Unit 2

Physical Layer

Physical Layer

•**Bit Transmission -** Converts digital data from the data link layer into electrical, optical, or radio signals. Transmits bits sequentially over the physical medium.

•**Physical Topology -** Defines the physical layout of devices and cables in a network (e.g., bus, star, ring, mesh).

•**Transmission Medium -** Determines how signals are carried over the medium (e.g., copper wire, fiber optics, wireless).

•**Data Rate (Bit Rate) Control -** Controls the speed of data transmission (measured in bps – bits per second).

•**Line Configuration -** Determines the way devices are connected (e.g., **point-to-point or multipoint**).

Transmission Mode - Determines the direction of signal flow:

- Simplex – one-way
- Half-duplex – both ways, one at a time
- Full-duplex – both ways, simultaneously

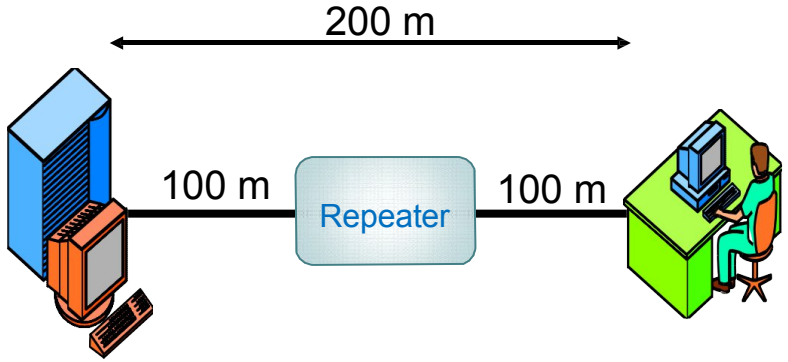
Networking Devices

- **HUB, Switches, Routers, ,Modems etc.**

Networking Devices

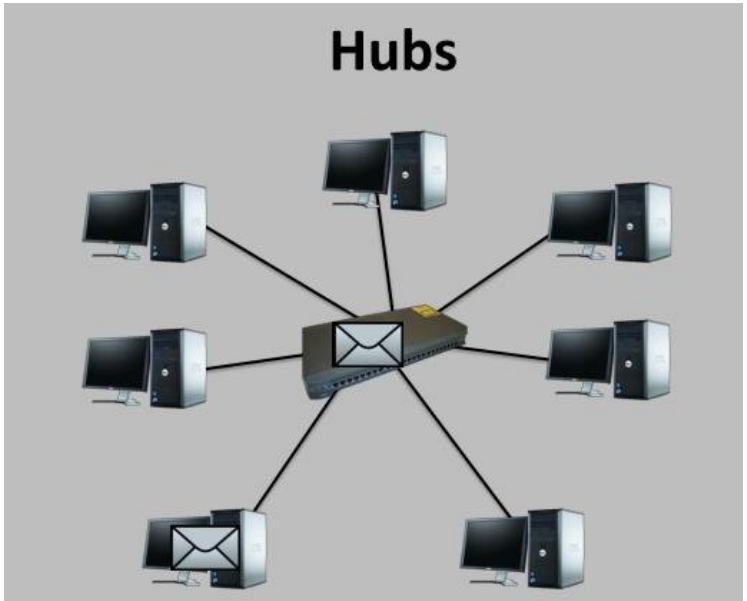
Repeater:

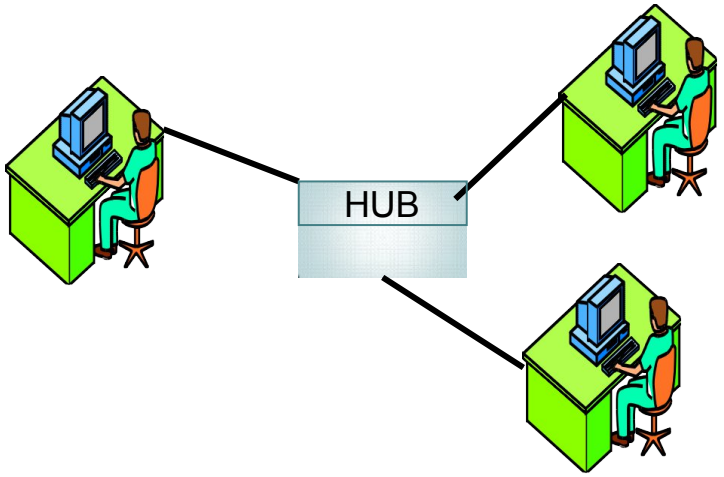
A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.



Hub:

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. When multiple devices (like computers) are connected to a **hub**, only one device can successfully send data at a time. If two devices try to send data at the same time, a **collision** occurs. They then need to retransmit, leading to delays and reduced efficiency. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.





Hub:

Types of Hub

Active Hub:-Not only connects devices but also amplifies (boosts) the signal before forwarding it.
Helps in extending the distance the signal can travel without degradation.
Acts like a repeater + hub — improves signal strength.

Passive Hub :-Simply connects multiple devices in a network. Does not amplify or regenerate the signal — just passes it along.
•Acts like a physical junction box.
•Often used in older or very simple networks.
No signal boosting — just basic connection

Intelligent Hub :- Performs the roles of an active hub plus network management features.
•Can monitor traffic, detect errors, and support remote management.
•More expensive and sophisticated.
•Rarely used today — switches and routers do this better.
Adds basic intelligence and diagnostics to a hub.

Bridge:

A **bridge** is a device used in a computer network that helps connect two smaller networks (LANs) and make them work as one. It works at the **Data Link Layer (Layer 2)** of the OSI model.

What does a bridge do?

•It **reads MAC addresses** (hardware addresses) to decide whether to forward or block data.

•It acts like a **smart repeater**: it receives a signal, cleans it up (if needed), and **forwards it only when necessary**.

•It can **filter traffic**: only lets data through if it's meant for the other side.

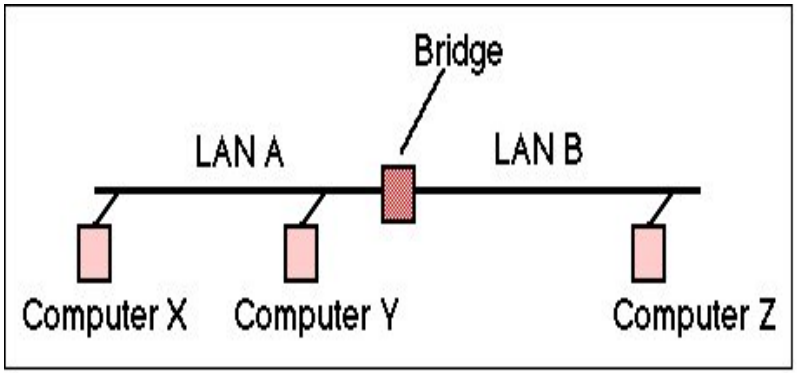
•It has **2 ports**: one input and one output — like a two-way door between two LANs.

Types of Bridges

Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

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

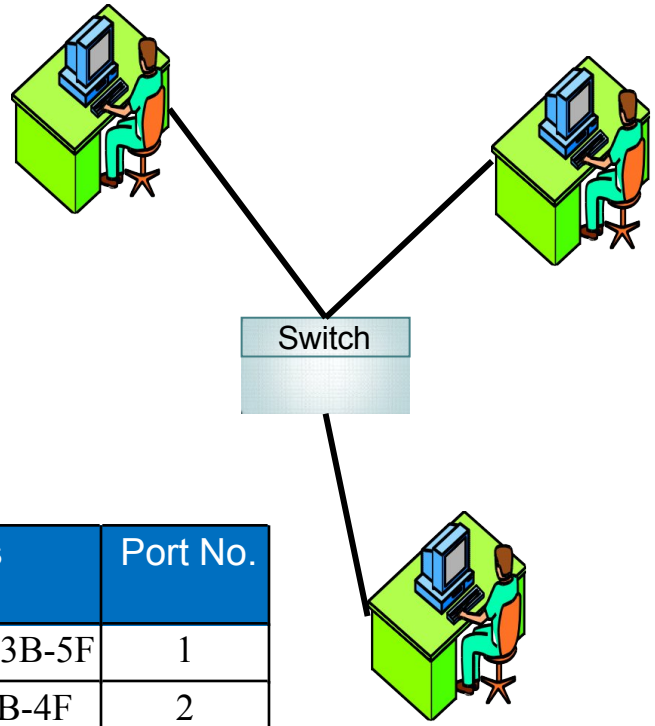


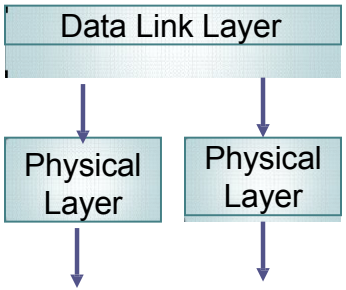
Bridges

Switch:

- A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.
- A switch is essentially a fast, multi-port bridge that can contain dozens of ports.
- A switch dynamically builds and maintains a MAC table, which holds all of the necessary MAC information for each port.
- The switch then forwards or discards frames based on the table entries.
- Table entries are called Content Addressable Memory.
- Switch works at **Data link Layer** of OSI Reference model

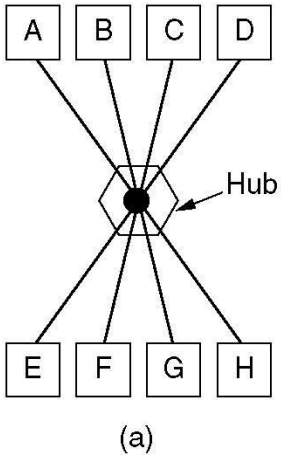
Networking Devices



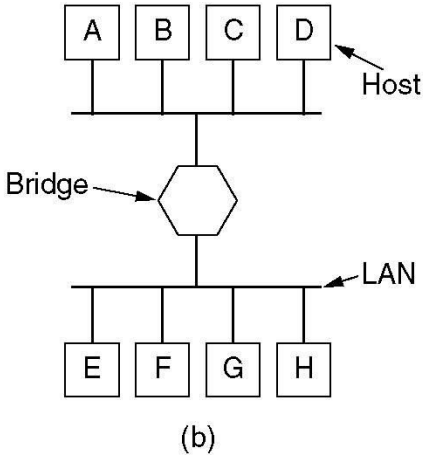


MAC Address	Port No.
2A-3B-AB-45-3B-5F	1
1b-3B-43-45-3B-4F	2
3F-35-6B-46-30-5F	3

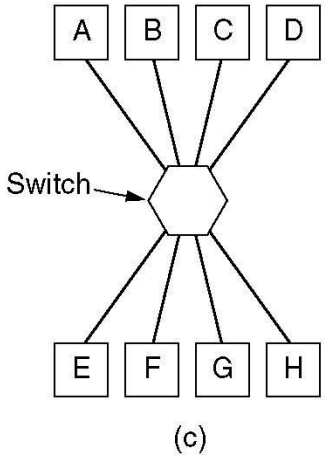
Networking Devices



(a) A hub.



(b) A bridge.



(c) a switch.

Router:

- A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.
- It has the same basic components as a standard desktop PC. It has a CPU, memory, a system bus, and various input/output interfaces. However, routers are designed to perform some very specific functions that are not typically performed by desktop computers.
- For example, routers connect and allow communication between two networks and determine the best path for data to travel through the connected networks.
- Router works at **Network Layer** of OSI Reference model.

Gateway

- As the name implies, a gateway is a network entity, also known as a protocol converter. It connects the computers of one network to another and defines the boundaries of the network. If two networks with different protocols want to be connected to each other, both networks need to have gateways that provide a point of presence and entry for computers from both networks to communicate. In other words, gateways can join different systems.
- Gateways exist in routers, switches, or PCs. When communication is carried out within the same network segment, there is no need to involve the gateway. Only when the host communicates with devices outside this network segment, all packets need to be sent to the gateway device and then forwarded through the processing protocol of the gateway device.

Gateway


Stateful Firewall
URL Filtering
Anti DDOS attack
Gateway
Extranet
Intranet
SPI
IPSec VPN

What is the difference between?

- **Bridge:** device to interconnect two LANs
- **Router:** device to interconnect SIMILAR networks, e.g. similar protocols and workstations and servers
- **Gateway:** device to interconnect DISSIMILAR protocols and servers, and Macintosh and IBM LANs and equipment

Data Transmission Media:

- Transmission media are the physical pathways that connect computers, other devices, and people on a network- the highways and byways that comprise the information superhighway.
- Each transmission medium requires specialized network hardware that has to be compatible with that medium.
- The transmission medium is the physical path by which a message travels from sender to receiver.
- Computers and telecommunication devices use signals to represent data.

Data Transmission Media:

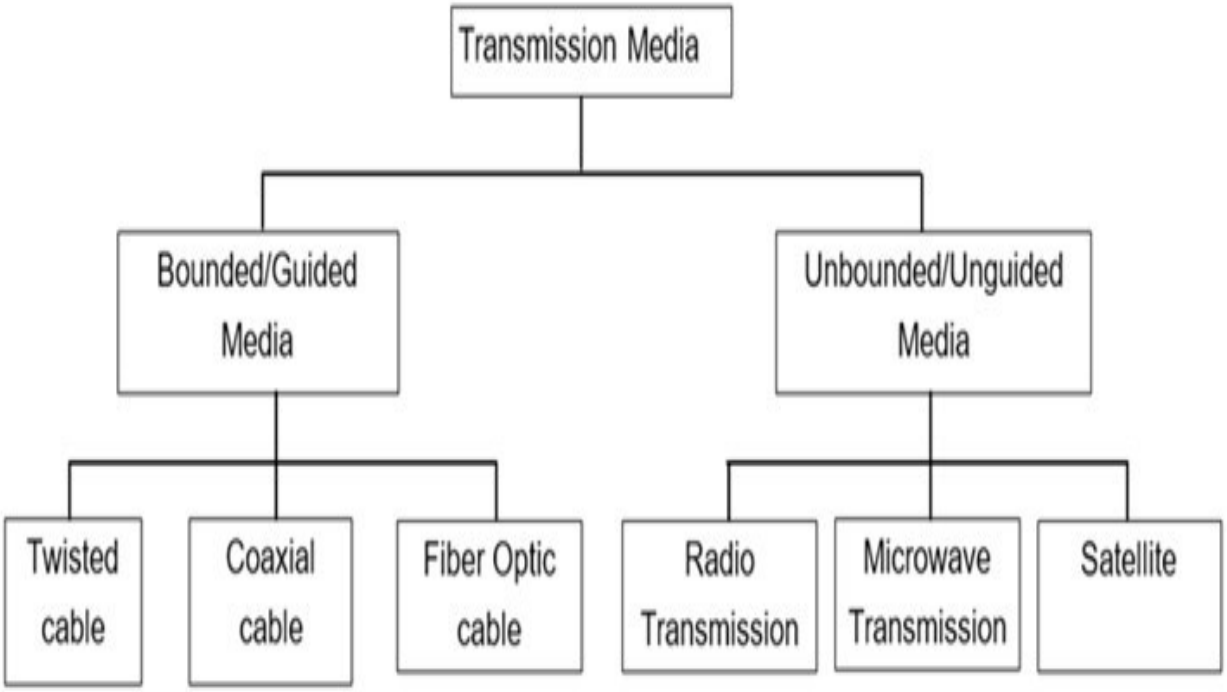
The transmission media can be grouped into.

Conducted/wired or guided media: use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver. Examples are twisted pair wires, coaxial cables and optical fiber.

Wireless or unguided media: use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals. Examples are terrestrial microwave, satellite microwave, broadcast radio and infrared.

Data Transmission Media:

- The transmission media can be grouped into.



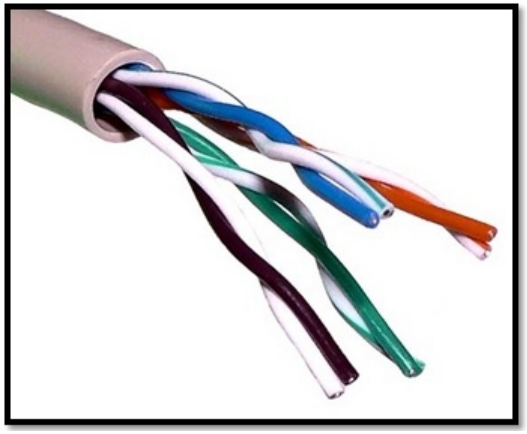
Twisted Pair (TP):

- One of the earliest guided transmission media is twisted pair cables. A twisted pair cable comprises of two separate insulated copper wires, which are twisted together and run in parallel. The copper wires are typically 1mm in diameter. One of the wires is used to transmit data and the other is the ground reference.
- A twisted pair cable consists of four pairs of copper wires coated with an insulating material like plastic or Teflon, twisted together. Twisting reduces electromagnetic interference (or noise) .
- Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable

Twisted Pair (TP):

Applications of Twisted-Pair Cables

- In telephone lines
- In LANs



- TP is of two kinds
  - Shielded Twisted Pair (STP),
  - Unshielded Twisted Pair (UTP).

Twisted Pair (TP):

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. I UTP is the most commonly used medium for transmission over short distances up to 100m. Out of the four pairs of wires in a UTP cable, only two pairs are used for communication.

Advantages:

- Least expensive
- Easy to install
- High-speed capacity
- Lower capacity and performance in comparison to STP
- Short distance transmission

Twisted Pair (TP):

Shielded Twisted Pair (STP):

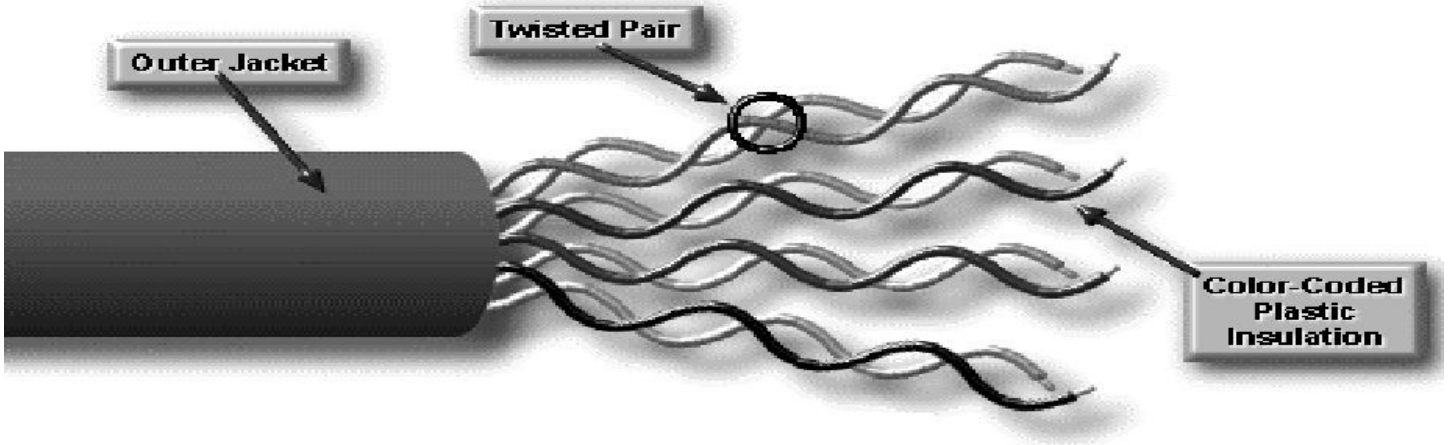
- This type of cable consists of a special jacket to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
- STP cable has an extra layer of metal foil between the twisted pair of copper wires and the outer covering. The metal foil covering provides additional protection from external disturbances. STP is costly and is generally used in networks where cables pass closer to devices that cause external disturbances.

Advantages:

- Better performance at a higher data rate in comparison to UTP
- Comparatively faster
- Comparatively difficult to install and manufacture
- More expensive
- Bulky

UTP

- Types of UTP
  - CAT 3: data rate up to 10 Mbps(Ethernet)
  - CAT 4: data rate up to 20 Mbps(Token Ring)
  - CAT 5: data rate up to 100 Mbps(Fast Ethernet)
  - CAT 5e: data rate up to 1000 Mbps(Gigabit Ethernet)
  - CAT 6: data rate up to 10 Gbps(Gigabit Ethernet)
- Maximum cable length with out repeater 100m



Cable Color Coding

- Cabling Standards :
- EIA/TIA 568 A color coding : g G o B b O br Br
- EIA/TIA 568 B color coding : o O g B b G br Br

- Where
  - g - light green or Stripped green (wire)
  - G - Solid Green (wire)
- Similar For other wire as well.

UTP Cable Types

- Straight through Cable: A-A or B-B setting, used to connect different layer device, e.g. hub to computer.

- Cross-over Cable: A-B or B-A setting, used to connect same layer device, e.g. computer to computer, router to computer.

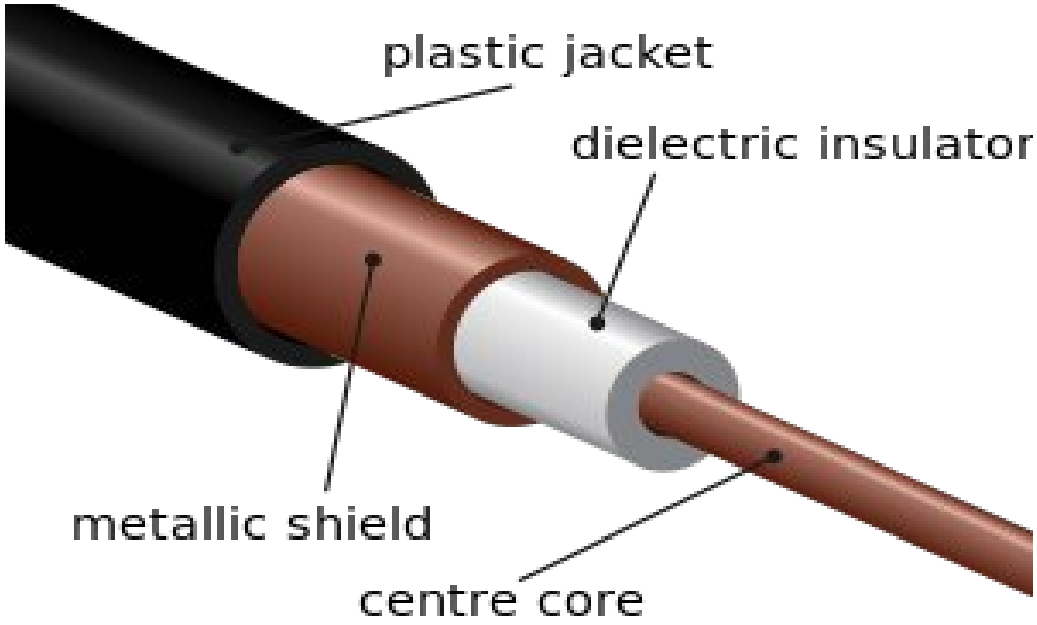
Coaxial Cable:

Coaxial cables are the guided media that transmit the signal of higher frequency range compared to twisted pair cable. Coaxial cables are also called *coax*. (short form).

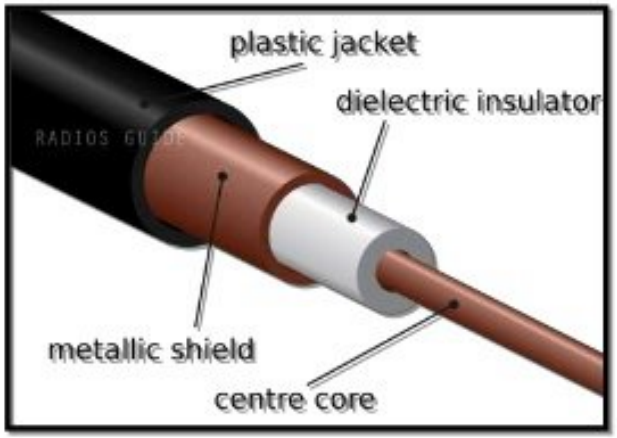
Two types of coaxial cables are widely used: 50 ohm cable and 75 ohm cable. 50 ohm cable is used for digital transmission and 75 ohm cable is used for analog transmission.

It has a large bandwidth and low losses. Co-axial cables are easy to install.

A coaxial cable consists of many small cables in a protective cover. The cover shields the cable from physical dangers as well as from electromagnetic interference.


plastic jacket
dielectric insulator
metallic shield
centre core

Coaxial Cable:



INSIDE VIEW

OUTSIDE VIEW

Coaxial Cable:

Advantages of Coaxial Cables

1. It can be used for both analog and digital transmission.
2. It offers higher bandwidth as compared to twisted pair cable.
3. Because of better shielding in coaxial cable, loss of signal is less.
4. Better shielding also offers good noise immunity.
5. It is relatively inexpensive as compared to optical fibers.
6. It has lower error rates as compared to twisted pair.

Coaxial Cable:

DISADVANTAGES

- Unwanted noise and picture ghosting.
- More expensive.
- High attenuation.
- The thicker the cable , the more difficult to work with.
- Effect of current flow.

Coaxial Cable:

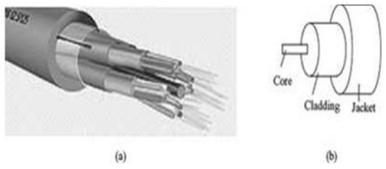
Applications of Co-axial Cables:

(1) Cable TV

(2) Digital transmission

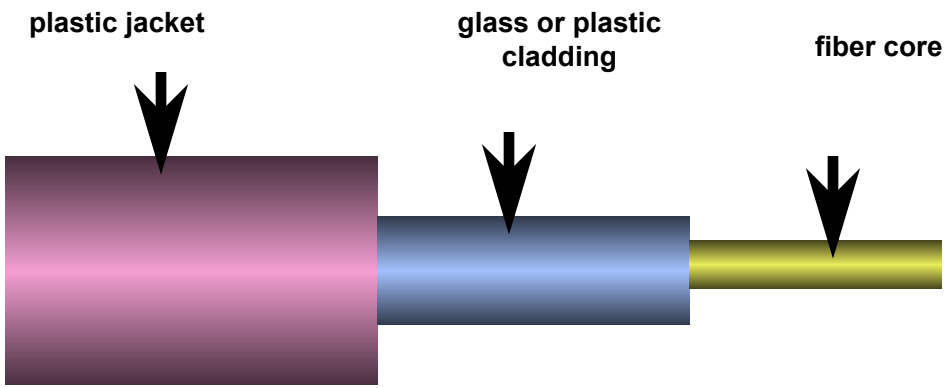
Optical Fiber:

- Optical fibers are being used for transmission of information over large distances more cost effectively than the copper wire connection. Communication systems are now unthinkable without fiber optics.
- Optical fiber transmits data as light signals instead of electric signals.
- An optical fiber cable consists of
  - ✓ Core - optical fiber conductor (glass) that transmits light,
  - ✓ Cladding - an optical material that surrounds the core to prevent any light from escaping the core, and
  - ✓ Jacket - outer covering made of plastic to protect the fiber from damage.



Fiber Optic Layers

- consists of three concentric sections



The Advantages of Optical Fibers over wires are:

Bandwidth - Fiber optic cables have a much greater bandwidth than metal cables.

Low Power Loss - An optical fiber offers low power loss, which allows for longer transmission distances

Interference - Fiber optic cables are immune to electromagnetic interference. It can also be run in electrically noisy environments without concern as electrical noise will not affect fiber.

Weight- Fiber optic cables are much thinner and lighter than metal wires.

The Disadvantages of Optical Fiber are:

- **Expensive to Install** - The optical fibers are more expensive to install, and they have to be installed by the specialists..
- **Highly Susceptible** - The fiber optic cable is a small and compact cable, and it is highly susceptible to becoming cut or damaged during installation or construction activities.
- **Can't Be Curved** -. The fibers can be broken or have transmission losses when wrapped around curves of only a few centimeters radius.

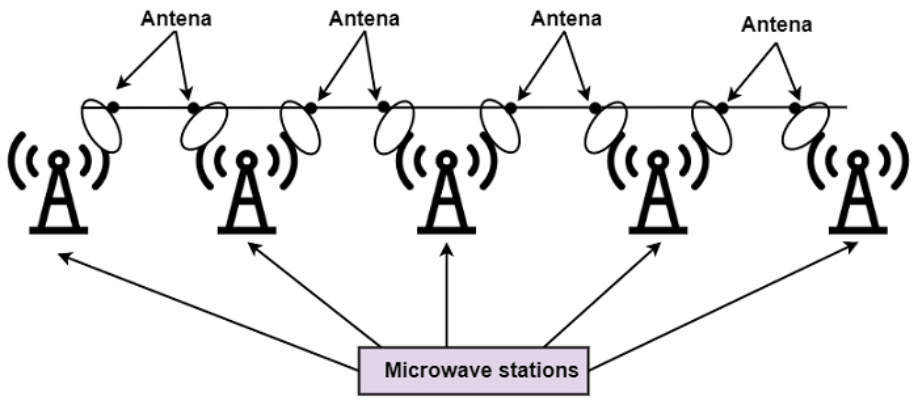
Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

Radio Waves

- Waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves. Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- These waves are easy to generate and these can travel along long distances. These waves are omni directional in nature which means that they can travel in all the directions. They are widely used for the communication between both indoor and outdoor because they have the property that they can penetrate through the walls very easily. These waves are usually used for AM and FM radio, television, cellular phones and wireless LAN. It is a technique where data is transmitted using radio waves and therefore energy travels through the air rather than copper or glass.

Microwave Transmission:

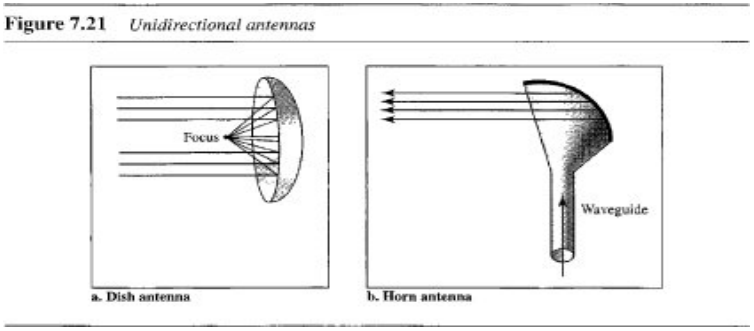
- The transmission of data through microwave in telecommunication involves the sending and receiving of microwave signals over a microwave link.
- Microwave links are used for point-to-point communications. It is a point-to-point, rather than a broadcast, transmission system. Additionally, each antenna must be within line of sight of the next antenna. If the frequencies are higher within the microwave band given in this impact is more than lower frequencies in the same band.



Microwave Communication

Micro Waves

- Electromagnetic waves having frequencies between 1 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. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.



Micro Waves

- 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 (see Figure). A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

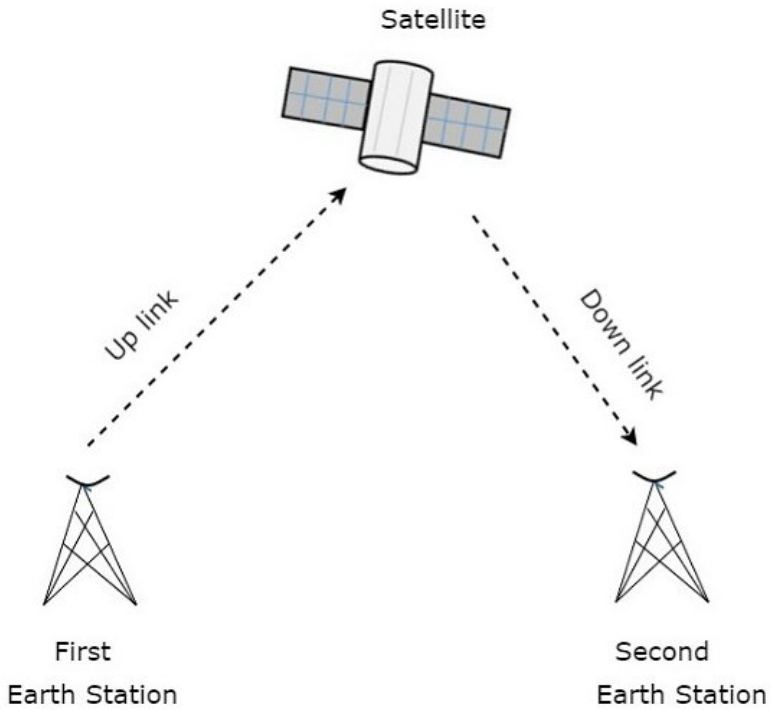
Infrared

- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. 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. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.
- The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

Satellite Transmission:

- If the communication takes place between any two earth stations through a satellite, then it is called as **satellite communication**. In this communication, electromagnetic waves are used as carrier signals.
- These signals carry the information such as voice, audio, video or any other data between ground and space and vice-versa.
- Telephone, radio, television, internet, and military applications use satellite communications. Believe it or not, more than 2000 artificial satellites are hurtling around in space right above your heads.

Satellite Transmission:



Satellite Transmission:

- A **satellite** is a body that moves around another body in a particular path. A communication satellite is nothing but a microwave repeater station in space. It is helpful in telecommunications, radio and television along with internet applications.
- A **repeater** is a circuit, which increases the strength of the received signal and then transmits it. But, this repeater works as a **transponder**. That means, it changes the frequency band of the transmitted signal from the received one.
- The frequency with which, the signal is sent into the space is called as **Uplink frequency**. Similarly, the frequency with which, the signal is sent by the transponder is called as **Downlink frequency**.

Switching Techniques

- Whenever we are dealing with a **large network** or say a very long-distance data transmission has to take place, this can't be done directly without any external hardware support. Hence, we must have a dedicated path for our data packets to traverse. Since there are so many choices for which path to take, so we have to select a particular path. This selecting of the path on which our data packets will be transmitted is known as **Switching**.
- In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels.
- There are three typical switching techniques available for digital traffic.
    1. **Circuit Switching**
    2. **Message Switching**
    3. **Packet Switching**

Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Advantages Of Circuit Switching:

- In the case of Circuit Switching technique, the communication channel is dedicated.
- Because the circuit is fixed, the data transfer rate remains constant throughout the session.
- Suitable for real-time applications like voice calls, as data is delivered in the correct order without delay.
- After a connection is established, there is no network congestion for that session since resources are reserved.

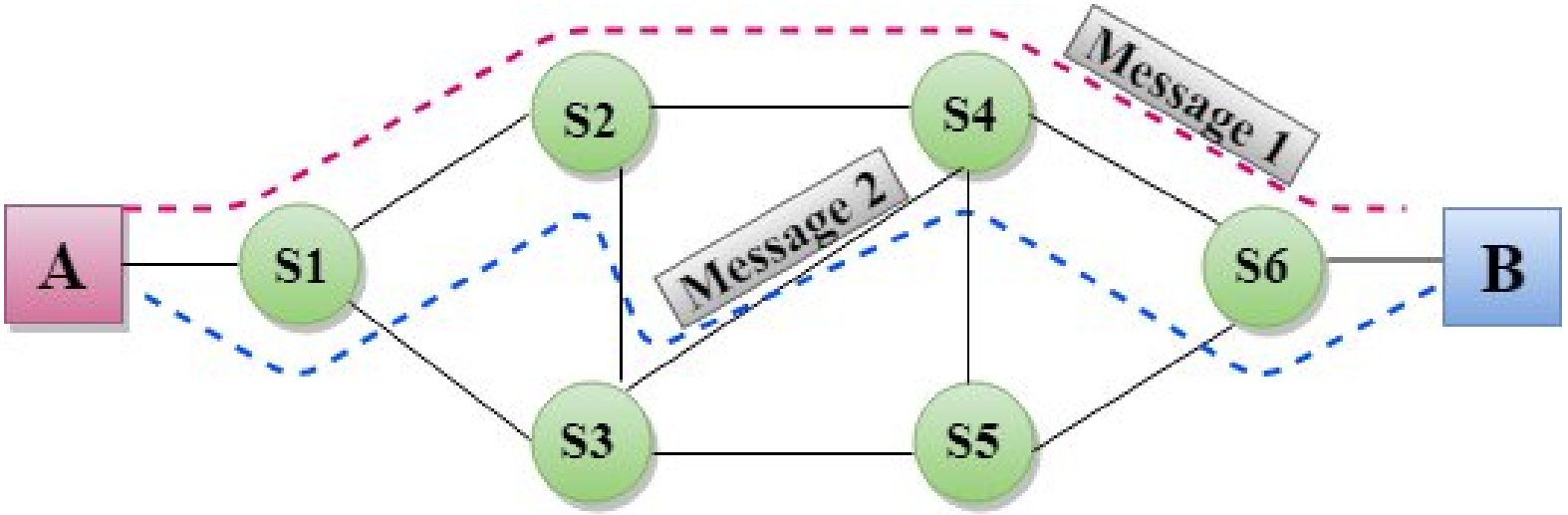
Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- • Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

Message Switching



Advantages Of Message Switching

- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Messages are stored at intermediate nodes and forwarded when the path is available, reducing the chance of data loss.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- Entire messages (not just small packets) can be transmitted, making it suitable for text documents and files.

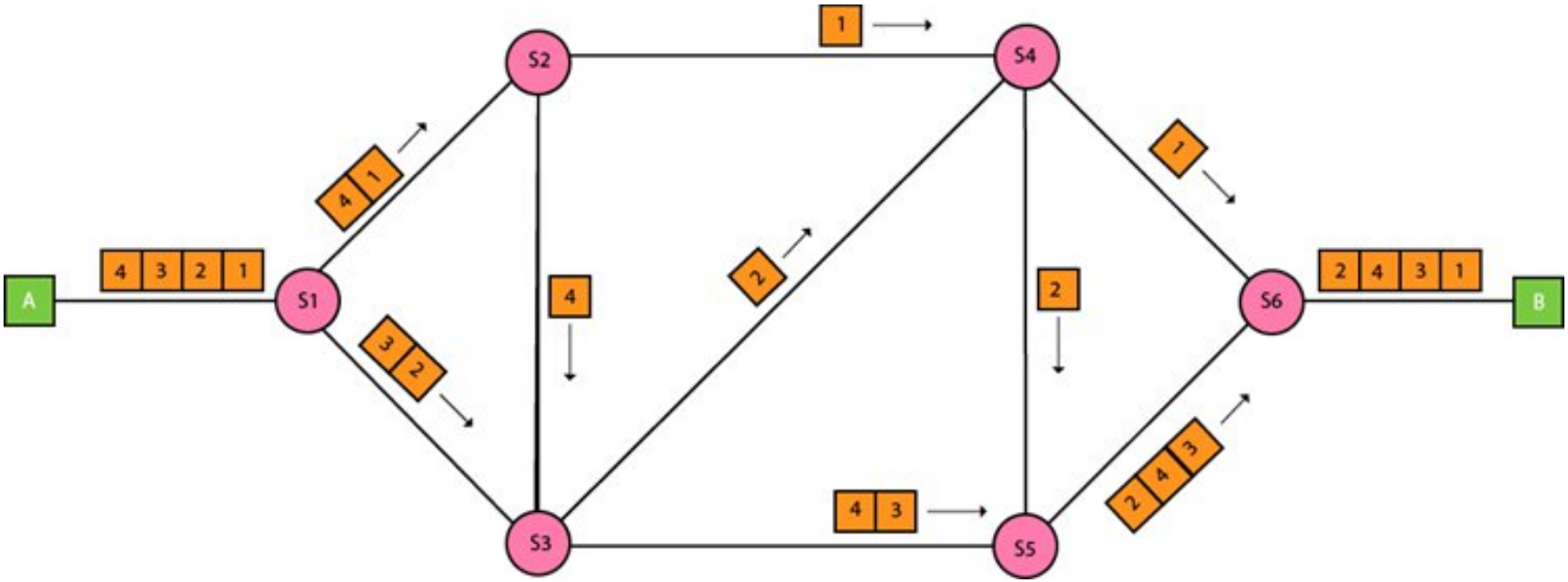
Disadvantages Of Message Switching

- Because the entire message is stored at each node before forwarding, it can take a long time to reach the destination.
- Intermediate devices need enough memory to store whole messages, which can be a problem for big messages.
- Not suitable for voice or video calls, where data must arrive instantly — message switching is too slow for that.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

Packet Switching



Feature	Circuit Switching	Message Switching	Packet Switching
Path Establishment	Before communication	No path – store and forward	No fixed path – per packet
Speed	Fast once connected	Slow (waiting at each node)	Fast and efficient
Example	Telephone call	Telegraph, email	Internet, Zoom call, browsing
Resource Allocation	Dedicated	Shared	Shared
Data Handling	Continuous stream	Whole message at once	Data divided into packets

Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

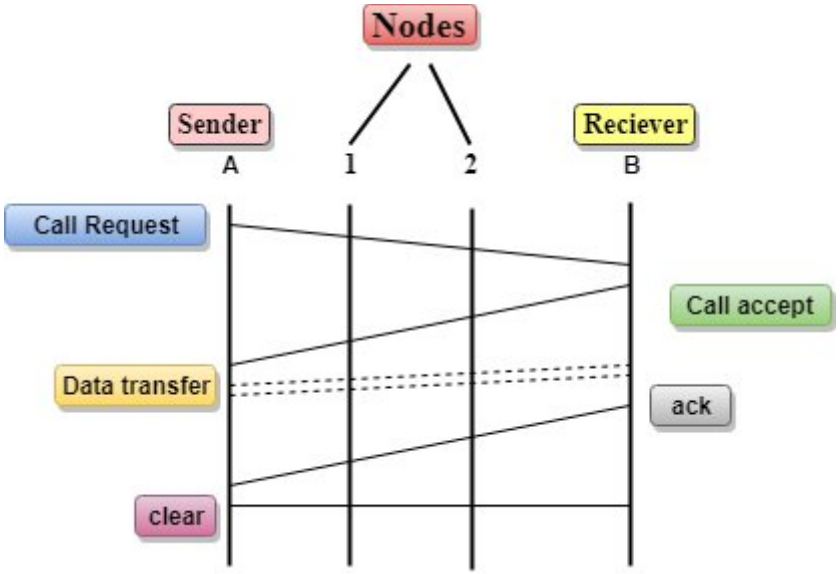
- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Approaches Of Packet Switching:

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Approaches Of Packet Switching:



Approaches Of Packet Switching:

- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Advantages Of Packet Switching:

•**Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

•**Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.

•**Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

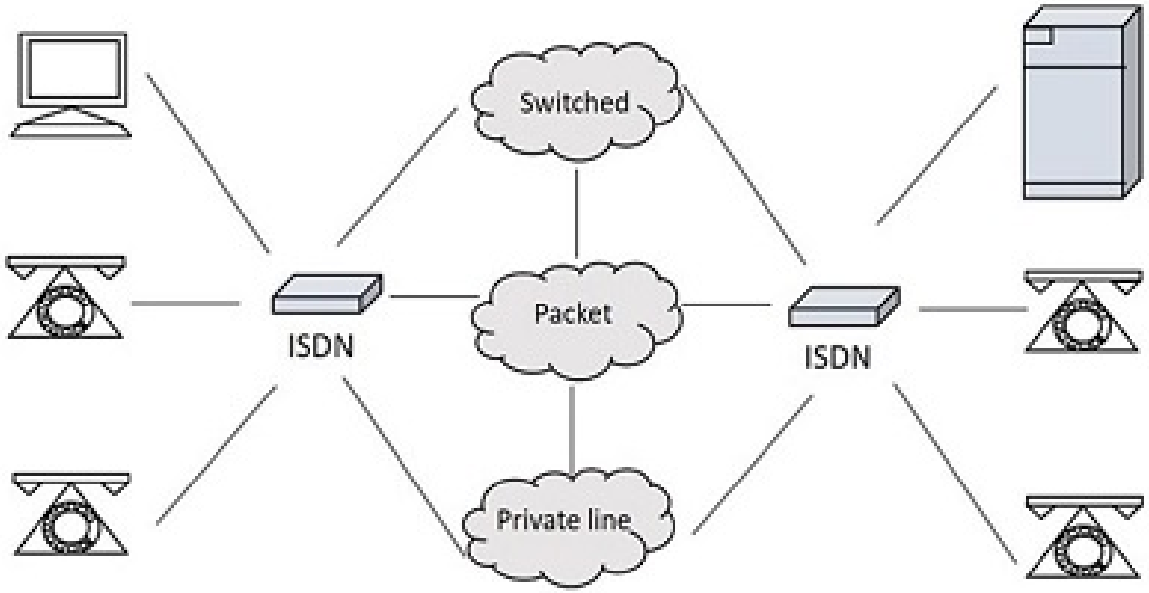
- Packets can take different routes to the destination, causing **delay** and **variation in arrival time** (jitter), which is bad for voice or video calls.
- In case of network congestion or failure, **some packets may be lost**, leading to incomplete data unless retransmitted.
- Every packet contains a **header** (address and control info), which adds overhead and reduces efficiency for small data.
- Needs **advanced protocols** (like TCP/IP) to manage packet ordering, delivery, error checking, and retransmission.

Integrated Service Digital Network (ISDN)

- Earlier, the transmission of data and voice both were possible through normal POTS, Plain Old Telephone Systems. With the introduction of Internet came the advancement in telecommunication too. Yet, the sending and receiving of data along with voice was not an easy task. One could use either the Internet or the Telephone. The invention of ISDN helped mitigate this problem.
- The process of connecting a home computer to the Internet Service Provider used to take a lot of effort. The usage of the modulator-demodulator unit, simply called the MODEM was the essential thing to establish a connection. The following figure shows how the model worked in the past.

Integrated Service Digital Network (ISDN)

- SDN was first defined in the CCITT red book in 1988.The **Integrated Services of Digital Networking**, in short ISDN is a telephone network-based infrastructure that allows the transmission of voice and data simultaneously at a high speed with greater efficiency. This is a circuit switched telephone network system, which also provides access to Packet switched networks.
- The model of a practical ISDN is as shown below.



Integrated Service Digital Network (ISDN)

ISDN supports a variety of services. A few of them are listed below −

- Voice calls
- Facsimile
- Videotext
- Teletext
- Electronic Mail
- Database access
- Data transmission and voice
- Connection to internet
- Electronic Fund transfer
- Image and graphics exchange
- Document storage and transfer
- Audio and Video Conferencing
- Automatic alarm services to fire stations, police, medical etc.

Features of ISDN

- Uses Digital Signal
- Uses Existing telephone wiring
- Charges are generally based on the duration of call (How long the WAN link was used)
- Can transport many types of Network traffic (Voice, Data, Video, Text, Graphics etc)
- Faster Data transfer rate than modems
- Faster Call setup than Modems

Integrated Service Digital Network (ISDN)

Types of ISDN

Among the types of several interfaces present, some of them contains channels such as the **B-Channels** or Bearer Channels that are used to transmit voice and data simultaneously; the **D- Channels** or Delta Channels (carry control signal) that are used for signaling purpose to set up communication.

The ISDN has several kinds of access interfaces such as −

- Basic Rate Interface (BRI)
- Primary Rate Interface (PRI)
- Narrowband ISDN
- Broadband ISDN

Integrated Service Digital Network (ISDN)

Basic Rate Interface (BRI)

The Basic Rate Interface or Basic Rate Access, simply called the **ISDN BRI Connection** uses the existing telephone infrastructure. The BRI configuration provides **two data** or bearer channels at **64 Kbits/sec** speed and one control or delta channel at **16 Kbits/sec**. This is a standard rate.

The ISDN BRI interface is commonly used by smaller organizations or home users or within a local group, limiting a smaller area.

Integrated Service Digital Network (ISDN)

Primary Rate Interface (PRI)

The Primary Rate Interface or Primary Rate Access, simply called the ISDN PRI connection is used by enterprises and offices. The PRI configuration is based on T-carrier or T1 in the US, Canada and Japan countries consisting of **23 data** or bearer channels and one control or delta channel, with 64kbps speed for a bandwidth of 1.544 M bits/sec. The PRI configuration is based on E-carrier or E1 in Europe, Australia and few Asian countries consisting of **30 data** or bearer channels and **two-control** or delta channel with 64kbps speed for a bandwidth of 2.048 M bits/sec.

The ISDN PRI interface is used by larger organizations or enterprises and for Internet Service Providers.

Integrated Service Digital Network (ISDN)

Narrowband ISDN

The Narrowband Integrated Services Digital Network is called the **N-ISDN**. This can be understood as a telecommunication that carries voice information in a narrow band of frequencies. This is actually an attempt to digitize the analog voice information. This uses 64kbps circuit switching.

The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Integrated Service Digital Network (ISDN)

Broadband ISDN

The Broadband Integrated Services Digital Network is called the **B-ISDN**. This integrates the digital networking services and provides digital transmission over ordinary telephone wires, as well as over other media. The broadband ISDN speed is around 2 MBPS to 1 GBPS and the transmission is related to ATM, i.e., Asynchronous Transfer Mode. The broadband ISDN communication is usually made using the fiber optic cables.

As the speed is greater than 1.544 Mbps, the communications based on this are called **Broadband Communications**. The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network. Though a user can access this flow of information, he cannot control it.

Integrated Service Digital Network (ISDN)

ISDN Standards:

The ISDN works based on the standards defined by ITU-T. The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

- To support switched and non-switched applications
- To support voice and non-voice applications
- Reliance on 64-kbps connections
- Intelligence in the network
- Layered protocol architecture
- Variety of configurations

Integrated Service Digital Network (ISDN)

Advantages of ISDN

Advantage	Explanation
Integrated Services	Voice, data, video on one line
Digital Quality	Clearer voice and data transmission
Fast Call Setup	Quick connection establishment
Multiple Channels	Simultaneous calls and data transfers
Higher Speed	Faster than analog modem speeds

Integrated Service Digital Network (ISDN)

Disadvantages of ISDN

Disadvantage	Explanation
Cost	High installation and service fees
Bandwidth	Limited to 64 Kbps per channel
Equipment	Needs special ISDN devices
Complexity	Setup and maintenance difficulties