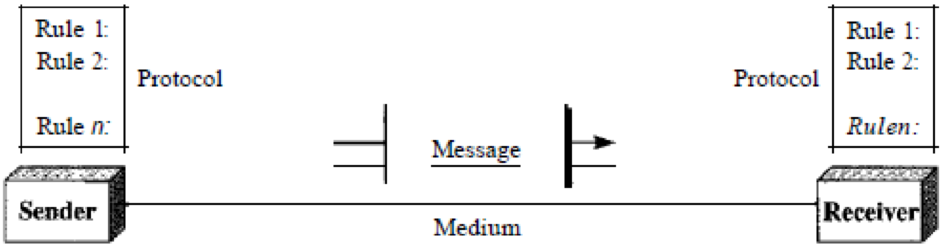
DATA COMMUNICATION AND NETWORK

UNIT-I

Data Communication

Data communications is the process of transferring digital information between two or more devices over a transmission medium. This process involves a communication system which is made of hardware (physical equipment) and software.

The effectiveness of a data communications system depends on four fundamental characteristics: **delivery, accuracy, timeliness, and jitter** (variation in packet arrival time)**.**
A data communications system has five components:



1. Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Examples of transmission media include twisted-pair wire, coaxial cable.

5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices.

Data Flow

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

1. 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

2. 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

3. In **full-duplex** both stations can transmit and receive simultaneously

Computer Network

A **computer network** is a set of interconnected computers. Computers on a network are called **nodes**. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others.

Applications of Networks

Some of the network applications in different fields are the following:

- **Marketing and sales**
- **Financial services**
- **Manufacturing**

Some other Applications:

- **Information Services**
- **Electronic messaging**
- **Electronic data interchange (EDI)**
- **Teleconferencing.**

Types of Connections in Network:

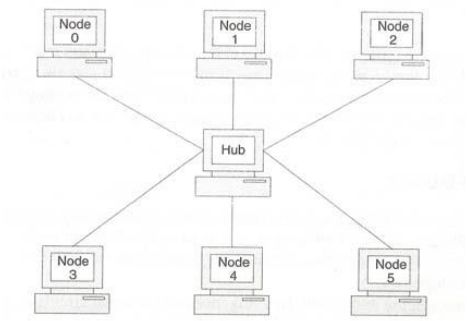
There are two possible types of connections: point-to-point and multipoint.

1. A **point-to-point** connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.
2. A **multipoint** connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared.

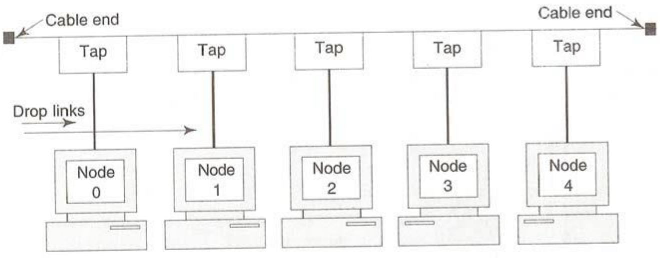
Network Topology:

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

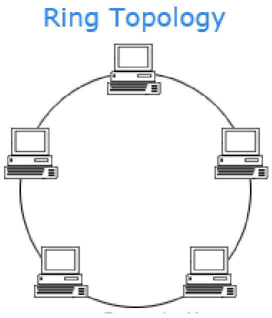
1. In **star topology,** each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which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



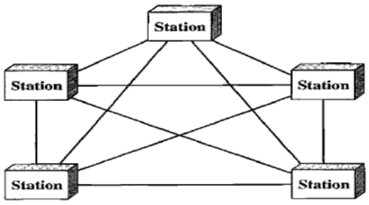
2. A **bus topology** is a multipoint connection. One long cable acts as a backbone to link all the devices in a network. The transmission from any station travels the length of the bus, in both directions, and can be received by another stations.



3. Ring Topology: In this topology, each node is connected to two neighbouring nodes. Data is accepted from one of neighbouring nodes and is transmitted onwards to another. Thus data travels in one direction only. After passing through each node, it returns to the sending node, which removes it.



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



NETWORK HARDWARE

Broadly speaking, there are two types of transmission technology that are in widespread use. They are as follows:

1. Broadcast links.
2. Point-to-point links.

Broadcast links.

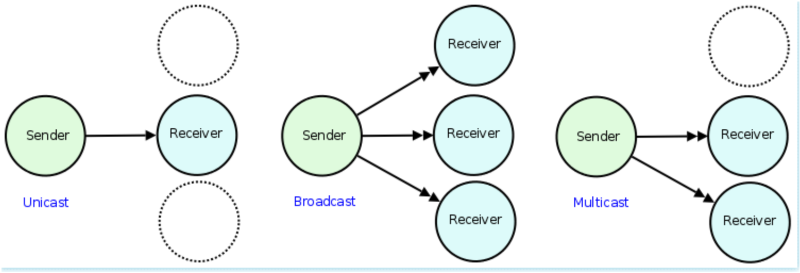
Broadcast networks have a single communication channel that is shared by all the machines on the network. Short messages, called packets in certain contexts, sent by any machine are received by all the others. An address field within the packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

Broadcast systems generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.

Some broadcast systems also support transmission to a subset of the machines known as multicasting. One possible scheme is to reserve one bit to indicate multicasting. Each machine can "subscribe" to any or all of the groups. When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.

Point-to-Point Network

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. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. Point-to-point transmission with one sender and one receiver is sometimes called unicasting.



Types of Network by Scale

1. **Local Area Networks (LAN):** LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.

2. **Metropolitan Area Network (MAN)**: A metropolitan area network covers a city. The best-known example of a MAN is the cable television network available in many cities.

3. **Wide Area Network (WAN):** A wide area network spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs. These machines are called as hosts. The hosts are connected by a communication subnet. The hosts are owned by the customers whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host.

Network Hardware Devices

1. Network Cables

Network cables are the transmission media to transfer data from one device to another. A commonly used network cable is category 5.

2. **Routers**

A router is a connecting device that transfers data packets between different computer networks. Typically, they are used to connect a PC or an organization's LAN to a broadband internet connection.

3. Repeaters, Hubs, and Switches

Repeaters, hubs and switches connect network devices together so that they can function as a single segment.

i. A repeater receives a signal and regenerates it before re-transmitting so that it can travel longer distances.

ii. A hub is a multiport repeater having several input/output ports, so that input at any port is available at every other port.

iii. A switch receives data from a port, uses packet switching to resolve the destination device and then forwards the data to the particular destination, rather than broadcasting it as a hub.

4. **Bridges**

A bridge connects two separate Ethernet network segments. It forwards packets from the source network to the destined network.

5. Gateways

A gateway connects entirely different networks that work upon different protocols. It is the entry and the exit point of a network and controls access to other networks.

6. Network Interface Cards

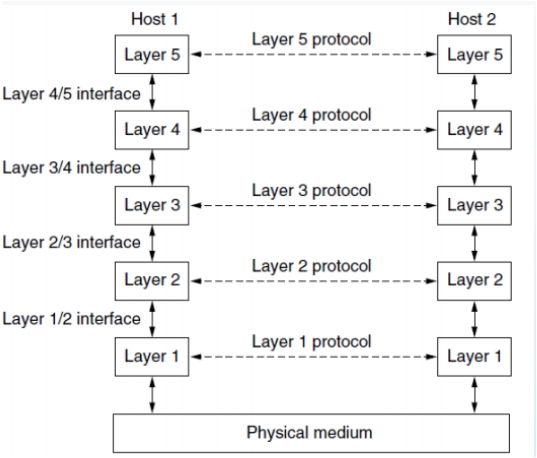
NIC is a component of the computer to connect it to a network. Network cards are of two types: Internal network cards and external network cards.

NETWORK SOFTWARE

Network software is highly structured. The Structuring techniques are given below.

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 layer, the contents of 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. Real data is transferred only at the physical layer.

In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs.

Each pair of adjacent layers is an **interface.** The interface defines which operations and services the lower layer makes available to the upper one.

Design Issues for the Layers

A number of design issues exist for the layer to layer approach of computer networks. They are,

Scalability
Networks sizes are continually increasing leading to congestion. The design should be done so that the networks are scalable and can accommodate to any additions and alterations.

Error Control
Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Flow Control
If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

Routing
There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Security
A major factor of data communication is to defend it against threats like eavesdropping and alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

Connection-Oriented and Connectionless Services

Layers can offer two different types of services namely connection-oriented and connectionless.

1. Connection-oriented service is modelled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases the order is preserved so that the bits arrive in the order they were sent.

2. In **connectionless service** is modelled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive.

Some services are reliable in the sense that they never lose data. Usually, a reliable service is implemented by having the receiver acknowledge the receipt of each message so the sender is sure that it arrived.

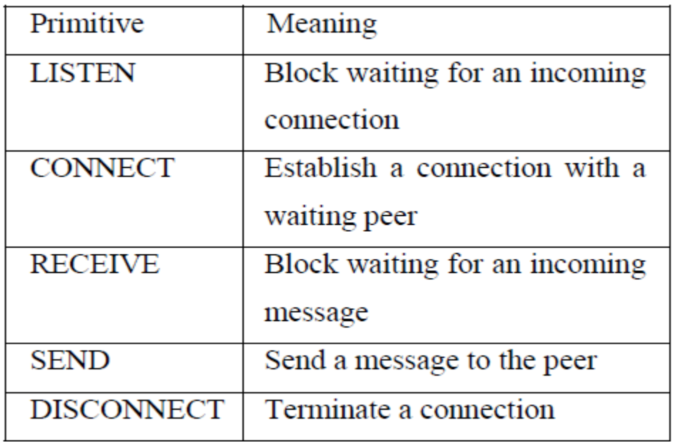
Some Services are Unreliable (meaning not acknowledged) connectionless service is often called datagram service, in analogy with telegram. User Datagram Protocol is an example of unreliable service.

Difference: Connection oriented and Connectionless service

1. In connection oriented service authentication is needed, while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while connectionless service protocol does not guarantees a message delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

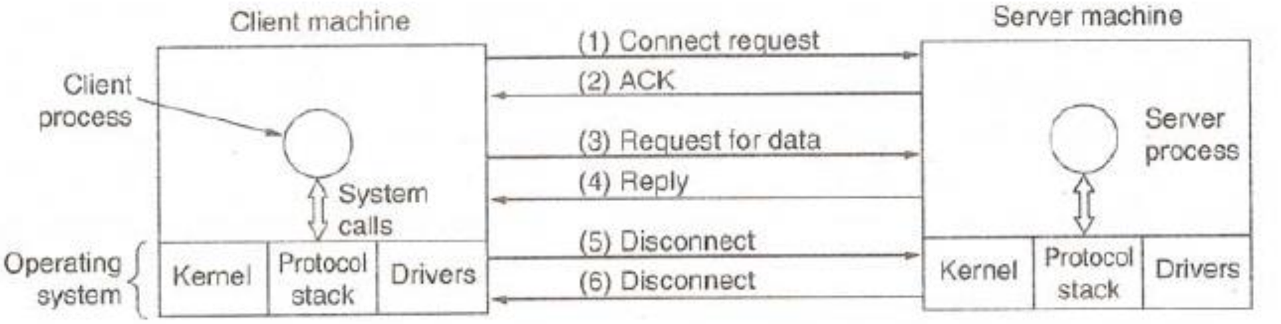
Service Primitives:

The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connectionless service.



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

SERVICE PRIMITIVES



Packets sent in a simple client-server interaction

NETWORK ARCHITECTURE

Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data.

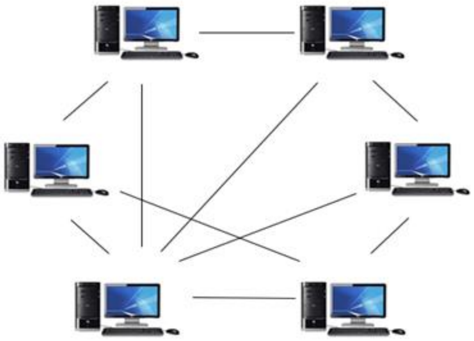
Network Architecture refers to how computers are organized in a network and what are the tasks allocated to the computers. It is also called as set of layers and protocols.

There are two types of Network Architecture:

i. Peer-To-Peer network
ii. 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.

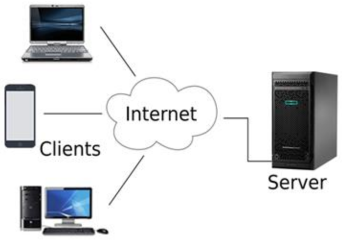


Advantages of Peer-To-Peer Network:

- 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.

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.



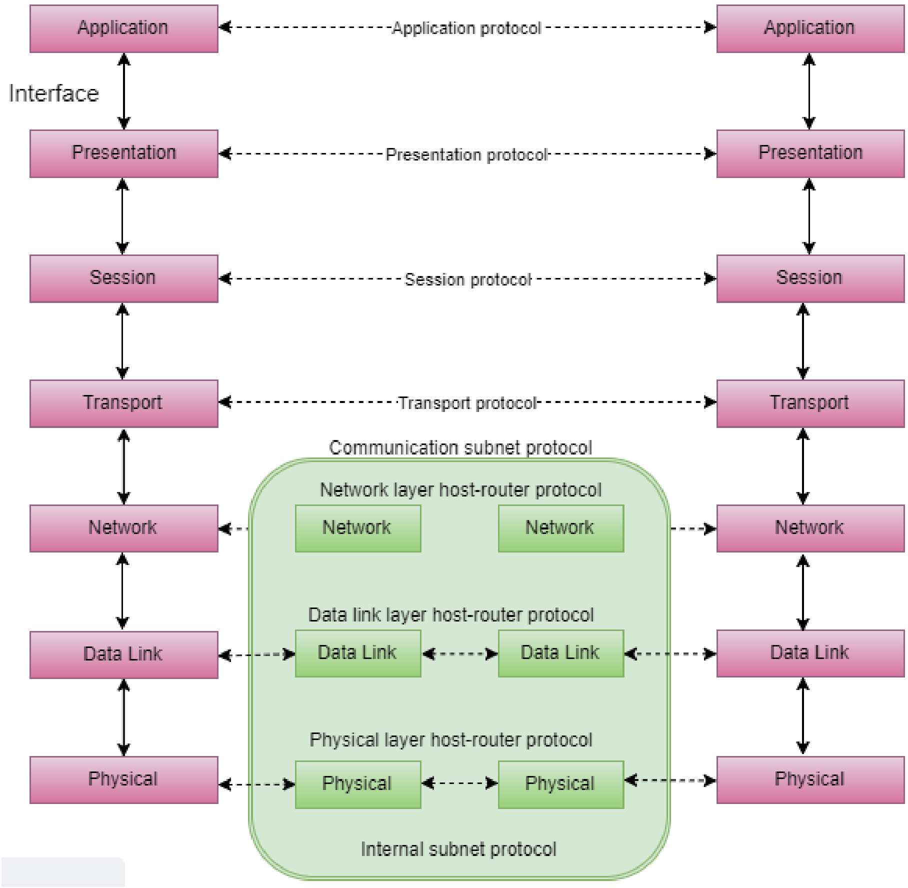
Advantages of Client/Server network:

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

The OSI Reference Model

The OSI (Open Systems Interconnection) Reference Model is a theoretical model because it deals with connecting open systems-that is, systems that are open for communication with other systems.

The OSI is not a protocol. It is a model for understanding and designing network architecture. It is a framework of seven layers that gives idea of functionality of each layer. Each layer has individual functions which differentiates from other layer in the OSI model.



1. Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer.

The main functions of physical layer are Digital transmission, Digital data to Digital Signal conversion and Line coding. Hub, Repeater, Modem, Cables are Physical Layer devices.

2. Data Link Layer

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Switch & Bridge are Data Link Layer devices.

The packet received from Network layer is further divided into frames depending on the frame size of NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header. The main functions are framing, physical addressing and error control.

3. Network Layer

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer. The main functions are routing and logical addressing.

4. Transport Layer

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

The main functions of transport layer includes segmentation, connection oriented and connectionless transmission. Data in the Transport Layer is called as **Segments**. Transport layer is operated by the Operating System.

5. Session Layer

The session layer is responsible to setup and maintain the connection between different systems. The main functions of the layers are Authentication, Authorization and Session management.

6. Presentation Layer

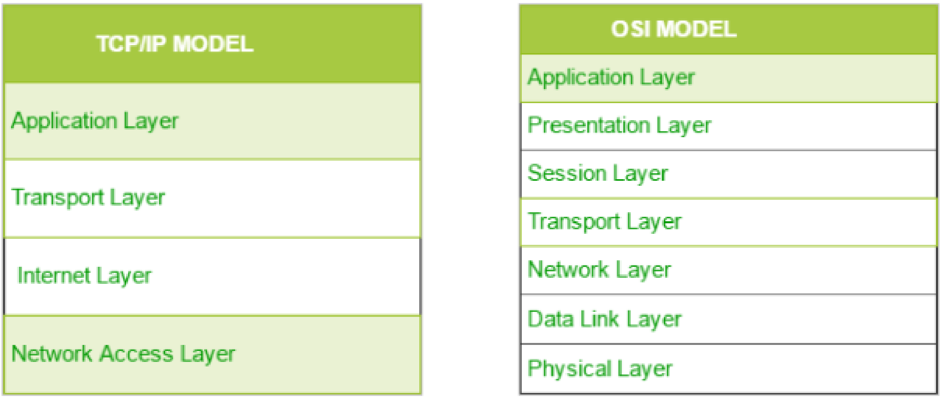
Presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. The main functions of this layer includes Translation, Encryption/Decryption and Compression.

7. Application Layer

Application layer which is implemented by the network applications. Application layer is used by computer applications such as google chrome, outlook, FireFox, Skype etc. It defines the protocols such as HTTP, FTP and SMTP. Application Layer is also called as Desktop Layer.

TCP/IP REFERENCE MODEL

The TCP/IP model was developed prior to the OSI model. But not exactly similar to the OSI model. It is the network model used in the current Internet architecture. The TCP/IP model consists of four layers: Application Layer, Transport Layer, Internet layer, Physical Layer.



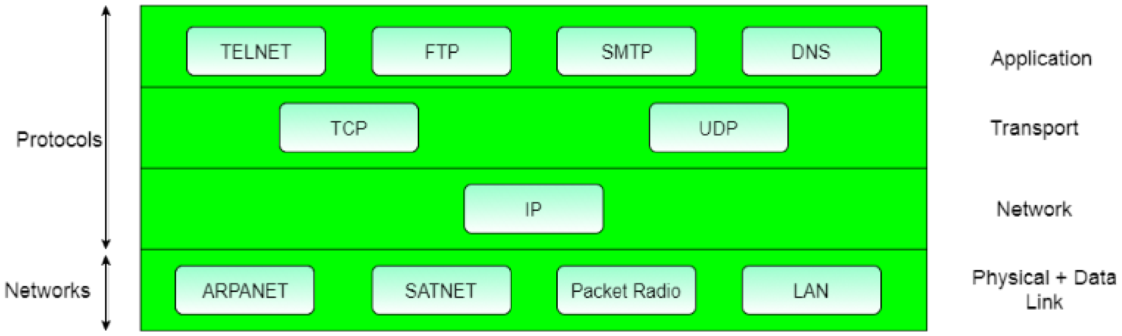
TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Comparison of TCP/IP and OSI models

Network Access Layer

- A network layer is the lowest layer of the TCP/IP model. It 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 and mapping of IP addresses into physical addresses.



Protocols and networks in the TCP/IP model:

Internet Layer

- An internet layer 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.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer to deliver IP packets where they have to reach.
- The various functions performed by the Internet Layer are:
  - Performing routing
  - Avoiding congestion

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.
  - UDP consists of the following fields such as Source port address, Destination port address, total length and checksum
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

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

- 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 is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment
- **SMTP:** The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol (SMTP). 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.
- **FTP:** FTP stands for File Transfer Protocol used for transmitting the files.

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP/IP is more reliable	OSI is less reliable
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

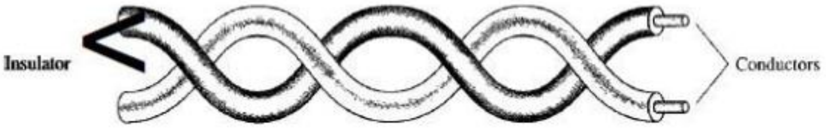
Guided Transmission Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media. It is the Safest and fast medium to transfer the information in a network.

There are different types of guided media through which information is shared. They are given below.

1. Twisted pair cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.



Twisted Pair is of two types:

i. Unshielded Twisted Pair (UTP):

This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications. Advantages are least expensive, Easy to install and High speed capacity.

ii. Shielded Twisted Pair (STP):

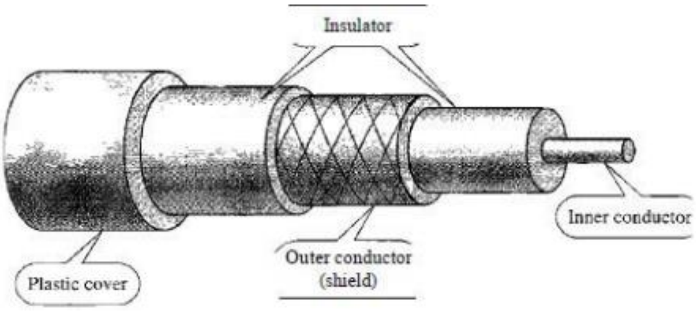
This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines. Advantages are

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

2. Coaxial Cable

Coaxial cable carries signals of higher frequency ranges than 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.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI(Electromagnetic Interference).**
- The outer conductor shield prevents noise and act as the second conductor. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages of Coaxial cable:

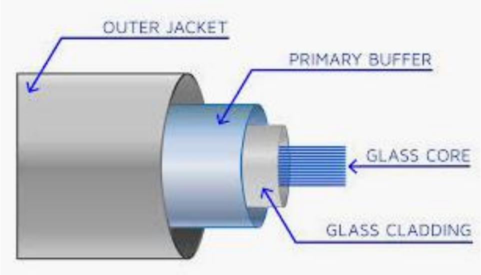
- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages of Coaxial cable:

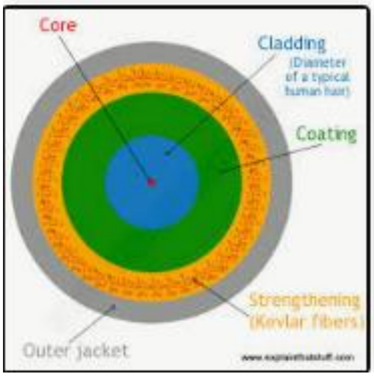
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

3. Fibre Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form 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.



Side View

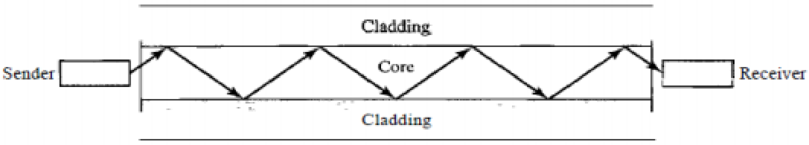

Core
Cladding (Diameter of a typical human hair)
Coating
Strengthening (Kevlar fibers)
Outer jacket
www.explainthatstuff.com

End View

Basic elements 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.

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



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.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand pressure than copper cable.

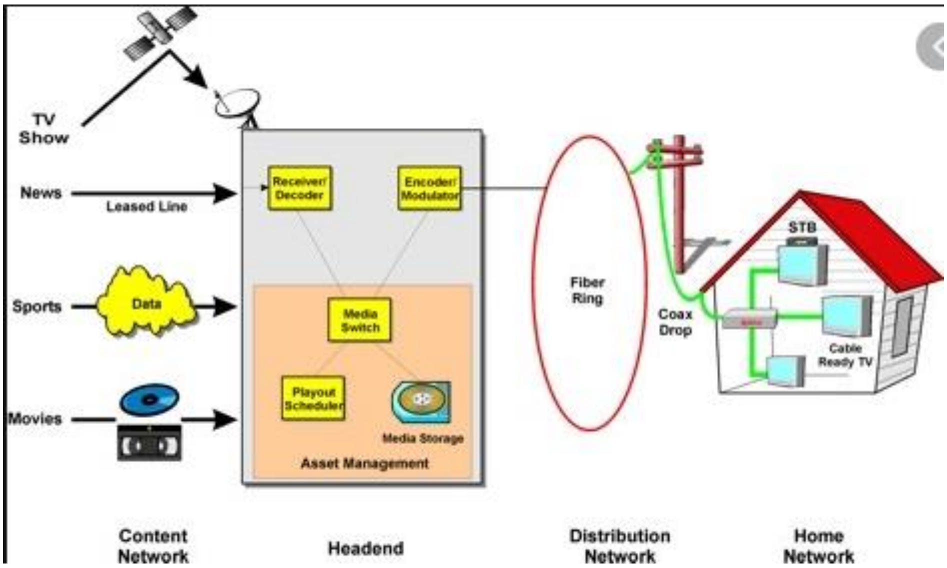
Cable Television

Cable Television was conceived in late 1940s to provide services in rural and hill areas. Initially the system was developed with big antennas along with amplifier called the headend to strengthen it and coaxial cable used to deliver services to houses. This cable television service was early called as Community Antenna Television.

The cable TV network had developed by new technologies and spread to more places. It used all new devices in to use makes the network as dynamic.

Internet over cable

A system with fibre for long distances and coaxial cable to the house is called an HFC (Hybrid Fibre Coax). The fibre nodes converts signals transmitted to other electrical systems.



Cable Television Network

The above diagram demonstrates the cable television network. The information is received and sent using wired technology and satellite technology. It used encoders and decoders to transmit signals. Fibre Ring acts as intermediate between headend and home network.

REFERENCES:

1. Andrew Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed. 2011.
2. B.A. Forouzan, Data Communications and Networking, 4rd Edition, McGraw Hill, 2007.