CST 303 COMPUTER NETWORKS

MODULE 1

.

Computer network/data network: A network can be defined as a group of computers and other devices connected in some way so as to be able to exchange data. A network allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes (data links). These data links are established over cable mediasuch as wires or optic cables, or wireless media such as Wi-Fi. Each of the devices on the network can be thought of as a node, each node has a unique address.

Advantages of Computer Networking

Some of the main advantages of Computer Networking are discussed below:

1. Ease of accessibility

Computer networks provide easy accessibility to resources, information, and online services from anywhere. Users can work remotely, access educational resources, and retrieve personal files. Communication and collaboration are seamless through email, instant messaging, and video conferencing. Resources can be shared and distributed, reducing costs and enabling efficient utilization. Modern computer networks are easy to explore. So, even if you are a kid or a person new to technology, you'll find it easy to connect.

2. Flexibility

Here, flexibility means that different people will be able to explore different things as per their requirements. For this purpose, computer networks provide you with a wide array of choices to share a particular piece of information. For example, e-mail or messaging apps like WhatsApp.

3. Convenient resource sharing

The main aim of a computer network is to enable sharing of resources among its users. You can use resources such as printers, scanners and photocopy machines that can be shared across multiple users. This resource sharing is important for big companies as they can use one single common network to connect with their employees.

4. Connectivity

Computer networks improve connectivity irrespective of a person's location. The pandemic brought this advantage to the forefront, with people regularly using video call apps like Zoom or Google Documents to connect with their friends and colleagues.

5. Security

Computer networks provide security through authorization. Authorization is done via user ID and password. So, it ensures that when we log in, we are only able to do it when there is a perfect match between our details and the details stored in the database.

6. Great storage capacity

Organizations have an abundance of data that needs to be stored. For that purpose, they are required to store them in a central server. A central server is a remote server that is accessible to every employee. So, if in case one loses the data, others have it.

7. Reduced cost

Cost is one of the crucial factors that one needs to consider while evaluating the pros and cons of a particular technology. In networking, a central server is used that enables companies to store files in one place, thus reducing file storage expenses.

8. Enhanced Collaboration

With a computer network, individuals can easily share files, documents, and information with each other, making it easier to work together on projects and tasks. This can lead to increased productivity and efficiency in the workplace. Additionally, computer networks often include communication tools such as email and instant messaging, allowing for real-time communication and collaboration regardless of physical location. Overall, computer networks facilitate seamless collaboration and teamwork.

Disadvantages of Computer Networks

While computer networks aid our work, they also come with their own set of disadvantages such as:

1. Lack of robustness

Computer networks rely on the main server called the central server. If the central server malfunctions or there is an issue in the central server, then the entire network will stop functioning. So, this is a major disadvantage due to dependency on a single server.

2. Spread of computer virus

As computers in a network are interconnected, there is a high probability that if one of the computers is affected by the virus, others too can get affected. This spread can actually damage the entire system. Also, if the central server gets corrupted, then it's quite dangerous as the network depends on the central server.

3. Costly to set-up and maintain

While computer networks save costs in terms of resource sharing and data storage, they also incur considerable implementation costs. Moreover, maintaining computer networks is a costly and time-consuming affair.

4. Lack of productivity

Since a network has a lot of advantages and applications, it certainly results in the simultaneous use of many services that cause distraction. Thus, due to employees focusing on a myriad of tasks, productivity issues are quite common.

5. Health issues

Computer network provides access to a gamut of services including entertainment, gaming, and movies. These result in making you addicted to the content and thus result in overuse of these services. This excessive screen time makes you feel lethargic and causes eye strain and body pain.

6. Lowers the ability to retain and analyze information

With computer networks storing vast amounts of data and processing basic requests in a fraction of the time, people are losing the ability to retain important information. Even processing basic information is a task, as individuals are becoming increasingly dependent on computer networks to do these tasks for them.

7. Unauthorized access

When multiple devices are connected to a network, there is a greater potential for unauthorized access and data breaches. Hackers can exploit vulnerabilities in the network infrastructure or gain access to sensitive information through one compromised device. This can lead to the theft of personal or confidential data, financial loss, and damage to the reputation of individuals or organizations. To mitigate this risk, network administrators must implement robust security measures, such as firewalls, encryption, and regular software updates, to protect the network and its connected devices from cyber threats.

USES OF COMPUTER NETWORK

1. **Communication:** Through computer networks individuals and organizations can collaborate using communicational channels that may include email, chat, and video conferencing.
2. **Resource sharing:** These bags are a boon to users since they provide a way to share the printer, scanner, and files, which will help to improve work activities and reduce costs.
3. **Remote access:** Network technologies bring the power of information and assistance by making it accessible from anywhere on the globe. Hence, this enables users to operate with more freedom and comfort.
4. **Collaboration:** Networks function to make collaboration gin and tonic by offering the opportunities to work jointly on something, share thoughts, and critique in the biggest way.
5. **E-commerce:** Online sales and payments processing are empowered with the computer networks, that enable businesses to sell products online and execute secure payments.

6. **Education:** From their use in the educational setting they are employed to provide a basis for distance learning, access to resources of higher education and give opportunity for collaboration among students and teachers.
7. **Entertainment:** Networks are applied to matters of entertainment like online gaming, online film and music streaming, and social networking.

NETWORK HARDWARE

Network hardware is a set of physical or network devices that are essential for interaction and communication between hardware units operational on a computer network. These are dedicated hardware components that connect to each other and enable a network to function effectively and efficiently. Examples of network hardware include:

1. Routers: Connects two or more networks
2. Switches: Connects multiple devices within a network
3. Network Interface Cards (NICs)
4. Wireless Access Points (APs): Connects a wired device to wireless device
5. Network cables (e.g., Ethernet cables)
6. Gateways: Connects one LAN to WAN/MAN/Internet
7. Hubs: Connects multiple devices within a network
8. Bridges: multiport repeater

There are two types of transmission technology that are in widespread use. They are as follows:

- Broadcast links
- Point to point links

Broadcast networks have a single communication channel that is shared by all the machines on the network. Packets sent by any machine are received by all the others. Address filed within the packet specifies intended recipient. upon receiving machine checks address fields. If the packet is intended for receiving machine it processes the packet else ignore it.

Broadcasting

Possibility of addressing the packet to all destinations by using special code in address field. It is received and processed by every machine on the network.

Multicasting

source node wants to send messages to some subset of other nodes, but not all of them. An example of wireless network WIFI point-point network consists of many connections between

individual pairs of machines. To go from source to destination, packet have to visit one or more intermediate machines.

smaller, geographically localized network tend to use broadcasting whereas larger networks usually are point-point.

Unicasting

Point-point transmission with one sender and one receiver.

Point-to-point networks consist of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Machine are received by all the others.

Types of computer network

- **Personal Area Network (PAN)**

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building.These types of networks are typically found in small offices or residences and are managed by one person or organization from a single device.

Eg : Bluetooth embedded headphones, USB, PDA

- **Local Area Network (LAN)**

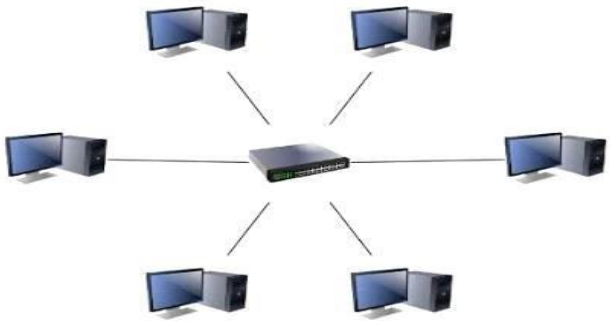
Privately owned networks within single building. They are widely used to connect PC and workstations in company offices and factories to share resources and exchanges information. LANS are distunguished from other kinds of network by three characteristics:

1. Size 2. Transmission technology 3. Topology

- Lans are restricted in size. This simplifies network management.
- Speed varies from 10 Mbps to 100 Mbps

- Uses category five cable for connection
- Two broadcast network-bus and ring
- IEEE 802.3 is the standard for LAN

LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs



LAN (Local Area Network) links the devices in local areas such as in your campus, building etc. It provides useful way of sharing resources such as printer &scanner, sharing of file server.

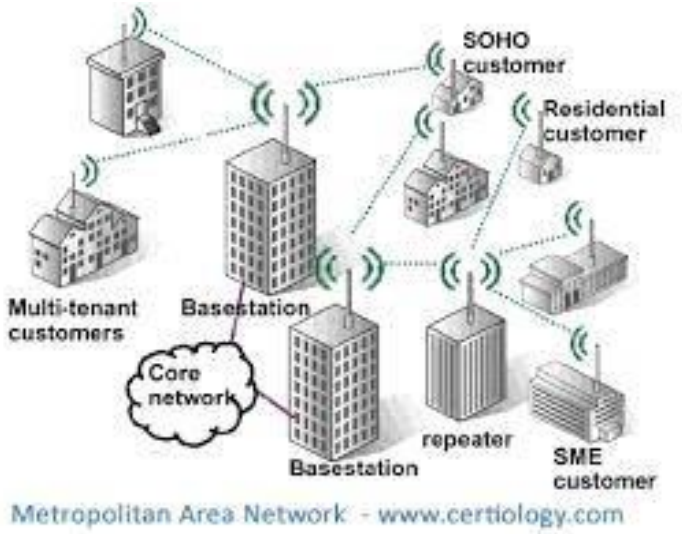
- **Wireless Local Area Network (WLAN)**

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

- **Metropolitan Area Network (MAN)**

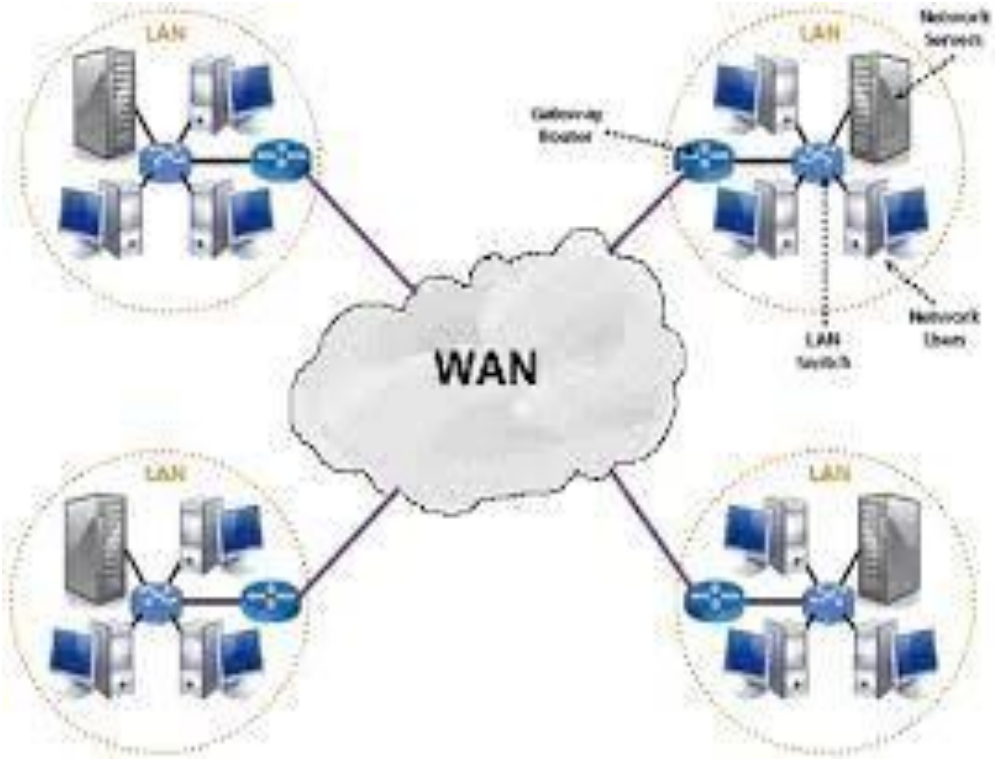
These types of networks are larger than LANs but smaller than WANs

– and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.). MAN covers a particular tower or large city. It exceeds to 32 to 40 km or 20 to 25 miles. Multiple LAN connected to form LAN. MAN provides uplink for LAN to WAN. They providefaster communication using optic cable. The backbone of MAN is high capacity &high- speed fibre optics.



- **Wide Area Network (WAN)**

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart. WAN covers a particular country. A WAN connects small network LAN & MAN.A computer user in one location can communicate with computer user in other location. It connects more than one LAN'S. It is used for large geographical area. It is active larger than 30miles.



BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More

HOME NETWORKS

Also known as Home Area Networks. This is a type of computer networks that facilitates communication among devices within a small area of home. It is a small sized LAN.

INTERNETWORKS

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfilment of this desire requires that different, and frequently incompatible networks, be connected, sometimes by means of machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or internet. An internetwork is formed when distinct networks are interconnected. Internetworking is the practice of connecting a computer through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks is called an internetwork. The most notable example of internetworking is the internet, a network of networks based on many underlying hardware technologies, but unified by an internetworking

protocol standard, the internet protocol suite, often also referred to as TCP/IP.

NETWORK SOFTWARE

Network software is the group of software used for design, operation, monitoring and implementation of computer networks. Traditional network were hardware base with software embedded. With the invention of SDN(Software Defined Network) the software is separated from hardware.

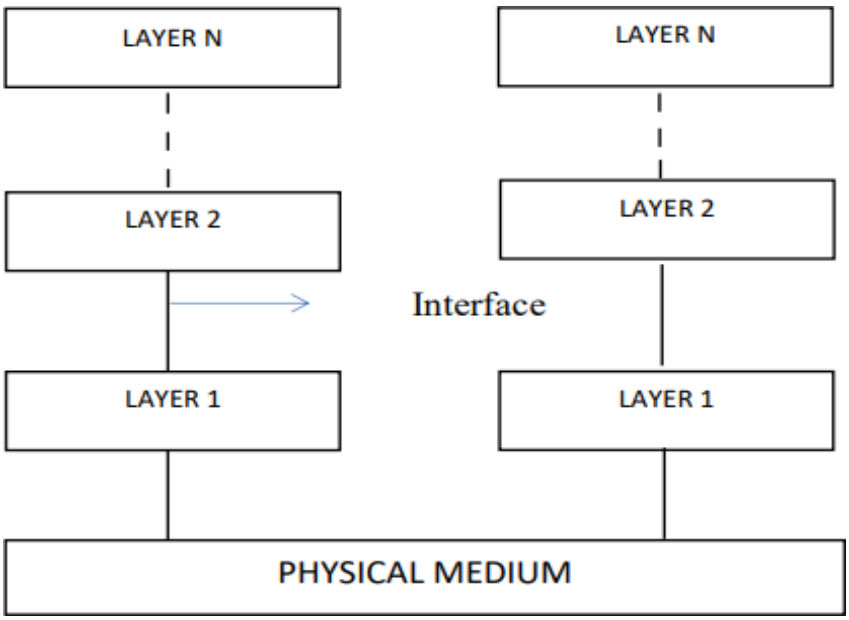
PROTOCOL

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. **A protocol is a set of rules and conventions agreed upon and followed by the communicating entities for data communication.** 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** − Syntax is the format of data which is to be sent or received.
- **Semantics** − Semantics is the meaning of every section of bits that are transferred.
- **Timings** − It refers to the time at which data is transferred as well as the speed at which it is transferred.

PROTOCOL HIERARCHIES

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol.



In order to understand how the actual communication is achieved between two remote hosts connected to the same network, a general network diagram is shown above divided into a series of layers. As it seen later on the on the course the actual number as well as their functionof each layer differs from network to network.

Each layer passes data and control information to the layer below it. As soon as the data are collected form the next layer, some functions are performed there and the data are upgraded and passed to the next layer. This continues until the lowest layer is reached. Actual communication occurs when the information passes layer 1 and reaches the Physical medium. This is shown with the solid lines on the diagram.

Theoretically layer n on one machine maintains a conversation with the same layer in the other machine. The way this conversation is achieved is by the protocol of each layer. Protocol is collection of rules and conventions as agreement between the communication parties on how communication is to proceed. The latter is known as virtual communication and is indicated with the dotted lines on the diagram above.

Layer n of one machine carries a conversion with the layer n of another machine. The rules andconversion are collectively known as protocol. Entities comprising layers of different machine is called peer process.

The data and information is passed by each layer to the lower layer. When the lower layer is reached it is passed to the physical medium which actual communication occurs. Between the pair of adjacent layer their lies the interface. The interface defines which type of services the lower layer offers to the upper layer.

Protocols are together called ***protocol stack*** or set of protocols.

As far as the above diagram is concerned another important issue to be discussed is the interface between each layer. It defines the services and operation the lower layer offers to the one above It. When a network is built decisions are made to decide how many layers to be included and what each layer should do. So each layer performs a different function and as a result the amount of information past from layer to layer is minimized.

Design issues for a layer

1. Reliability

Reliability is a cornerstone design issue in computer networks. Networks are composed of various components, and some of these components may be inherently unreliable, leading to potential data loss during transmission. Ensuring that data is transferred without distortion or corruption is paramount. *Robust error detection and correction mechanisms* are essential for preserving data integrity, especially in the face of unreliable communication channels.

2. Addressing

Addressing is a fundamental aspect of network layers. In a network, numerous processes run on multiple machines, and each layer requires a mechanism to identify both senders and receivers accurately. Effectively assigning and managing addresses helps facilitate efficient communication, ensuring that data reaches its intended destination

3. Error Control

The inherent imperfections in physical communication circuits necessitate error control as a vital design issue. To safeguard data integrity, error-detecting and error-correcting codes are employed. However, it's imperative that both the sending and receiving ends reach a consensus on the specific error detection and correction codes to be used, ensuring effective data packet protection.

4. Flow Control

Maintaining an equilibrium between data senders and receivers is essential to prevent data loss due to speed mismatches. A fast sender transmitting data to a slower receiver necessitates the implementation of a flow control mechanism. Several approaches are used, such as **increasing buffer sizes at receivers or slowing down the fast sender.** Additionally, the network should handle processes that cannot accommodate arbitrarily long messages by disassembling, transmitting, and reassembling messages as required.

5. Multiplexing and De-multiplexing

Efficient data transmission on a network often involves transmitting data separately on the transmission medium. Setting up separate connections for every pair of communicating processes is neither practical nor cost-effective. To address this challenge, multiplexing is employed at the sender's end, allowing data from multiple sources to be combined into a single transmission stream. De-multiplexing is then performed at the receiver's end to separate and direct the data to the appropriate recipients.

6. Scalability

As networks expand in size and complexity, new challenges inevitably arise. Scalability is crucial to ensuring that networks can continue to function effectively as they grow. The network's design should accommodate increasing sizes, reducing the risk of congestion and compatibility issues when new technologies are introduced. Scalability is a cornerstone for ensuring the network's long-term viability.

7. Routing

Routing is a critical function within the network layer. When multiple paths exist between a source and destination, the network must select the most optimal route for data transmission. Various routing algorithms are utilized to make this determination, with the aim of minimizing cost and time, thereby ensuring efficient and reliable data transfer.

8. Confidentiality and Integrity

The security of a network is critical. Confidentiality methods are critical for protecting against risks like eavesdropping and preventing unauthorized parties from accessing sensitive data. Data integrity is also crucial since it protects against tampering and unauthorized changes to messages during transmission.

9. Service Quality (QoS):

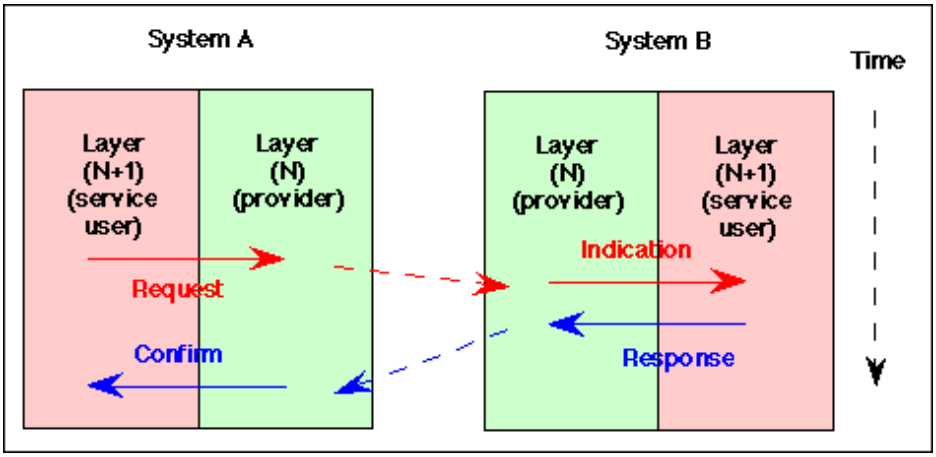
QoS refers to a network's ability to deliver varying levels of service to different types of traffic. Video streaming, VoIP, and data transmission all have varying bandwidth, latency, and reliability needs. It is a difficult challenge to ensure that the network can prioritize and distribute resources effectively to satisfy these objectives.

10. Network management:

Network management includes monitoring and maintaining the health and performance of different network components such as routers, switches, and servers. Device configuration, fault detection, performance analysis, and security monitoring all need network management tools and

protocols. Effective network administration is critical for detecting and resolving problems in real time, optimizing resource utilization, and maintaining a positive user experience.

Service Primitives : Each protocol which communicates in a layered architecture communicates in a peer to peer manner with its remote protocol entity. Communication between adjacent protocol layers (i.e. within the same communications node) are managed by calling functions, called Primitives, between the layers. A service is formally specified by a setof primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer .



There are various types of actions that may be performed by primitives. Examples of primitivesinclude: Connect, Data, FlowControl, and Disconnect.

Some of the services are:

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Each primitive specifies the action to be performed or advises the result of a previously requested action. A primitive may also carry the parameters needed to perform its functions. One parameter is the packet to be sent/received to the layer above/below (or, more accurately, includes a pointer

to data structures containing a packet, often called a "buffer").

There are four types of primitive used for communicating data. The four basic types of primitive are :

Request : A primitive sent by layer (N + 1) to layer N to request a service. It invokes the service and passes any required parameters.

Indication : A primitive returned to layer (N + l) from layer N to advise of activation of a requested service or of an action initiated by the layer N service.

Response : A primitive provided by layer (N + 1) in reply to an indication primitive. Itmay acknowledge or complete an action previously invoked by an indication primitive.

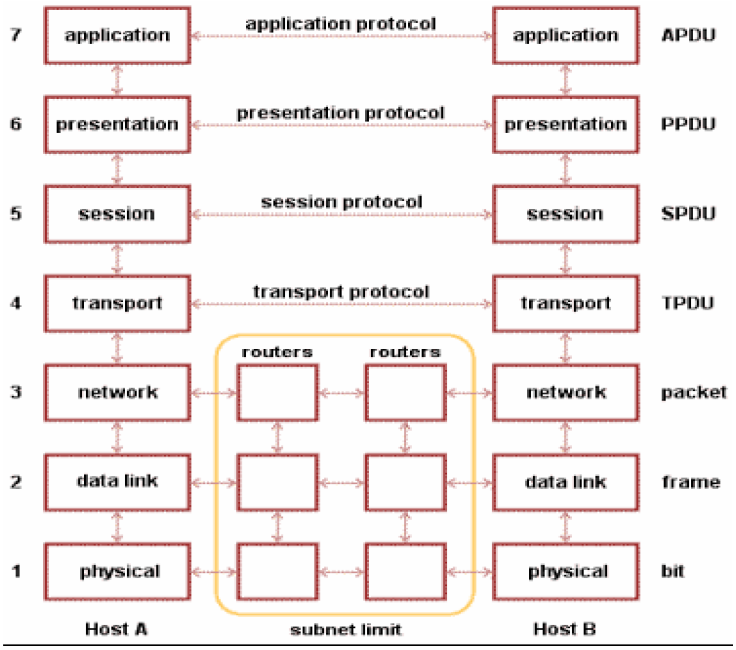
Confirm : A primitive returned to the requesting (N + l) st layer by the Nth layer to acknowledge or complete an action previously invoked by a request primitive.

To send Data, the sender invokes a Data. Request specifying the packet to be sent, and the Service Access Point (SAP) of the layer below. At the receiver, a Data. Indication primitive is passed up to the corresponding layer, presenting the received packet to the peer protocol entity.

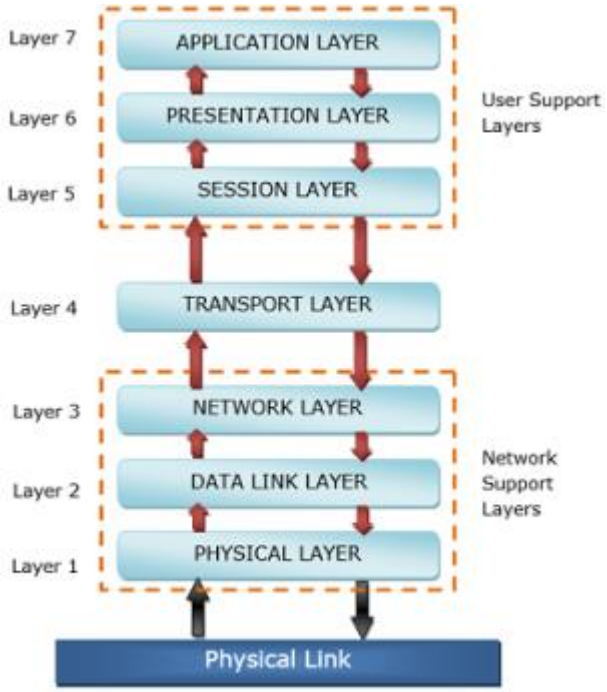
REFERENCE MODELS

1. OSI MODEL 2. TCP/IP MODEL

OSI REFERENCE MODEL



OSI or Open System Interconnection model was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer, as shown in the following diagram



The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups.

The main functions of each of the layers are as follows −

- **Physical Layer** − Its function is to transmit individual bits from one node to another over a physical medium.
- **Data Link Layer** − It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
- **Network Layer** − It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
- **Transport Layer** −It is responsible for delivery of the entire message from the source host to destination host.
- **Session Layer** − It establishes sessions between users and offers services like dialog control and synchronization.

- **Presentation Layer** − It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
- **Application Layer** − It provides high-level APIs (application program interface) to the users.

Physical Layer

The Physical Layer is the lowermost layer in the OSI model and its major responsibility includes the actual propagation of the unstructured data bits (0's and 1's) across the network, from the physical layer of the sending device to the physical layer of the receiving device. The Physical layer contains information in the form of bits. It transmits individual bits from one node to the next node. The transmission media defined by the physical layer include metallic cable, optical fibre, and the wireless radio-wave.

Data Link Layer

It is the second layer of the OSI model. The data link layer is responsible for providing error-free communication across the physical link connecting the primary and secondary nodes within a network. It provides hop-to-hop delivery. It packages the data from the physical layer into a group called blocks. The data link layer provides the final framing of the information signal, and it provides synchronization facilities for the orderly flow of data between the nodes.

Main functions are

- **Framing** − Breaks messages into frames and reassembles frames into messages.
- **Error handling** − It is used to soles the damaged, lost, and duplicate frames.
- **Flow Control** − It keeps a fast transmitter from flooding a slow receiver.

Network Layer

The network layer provides details that enable data to be routed between devices in an environment using multiple networks, sub-networks, or both. The networking components that operate at the network layer include routers and their software. It determines which network configuration is most appropriate for the function provided by the network and addresses and routes data within a network by establishing, maintaining, and terminating connectors between them. The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP , ARP & RARP etc

Transport Layer

We can say that the transport layer controls and ensures the end-to-end integrity of the data message propagated through the network between two devices, providing the reliable, transparent transfer of data between the endpoints. The protocol used in this layers are TCP, UDP & SCTP etc

Main functions are

- **Segmentation and Reassembly** − In this, a message is divided into small pieces. Reassemble the message correctly upon arriving at the destination.
- **Reliability** − It ensures that packets arrive at their destination. Reassembles out-of-order messages.
- **Service Decisions** − It is used to check what types of service to provide error-free point-to-point, datagram, etc.
- **Mapping** − It determines which messages belong to which connections.

Session Layer

The session layer creates communication channels between devices. It is responsible for opening sessions, ensuring they remain open and functional while the data is being transferred, and close the session when the communication ends. The session layer can also set checkpoints during a data transfer. If a session is interrupted, then the devices can resume data transfer from the last checkpoint. The protocols used in this layer are SSH and RPC etc.

Presentation Layer

The presentation layer prepares the data for its upper layer or the application layer. It defines how two devices should encode, encrypt, and compress the data. The presentation layer receives any data transmitted by the application layer and prepares it for transmission over the session layer.
It specifies how the end-user applications should format the data. Presentation layer protocols are SSL, TSL etc.

Application Layer

The application layer is the topmost layer in the OSI model and acts as the general manager of the network by proving access to the OSI environment. This layer provides distributed information services and controls the sequence of activities within an application and also the sequence of events between the computer application and the user of the application. It communicates directly with the user's application program. The application layer uses HTTP, FTP, POP, SMTP, and DNS protocols that allow the software to send and receive information and present meaningful data to users

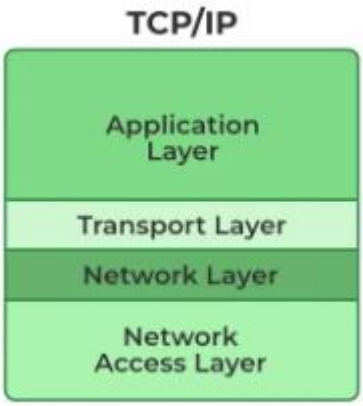
Application Layer

The application layer is the topmost layer in the OSI model and acts as the general manager of the network by proving access to the OSI environment. This layer provides distributed information services and controls the sequence of activities within an application and also the sequence of events between the computer application and the user of the application. It communicates directly with the user's application program.

The application layer uses HTTP, FTP, POP, SMTP, and DNS protocols that allow the software to send and receive information and present meaningful data to users.

TCP/IP REFERENCE MODEL

The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers: the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks. TCP/IP was designed and developed by the Department of Defense (DoD) ie ARPANET in the 1960s and is based on standard protocols.



APPLIATION LAYER

This is the topmost layer which indicates the applications and programs that utilize the TCP/IP model for communicating with the user through applications and various tasks performed by the layer, including data representation for the applications executed by the user and forwards it to the transport layer. The application layer maintains a smooth connection between the application and user for data exchange and offers various features as remote handling of the system, e-mail services, etc. Some of the protocols used in this layer are:

- HTTP: Hypertext transfer protocol is used for accessing the information available on the internet.
- SMTP: Simple mail transfer protocol, assigned the task of handling e-mail-related steps and issues.

- FTP: This is the standard protocol that oversees the transfer of files over the network channel.

TRANSPORT LAYER

This layer is responsible for establishing the connection between the sender and the receiver device and also performs the task of dividing the data from the application layer into packets, which are then used to create sequences.

It also performs the task of maintaining the data, i.e., to be transmitted without error, and controls the data flow rate over the communication channel for smooth transmission of data.

The protocols used in this layer are:

- TCP: Transmission Control Protocol is responsible for the proper transmission of segments over the communication channel. It also establishes a network connection between the source and destination system.
- UDP: User Datagram Protocol is responsible for identifying errors, and other tasks during the transmission of information.

UDP maintains various fields for data transmission such as:

- Source Port Address: This port is responsible for designing the application that makes up the message to be transmitted.
- Destination Port Address: This port receives the message sent from the sender side.
- Total Length: The total number of bytes of the user datagram.
- Checksum: Used for error detection of the message at the destination side.

INTERNET LAYER

The Internet layer performs the task of controlling the transmission of the data over the network modes and enacts protocols related to the various steps related to the transmission of data over the channel, which is in the form of packets sent by the previous layer.

This layer performs many important functions in the TCP/IP model, some of which are:

1. It is responsible for specifying the path that the data packets will use for transmission.
2. This layer is responsible for providing IP addresses to the system for the identification matters over the network channel.

Some of the protocols applied in this layer are:

1. IP: This protocol assigns your device with a unique address; the IP address is also responsible for routing the data over the communication channel.

2. ARP: This protocol refers to the Address Resolution Protocol that is responsible for finding the physical address using the IP address.

NETWORK ACCESS LAYER

This layer is the combination of data-link and physical layer, where it is responsible for maintaining the task of sending and receiving data in raw bits, i.e., in binary format over the physical communication modes in the network channel.

- It uses the physical address of the system for mapping the path of transmission over the network channel.

COMPARISON BETWEEN OSI AND TCP/IP REFERENCE MODEL

OSI	TCP/IP
The OSI model consists of 7 layers.	TCP/IP model comprises 4 layers.
The OSI model has separate session and presentation layers.	This model comprises a session and presentation layer in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model.	It is an implemented model of an OSI model.
It is low in usage	It is mostly used
It is vertically approached	It is horizontally approached
Replacement of tools and changes can easily be done in this model	Replacing the tools is not easy as it is in OSI Model
It is less reliable than TCP/IP Model	It is more reliable than OSI Model
In the OSI model, the network layer provides connection-oriented and connectionless services.	In this model, the network layer provides only connectionless service.

DATA COMMUNICATIONS

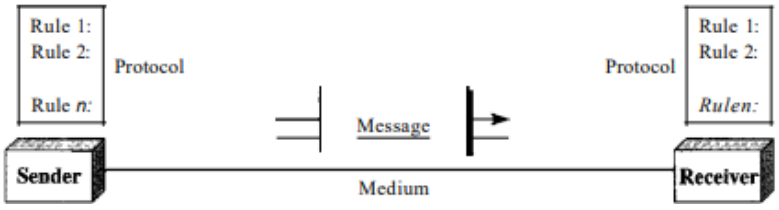
When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (teleis Greek for "far"). The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. 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 a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

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

COMPONENTS

A data communications system has five components

Figure 1.1 *Five components ofdata communication*



1. **Message**. The message is the information (data) to be communicated. Popularforms of information include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** The transmission medium is the physical path by whicha message travels from sender to receiver. Some examples of transmission mediainclude twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves
5. **Protocol.** A protocol is a set of rules that govern data communications. It represents anagreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking Frenchcannot be understood by a person who speaks only Japanese.

DATA FLOW(MODES OF COMMUNICATION)

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1

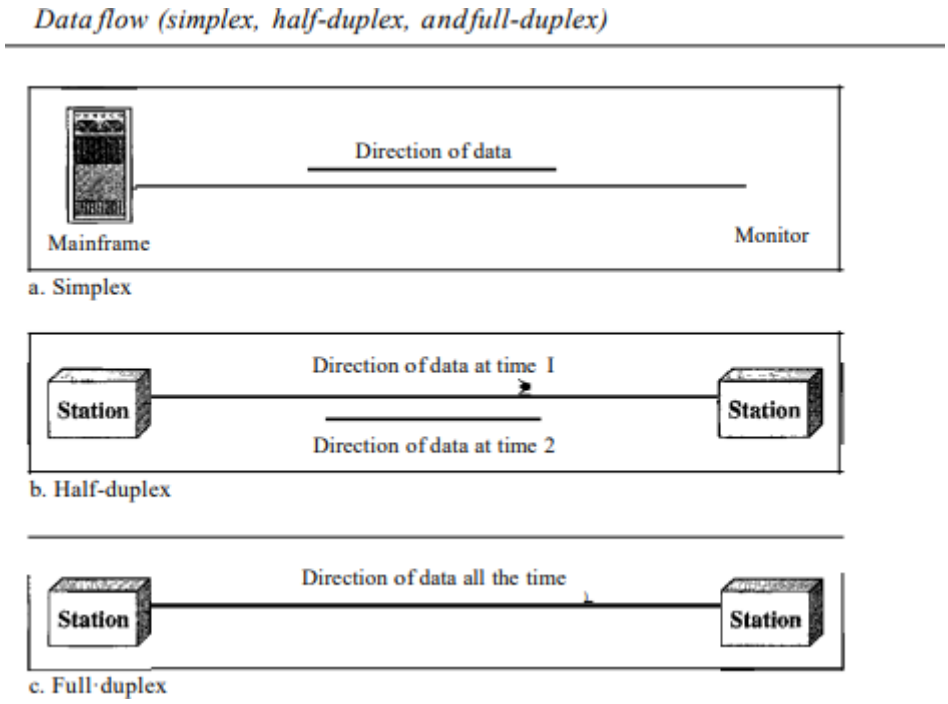


Figure 1

Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.a). Keyboards and

traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both direction at the same time; the entire capacity of the channel can be utilized for each direction.

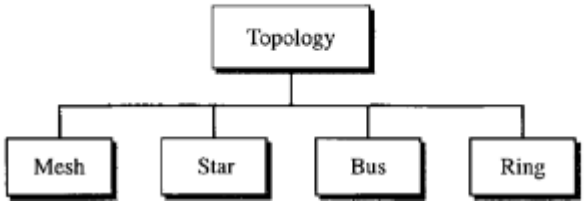
Full-Duplex

In full-duplex both stations can transmit and receive simultaneously (see Figure 1 c). The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. In full-duplex mode, signals s going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

PHYSICAL TOPOLOGY

The term physical topology refers to the way in which a network is laid out physically.: Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Categories of topology

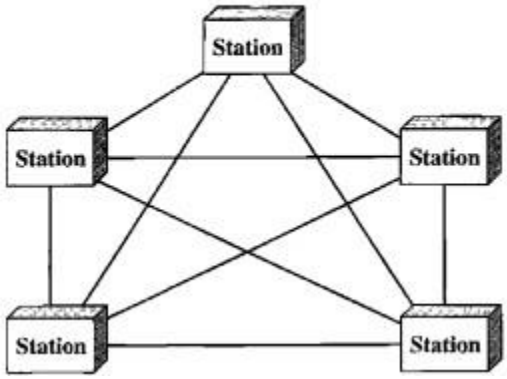


There are four basic topologies possible: mesh, star, bus, and ring

MESH

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

A fully connected mesh topology (five devices)



To accommodate that many links, every device on the network must have n - 1input/output (VO) ports to be connected to the other n - 1 stations.

A mesh offers several advantages over other network topologies.

- First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other usersfrom gaining access to messages.
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

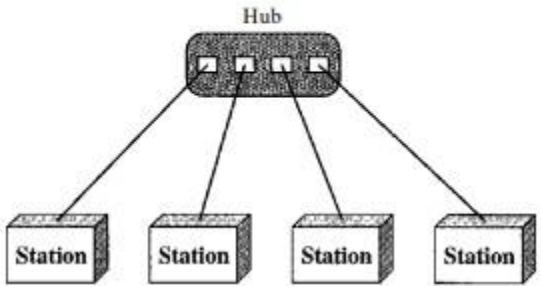
One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlikea mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .

- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation.
- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies(such as ring or bus).
- High-speed LANs often use a star topology with a central hub.

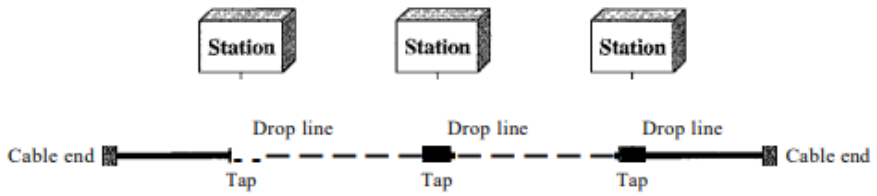
A star topology connecting four stations



Bus Topology

- A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.
- Advantages of a bus topology include ease of installation.
- Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality.

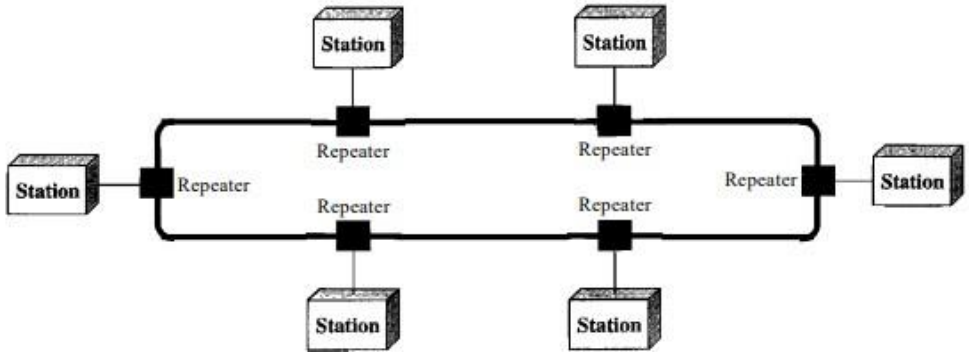
Figure 1.7 *A bus topology connecting three stations*



Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.
- A ring is relatively easy to install and reconfigure. Each device is linked to only itsimmediate neighbors.
- To add or delete a device requires changing only two connections.
- However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring(such as a disabled station) can disable the entire network.

Figure 1.8 *A ring topology connecting six stations*



TRANSMISSION MEDIA

Transmission media refer to the physical pathways through which data is transmitted from one device to another within a network. These pathways can be wired or wireless. The choice of medium depends on factors like distance, speed, and interference. 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.

GUIDED MEDIA

Guided Media 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.

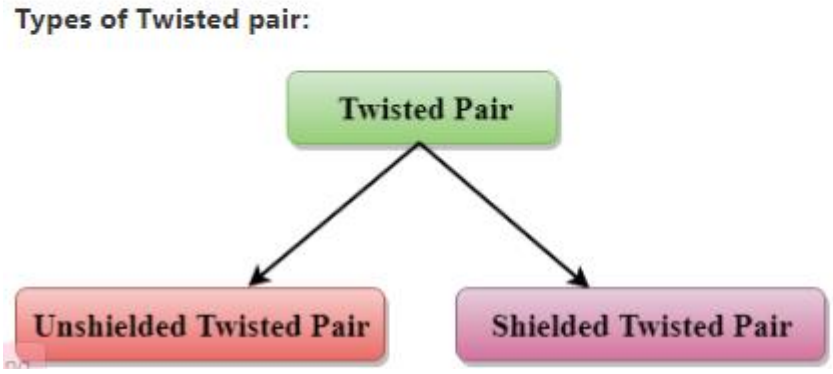
Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

1. Twisted Pair Cable

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz. A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

Category 1: Category 1 is used for telephone lines that have low-speed data.

Category 2: It can support upto 4Mbps.

Category 3: It can support upto 16Mbps.

Category 4: It can support upto 20Mbps. Therefore, it can be used for long-distance communication.

Category 5: It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

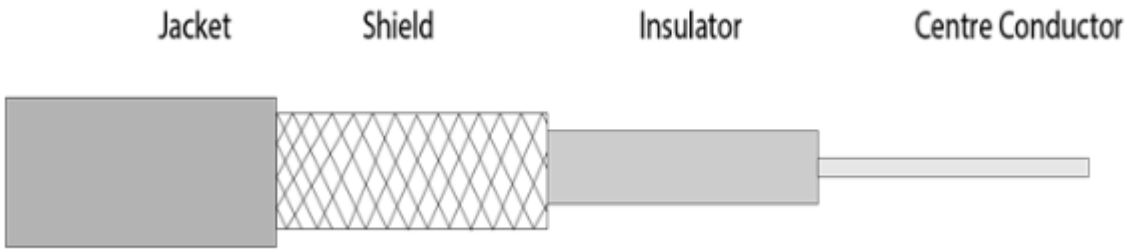
Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

2. <u>Coaxial Cable</u>

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor

from the outer conductor.



Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

3. <u>Fibre Optics</u>

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the

cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.

UNGUIDED TRANSMISSION

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

1. 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 khz.
- 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**

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 wave.

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 the walls.

- Radio transmission provides a higher transmission rate.

2. Microwaves

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task

3. Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- 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.

RADIO WAVES	**MICROWAVES**	**INFRARED**
Omnidirectional	Unidirectional	Unidirectional
Penetrate through objects	Penetrate through objects	Cannot penetrate
Freq range : 3KHz to 1 GHz	Freq range : 1GHz to 300 GHz	Freq range : 300 GHz to 400 GHz
Less security	Medium security	High security
Long distance communication	Long distance communication	Short distance communication
Sending and receiving antenna need not be aligned	Sending and receiving antenna need to be aligned	Sending and receiving antenna need to be aligned

PERFORMANCE INDICATORS

The performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. Finding the performance of a network depends on both quality of the network and the quantity of the network.

Parameters for Measuring Network Performance

- Bandwidth
- Latency (Delay)
- Bandwidth – Delay Product
- Throughput

BANDWIDTH

One of the most essential conditions of a website's performance is the amount of bandwidth allocated to the network. Bandwidth determines how rapidly the webserver is able to upload the requested information.

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices, the bandwidth is measured in bits per second(bps) or bytes per

second. In the case of analog devices, the bandwidth is measured in cycles per second, or Hertz (Hz).

LATENCY

In a network, during the process of data communication, latency(also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination. The network connections where small delays occur are called “Low-Latency-Networks” and the network connections which suffer from long delays are known as “High-Latency-Networks”.

Latency = Propagation Time + Transmission Time + Queuing Time + Processing Delay

Propagation Time

It is the time required for a bit to travel from the source to the destination. Propagation time can be calculated as the ratio between the link length (distance) and the propagation speed over the communicating medium. For example, for an electric signal, propagation time is the time taken for the signal to travel through a wire.

Propagation time = Distance / Propagation speed

Transmission Time

Transmission Time is a time based on how long it takes to send the signal down the transmission line. It consists of time costs for an EM signal to propagate from one side to the other, or costs like the training signals that are usually put on the front of a packet by the sender, which helps the receiver synchronize clocks

Transmission time = Message size / Bandwidth

Queuing Time

Queuing time is a time based on how long the packet has to sit around in the router. Quite frequently the wire is busy, so we are not able to transmit a packet immediately. The queuing time is usually not a fixed factor, hence it changes with the load thrust in the network. In cases like these, the packet sits waiting, ready to go, in a queue. These delays are predominantly characterized by the measure of traffic on the system.

Processing Delay

Processing delay is the delay based on how long it takes the router to figure out where to send the packet. As soon as the router finds it out, it will queue the packet for transmission. These costs are predominantly based on the complexity of the protocol. The router must decipher enough of the packet to make sense of which queue to put the packet in. Typically the lower-level layers of the stack have simpler protocols. If a router does not know which physical port to send the packet to, it will send it

to all the ports, queuing the packet in many queues immediately.

BANDWIDTH – DELAY PRODUCT

Bandwidth and Delay are two performance measurements of a link. However, what is significant in data communications is the product of the two, the bandwidth-delay product.

THROUGHPUT

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio, and hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption. The terms ‘throughput’ and ‘bandwidth’ are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.