UNIT-I

DATA COMMUNICATIONS

The word **Data** refers to **Information.**

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:

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 should not be altered. If the data is altered 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** It refers to the variation in the packet arrival time. Jitter is the uneven delay in the delivery of audio or video packets.

   Example: Let us assume that video packets are sent every 3ms. If some of the packets arrive with 3ms delay and others with 4ms delay, an uneven quality in the video is the result.

COMPONENTS

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.

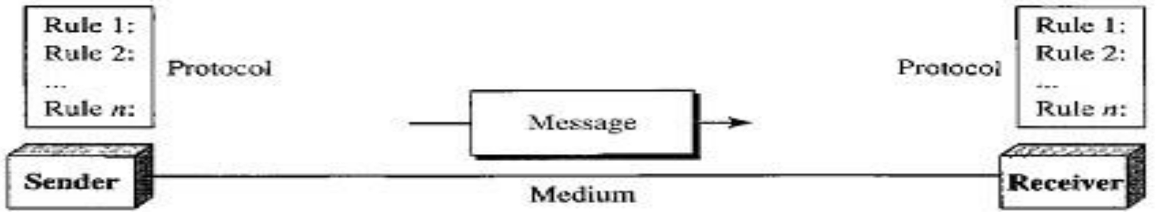
4. **Transmission medium**

   The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

5. **Protocol**

A protocol is **a set of rules** that govern data communications. It represents an **agreement** between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

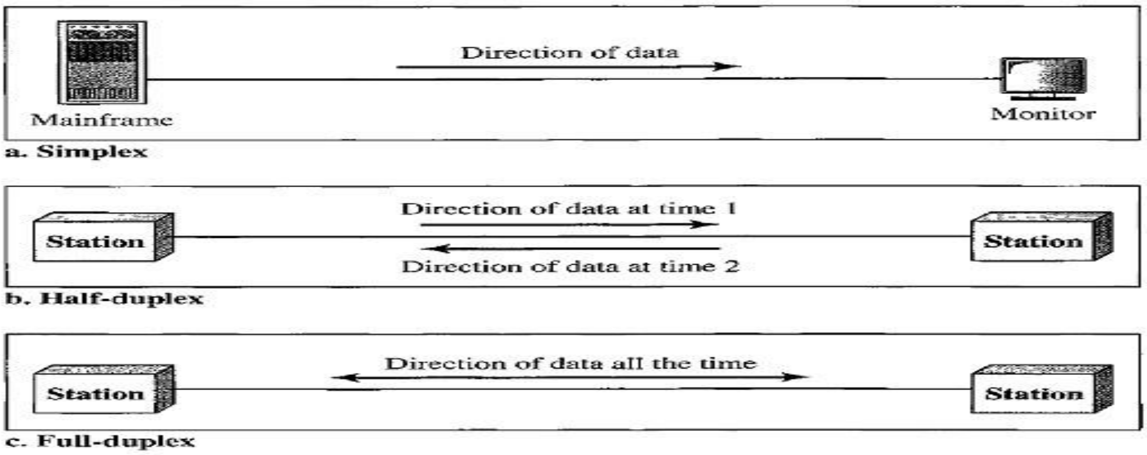
Five components of data communication



Note: The term ***TELECOMMUNICATION*** includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for "far").

DIRECTION OF DATA FLOW

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


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

a. Simplex

b. Half-duplex

c. Full-duplex

Simplex

- In simplex mode, the communication is unidirectional (i.e. one direction only).
- Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Examples - **Keyboards** and **Monitors,** the keyboard can only introduce input, the monitor can only accept output.

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.
- 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.
- The half-duplex mode is used, where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

- **Examples** - Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

- In full-duplex mode (or duplex), both stations can transmit and receive simultaneously.
- In full-duplex mode signals 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 channel is divided between signals traveling in both directions.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.
- **Example -** Telephone network. Two people talk and listen at the same time.

NETWORKS

A **Network** is a set of devices (also called as nodes) connected by communication links. (or) A **Network** is two or more devices connected through links.

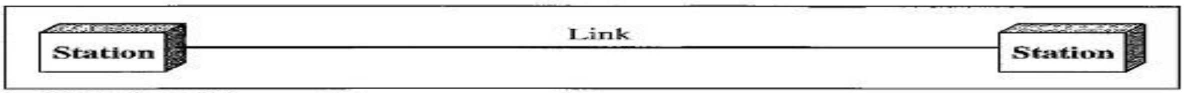
A **Node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

A **Link** is a communications pathway that transfers data from one device to another.

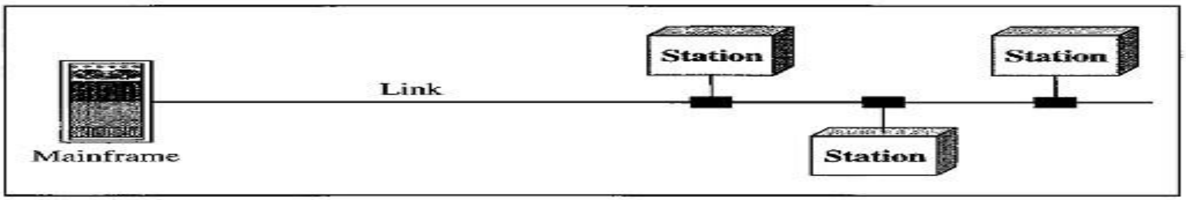
Type of Connection

Two devices must be connected in some way to the same link at the same time for occurring of communication. There are two possible types of connections:

1. Point-to-Point Connection
2. Multipoint Connection



a. Point-to-point



b. Multipoint

Point-to-Point Connection

- 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.
- Point-to-Point connections use an actual length of wire or cable to connect the two ends and microwave or satellite links.
- Example: When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

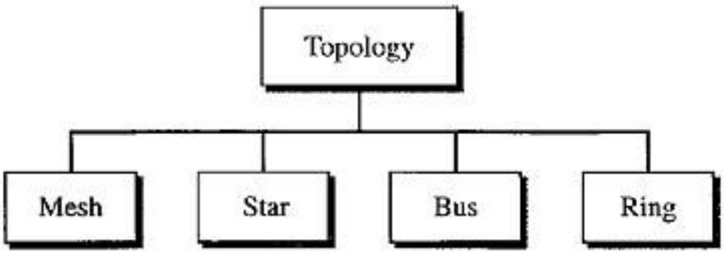
Multipoint (or) Multi-drop Connection

- A multipoint connection is more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

TOPOLOGIES

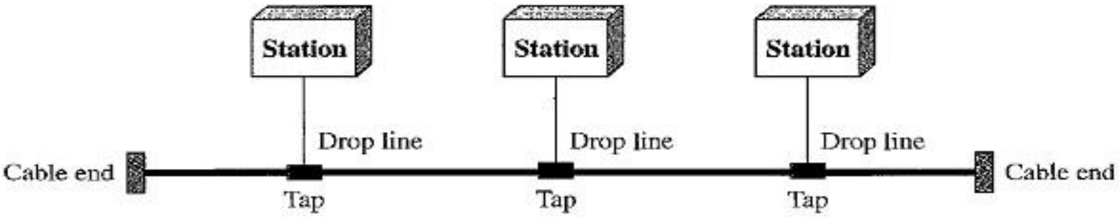
The term physical topology refers to the way in which a network is connected physically.
Two or more devices connect to a link. Two or more links form a topology. There
are four basic topologies are present:

1. Bus
2. Ring
3. Star
4. Mesh



Bus Topology

- A **bus topology** is multipoint connection, one long cable acts as a **backbone** to link all the devices in a network. Here the cable is called the bus.
- Bus topology was the one of the first topologies used in the design of early local area networks.
- 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 splices into (attached to) the main cable.



Advantages:

1. Installation is easy. Bus Backbone cable can be laid along the most efficient path and then connected to the nodes by drop lines of various lengths.
2. A bus uses less cabling than mesh or star topologies.

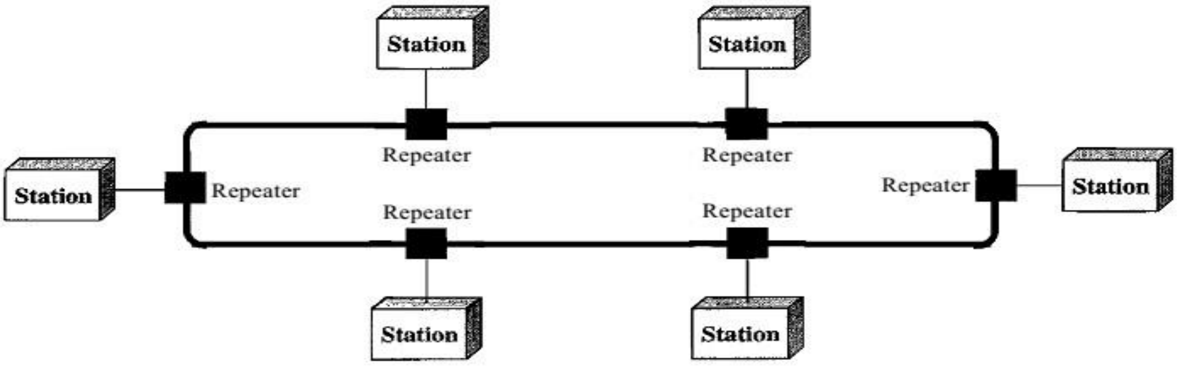
Disadvantages:

1. All the devices are connected to bus backbone cable, so that if the backbone cable fails the entire system fails.

2. Difficult Reconnection and Fault Isolation. It is difficult to add new devices.
3. There is a limit on the number of taps a bus can support and on the distance between those taps.
4. More heat is generated if the number of taps are more. Heat degrades the quality of signal.

Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages:

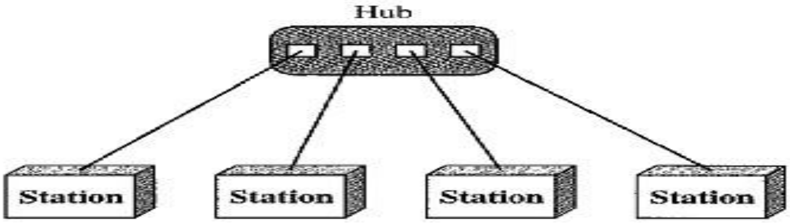
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. The only constraints are media and traffic considerations (maximum ring length and number of devices).

Disadvantage:

1. Unidirectional traffic can be a disadvantage.
2. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller called a Hub or Switch. The devices are not directly linked to one another.
- 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, and the controller transfers the data to the other connected device.



Advantages:

1. 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
2. Less cabling is required than mesh topology.
3. Star topology is robust, If one link fails, only that link is affected. All other links remain active.

Disadvantages:

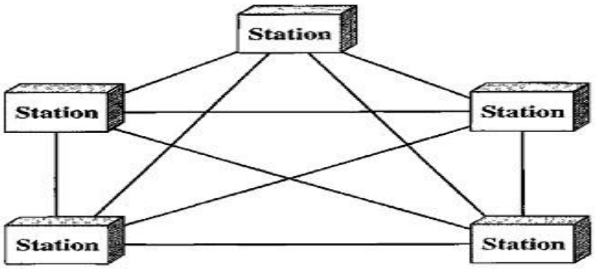
1. If hub fails entire processing will be stopped working. Uses:

1. It is used in High-speed LAN's often use a star topology with a central hub.

Mesh Topology

- In a mesh topology, every device has a **Dedicated Point-to-Point** link to every other device. (i.e.) for each node there is a link to all other nodes.
- The term **Dedicated** means that the link carries traffic only between the two devices it connects.

Advantages:

1. A mesh topology is robust. If one link becomes unusable, it does not affect the entire system.
2. 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.
3. **Privacy or Security.** When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-Point links make **Fault Identification** and **Fault Isolation** easy.
5. 

Disadvantages:

1. **High Cost:** Every device must be connected to every other device then there is a high amount of cabling and huge number of I/O ports required, this will make installation and reconnection are difficult.
2. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
3. More hardware (i.e. cables) and space is required **Example**: Telephone offices and Police stations.

Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

CATEGORIES OF NETWORKS

There are 3 categories of networks depend on its size:

1. Local Area Networks (LAN)
2. Metropolitan Area Networks (MAN)
3. Wide Area Networks (WAN)

Local Area Networks

- A Local Area Network (LAN) provides short-distance transmission of data over small geographic areas that may comprise a single office, building, or campus.
- **Size:** LAN size is limited to a few kilometres.
- **Speed:** Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range but now speeds are increased to 100 or 1000 Mbps.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
- A local area network (LAN) is usually privately owned.
- LAN will use only one type of transmission medium.
- The most common LAN topologies are bus, ring, and star.

Wide Area Network

A Wide Area Network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.

The point-to-point WAN is often used to provide Internet access. A line leased from a telephone provider that connects a home computer or a small LAN to an Internet service provider (lSP).

Metropolitan Area Networks

A Metropolitan Area Network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

It is designed for customers who need a high-speed connectivity to the Internet, and have endpoints spread over a city or part of city.

Example of a MAN is the part of the telephone company network that can provide a high speed DSL line to the customer.

PROTOCOLS AND STANDARDS

PROTOCOLS

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. For communication to occur, the entities must agree on a protocol.

The key elements of a protocol are:

1. Syntax
2. Semantics
3. Timing.

Syntax

- The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

- The word *semantics* refers to the meaning of each section of bits. How are a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

Timing

- The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

STANDARDS

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Standards Organizations

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

Standards Creation Committees

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

NETWORK MODELS

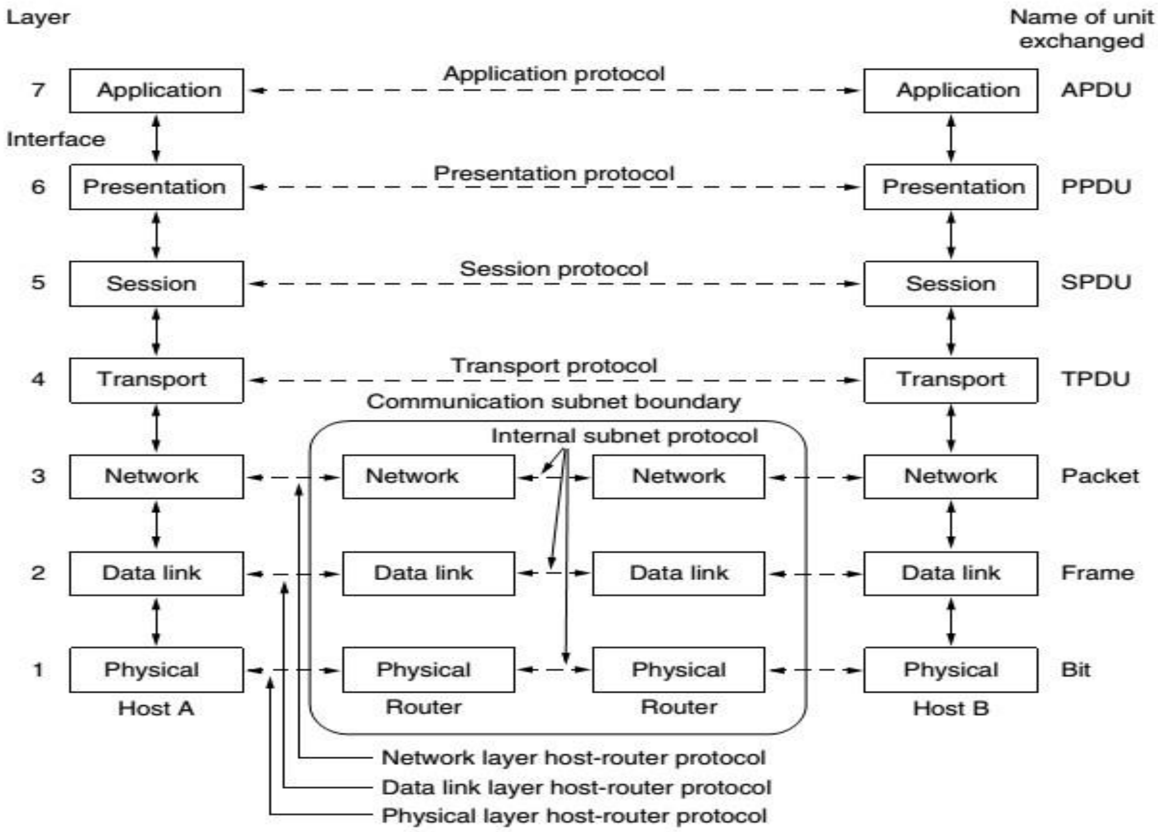
There are two types of network models are used:

1. ISO/OSI Model.
2. TCP/IP protocol model

ISO/OSI Model

- **ISO** is the **Organization**. **OSI** is the **Model**. ISO was established in 1947. OSI was first introduced in 1970.
- The **International Standards Organization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection model**.
- An **Open System** is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- **The purpose** of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

.



Interfaces Between Layers

- The passing of the data and network information between the layers in the device is made possible by an interface between each pair of adjacent layers.

- Each interface defines the information and services a layer must provide for the layer above it. These interfaces provide modularity to the network.

The Seven Layers in OSI Model are:

1. Physical Layer
2. Data link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical Layer

The **Physical Layer** is concerned with transmitting raw bits over a communication channel.

Physical Layer is responsible for:

- It defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- It also defines the type of transmission medium.
- It defines the data transmission rate, synchronization of data between sender and receiver.
- It defines type of connection (point-to-point or multipoint), type of topology, type of transmission mode, type of dataflow (simplex, half duplex, duplex).

The Data Link Layer

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

The **main task** of the Data link layer is **Error Free Transmission**. At the sender the data link layer break up the input data into **data frames** and transmits the frames sequentially.

Frame is typically a few hundred or a few thousand bytes.

Other responsibilities of the data link layer include the following:

- **Framing** - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
- **Physical addressing -** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and receiver of the frame.
- **Flow control** - If the rate at which the data are received by the receiver is less than the rate at which data sent by the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control** - The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control** - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Network Layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host through single or multiple networks.

Responsibilities of the Network layer include the following:

Logical addressing

- The physical addressing is implemented by Data-link layer, whereas logical addressing is implemented by network layer.
- Data-link layer handles the addressing problem locally, but if packets passes the network boundary there is a need for logical addressing system to help distinguish source and destination systems.
- The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.

Routing

When independent networks or links are connected to create inter-networks (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route the packets to their final destination.

Transport Layer

The transport layer is a true end-to-end layer; it carries from the source to the destination.

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

Responsibilities of the Transport Layer Include:

Port addressing (or) Service point addressing

- Source-to-Destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
- The transport layer header must therefore include a type of address called a *service-point address* (or port address).
- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and Reassembly

- A message is divided into transmittable segments, with each segment containing a sequence number.
- These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and the sequence numbers are used for identifying and replace packets that were lost during transmission.

Connection control

- The transport layer can be either connectionless or connection oriented.
- A **Connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A **Connection-Oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

- After all the data are transferred, the connection is terminated.

Flow control and Error control

- Like the data link layer, the transport layer is responsible for flow control.
- Flow control at this layer is performed end to end rather than across a single link.
- Like the data link layer, the transport layer is responsible for error control.
- Error control at this layer is performed Process-to-Process rather than across a single link.
- Error control achieved through **Retransmission.**

Session Layer

The session layer allows users on different machines to establish **sessions** between them. The session layer is the network *dialog controller.* It establishes, maintains, and synchronizes the interaction among communicating systems.

Responsibilities of the session layer include the following

- **Dialog Control** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. Check-Pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery
- **Token management** prevents two parties from attempting the same critical operation simultaneously.

Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

The presentation layer is responsible for **Translation, Compression, and Encryption**.

Translation

- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers etc. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- The presentation layer at the sender changes the information from its sender-dependent format into a common format.
- The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption

- Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
- Decryption reverses the original process to transform the message back to its original form. Encryption and Decryption is done for privacy of the sensitive information. **Compression**
- Data compression reduces the number of bits contained in the information.

- Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer

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

The **application layer** contains a variety of protocols that are commonly needed by users. The application layer enables the user to access the network.

Specific services provided by the application layer include the following:

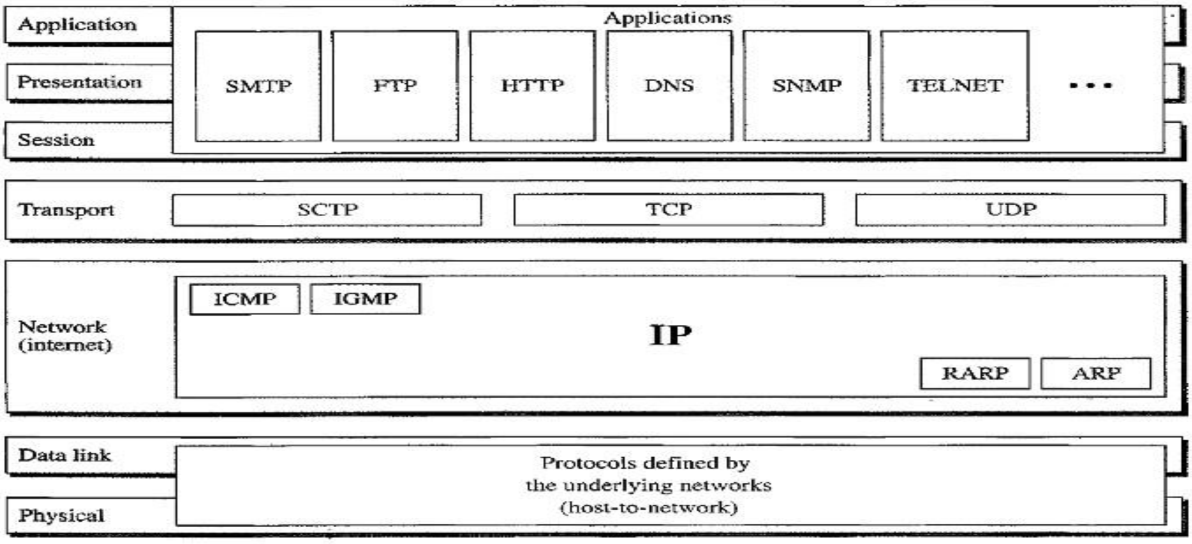
- **A network virtual terminal** is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **File** transfer, access, and management in a remote host.
- **Mail services** such as email forwarding and mail storage.
- **Directory services** are an application provides distributed database sources and access for global information about various objects and services.

TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite was developed prior to the OSI model.

The original TCP/IP protocol suite was defined as having four layers:

1. Host-To-Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer



Layers comparison in TCP/IP and OSI:

- **Host-to-Network** layer is equivalent to the combination of the **Physical** and **Data link** layers.
- The **Internet Layer** is equivalent to the **Network layer**.
- The **Transport layer** is similar in both OSI and TCP/IP, except that in TCP/IP it will take care of part of the duties of the session layer.

- The **Application Layer** is roughly doing the job of the **Session, Presentation,** and **Application** layers.

Functionality in TCP/IP and OSI:

- ***TCP/IP*** is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- **OSI model** specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term *hierarchical* means that each upper-level protocol is supported by one or more lower-level protocols.

Host-to- Network Layer

- At the Host-to-Network layer is a combination of Physical Layer and Data-link layer in OSI model.
- It is an interface between hosts and transmission links.
- **TCP/IP** does not define any specific protocol. It supports all the standard and proprietary protocols.
- A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Internet Layer (or) **Network Layer**

- In this layer *TCP/IP* supports the Internetworking Protocol (IP). The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- It is an unreliable and connectionless protocol-a best-effort delivery service.
- The term *best effort* means that IP provides no error checking or tracking.
- The transmission is unreliable (i.e.) there is no guarantee for the data.
- IP transports data in packets called *datagrams,* each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

IP uses four supporting protocols

1. ARP (Address Resolution Protocol)
2. RARP(Reverse Address Resolution Protocol)
3. ICMP(Internet Control Message Protocol)
4. IGMP(Internet Group Message Protocol)

Transport Layer

Transport layer in *TCP/IP* has three protocols:

1. **TCP** (*Transmission Control Protocol)*
2. **UDP**(*User Datagram Protocol)*
3. **SCTP**(Stream Control Transmission Protocol)

Transmission Control Protocol

- TCP provides full transport-layer services to applications. TCP is a reliable stream transport protocol.
- The term ***stream*** means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
- At the sending side for each transmission TCP divides a stream of data into smaller units called *Segments.* Each segment includes a sequence number for reordering at the destination side. Segments are carried across the internet inside of IP datagrams.
- For every segment there is a corresponding acknowledgement to be sent from the destination to the source.
- At the receiving side TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

User Datagram Protocol

- UDP is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
- It is also widely used for client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

Stream Control Transmission Protocol

- The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

Application Layer

On top of the transport layer is the **application layer**. It contains all the higher-level protocols such as:

- **Telnet protocol** used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
- **File Transfer Protocol (FTP)** used for file transfer.
- **Simple Mail Transfer Protocol (SMTP)** used for mail services.
- **Domain Name System (DNS)** used for mapping host names onto their network addresses.
- **Hyper Text Transfer Protocol (HTTP)** used for fetching pages on the World Wide Web (WWW).
- **Real-time Transport Protocol (RTP)** used for delivering real-time media such as voice or movies.

TRANSMISSION MODES

MULTIPLEXING

Modulation and Demodulation

Converting digital Signal to analog signal is called Modulation, whereas demodulation is converting Analog signal to digital signal.

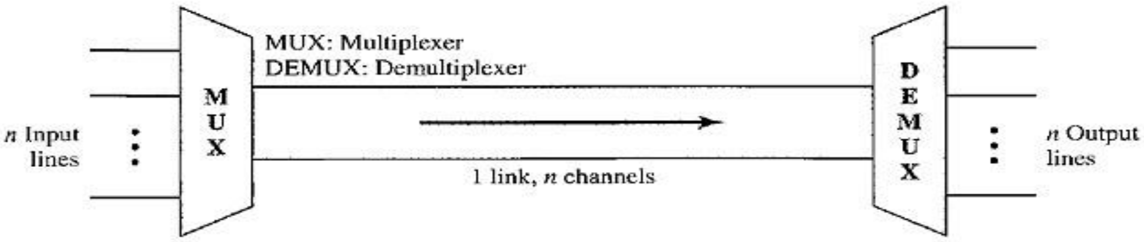


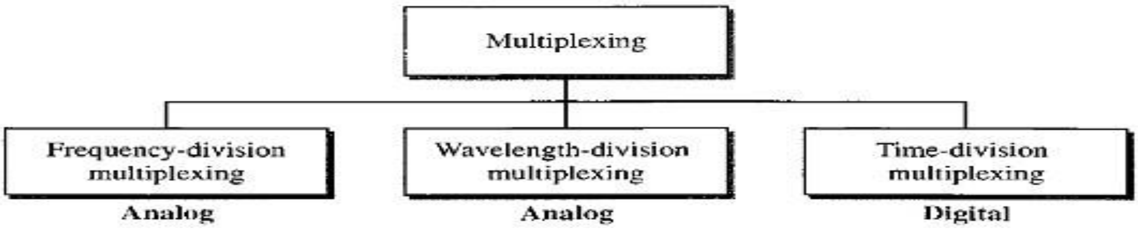
Fig: Dividing the link into channels

In a multiplexed system, *n* lines share the bandwidth of one link.

- **Link** refers to the physical path.
- **Channel** refers to the portion of a link that carries a transmission between a given pair of lines.
- The lines on the left direct their transmission streams to a **Multiplexer (MUX)**, which combines them into a single stream (many-to-one).
- At the receiving end, that stream is fed into a **Demultiplexer (DEMUX)**, which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.

Multiplexing is categorized into 3 types:

1. Frequency Division Multiplexing
2. Wavelength Division Multiplexing
3. Time Division Multiplexing


Multiplexing
Frequency-division multiplexing
Analog
Wavelength-division multiplexing
Analog
Time-division multiplexing
Digital

Frequency Division Multiplexing (FDM)

FDM is an analog multiplexing technique that combines analog signals.

That means:

- FDM is an analog technique that can be applied when :
  Bandwidth of link (in Hz) >= Combined bandwidth of the signal to be transmitted.
- In FDM, signals generated by each sending device modulate different carrier frequencies.
- These modulated signals are then combined into a single composite signal that can be transported by the link.
- **Carrier frequencies** are separated by sufficient bandwidth to accommodate the modulated signal.

- These bandwidth ranges are the channels through which the various signals travel.
- **Channels** can be separated by strips of unused bandwidth called **Guard Bands.**
- **Guard bands** are used to prevent signals from overlapping.
- In addition, carrier frequencies must not interfere with the original data frequencies.

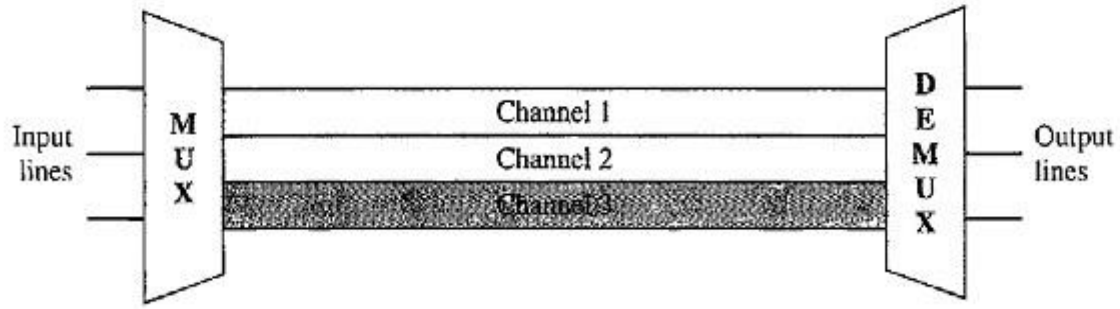


Fig: Frequency Division Multiplexing

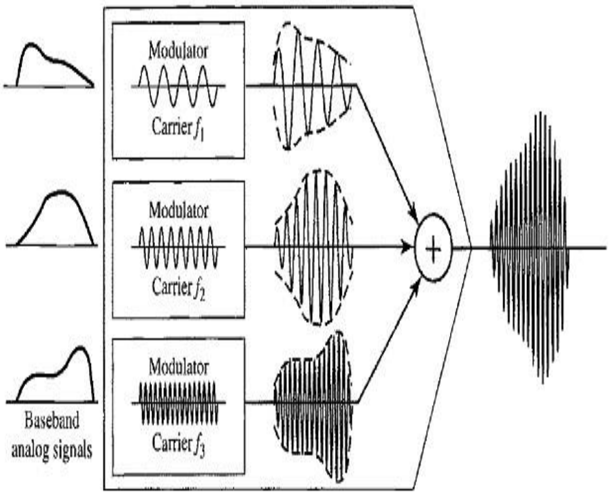
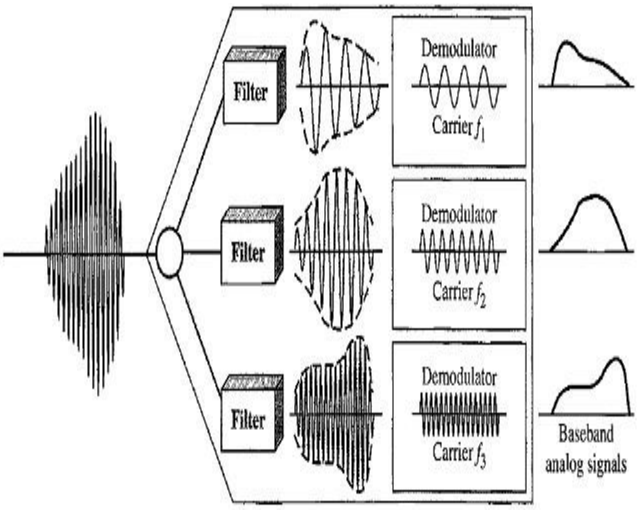
In the above figure, the transmission path is divided into three parts, each representing a channel that carries one transmission.

Multiplexing Process

- Each source generates a signal of a similar frequency range.
- Inside the multiplexer, these similar signals modulate different carrier frequencies (f1, f2, f3).
- The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

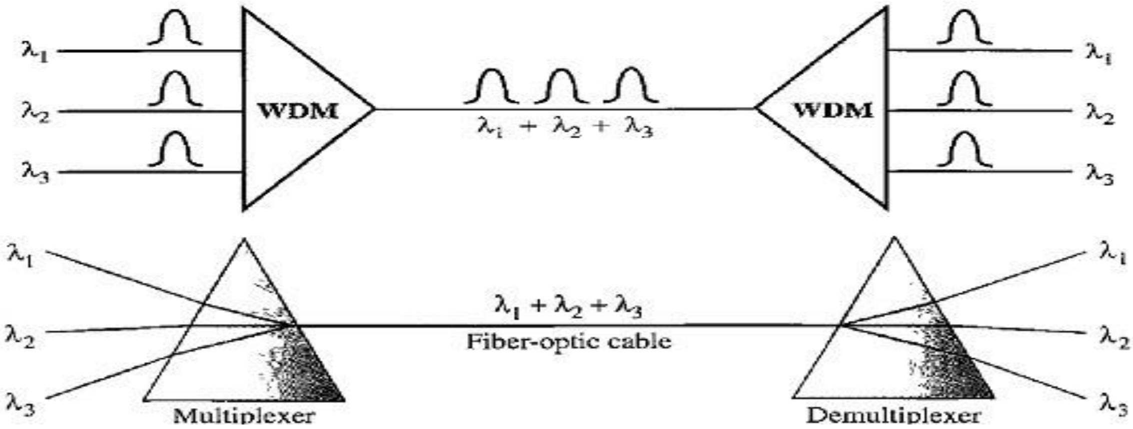
Demultiplexing Process

- The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals.
- The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines.

FDM Multiplexing	**FDM Demultiplexing**
 Modulator Carrier f_1 Modulator Carrier f_2 Modulator Carrier f_3 Baseband analog signals	 Filter Filter Filter Demodulator Carrier f_1 Demodulator Carrier f_2 Demodulator Carrier f_3 Baseband analog signals

Wavelength-Division Multiplexing (WDM)

- WDM is an analog multiplexing technique to combine optical signals.WDM is designed to use the high-data-rate capability of fiber-optic cable.
- The optical fiber data rate **higher than** the data rate of metallic transmission cable
- Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.



- Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.
- The combining and splitting of light sources are easily handled by a **Prism**. A Prism bends a beam of light based on the angle of incidence and the frequency.
- A multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies.
- A demultiplexer can be made to divide wider band of frequencies by decomposing the light beams into narrow band frequencies.

Advantages: High Speed and High frequency, uses narrow bands of light sources.

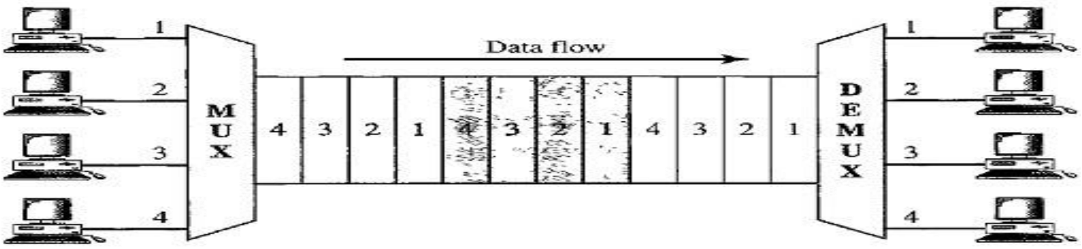
Disadvantages: Expensive than FDM.

Time-Division Multiplexing (TDM)

TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate channel. Digital data from different sources are combined into one timeshared link

(i.e.) The **data rate** capacity of transmission medium >= The **data rate** required by sending and receiving devices.

TDM is a digital process that allows several connections to share the high bandwidth of a link. Each connection occupies a portion of time in the link.

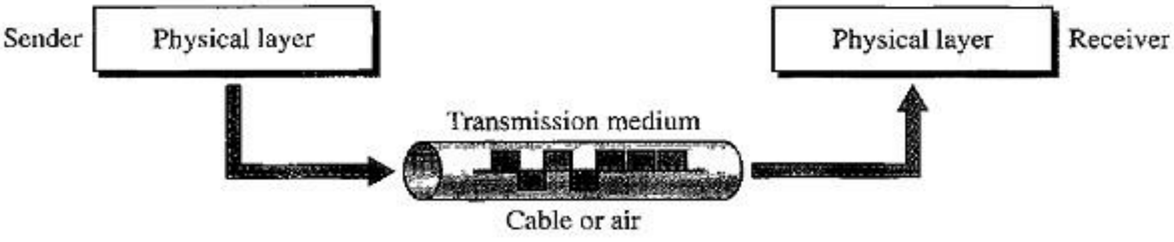


In the above figure all the data in a message from source 1 always go to one specific destination either of 1, 2, 3, or 4. The delivery is fixed and unvarying.

TRANSMISSION MEDIA

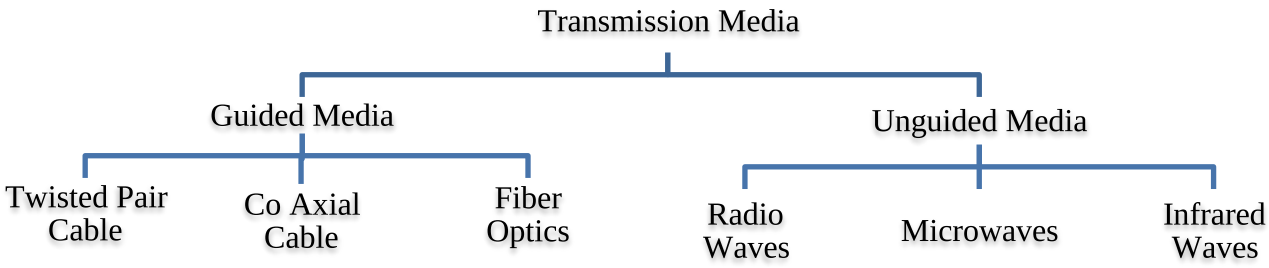
Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. In data communications the information is usually a signal.



Transmission media can be categorized into following ways:

1) **Guided or Wired Media**: Twisted pair cable, Coaxial cable, Fiber Optic cable.
2) **Unguided or Wireless Media**: Radio Waves, Micro waves, Infrared Waves.



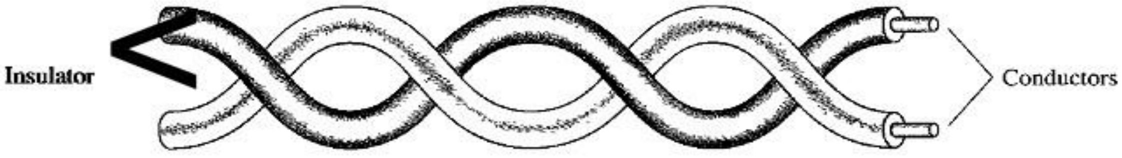
Guided or Wired Media

A signal traveling along this media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

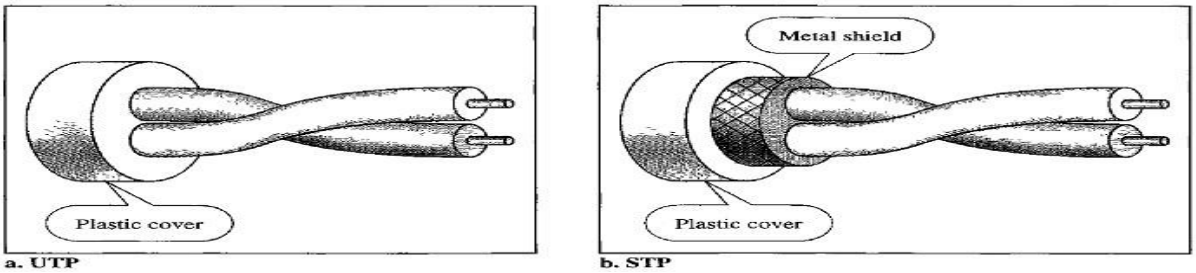
Twisted-Pair Cable

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.



The signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.



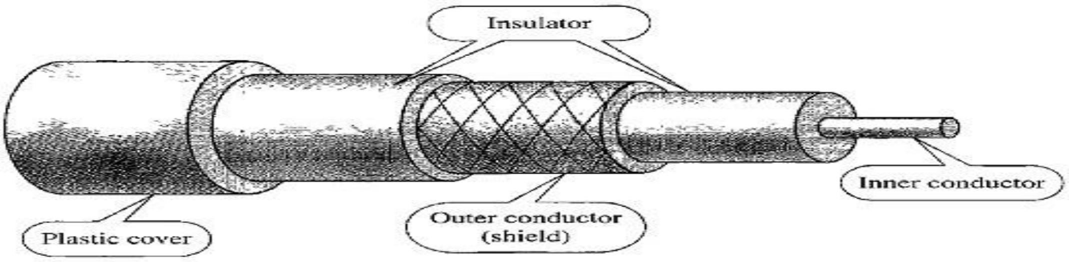
STP v/s UTP

Shielded Twisted Pair (STP) cable has a **metal foil** or braided mesh covering that encases each pair of insulated conductors. A twisted-pair cable can pass a wide range of frequencies. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Unshielded Twisted pair (UTP) cables don't have the metal foil covering the cables. The most common UTP connector is RJ45 (Registered Jack 45).

Coaxial Cable (Coax)

Coaxial cable carries signals of higher frequency ranges than those in twisted pair cable.



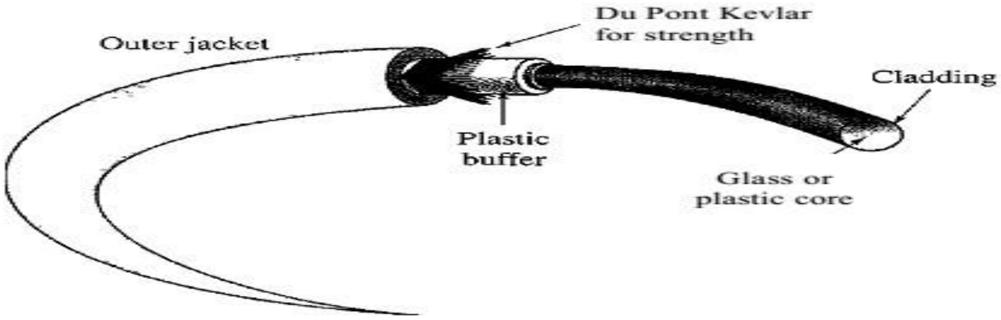
Coaxial cable has a central core conductor of copper wire enclosed in an insulating sheath.

Insulating sheath encased in an outer conductor of metal foil.

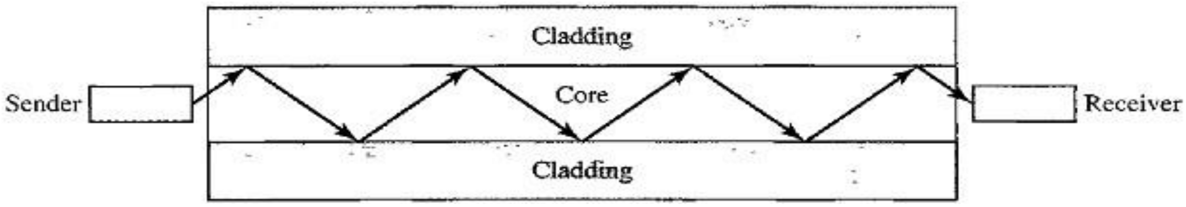
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
  - This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Fiber-Optic Cable

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable.
- Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.



- Optical fibers 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

Fiber-optic cable has several advantages over metallic cable Twisted pair or coaxial.

- **Higher bandwidth**. Fiber-optic cable can support higher bandwidths than either twistedpair or coaxial cable.
- **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration.
  We need repeaters every 5 km for coaxial or twisted-pair cable.
- **Immunity to electromagnetic interference**. Electromagnetic noise cannot affect fiberoptic cables.

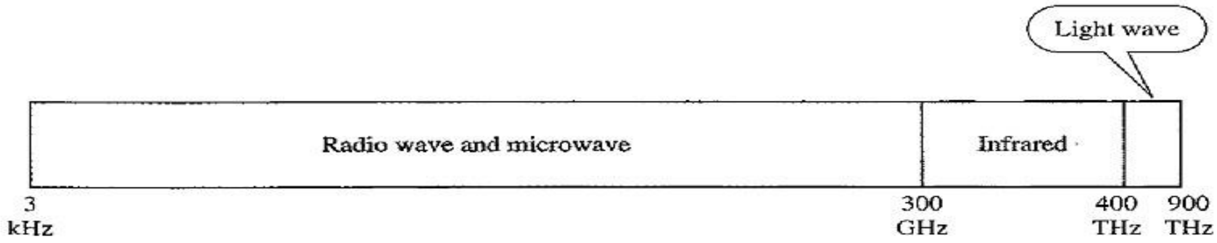
- **Resistance:** Glass is more resistant to corrosive materials than copper.
- **Light weight.** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping**: Fiber-optic cables are more immune to tapping than copper cables.

Disadvantages

- **Installation and maintenance:** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation**: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost:** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high the use of optical fiber cannot be justified.

UNGUIDED MEDIA (or) WIRELESS COMMUNICATION

Unguided media transport **Electromagnetic Waves** without using a physical conductor. This type of communication is often referred to as wireless communication. Electromagnetic spectrum ranging from **3 kHz to 900 THz** used for wireless communication.



Categories of Wireless Communication:

- Radio Waves (3kHz – 1GHz)
- Microwaves (1GHz- 300 GHz)
- Infrared Waves (300 GHz - 400 THz)

Radio Waves

- Radio waves ranges between 3 kHz and 1 GHz. Radio waves are Omni-directional.
- When an antenna transmits radio waves, they are propagated in all directions. Hence the sending and receiving devices don't have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves can travel long distances, hence it is used in long distance AM Radio broadcasting.
- Radio waves of low and medium frequencies can penetrate walls.

Disadvantage

- The Omni-directional property has a **disadvantage**; the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves leads to low data rate for digital communication.

Applications

Radio waves are used in Multicasting applications such as AM Radio and FM radio, Television, Maritime Radio, Cordless Phones, and Paging.

Microwaves

- Electromagnetic waves having frequencies between 1GHz and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.
- Microwave propagation is line-of-sight. Repeaters are often needed for long distance communication.
- Higher data rates are possible due to assigning of wider sub-bands.

Advantage

The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Disadvantage

Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

Applications

Microwaves used in Uni-casting communication between sender and receiver such as cellular phones, satellite networks and wireless LANs.

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication upto few meters.

Advantages

Infrared waves having high frequencies cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

Disadvantage

- We cannot use Infrared waves for long range communication.
- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

- Due to its wide bandwidth, it can be used to transmit digital data at high data rate.
- It can be used in Communication between devices such as keyboards, mice, PCs, and printers

SWITCHING

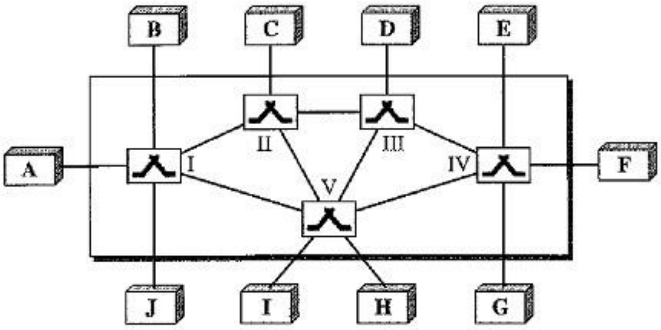
A network is a set of connected devices. We use any of the topologies to connect those devices and then devices transfer their data. But every topology have their own disadvantages such size, cost of the material and efficiency etc.

A better solution to overcome these disadvantages is **switching**.

- A **Switched Network** consists of a series of interlinked nodes, called switches.
- **Switches** are devices capable of creating temporary connections between two or more devices linked to the switch.
- In a switched network, some of the nodes are connected to the end systems such as computers or telephones.
- Other nodes are used only for **Routing**.

The below figure shows a Switched Network:

- The **End Systems** (communicating devices) are labeled with capital letters from A to J.
- The **Switches** are labeled with roman numbers I, II, III, IV, and V.
- Each switch is connected to multiple **Links.**



Types of switched networks

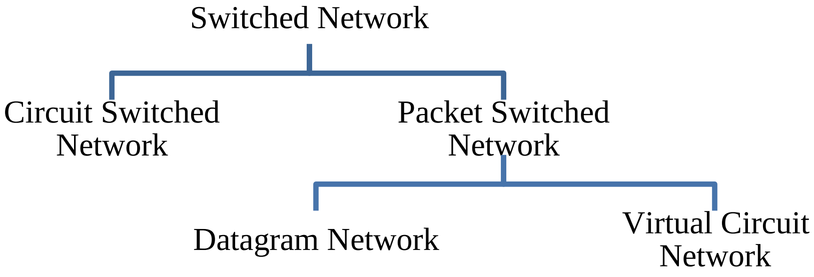
Switched networks can be divided into two types:

1. Circuit Switched Networks
2. Packet Switched Networks

Whereas packet switched networks can be further divided into 2 types:

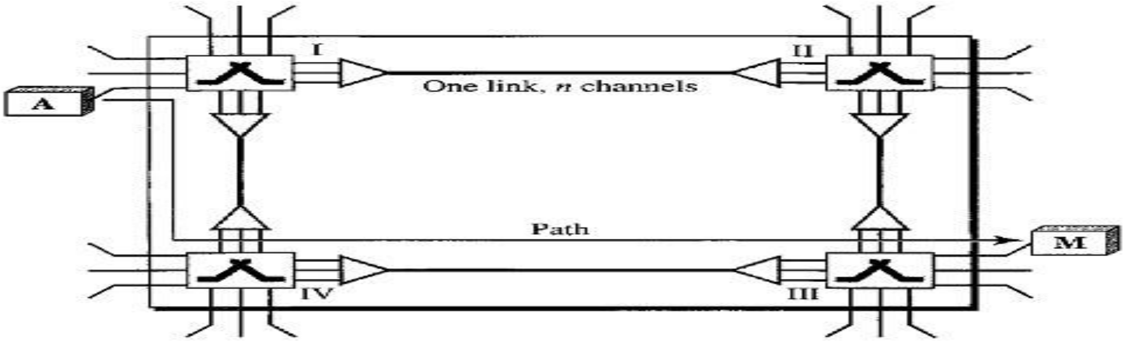
1. Datagram networks

2. Virtual Circuit networks.



Circuit-Switched Networks

- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- Each connection uses only one dedicated channel on each link.
- Each link is normally divided into *n* channels by using FDM or TDM.



The above figure is a circuit switched network with **4 Switches** and **4 Links**. Each link is divided into **3 Channels** by using FDM or TDM. There are two end systems namely A and M. The end systems may be computers or telephones.

Resources used in Circuit Switching Communication are: Channels (Bandwidth in FDM and Time Slots in TDM), Switch Buffers, Switch Processing Time, Switch Input/ Output Ports. The actual communication in a circuit-switched network requires three phases:

1. Setup Phase
2. Data Transfer Phase
3. Connection Teardown Phase

Setup Phase:

- Connection Setup means **creating dedicated channels** between the switches.

Data Transfer: After the dedicated path made of connected channels is established, data transfer can take place.

Tear-Down Phase: After all data have been transferred, a signal is sent to each switch to release the resources.

Properties of Circuit Switching Networks

1. **Data is not Packetized**

Circuit switching takes place at the Physical Layer. Hence data transferred between the two stations are not packetized.

2. Continuous flow of data

The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.

3. Resource Reservation

Before starting communication, the stations must make a reservation for the resources to be used during the communication.

4. Resource Dedication

The resources must remain dedicated (unchanged) during the entire duration of data transfer until the teardown phase.

5. **No Addressing**

There is **no addressing** involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM).

Disadvantage: Less Efficiency

Resource Reservation makes it less efficient, resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Advantage: Minimal Delay

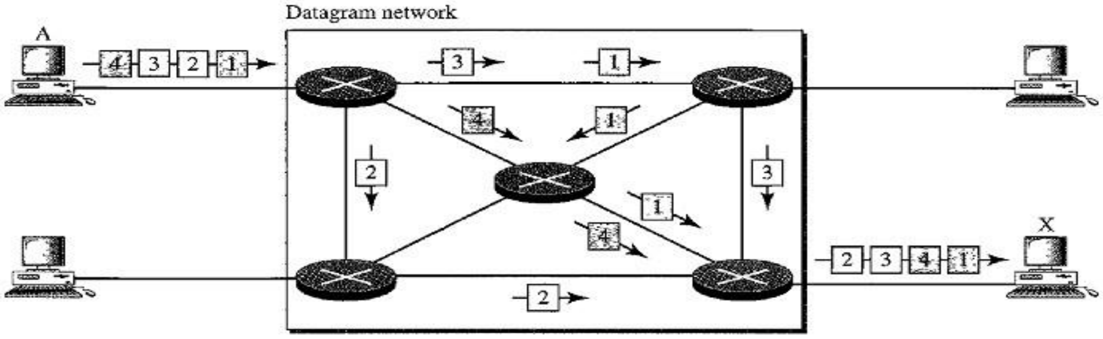
During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

<u>Datagram Networks or Datagram Switching</u>

Datagram Switching takes place at the Network Layer

- Packets in this approach are referred to as **Datagrams**.
- The size of the packet can be determined by network and the governing protocol.
- The switches in a datagram network are traditionally referred to as routers.
- To send messages from one end system to another end system, if the message is going to pass through a Packet Switched Network, then the message needs to be divided into packets.

Consider the below figure the entire message is divided into four packets from station A and travels through different paths to reach their destination station X.



Properties of Datagram Network:

1. Data is packetized
2. No Resource Reservation
3. On Demand Resource Allocation
4. No continuous flow of data
5. Connection less Network
6. Loss of packets
7. Routing table
8. Addressing

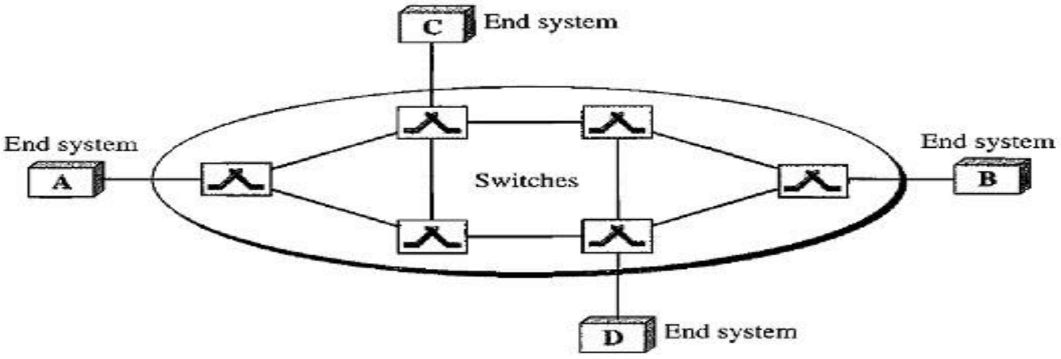
Advantage: High Efficiency

Disadvantage: Greater Delay

<u>VIRTUAL-CIRCUIT NETWORKS</u>

A virtual-circuit network is normally implemented in the data link layer.

Virtual Circuit Networks are implemented by taking the common characteristics of both circuit switched networks and Datagram networks.



Characteristics of Virtual Circuit Networks

1. Three phase data transfer

As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

2. Resource Allocation

Resources can be allocated during the **Setup Phase**, as in a circuit-switched network or Resources can be allocated **On Demand** as in a datagram network.

3. Packetized Data

As in a datagram network, data are **packetized** and each packet carries an address in the header.

4. Data Order is Maintained

As in a circuit-switched network, all packets follow the same path established during the connection.

Virtual-Circuit Identifier (VCI)

- The identifier that is actually used for data transfer is called the **Virtual-Circuit Identifier**.
- A VCI is a small number that has only switch scope. It is used by a frame between two switches.
- When a frame arrives at a switch it has a VCI. When the same frame leaves at a switch it has a different VCI.

Phases in Virtual Circuit Network

There are 3 phases are there: Setup, Data Transfer, Teardown.

Setup Phase

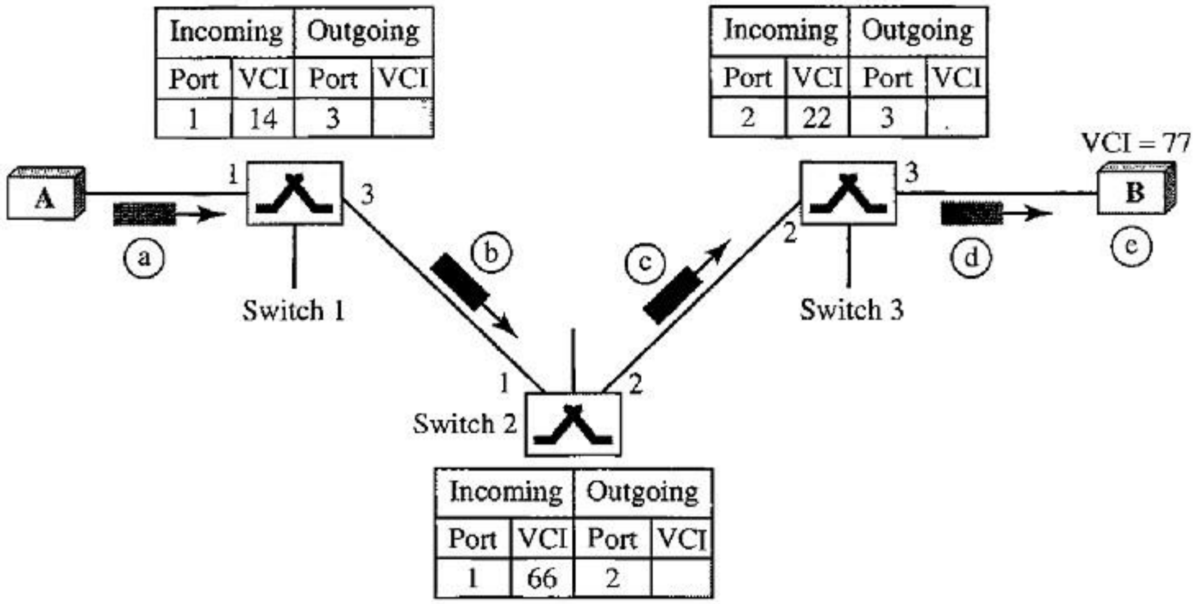
In the setup phase, a switch creates an entry for a virtual circuit.

For example, suppose source A needs to create a virtual circuit to B. Two steps are required:

- Setup Request
- Acknowledgment

Setup Request

- A setup request frame is sent from the source to the destination.
- Source A sends a setup frame to switch 1.
- Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3.
- The switch in the setup phase, acts as a packet switch; it has a routing table which is different from the switching table.
- The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns.
- The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.
- Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are filled: they are incoming port (l), incoming VCI (66), and outgoing port (2).
- Switch 3 receives the setup request frame. Again, three columns are filled: incoming port (2), incoming VCI (22), and outgoing port (3).
- Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.



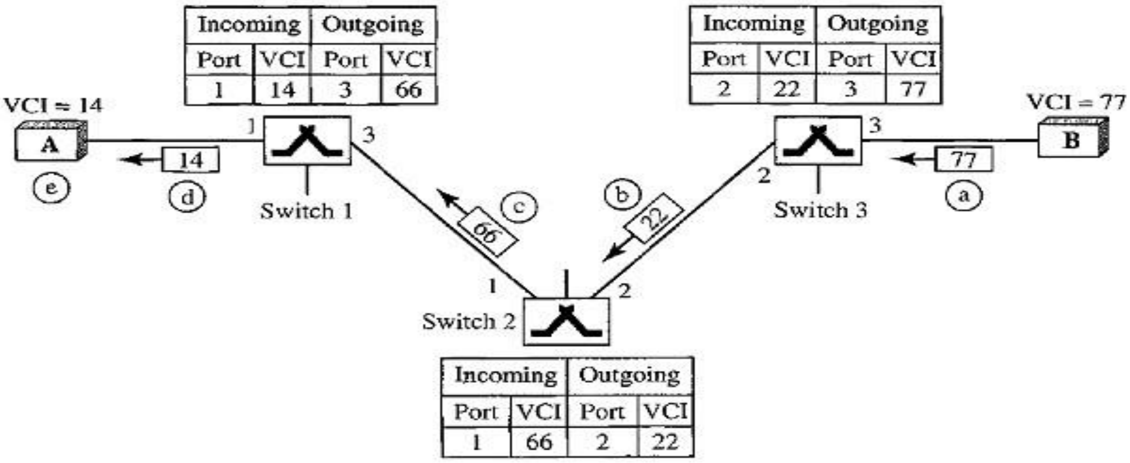
Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	.

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	

Acknowledgment

Acknowledgment is a special frame that is transferred from destination to source.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22

- The destination sends an acknowledgment to switch 3.
- The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed.
- The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A.
- Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.
- Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.
- Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.
- Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.
- The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Virtual-Circuit Networks: Frame Relay and ATM

FRAME RELAY

Features of Frame Relay

1. Frame Relay operates at a higher speed (initially 1.544 Mbps and recently 44.376 Mbps).
2. Frame Relay operates in the physical and data link layers.
3. Frame Relay allows burst data.
4. It allows a frame size of 9000 bytes, which can accommodate all LAN frame sizes.
5. Frame Relay is less expensive than other traditional WANs.
6. Frame Relay has error detection at the data link layer only.

Note:

- Frame relay has no flow control or error control.
- Frame relay doesn’t have a retransmission policy if a frame is damaged then the frame is dropped.
- Frame Relay was designed to provide fast transmission capability for ***more reliable media*** and for those protocols that have flow and error control at the higher layers.

ASYNCHRONOUS TRANSFER MODE (ATM)

ATM is the cell relay protocol designed by the ATM Forum and adopted by the ITU-T.

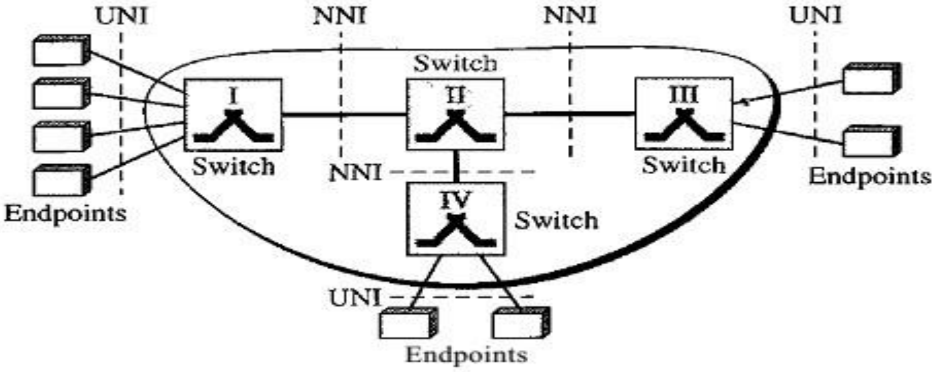
ATM can be thought of as the "highway" of the information superhighway.

Design Goals

1. **High Data Rates**: The need for a transmission system to optimize the use of high-datarate transmission media, in particular optical fiber.
2. **Interfacing:** The system must interface with existing systems and provide wide-area interconnectivity between them without lowering their effectiveness or requiring their replacement.
3. **Inexpensive:** The design must be implemented inexpensively so that cost would not be a barrier to adoption.
4. **Adoptability:** The new system must be able to work with and support the existing telecommunications hierarchies (local loops, local providers etc).
5. **Connection Oriented:** The new system must be connection-oriented to ensure accurate and predictable delivery.
6. **Moving Functions:** One objective is to move as many of the functions to hardware as possible (for speed) and eliminate as many software functions as possible (for speed).

Architecture of ATM

- ATM is a cell-switched network.
- The user access devices called the endpoints are connected through a user-to-network interface (UNI) to the switches inside the network.
- The switches are connected through network-to-network interfaces (NNIs).


UNI
NNI
NNI
UNI
Switch
I
II
III
Switch
Switch
NNI
IV
Switch
UNI
Endpoints
Endpoints
Endpoints