCP/IP



Physical Addresses

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. LOWEST ADDRESS

- The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
- Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
- Example: Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below: A 6-byte (12 hexadecimal digits) physical address **07:01:02:01:2C:4B**

Logical Addresses

- Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers **132.24.75.9**

- 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 remain the same.

- The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

Port Addresses

- There are many applications running on the computer. Each application run with a port number. (Logically) on the computer.

- A port number is part of the addressing information used to identify the senders and receivers of messages.

- Port numbers are most commonly used with TCP/IP connections.

- These port numbers allow different applications on the same computer to share network resources simultaneously.

- The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.

- Example: a port address is a 16-bit address represented by one decimal number **753**

Application-Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.