**Networking Topologies:**

1. In computer networking, a network topology refers to the arrangement or layout of the various interconnected elements (nodes, devices, and links) within a network.
2. It describes how these components are connected and how data flows between them.
3. Different network topologies provide different levels of performance, scalability, fault tolerance, and cost-effectiveness.

Here are some commonly used network topologies:

* Mesh Topology
* Star Topology
* Bus Topology
* Ring Topology
* Hybrid Topology

1. **Mesh Topology:**

In a mesh topology, every device is connected to every other device in the network. This provides multiple paths for data to travel, improving fault tolerance and redundancy. Mesh topologies can be full mesh (direct connection between every pair of devices) or partial mesh (only some devices have direct connections).

**Advantages of Mesh Topology**

* Communication is very fast between the nodes.
* Mesh Topology is robust because a mesh topology refers to its ability to maintain connectivity, adapt to failures, and provide uninterrupted communication even in challenging circumstances.
* The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
* Provides security and privacy. (not centralized)

**Drawbacks of Mesh Topology**

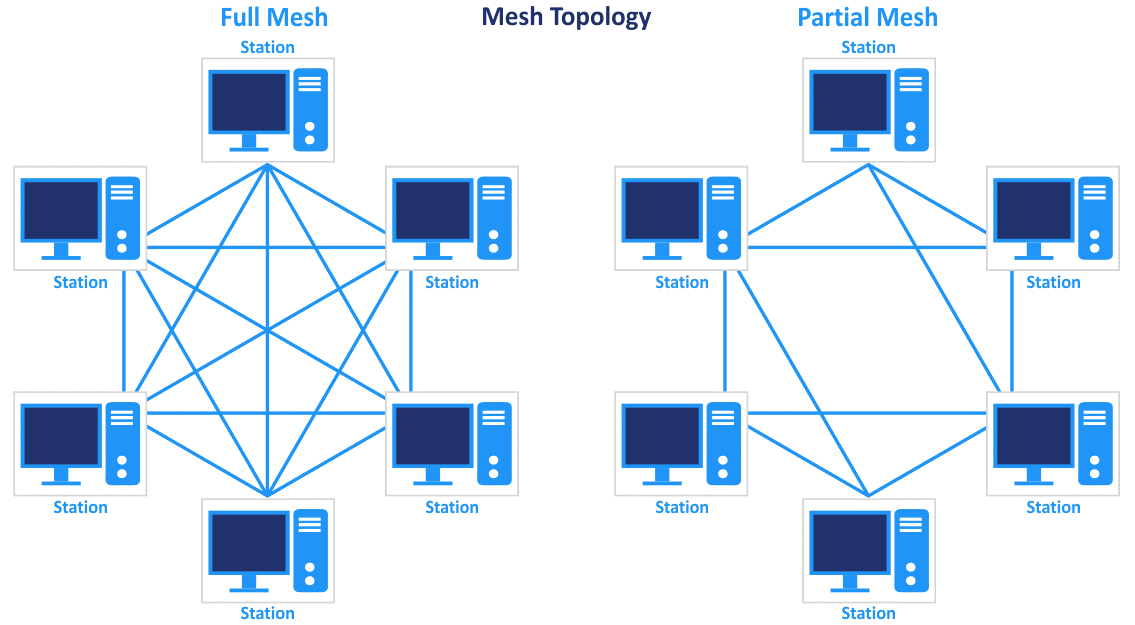
* Installation and configuration are difficult.
* The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
* The cost of maintenance is high.

**Protocols:**

The protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

**Example:**

* 1. A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels.
  2. This topology is also used in military communication systems and aircraft navigation systems.



1. **Star Topology:**

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. Coaxial cables or RJ-45 cables are used to connect the computers.

**Protocols:**

In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

**Advantages:**

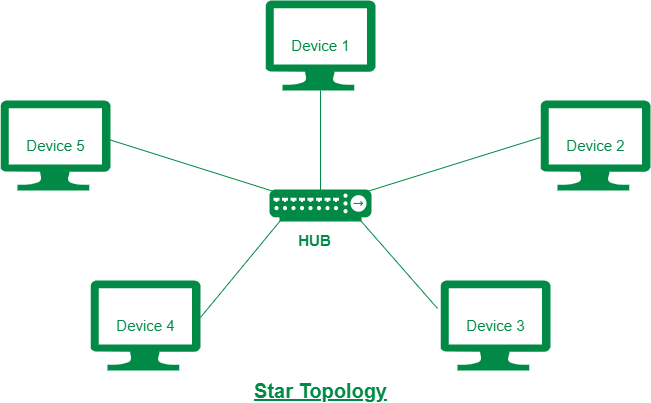
* If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
* Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
* It is Robust. If one link fails only that link will affect and not other than that.
* Easy to fault identification and fault isolation.
* Star topology is cost-effective as it uses inexpensive coaxial cable.

**Disadvantages:**

* If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
* The cost of installation is high.
* Performance is based on the single concentrator i.e. hub.

**Example:**

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.



1. **Bus Topology:**

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

**Advantages:**

* It is very simple to design.
* The cost of the cable is less compared to other topologies, but it is used to build small networks.
* Bus topology is familiar technology as installation and troubleshooting techniques are well known.
* Adding a new device or network node is relatively easy by connecting it to the main bus cable.

**Disadvantages:**

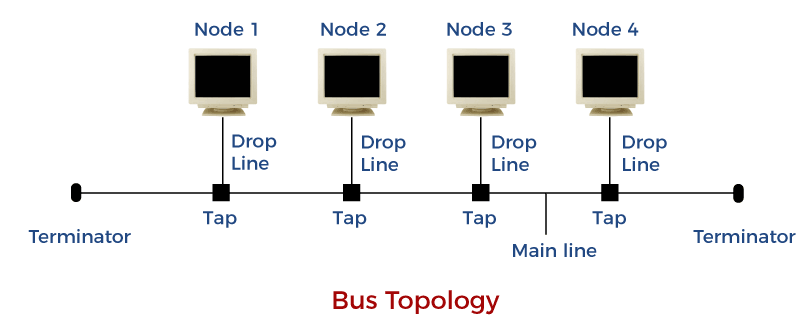
* A bus topology is quite simpler, but still, it requires a lot of cabling.
* If the common cable fails, then the whole system will crash down.
* Adding new devices to the network would slow down networks.
* Security is very low.
* It is very difficult to troubleshoot in a bus topology, as each node has to be checked.
* As the traffic is shared by all the nodes in the network, the performance of the network decreases as the traffic increases.

**Protocols:**

In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

**Example:**

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.



1. **Ring Topology:**

In a ring topology, devices are connected in a circular manner, where each device is connected to exactly two other devices, forming a ring-like structure. Data is transmitted around the ring in one direction, and each device receives and forwards the data until it reaches its intended destination.

**Protocol:**

In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

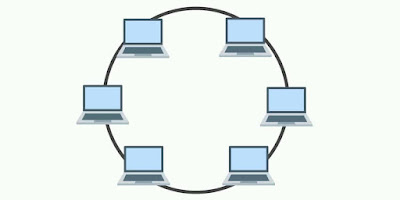
To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.

**Advantages:**

* The data transmission is high-speed.
* The possibility of collision is minimum in this type of topology.
* Easy to configure.
* Cheap to install and expand.
* It is less costly than a star topology.

**Disadvantages:**

* The failure of a single node in the network can cause the entire network to fail.
* Troubleshooting is difficult in this topology.
* The addition of stations in between or the removal of stations can disturb the whole topology.
* Less secure.

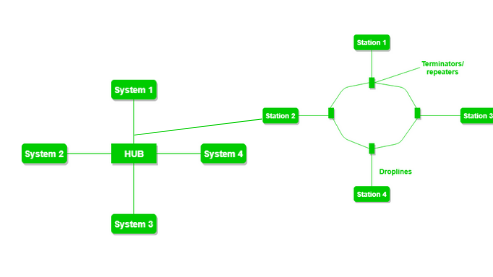


1. **Hybrid Topology:**

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above.

**Protocols:**

Each individual topology uses the protocol that has been discussed earlier.



**Figure 6**: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

**Advantages of Hybrid Topology**

* This topology is **very flexible**.
* The size of the network can be easily expanded by **adding new devices.**

**Drawbacks of Hybrid Topology**

* It is challenging**to design the architecture** of the Hybrid Network.
* **Hubs**used in this topology are**very expensive.**
* The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

**Example:**

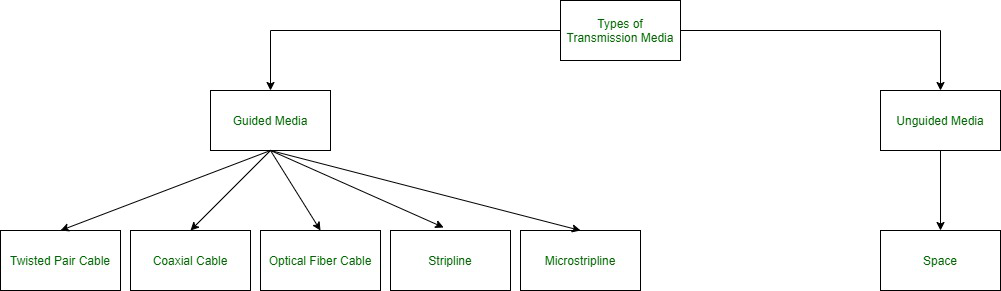
A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices.

**Transmission Media:**

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

Some factors need to be considered for designing the transmission media:

* **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
* **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
* **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.



**1. Guided Media:**

It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

**Features**:

* High Speed
* Secure
* Used for comparatively shorter distances

There are 3 major types of Guided Media:

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

* **Unshielded Twisted Pair (UTP):**   
  UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



**Advantages:**

⇢ Least expensive

⇢ Easy to install

⇢ High-speed capacity

**Disadvantages:**

⇢ Susceptible to external interference

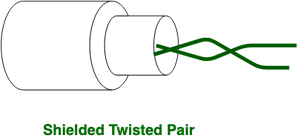
⇢ Lower capacity and performance in comparison to STP

⇢ Short distance transmission due to attenuation

**Applications:**

Used in telephone connections and LAN networks

* **Shielded Twisted Pair (STP):**   
  This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



**Advantages:**

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

**Disadvantages:**

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

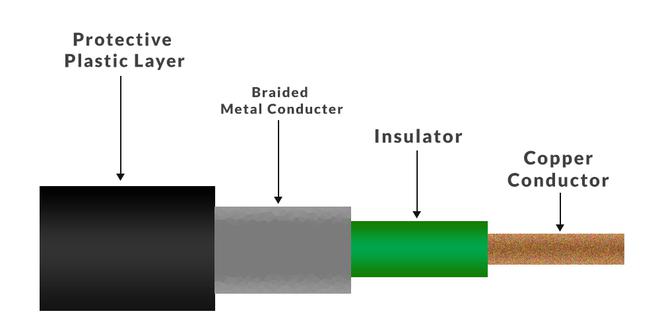
**Applications:**

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

**2) Coxial Cable:**   
A coaxial cable is an electrical cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevents signal interference and cross talk. Coaxial cable is also known as **coax.**

The core copper conductor is used for the transmission of signals and the insulator is used to provide insulation to the copper conductor and the insulator is surrounded by a braided metal conductor which helps to prevent the interference of electrical signals and prevent cross talk. This entire setup is again covered with a protective plastic layer to provide extra safety to the cable.

**Structure of Coaxial Cable**



**Copper conductor:**A central conductor, which consists of copper. The conductor is the point at which data transmits.

**Insulator:** Dielectric plastic insulation around the copper conductor. it is used to maintain the spacing between the center conductor and shield.

**Braided mesh:** A braided mesh of copper helps to shield from electromagnetic interference, The braid provides a barrier against EMI moving into and out of the coaxial cable.

**Protective plastic layer:** An external polymer layer, which has a plastic coating. It is used to protect internal layers from damages.

**Types of Coaxial cables**

1. **Hardline coaxial cable**
2. **Flexible coaxial cable**
3. **Semi-rigid coaxial cable**
4. **Formable coaxial cable**
5. **Twinaxial cable**
6. **Triaxial cable**
7. **Rigid coaxial cable**

**Applications of Coaxial cable:**

The coaxial cables are used in Ethernet LANs and also used in MANs

1. **Television:**Coaxial cable used for television would be 75 Ohm and RG-6 coaxial cable.
2. **Internet:**Coaxial cables are also used for carrying internet signals, RG-6 cables are used for this.
3. **CCTV:** The coaxial cables are also used in CCTV systems and both RG-59 AND RG-6 cables can be used.
4. **Video:**The coaxial cables are also used in video Transmission the RG-6 is used for better digital signals and RG-59 for lossless transmission of video signals.
5. **HDTV**: The HDTV uses RG-11 as it provides more space for signals to transfer.

**Advantages**

1. Coaxial cables support high bandwidth.
2. It is easy to install coaxial cables.
3. coaxial cables have better cut-through resistance so they are more reliable and durable.
4. Less affected by noise or cross-talk or electromagnetic inference.
5. Coaxial cables support multiple channels

**Disadvantages**

1. Coaxial cables are expensive.
2. The coaxial cable must be grounded in order to prevent any crosstalk.
3. As a Coaxial cable has multiple layers it is very bulky.
4. There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

**3) Fibre Optic:**

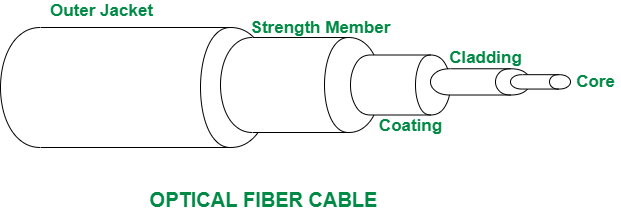
Fiber optics, or optical fiber, refers to the technology that transmits information as light pulses along a glass or plastic fiber.

A fiber optic cable can contain a varying number of these glass fibers -- from a few up to a couple hundred. Another glass layer, called *cladding*, surrounds the glass fiber core. The buffer tube layer protects the cladding, and a jacket layer acts as the final protective layer for the individual strand.

Fiber optics transmit data in the form of light particles -- or photons -- that pulse through a fiber optic cable. The glass fiber core and the cladding each have a different refractive index that bends incoming light at a certain angle.

When light signals are sent through the fiber optic cable, they reflect off the core and cladding in a series of zig-zag bounces, following a process called *total internal reflection*. The light signals do not travel at the [speed of light](https://www.techtarget.com/whatis/definition/speed-of-light) because of the denser glass layers, instead traveling about 30% slower than the speed of light.

Fiber optic cables are now able to support up to 10 Gbps signals. Typically, as the bandwidth capacity of a fiber optic cable increases, the more expensive it becomes.



**Advantages and disadvantages of fiber optics**

Fiber optic cables are used mainly for their advantages over copper cables. Advantages include the following:

* They support higher bandwidth capacities.
* Light can travel further without needing as much of a signal boost.
* They are less susceptible to interference, such as electromagnetic interference.
* They can be submerged in water.
* Fiber optic cables are stronger, thinner and lighter than copper wire cables.
* They do not need to be maintained or replaced as frequently.

**Disadvantages:**

* Copper wire is often cheaper than fiber optics.
* Glass fiber requires more protection within an outer cable than copper.
* Installing new cabling is labor-intensive.
* Fiber optic cables are often more fragile. For example, the fibers can be broken or a signal can be lost if the cable is bent or curved around a radius of a few centimeters.

**Applications:**

1. Computer networking and broadcasting
2. Internet and cable television
3. Undersea environments
4. Military and space
5. Medical

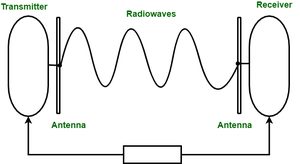
**2. Unguided Media:**   
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

**Features:**

* The signal is broadcasted through air
* Less Secure
* Used for larger distances

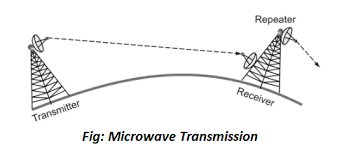
There are 3 types of Signals transmitted through unguided media:

**(i) Radio waves –**   
These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



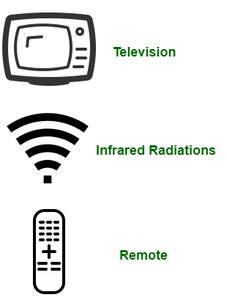
Further Categorized as (i) Terrestrial and (ii) Satellite.

**(ii) Microwaves –**   
It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.



*Microwave Transmission*

**(iii) Infrared –**   
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



**Transmission Modes:**

Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

**There are three types of transmission mode:-**

https://media.geeksforgeeks.org/wp-content/uploads/transmissionmodes.png

These are explained as following below.

**1. Simplex Mode** **–**  
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.   
**Example**: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

https://media.geeksforgeeks.org/wp-content/uploads/SiMpleduplex.png

**Advantages:**

* Simplex mode is the easiest and most reliable mode of communication.
* It is the most cost-effective mode, as it only requires one communication channel.
* There is no need for coordination between the transmitting and receiving devices, which simplifies the communication process.
* Simplex mode is particularly useful in situations where feedback or response is not required, such as broadcasting or surveillance.

**Disadvantages:**

* Only one-way communication is possible.
* There is no way to verify if the transmitted data has been received correctly.
* Simplex mode is not suitable for applications that require bidirectional communication.

**2. Half-Duplex Mode** **–**  
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases 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.   
**Example**: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

Channel capacity=Bandwidth \* Propagation Delay

https://media.geeksforgeeks.org/wp-content/uploads/halfduplex.png

**Advantages:**

* Half-duplex mode allows for bidirectional communication, which is useful in situations where devices need to send and receive data.
* It is a more efficient mode of communication than simplex mode, as the channel can be used for both transmission and reception.
* Half-duplex mode is less expensive than full-duplex mode, as it only requires one communication channel.

**Disadvantages:**

* Half-duplex mode is less reliable than Full-Duplex mode, as both devices cannot transmit at the same time.
* There is a delay between transmission and reception, which can cause problems in some applications.
* There is a need for coordination between the transmitting and receiving devices, which can complicate the communication process.

**3. Full-Duplex Mode** **–**  
In full-duplex mode, 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 another 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 is divided between signals traveling in both directions.

Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.   
**Example**: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

Channel Capacity=2\* Bandwidth\*propagation Delay

https://media.geeksforgeeks.org/wp-content/uploads/fullduplex.png

**Advantages:**

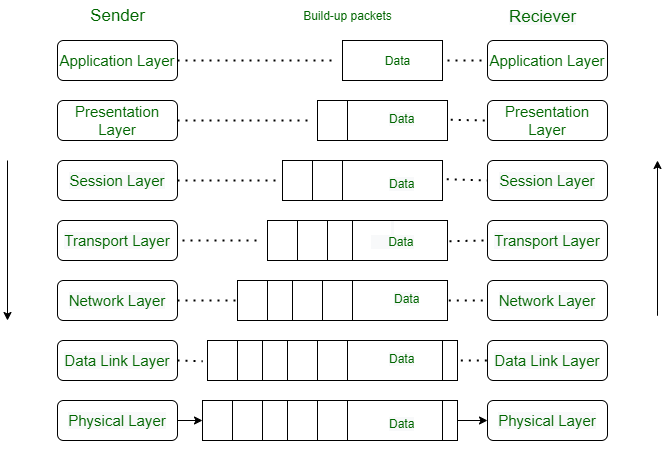
* Full-duplex mode allows for simultaneous bidirectional communication, which is ideal for real-time applications such as video conferencing or online gaming.
* It is the most efficient mode of communication, as both devices can transmit and receive data simultaneously.
* Full-duplex mode provides a high level of reliability and accuracy, as there is no need for error correction mechanisms.

**Disadvantages:**

* Full-duplex mode is the most expensive mode, as it requires two communication channels.
* It is more complex than simplex and half-duplex modes, as it requires two physically separate transmission paths or a division of channel capacity.
* Full-duplex mode may not be suitable for all applications, as it requires a high level of bandwidth and may not be necessary for some types of communication.

**OSI MODEL:**

1. OSI stands for **Open Systems Interconnection**.
2. It has been developed by ISO – ‘**International Organization for Standardization**‘, in the year 1984.
3. It is a 7-layer architecture with each layer having specific functionality to perform.
4. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

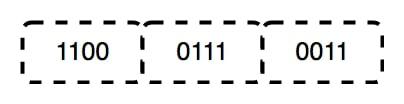


**Layers of OSI Model**

1. [Physical Layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/)
2. [Data Link Layer](https://www.geeksforgeeks.org/data-link-layer/)
3. [Network Layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/)
4. [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/)
5. [Session Layer](https://www.geeksforgeeks.org/session-layer-in-osi-model/)
6. [Presentation Layer](https://www.geeksforgeeks.org/presentation-layer-in-osi-model/)
7. [Application Layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/)

**Layer 1- Physical Layer**

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



**Devices used in Layer1: Hub, Repeater, Modem, and Cables are Physical Layer devices.**

**Layer 2- Data Link Layer (DLL)**

The data link layer is responsible for the node-to-node delivery of the message.

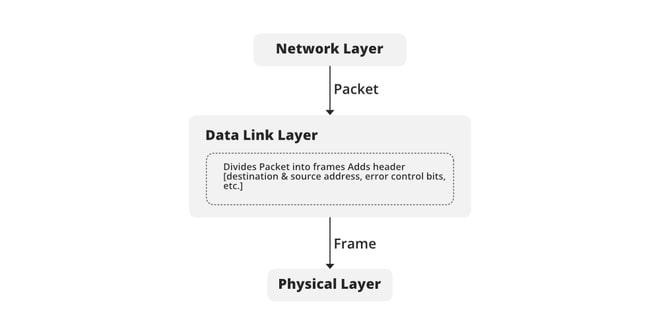
The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The packet received from the Network layer is further divided into frames.

DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an [ARP(Address Resolution Protocol)](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/)request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.



           Devices: **Switch** & **Bridge** are Data Link Layer devices.

**Layer 3- Network Layer**

The network layer works for the transmission of data from one host to the other located in different networks.

It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

The sender & receiver’s IP addresses are placed in the header by the network layer.

Network layer is implemented by networking devices such as **routers**.

**Layer 4- Transport Layer**

The data in the transport layer is referred to as *Segments*.

It is responsible for the End to End Delivery of the complete message.

The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

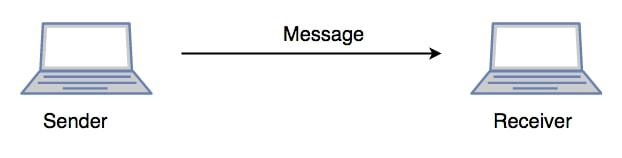
  The transport layer is called as **Heart of the OSI** model.

**Layer 5- Session Layer**

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

**Scenario**

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



**Layer 6- Presentation Layer**

The presentation layer is also called the **Translation layer**.

The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

In this layer, the data is encrypted**.** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text.

**Layer 7- Application Layer**

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications.

These applications produce the data, which has to be transferred over the network.

This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

The application Layer is also called **Desktop** **Layer**.

**Example of OSI Model (Just For Understanding):**

Certainly! Let's consider a scenario of Alice and Bob, who want to communicate using their computers over a network. Each layer of the OSI model can be illustrated through their interaction:

1. Physical Layer:
   * Alice wants to send a message to Bob. She types the message on her computer and presses the "Send" button.
   * The message is converted into electrical signals by the network interface card (NIC) in Alice's computer.
2. Data Link Layer:
   * The Data Link layer adds a header to the message, including source and destination MAC addresses, to create a data frame.
   * The frame also contains error detection information, such as a checksum, to ensure data integrity.
   * The NIC in Alice's computer sends the data frame over the network cable to the switch.
3. Network Layer:
   * The Network layer adds an IP (Internet Protocol) header to the data frame, including the source and destination IP addresses.
   * The IP address uniquely identifies Alice's and Bob's computers on the network.
   * The data frame is then forwarded to the appropriate router based on the destination IP address.
4. Transport Layer:
   * The Transport layer segments the data frame into smaller packets and adds a transport layer header, such as a TCP (Transmission Control Protocol) header.
   * The TCP header includes source and destination port numbers, ensuring that the message reaches the correct application on Bob's computer.
5. Session Layer:
   * The Session layer establishes and manages a session between Alice and Bob's computers.
   * It coordinates the communication and ensures that both parties are ready to receive and send data.
6. Presentation Layer:
   * The Presentation layer is responsible for data formatting and encryption, ensuring that the message is in a suitable format for transmission.
   * It may compress the message and encrypt it to maintain confidentiality and security during transmission.
7. Application Layer:
   * The Application layer is where the actual application or program resides. It allows Alice to compose the message and Bob to receive and read it.
   * Examples of application layer protocols include email (SMTP), file transfer (FTP), and web browsing (HTTP).

Once the message reaches Bob's computer, the process reverses as the layers work together to interpret and deliver the message to Bob's application for him to read it.

This example/story covers all seven layers of the OSI model, demonstrating how each layer plays a distinct role in the communication process between Alice and Bob over the network.