



Nepal Institute of Computer Networking

Compiled by:- Er. Nagendra Karn

Terminology :-

- ▶ **Data** refers to digital information while communication refers to the transmission of information between two or more users via any method possible, such as speaking, texting, or any other media.
- ▶ The source is the user or device that sends the data, and the receiver is the person who receives it.
- ▶ The communicating device must be part of a system that includes both hardware and software in order for data to be exchanged.
- ▶ **Characteristics :-**
- ▶ **Delivery :-** Data must be transmitted to the correct location and must only be received by the intended recipient.
- ▶ **Accuracy :-** the information provided must be correct. Any tampering with the data while it is being transmitted renders it unusable.
- ▶ **Timeliness :** data must be given on time or it will be useless. In the case of audio and video, the data must be supplied in the same order in which it was created, with no significant delay.
- ▶ **Jitter :** it is the difference in the arrival time of audio or video packets or the uneven delivery of audio or video packets.

Protocol :

- ▶ In computer science and telecommunications, a communication protocol is a system of digital rules for data exchange within or between computers.
- ▶ When data is exchanged through computer network, the rule system is called a network protocol.

Protocol Layer

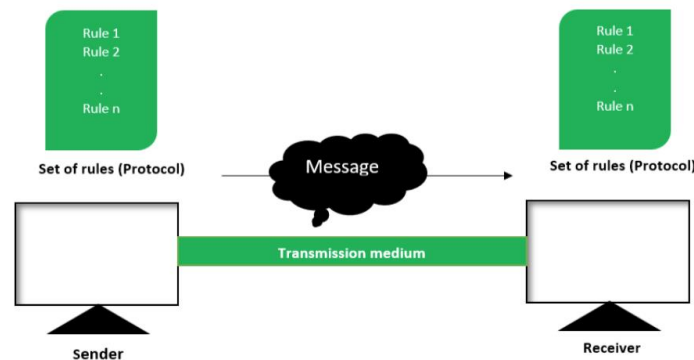
- ▶ A network protocol may be thought of as a set of more or less independent protocols, each in a different layer or level.
- ▶ The lowest layer governs direct host-to-host communication between the hardware at different hosts; the highest consists of user application programs.
- ▶ Each layer uses the layer beneath it and provides a service for the layer above.
- ▶ Each networking components hardware or software on one host uses protocols appropriate to its layer to communicate with the corresponding component on another host.

Protocol :

- ▶ A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated.
- ▶ The key elements of a protocol are syntax, semantics, and timing.
 - ▶ **Syntax** : The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
 - ▶ **Semantics**. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
 - ▶ **Timing**. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

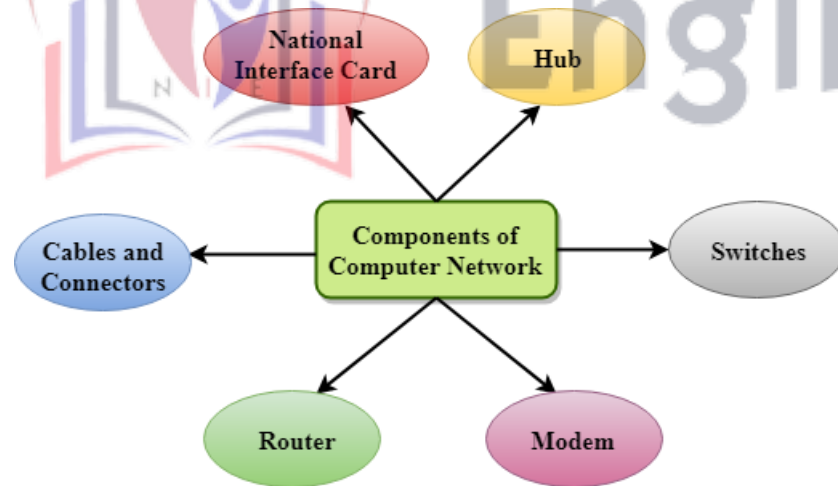
Standards :-

- ▶ **Standards** are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.
- ▶ **Standards** provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- ▶ Data communication standards fall into two categories: **de facto** (meaning "by fact" or "by convention") and **de jure** (meaning "by law" or "by regulation").
 - ▶ **De facto.** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
 - ▶ **De jure.** Those standards that have been legislated by an officially recognized body are de jure standards.



What is Computer Network :-

- ▶ **Computer Network** is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network.
- ▶ The aim of the computer network is the sharing of resources among various devices.
- ▶ In the case of computer network technology, there are several types of networks that vary from simple to complex level.



Features of Computer Network :

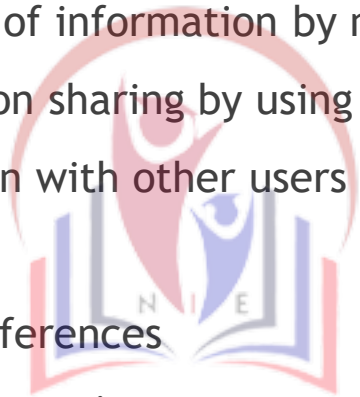
- ▶ **Communication speed** :- Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet.
- ▶ **File sharing** :- File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.
- ▶ **Back up and Roll back is easy** :- Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.
- ▶ **Software and Hardware sharing** :- We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.
- ▶ **Security** :- Network allows the security by ensuring that the user has the right to access the certain files and applications.
- ▶ **Scalability** :- Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices.
- ▶ **Reliability** :- Computer network can use the alternative source for the data communication in case of any hardware failure.

Internet :-

- ▶ A network is a group of connected communicating devices such as computers and printers. An internet is two or more networks that can communicate with each other.
- ▶ The **internet** is a globally connected network system that uses TCP/IP to transmit data via various types of media. Simply, internet is a means of connecting a computer to any other computer anywhere in the world via dedicated routers and servers.
- ▶ An **Extranet** is a communication network based on the internet protocol such as **TCP/IP**. The access to the extranet is restricted to only those users who have login credentials. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, at least it must have one connection to the external network.
- ▶ An **Intranet** is a private network based on the internet protocol such as **TCP/IP**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Applications :-

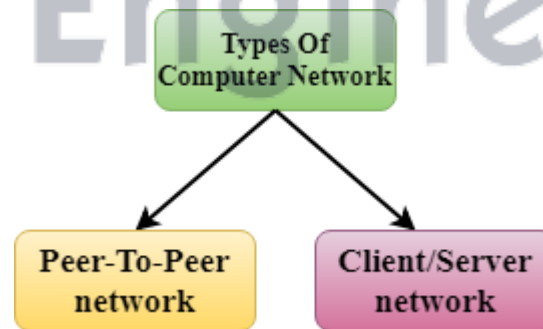
- ▶ Computer systems and peripherals are connected to form a network. They provide numerous advantages:
 - ▶ Resource sharing such as printers and storage devices
 - ▶ Exchange of information by means of e-Mails and FTP
 - ▶ Information sharing by using Web or Internet
 - ▶ Interaction with other users using dynamic web pages
 - ▶ IP phones
 - ▶ Video conferences
 - ▶ Instant messaging



Nepal Institute of
Engineering

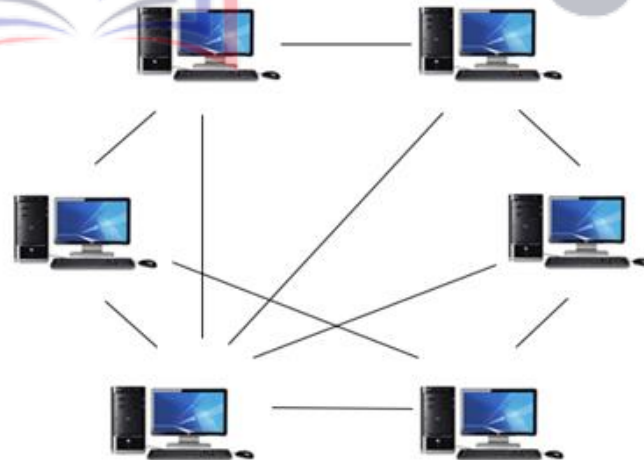
Network Architecture :-

- ▶ Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.
- ▶ Simply we can say that how computers are organized and how tasks are allocated to the computer.
- ▶ The two types of network architectures are used:
 - Peer to Peer network
 - Client/Server network



Peer-to-Peer Network :-

- ▶ Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- ▶ Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- ▶ Peer-To-Peer network has no dedicated server.
- ▶ Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

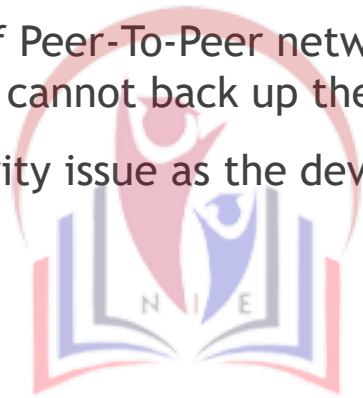


Advantages Of Peer-To-Peer Network:

- ▶ It is less costly as it does not contain any dedicated server.
- ▶ If one computer stops working but, other computers will not stop working.
- ▶ It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

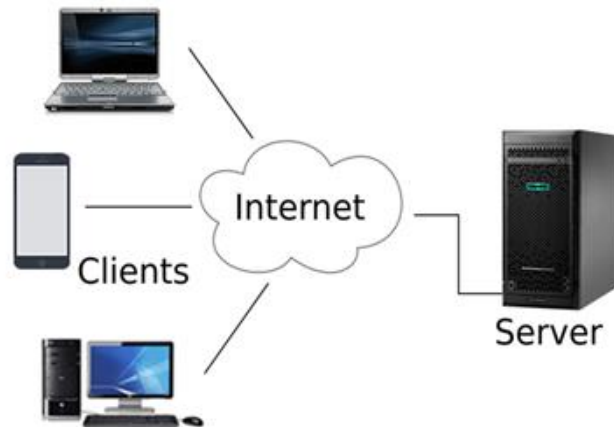
- ▶ In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- ▶ It has a security issue as the device is managed itself.



Nepal Institute of
Engineering

Client/Server Network:-

- ▶ Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- ▶ The central controller is known as a **server** while all other computers in the network are called **clients**.
- ▶ A server performs all the major operations such as security and network management.
- ▶ A server is responsible for managing all the resources such as files, directories, printer, etc.
- ▶ All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.

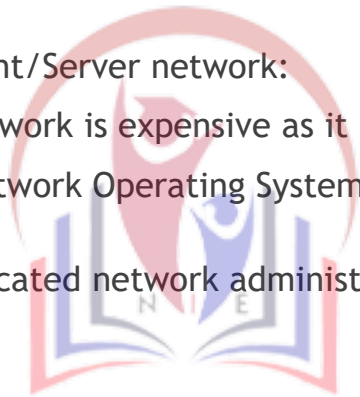


Advantages Of Client/Server network:

- ▶ A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- ▶ A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- ▶ Security is better in Client/Server network as a single server administers the shared resources.
- ▶ It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- ▶ Client/Server network is expensive as it requires the server with large memory.
- ▶ A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- ▶ It requires a dedicated network administrator to manage all the resources.



Nepal Institute of
Engineering

Computer Network Types:-

- ▶ A computer network can be categorized by their size. A **computer network** is mainly of **four types**:

- ❖ LAN(Local Area Network)
- ❖ PAN(Personal Area Network)
- ❖ MAN(Metropolitan Area Network)
- ❖ WAN(Wide Area Network)
- ❖ Wireless Local Area Network (WLAN)



- ▶ **LAN(Local Area Network) :-**
- ▶ Local Area Network is a group of computers connected to each other in a small area such as building, office.
- ▶ LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- ▶ It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- ▶ The data is transferred at an extremely faster rate in Local Area Network.
- ▶ Local Area Network provides higher security.

PAN(Personal Area Network) :-

- ▶ Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- ▶ Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- ▶ Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

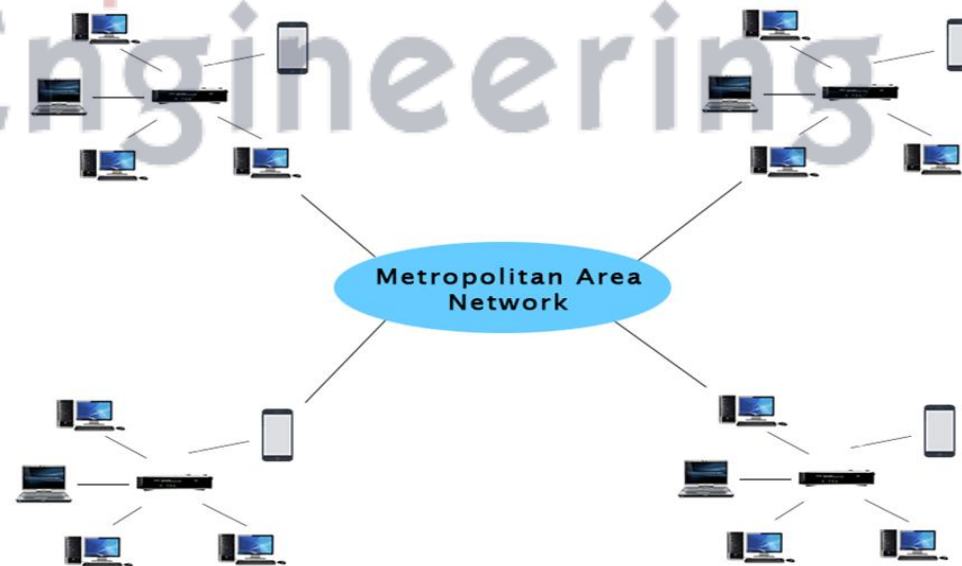
There are two types of Personal Area Network:

- ❖ Wired Personal Area Network
- ❖ Wireless Personal Area Network



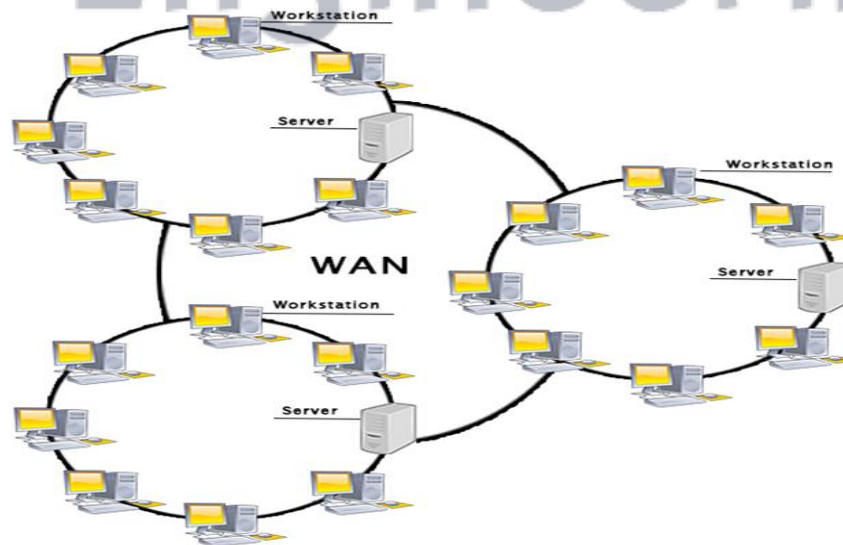
MAN(Metropolitan Area Network) :-

- ▶ A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- ▶ Government agencies use MAN to connect to the citizens and private industries.
- ▶ In MAN, various LANs are connected to each other through a telephone exchange line.
- ▶ The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- ▶ It has a higher range than Local Area Network(LAN).
- ▶ Uses Of Metropolitan Area Network:
 - ▶ MAN is used in communication between the banks in a city.
 - ▶ It can be used in an Airline Reservation.
 - ▶ It can be used in a college within a city.
 - ▶ It can also be used for communication in the military.



WAN(Wide Area Network):

- ▶ A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- ▶ A Wide Area Network is quite bigger network than the LAN.
- ▶ A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- ▶ The internet is one of the biggest WAN in the world.
- ▶ A Wide Area Network is widely used in the field of Business, government, and education.
- ▶ Examples Of Wide Area Network:
 - ▶ **Mobile Broadband:** A 4G network is widely used across a region or country.
 - ▶ **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
 - ▶ **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the tel



Advantages Of Wide Area Network:

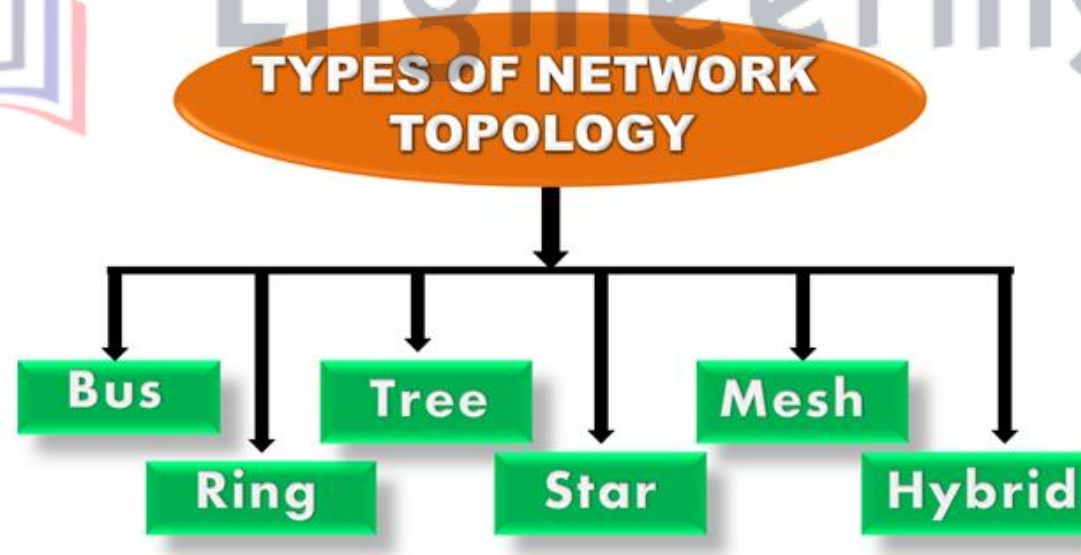
- ▶ **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- ▶ **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- ▶ **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- ▶ **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- ▶ **Global business:** We can do the business over the internet globally.
- ▶ **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

▶ Disadvantages of Wide Area Network:

- ▶ **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- ▶ **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- ▶ **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- ▶ **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

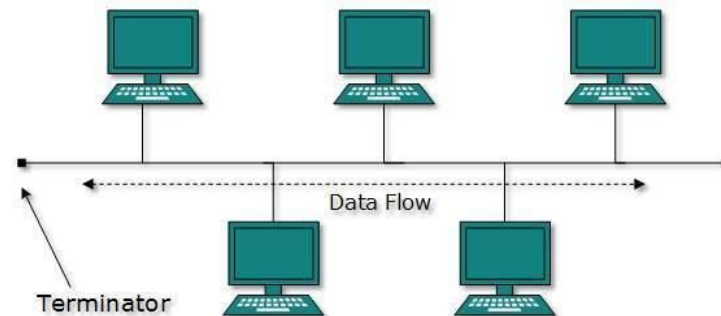
Network Topology:

- ▶ A Network Topology is the arrangement with which computer systems or network devices are connected to each other.
- ▶ There are two types of topology: physical and logical topology.
- ▶ Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.
- ▶ Physical topology is the geometric representation of all the nodes in a network.
- ▶ Some of the factors that affect choice of topology for a network are –
 - ▶ Cost
 - ▶ Flexibility
 - ▶ Reliability
 - ▶ Scalability
 - ▶ Ease of installation
 - ▶ Ease of maintenance



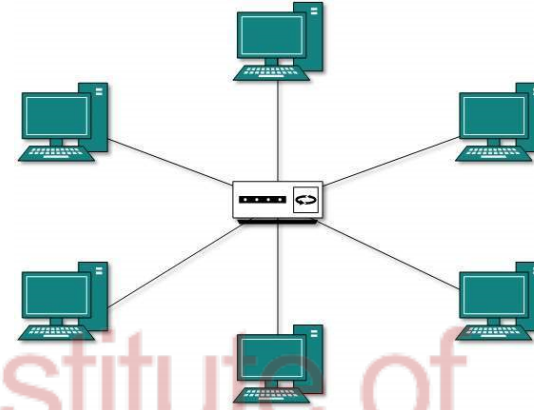
Bus Topology:

- ▶ In case of Bus topology, all devices share single communication line or cable.
- ▶ Bus topology may have problem while multiple hosts sending data at the same time.
- ▶ Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue.
- ▶ It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.
- ▶ Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.
- ▶ In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- ▶ Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- ▶ Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.



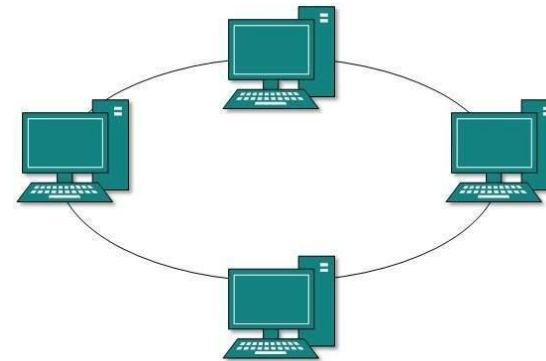
Star Topology :

- ▶ All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub.
- ▶ The hub device can be any of the following:
 - ▶ Layer-1 device such as hub or repeater
 - ▶ Layer-2 device such as switch or bridge
 - ▶ Layer-3 device such as router or gateway
- ▶ As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails.
- ▶ Every communication between hosts, takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.
- ▶ As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- ▶ It is easily expandable as new stations can be added to the open ports on the hub.
- ▶ Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- ▶ If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.



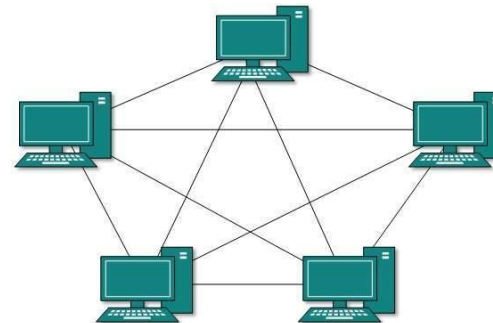
Ring Topology :-

- ▶ In ring topology, each host machine connects to exactly two other machines, creating a circular network structure.
- ▶ When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. The data flows in one direction, i.e., it is unidirectional.
- ▶ To connect one more host in the existing structure, the administrator may need only one more extra cable.
- ▶ Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.
- ▶ The most common access method of the ring topology is **token passing**.
 - ▶ **Token passing:** It is a network access method in which token is passed from one node to another node.
 - ▶ **Token:** It is a frame that circulates around the network.
- ▶ Working of Token passing
 - ▶ A token moves around the network, and it is passed from computer to computer until it reaches the destination.
 - ▶ The sender modifies the token by putting the address along with the data.
 - ▶ The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- ▶ In a ring topology, a token is used as a carrier.



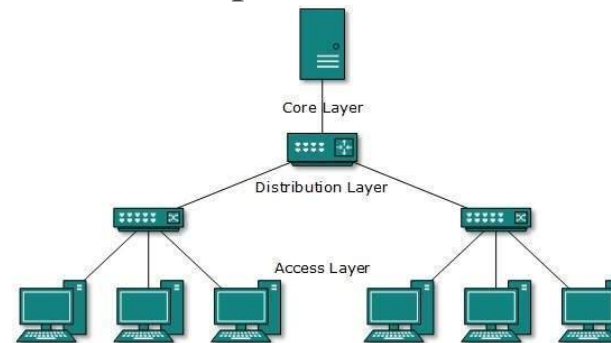
Mesh Topology :

- ▶ In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.
- ▶ There are multiple paths from one computer to another computer.
- ▶ Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- ▶ Mesh topology can be formed by using the formula:
Number of cables = $(n*(n-1))/2$; Where n is the number of nodes that represents the network
- ▶ Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:
 - ▶ **Full Mesh:** All hosts have a point-to-point connection to every other host in the network. Thus for every new host $n(n-1)/2$ connections are required. It provides the most reliable network structure among all network topologies.
 - ▶ **Partially Mesh:** Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrary fashion. This topology exists where we need to provide reliability to some hosts out of all.



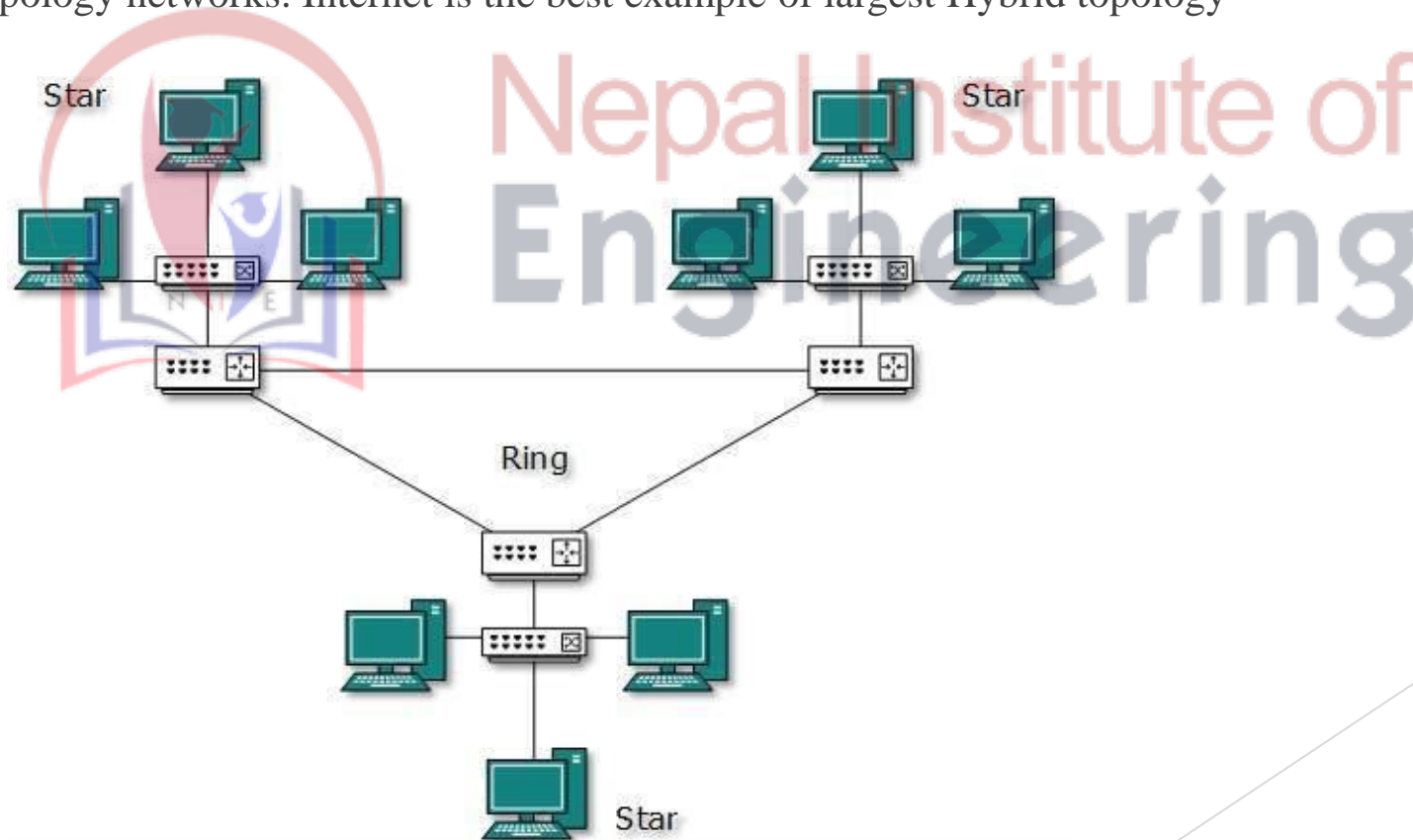
Tree Topology :

- ▶ Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology.
- ▶ This topology divides the network in to multiple levels/layers of network.
- ▶ Mainly in LANs, a network is bifurcated into three types of network devices.
- ▶ The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer.
- ▶ The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.
- ▶ All neighboring hosts have point-to-point connection between them.
- ▶ Similar to the Bus topology, if the root goes down, then the entire network suffers even though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.



Hybrid Topology :-

- ▶ A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.
- ▶ The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies.
- ▶ Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology



Layered Architecture :

- ▶ A reference model (OSI and TCP/IP) is a conceptual rule of how communications should take place.
- ▶ It addresses all the processes required for effective communication and divides these processes into logical groupings called layers.
- ▶ When a communication system is designed in this manner, it is known as layered architecture.
- ▶ **Need of Layered Architecture**
- ▶ It divides the network communication process into smaller and simpler components, thus aiding component development, design and troubleshooting.
- ▶ It allows multi-vendor development through standardization of network components.
- ▶ It allows different various types of network software and hardware to communicate.

OSI Layer

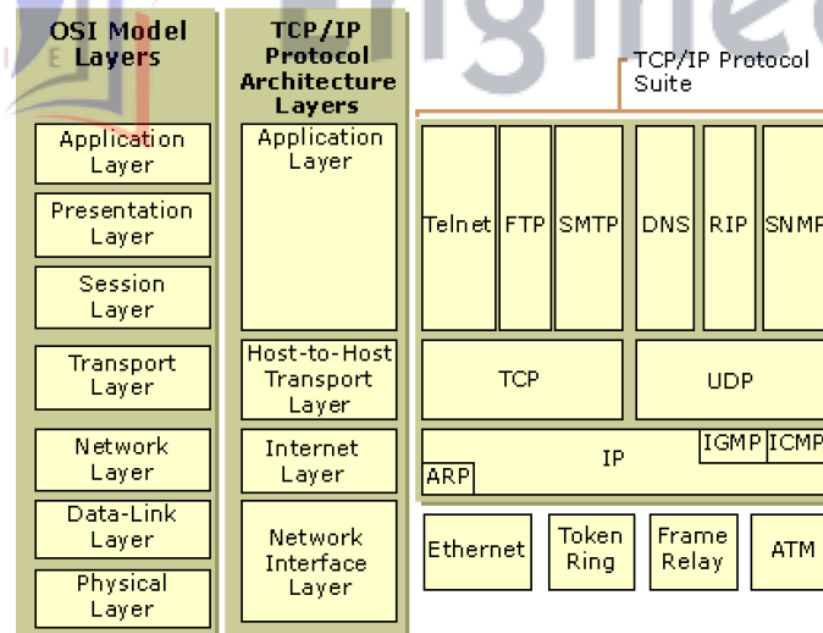
Application
Presentation
Session
Transport
Network
Data link
Physical

TCP/IP Layer

Application
Transport
Internet
Network Access

Principles of OSI Reference Model :-

- ▶ A layer should be created where a different 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 architecture does not become unwieldy.

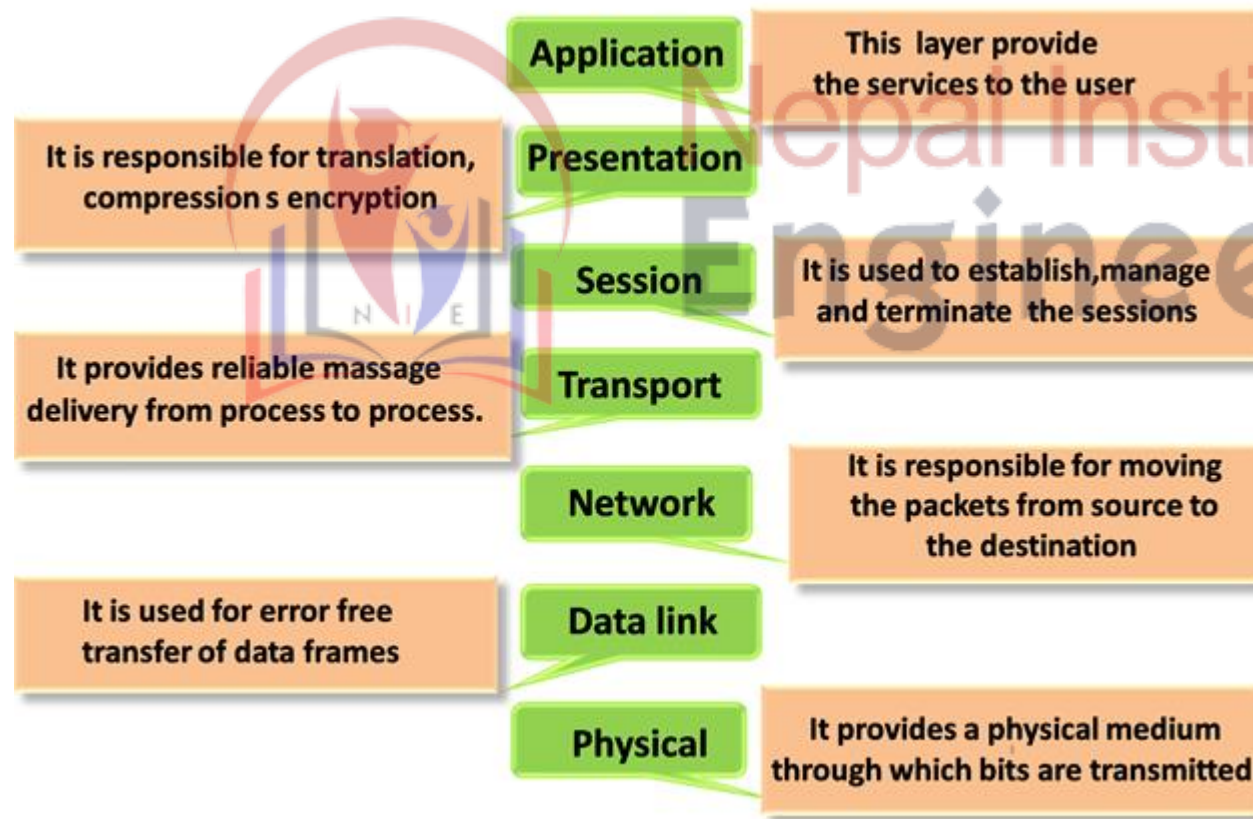


OSI Model

- ▶ OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- ▶ OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- ▶ OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- ▶ The OSI model is divided into two layers: upper layers and lower layers.
- ▶ The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- ▶ The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

- There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

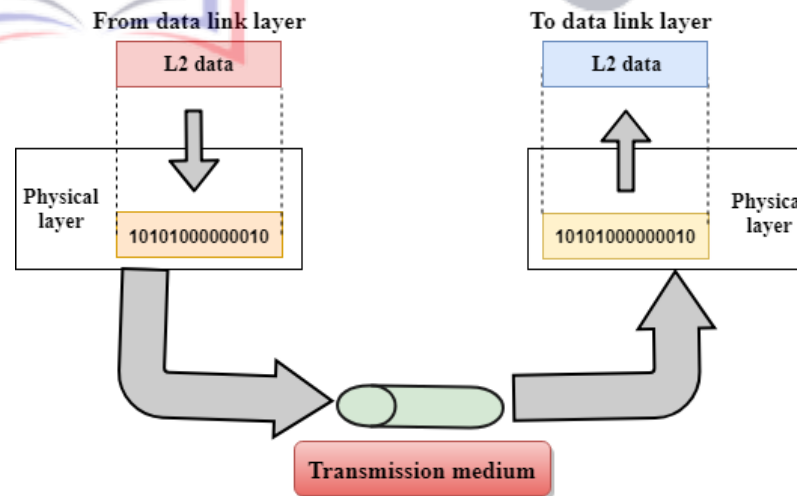


Physical layer:

- ▶ The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- ▶ It establishes, maintains and deactivates the physical connection.
- ▶ It specifies the mechanical, electrical and procedural network interface specifications.

- ▶ **Functions of a Physical layer:**

- ▶ **Line Configuration:** It defines the way how two or more devices can be connected physically.
- ▶ **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ▶ **Topology:** It defines the way how network devices are arranged.
- ▶ **Signals:** It determines the type of the signal used for transmitting the information.



Data-Link Layer :

- ▶ This layer is responsible for the error-free transfer of data frames.
- ▶ It defines the format of the data on the network.
- ▶ It provides a reliable and efficient communication between two or more devices.
- ▶ It is mainly responsible for the unique identification of each device that resides on a local network.
- ▶ It contains two sub-layers:
- ▶ **Logical Link Control Layer**
 - ▶ It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
 - ▶ It identifies the address of the network layer protocol from the header.
 - ▶ It also provides flow control.
- ▶ **Media Access Control Layer**
 - ▶ A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
 - ▶ It is used for transferring the packets over the network.

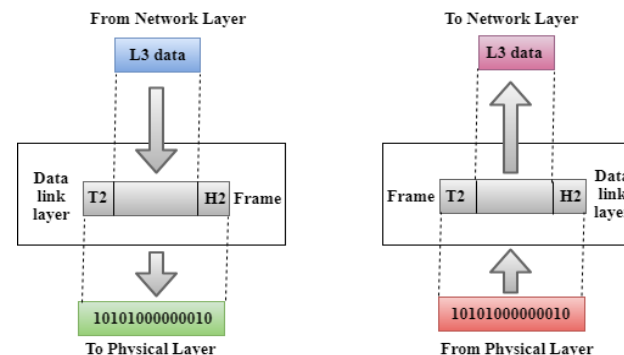
Nepal Institute of
Engineering

Functions of the Data-link layer :

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

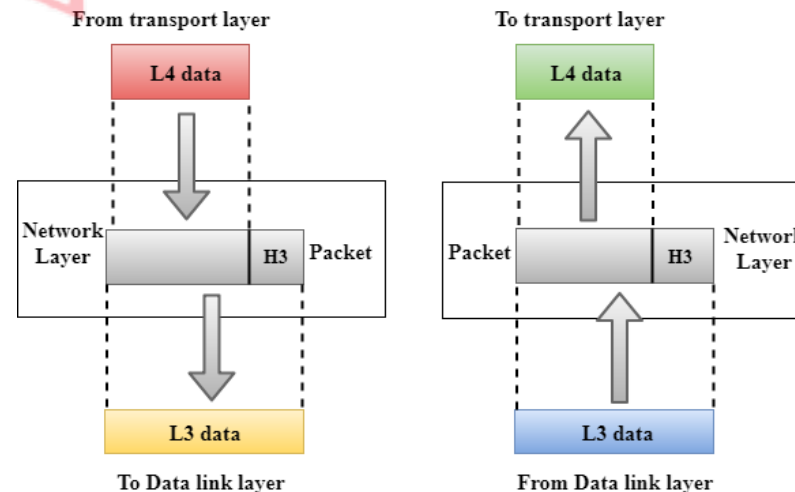


- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.



Network Layer :

- ▶ It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- ▶ It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- ▶ The Network layer is responsible for routing and forwarding the packets.
- ▶ Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- ▶ The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

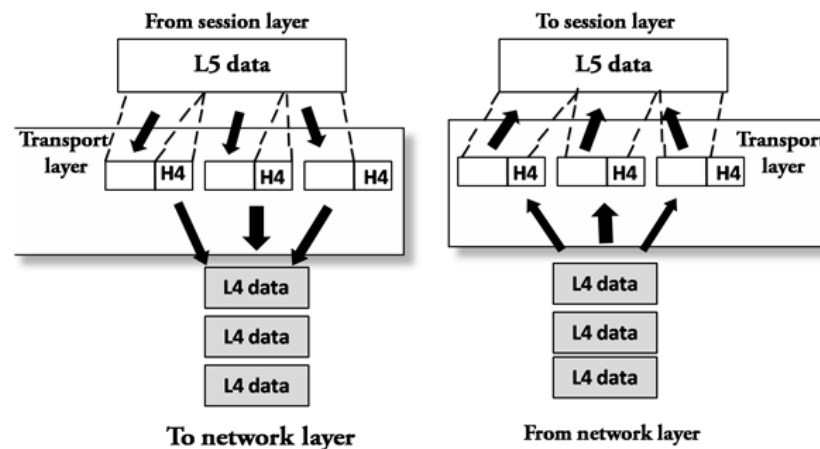


Functions of Network Layer:

- ▶ **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- ▶ **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- ▶ **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- ▶ **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).
- ▶ Responsibilities of the network layer include the following:
 - ▶ **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
 - ▶ **• Routing.** When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer

- ▶ The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- ▶ The main responsibility of the transport layer is to transfer the data completely.
- ▶ It receives the data from the upper layer and converts them into smaller units known as segments.
- ▶ This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.



- ▶ **The two protocols used in this layer are:**

- ▶ **Transmission Control Protocol**

- ▶ It is a standard protocol that allows the systems to communicate over the internet.
- ▶ It establishes and maintains a connection between hosts.
- ▶ When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- ▶ **User Datagram Protocol**

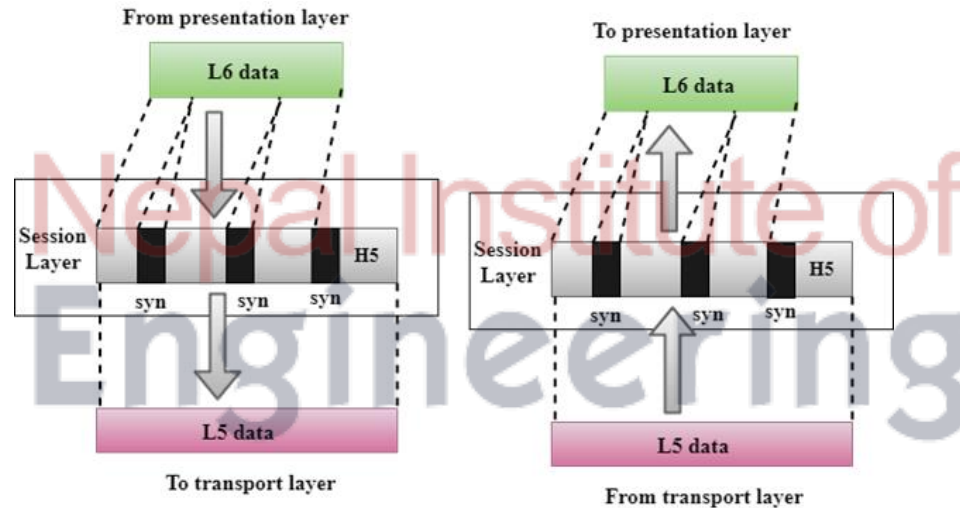
- ▶ User Datagram Protocol is a transport layer protocol.
- ▶ It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- ▶ **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- ▶ **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- ▶ **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- ▶ **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- ▶ **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

Session Layer

- The session layer is the network dialog controller. The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

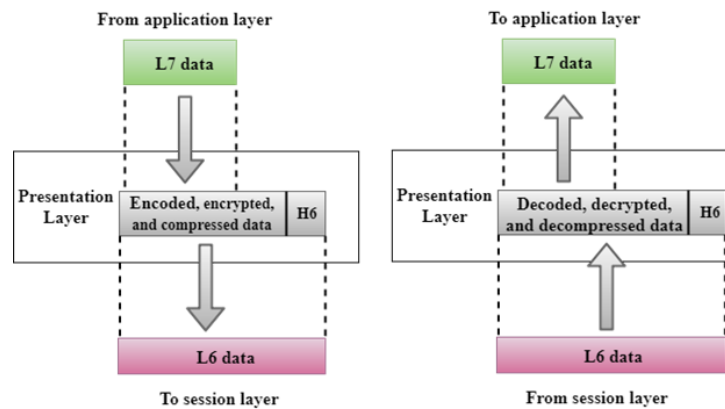


- **Functions of Session layer:**

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

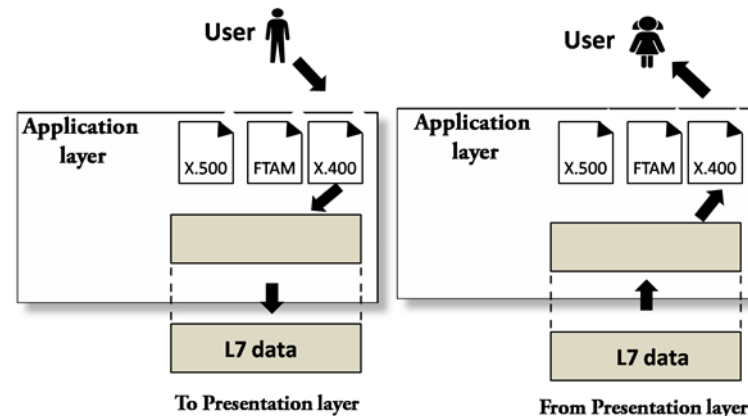
Presentation Layer

- ▶ A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- ▶ It acts as a data translator for a network.
- ▶ This layer is a part of the operating system that converts the data from one presentation format to another format.
- ▶ The Presentation layer is also known as the syntax layer.
- ▶ **Functions of Presentation layer:**
 - ▶ **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
 - ▶ **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
 - ▶ **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.



Application Layer

- ▶ An application layer serves as a window for users and application processes to access network service.
- ▶ It handles issues such as network transparency, resource allocation, etc.
- ▶ An application layer is not an application, but it performs the application layer functions.
- ▶ This layer provides the network services to the end-users.
- ▶ Functions of Application layer:
 - ▶ **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
 - ▶ **Mail services:** An application layer provides the facility for email forwarding and storage.



Merits of OSI reference model:

- ▶ OSI model distinguishes well between the services, interfaces and protocols.
- ▶ Protocols of OSI model are very well hidden.
- ▶ Protocols can be replaced by new protocols as technology changes.
- ▶ Supports connection oriented services as well as connectionless service.

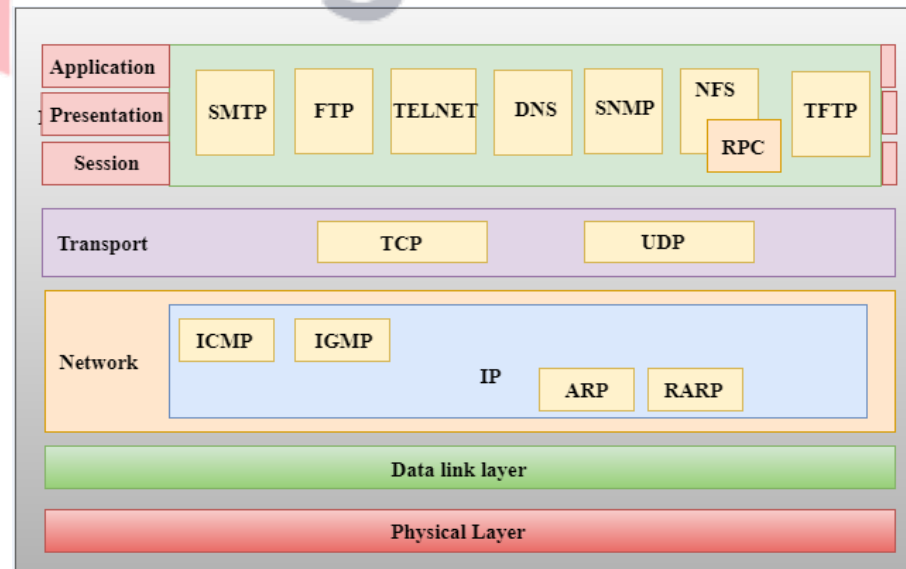
Demerits of OSI reference model:

- ▶ Model was devised before the invention of protocols.
- ▶ Fitting of protocols is tedious task.
- ▶ It is just used as a reference model.

Nepal Institute of
Engineering

TCP/IP model:

- ▶ The TCP/IP model was developed prior to the OSI model.
- ▶ The TCP/IP model is not exactly similar to the OSI model.
- ▶ The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- ▶ The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- ▶ TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.
- ▶ Note :- Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.



Network Access Layer

- ▶ A network layer is the lowest layer of the TCP/IP model.
- ▶ A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- ▶ It defines how the data should be sent physically through the network.
- ▶ This layer is mainly responsible for the transmission of the data between two devices on the same network.
- ▶ The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- ▶ The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- ▶ An internet layer is the second layer of the TCP/IP model. It is also known as the network layer.
- ▶ The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.
- ▶ Following are the protocols used in this layer are:
 - ▶ **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
 - ▶ **Host-to-host communication:** It determines the path through which the data is to be transmitted.
 - ▶ **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
 - ▶ **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
 - ▶ **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ▶ ARP stands for **Address Resolution Protocol**.
- ▶ ARP is a network layer protocol which is used to find the physical address from the IP address.
- ▶ **The two terms are mainly associated with the ARP Protocol:**
 - ▶ **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
 - ▶ **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- ▶ ICMP stands for Internet Control Message Protocol.
- ▶ It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- ▶ A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- ▶ An ICMP protocol mainly uses two terms:
 - ICMP Test: ICMP Test is used to test whether the destination is reachable or not.
 - ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

- ▶ The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
- ▶ The two protocols used in the transport layer are User Datagram protocol and Transmission control protocol.

User Datagram Protocol (UDP)

- ▶ It provides connectionless service and end-to-end delivery of transmission.
- ▶ It is an unreliable protocol as it discovers the errors but not specify the error.
- ▶ User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

Transmission Control Protocol (TCP)

- ▶ It provides a full transport layer services to applications.
- ▶ It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- ▶ TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- ▶ At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- ▶ At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- ▶ An application layer is the topmost layer in the TCP/IP model.
- ▶ It is responsible for handling high-level protocols, issues of representation.
- ▶ This layer allows the user to interact with the application.
- ▶ When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

Following are the main protocols used in the application layer:

- ▶ **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- ▶ **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- ▶ **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- ▶ **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- ▶ **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- ▶ **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Merits of TCP/IP model :

- ▶ It operated independently.
- ▶ It is scalable.
- ▶ Client/server architecture.
- ▶ Supports a number of routing protocols.
- ▶ Can be used to establish a connection between two computers.

Demerits of TCP/IP model :

- ▶ In this, the transport layer does not guarantee delivery of packets.
- ▶ The model cannot be used in any other application.
- ▶ Replacing protocol is not easy.
- ▶ It has not clearly separated its services, interfaces and protocols.

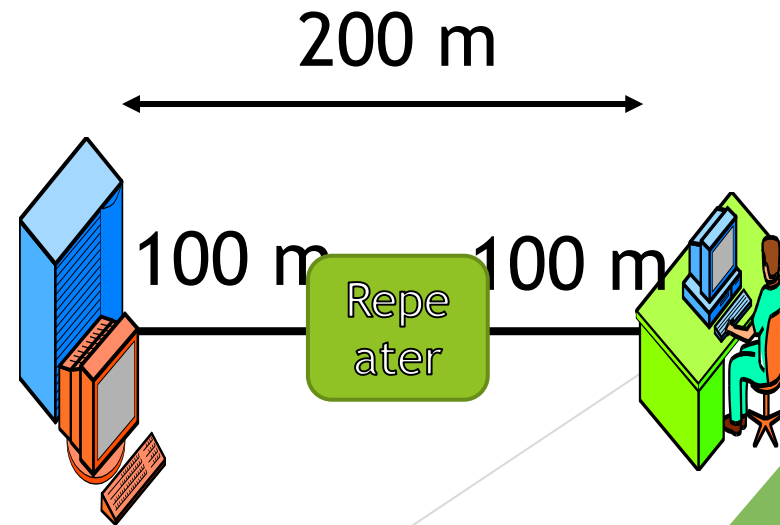
Comparison :-

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. OSI model has a separate Presentation layer and Session layer.	3. TCP/IP does not have a separate Presentation layer or Session layer.
4. Transport Layer is Connection Oriented.	4. Transport Layer is both Connection Oriented and Connection less.
5. Network Layer is both Connection Oriented and Connection less.	5. Network Layer is Connection less.
6. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	6. TCP/IP model is, in a way implementation of the OSI model.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.

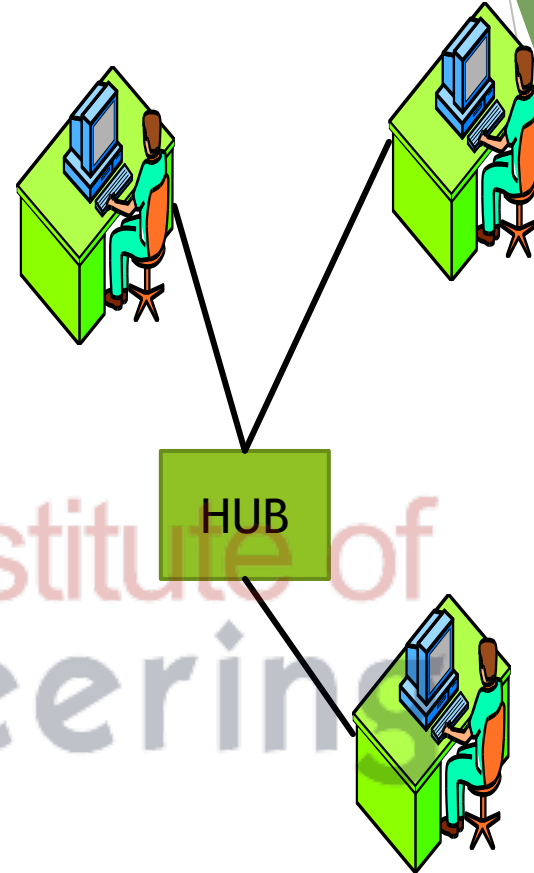
Networking Devices

► Repeater

- Physical Layer Device
- Regenerates the signal
- Extend the distance over which a signal may travel down a cable
- It is an electronic device that receives a signal and retransmits it at a higher level or higher power, and onto the other side of an abstraction, so that the signal can cover long distances.



Networking Devices



► Hub

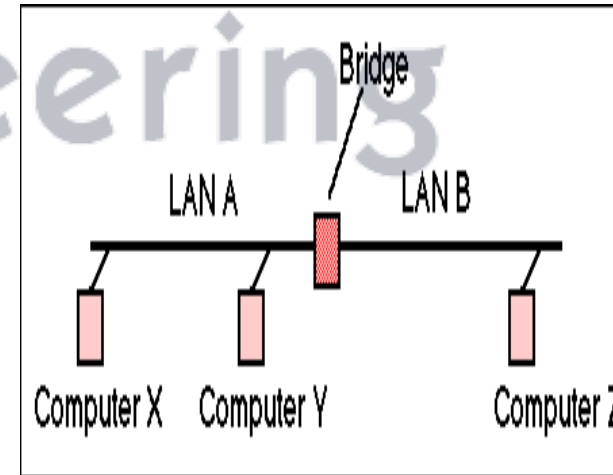
- Physical Layer Device
- Like a Multiport Repeater
- Two Types
 - Active Hub
 - Regeneartes Signal, needs power
 - Passive Hub
 - A simple Connector (no signal Regeneration)
- It has multiple I/O ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming.

Networking Devices

► Bridge

- Data Link Layer Device
- Maintains MAC table with MAC address and port no. and decides whether to forward the frame or not.
- Divides Network into different LAN Segments
- Smarter than Repeaters

MAC Address	Port No.
2A-3B-AB-45-3B-5F	1
1b-3B-43-45-3B-4F	2
3F-35-6B-46-30-5F	1

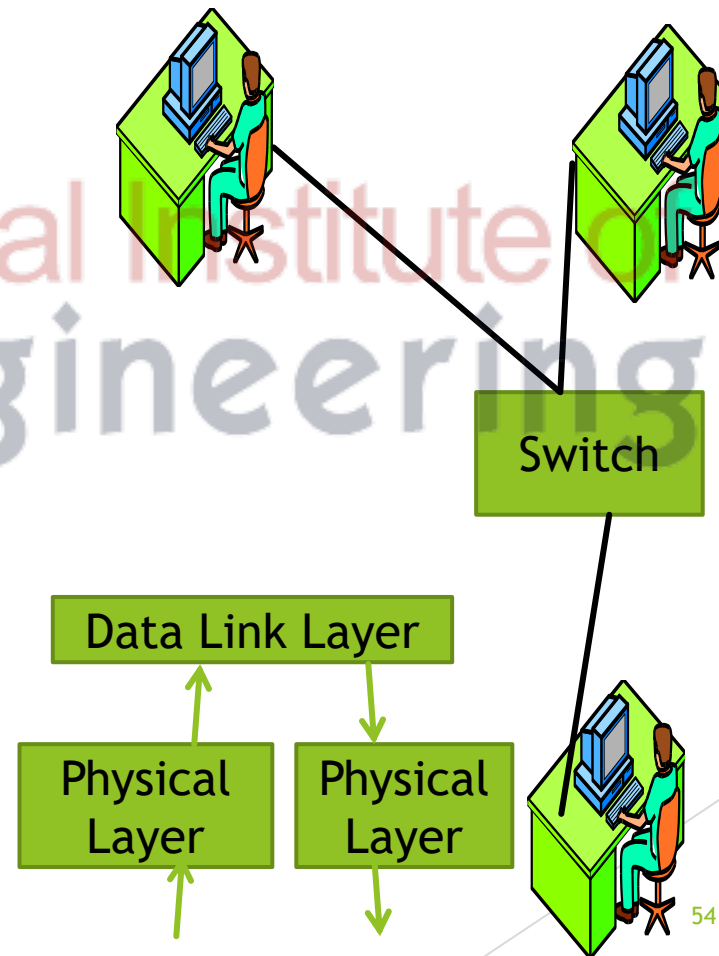


Networking Devices

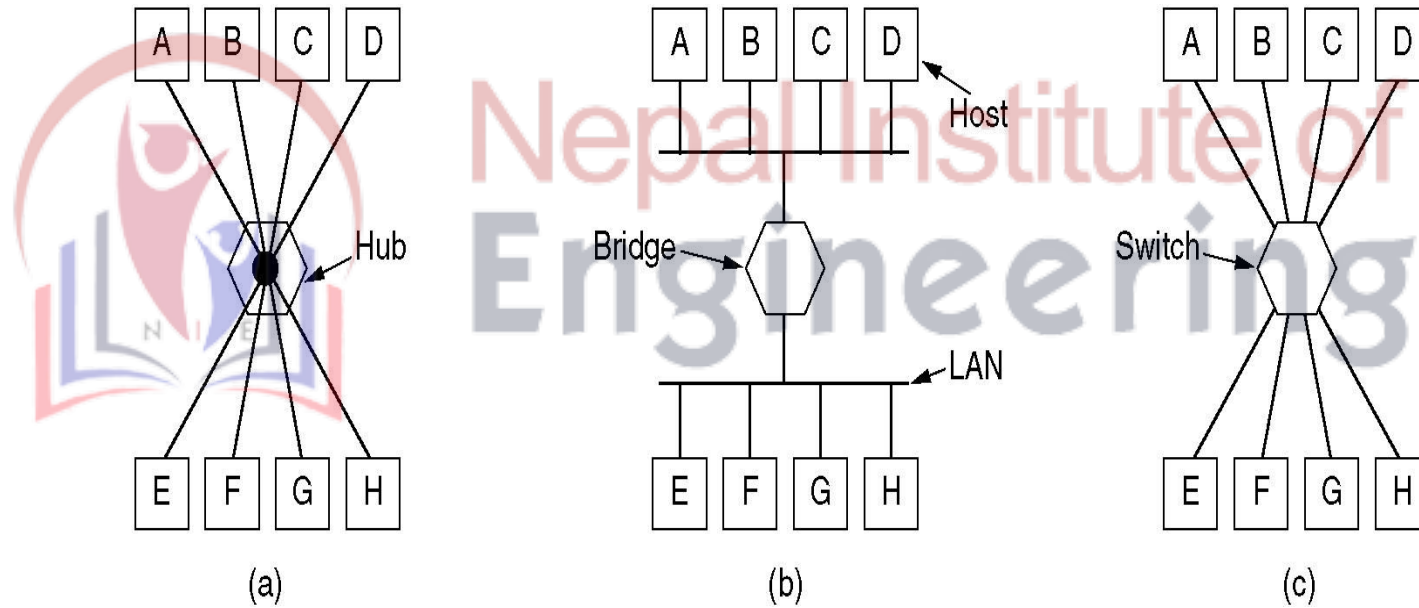
► Switch

- Data Link Layer Device
- A Multiport Bridge
- Divides Network into different LAN Segments

MAC Address	Port No.
2A-3B-AB-45-3B-5F	1
1b-3B-43-45-3B-4F	2
3F-35-6B-46-30-5F	3



Networking Devices



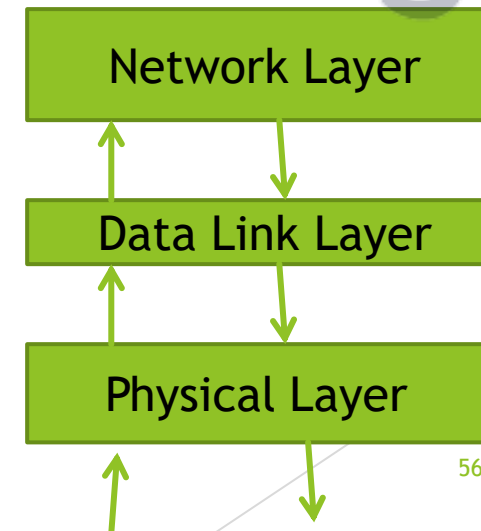
(a) A hub. (b) A bridge. (c) a switch.

Networking Devices

► Routers

- Network Layer Device
- Able to analyse Network layer address and find the route
- Maintains Routing table to route packet to destⁿ address
- Expensive and Slower than switch
- Supports Hierarchical addressing
- “Use Switch where you can,

Use Router where you must.”



Networking Devices

► Gateway

- Allows devices in different networks to communicate
- Generic term for routers
- The term “gateway” is also used for device that interconnects different Networks and which perform translation of protocols(Multi-Protocol Routers).





Repeater



Router



Hub



Bridge



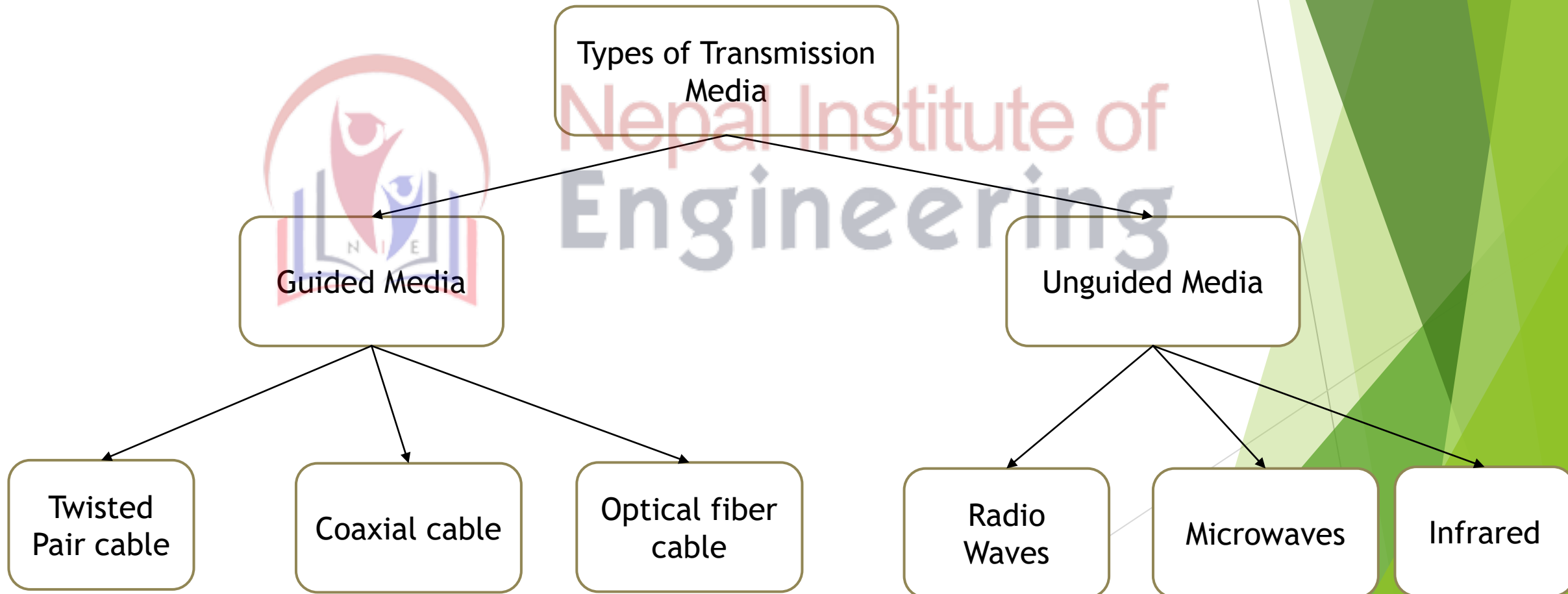
Switch



Gateway

Transmission media

- ▶ In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.
- ▶ Transmission Media is broadly classified into the following types:



Guided Media

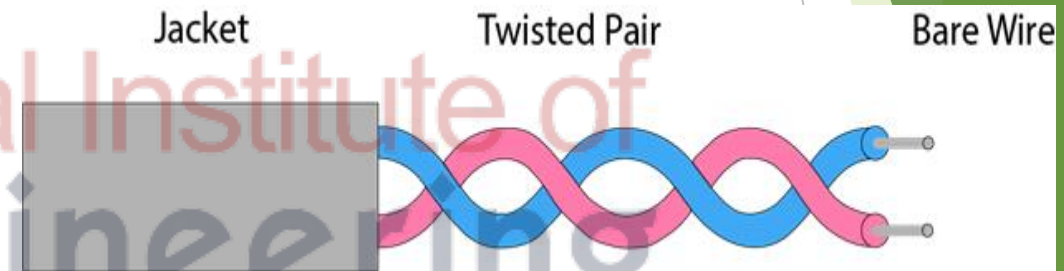
- ▶ It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.
- ▶ The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.

Features :-

High Speed

Secure

Used for comparatively shorter distances.



(i) Twisted Pair Cable –

- ▶ It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:
 - i. Unshielded Twisted Pair (UTP)
 - ii. Shielded Twisted Pair (STP)

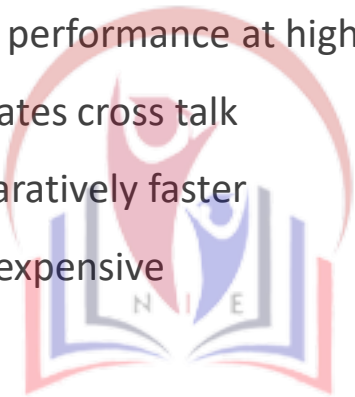
Unshielded Twisted Pair (UTP)

- ▶ UTP consists of two insulated copper wires twisted around one another. 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.
- ▶ Advantage :-
 - ▶ Least expensive
 - ▶ Easy to install
 - ▶ High-speed capacity
 - ▶ Lower capacity and performance in comparison to STP
 - ▶ Short distance transmission due to attenuation

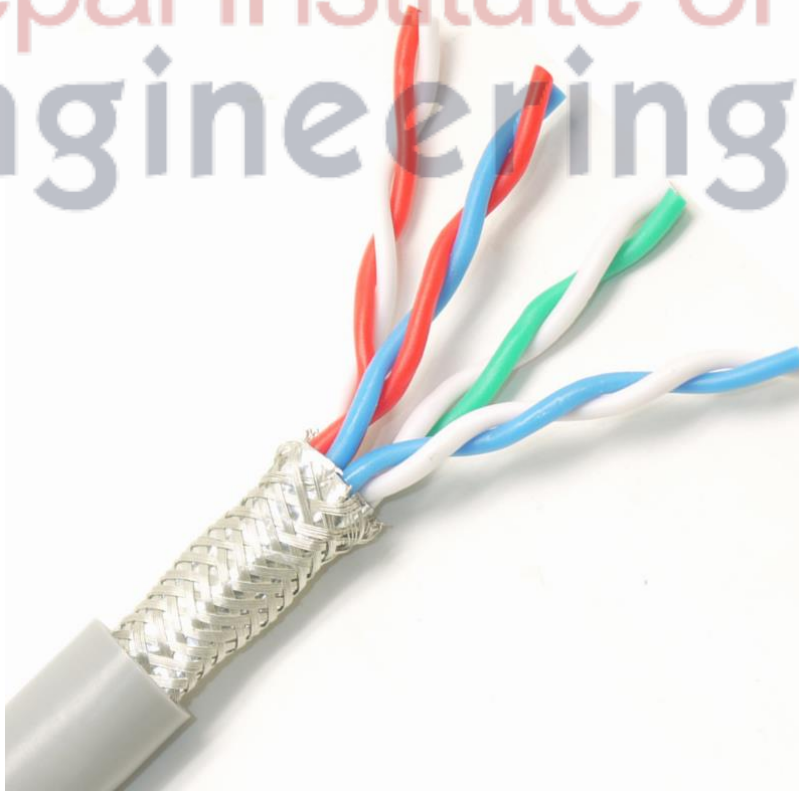


Shielded Twisted Pair (UTP)

- ▶ This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
- ▶ Advantages :-
 - ▶ Better performance at higher data rate in comparison to UTP
 - ▶ Eliminates cross talk
 - ▶ Comparatively faster
 - ▶ More expensive
 - ▶ Bulky

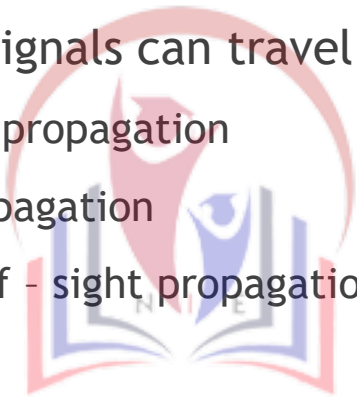


Nepal Institute of
Engineering



Unguided Media:

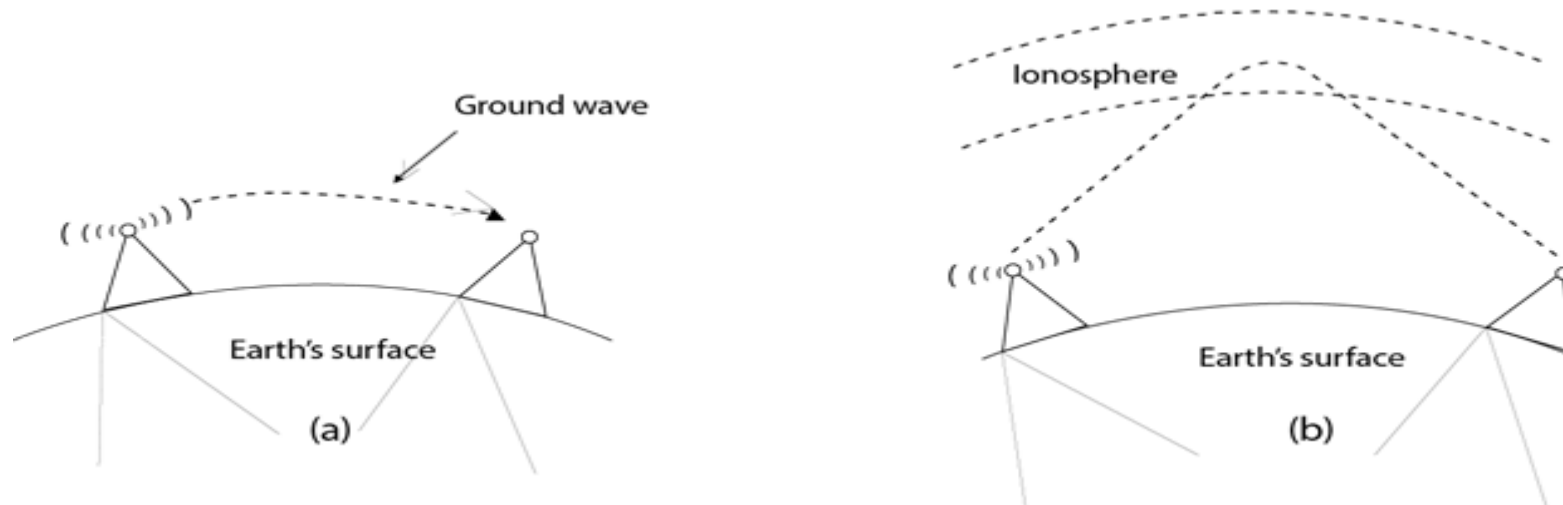
- ▶ An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- ▶ They transport data in the form of electromagnetic waves that do not require any cables for transmission. These media are bounded by geographical boundaries.
- ▶ Unguided signals can travel in three ways –
 - ▶ Ground propagation
 - ▶ Sky propagation
 - ▶ Line - of - sight propagation
- ▶ Features :-
 - ▶ Signal is broadcasted through air
 - ▶ Less secure
 - ▶ Used for larger distances



Nepal Institute of
Engineering

Radio Waves :-

- ▶ Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- ▶ Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- ▶ The range in frequencies of radio waves is from 3Khz to 1 Ghz.
- ▶ In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- ▶ An example of the radio wave is **FM radio**.



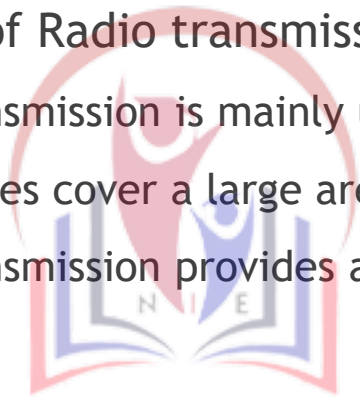
Radio wave (contd...)

► Applications of Radio waves :-

- A radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio waves.

► Advantages of Radio transmission :-

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate walls.
- Radio transmission provides a higher transmission rate.



Nepal Institute of
Engineering

Microwaves:-

- ▶ 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.
- ▶ It is unidirectional. These waves move in the unidirectional from the sender to the receiver. This means that it can send and receive those waves which have required the alliance.
- ▶ Micro-waves are mostly used in unicast communication
- ▶ These are majorly used for mobile phone communication and television distribution.

Infrared wave

- ▶ Infrared waves are used for very short distance communication. They cannot penetrate through obstacles.
- ▶ This prevents interference between systems. Frequency Range: 300GHz - 400THz.
- ▶ It is used in TV remotes, wireless mouse, keyboard, printer.
- ▶ Characteristics :-
 - ▶ It supports high bandwidth, and hence the data rate will be very high.
 - ▶ Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
 - ▶ An infrared communication provides better security with minimum interference.
 - ▶ Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Satellites :

- ▶ A satellite is an object that revolves around another object. For example, earth is a satellite of The Sun, and moon is a satellite of earth.
- ▶ A **communication satellite** is a **microwave repeater station** in a space that is used for telecommunication, radio and television signals.
- ▶ The satellites **receive** and **retransmit** the signals back to earth where they are received by other earth stations in the coverage area of the satellite.
- ▶ **Satellite's footprint** is the area which receives a signal of useful strength from the satellite.
- ▶ **Uplink frequency** is the frequency at which ground station is communicating with satellite. The satellite transponder converts the signal and sends it down to the second earth station, and this is called **Downlink frequency**.
- ▶ The satellite frequency bands which are commonly used for communication are the **C band**, **Ku-band**, and **Ka band**

Advantages and Disadvantages of Satellite

- ▶ The **advantages** of satellite include the following:
 - ▶ Access to remote areas
 - ▶ Coverage of large geographical areas
 - ▶ Insensitivity to topology
 - ▶ Distance-insensitive costs
 - ▶ High bandwidth
- ▶ The **disadvantages** of satellite include the following:
 - ▶ High initial cost
 - ▶ Propagation delay with GEO systems
 - ▶ Environmental interference problems
 - ▶ Licensing requirements
 - ▶ Regulatory constraints in some regions
 - ▶ Danger posed by space debris, solar flare activity, and meteor showers

Nepal Institute of
Engineering