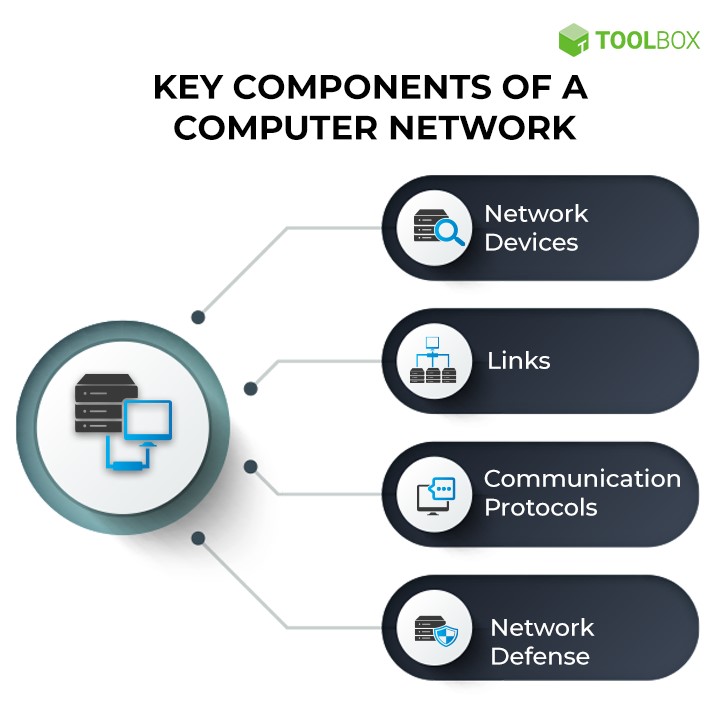
**What Is a Computer Network?**

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also

## Key Components of a Computer Network

From a broader lens, a computer network is built with two basic blocks: nodes or network devices and links. The links connect two or more nodes with each other. The way these links carry the information is defined by communication protocols. The communication endpoints, i.e., the origin and destination devices, are often called ports.



**Main Components of a Computer Network**

### 1. Network Devices

Network devices or nodes are computing devices that need to be linked in the network. Some network devices include:

* **Computers, mobiles, and other consumer devices**: These are end devices that users directly and frequently access. For example, an email originates from the mailing application on a laptop or mobile phone.
* **Servers**: These are application or storage servers where the main computation and data storage occur. All requests for specific tasks or data come to the servers.
* **Routers**: Routing is the process of selecting the network path through which the data packets traverse. Routers are devices that forward these packets between networks to ultimately reach the destination. They add efficiency to large networks.
* **Switches**: Repeaters are to networks what transformers are to electricity grids—they are electronic devices that receive network signals and clean or strengthen them. Hubs are repeaters with multiple ports in them. They pass on the data to whichever ports are available. Bridges are smarter hubs that only pass the data to the destination port. A switch is a multi-port bridge. Multiple data cables can be plugged into switches to enable communication with multiple network devices.
* **Gateways**: [Gateways](https://www.spiceworks.com/it-security/network-security/articles/what-is-secure-web-gateway/) are hardware devices that act as ‘gates’ between two distinct networks. They can be firewalls, routers, or servers.

### 2. Links

Links are the transmission media which can be of two types:

* **Wired**: Examples of wired technologies used in networks include coaxial cables, phone lines, twisted-pair cabling, and optical fibers. Optical fibers carry pulses of light to represent data.
* **Wireless**: Network connections can also be established through radio or other electromagnetic signals. This kind of transmission is called ‘wireless’. The most common examples of wireless links include communication satellites, [cellular networks](https://www.spiceworks.com/tech/innovation/articles/how-edge-and-5g-can-unlock-the-true-potential-of-ar-and-vr/), and radio and technology spread spectrums. Wireless LANs use spectrum technology to establish connections within a small area.

### 3. Communication protocols

A communication protocol is a set of rules followed by all nodes involved in the information transfer.

### 4. Network Defense

While nodes, links, and protocols form the foundation of a network, a modern network cannot exist without its defenses. Security is critical when unprecedented amounts of data are generated, moved, and processed across networks. A few examples of network defense tools include [firewall](https://www.spiceworks.com/security/web-security/articles/what-is-firewall-definition-key-components-best-practices/), network access control (NAC) and load balancers.

**Goals of Computer Networks:** The following are some important goals of computer networks:

1. **Resource Sharing –** The main goal of the computer network is Resource Sharing. It is to create all the programs, data and hardware accessible to anyone on the network without considering the resource’s physical area and the client.

1. **High Reliability –** If there are alternate sources of supply, all files could be replicated on two or more machines. If one of them is not available, due to hardware failure, the other copies could be used.

1. **Flexible access –** Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.
2. **Security**– Computer networks must be secure to protect against unauthorized access, data breaches, and other security threats. This includes implementing measures such as firewalls, antivirus software, and encryption to ensure the confidentiality, integrity, and availability of data.

### Communication Medium

The fifth goal of the computer network offers a powerful communication medium. The different user on the network can immediately identify a document that has been refreshed on a network.

### ****Advantages of Network****

These are the main advantages of Computer Networks:

1. **Central Storage of Data:**Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization.

## ****Faster Problem-solving**:**Since an extensive procedure is disintegrated into a few littler procedures and each is taken care of by all the associated gadgets, an explicit issue can be settled in lesser time.

## ****Reliability:**** Reliability implies backing up information. Due to some reason equipment crashes, and so on, the information gets undermined or inaccessible on one PC, and another duplicate of similar information is accessible on another workstation for future use, which prompts smooth working and further handling without interruption.

## ****Storage capacity:****Since you will share data, records, and assets with other individuals, you need to guarantee all information and substances are legitimately put away in the framework. With this systems administration innovation, you can do the majority of this with no issue, while having all the space you require for capacity.

### ****Disadvantages of the Network****

## 

1. **Virus and Malware:**On the off chance that even one PC on a system gets contaminated with an infection, there is a possibility for alternate frameworks to get tainted as well. Infections can spread on a system effectively, in view of the availability of different gadgets.
2. **Cost of the** **network:**The expense of executing the system including cabling and equipment can be expensive.

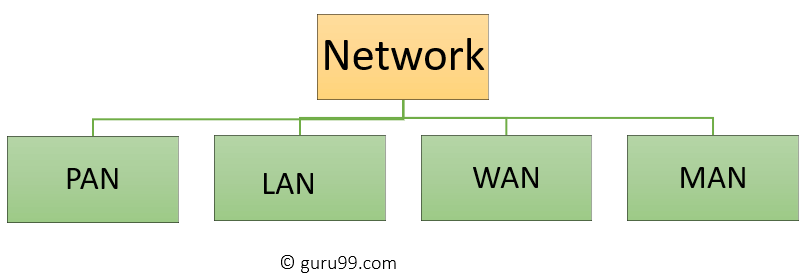
PC systems administration will dependably be a quick and advantageous method for exchanging and sharing data, yet individuals ought to know about its outcomes too.

## Different Types of Computer Networks

The classification of network in computers can be done according to their size as well as their purpose.

The size of a network should be expressed by the geographic area and number of computers, which are a part of their networks. It includes devices housed in a single room to millions of devices spread across the world.

Following are the popular types of Computer Network:



**Types of Computer Networks**

Some of the most popular computer network types are:

* PAN (Personal Area Network)
* LAN (Local Area Network)
* MAN (Metropolitan Area Network)
* WAN (Wide Area Network)

## What is PAN (Personal Area Network)?

**PAN** (Personal Area Network) is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

### Characteristics of PAN

Below are the main characteristics of PAN:

* It is mostly personal devices network equipped within a limited area.
* Allows you to handle the interconnection of IT devices at the surrounding of a single user.
* PAN includes mobile devices, tablet, and laptop.
* It can be wirelessly connected to the internet called WPAN.
* Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

### Advantages of PAN

Here are the important pros/benefits of PAN network:

* PAN networks are relatively secure and safe
* It offers only short-range solution up to ten meters
* Strictly restricted to a small area

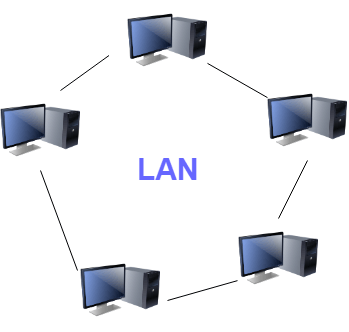
### Disadvantages of PAN

Here are the cons/drawbacks of using PAN network:

* Distance limits.

## What is a LAN (Local Area Network)?

A **Local Area Network** (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone’s home or office. In general, LAN will be used as one type of transmission medium. It is a network which consists of less than 5000 interconnected devices across several buildings.



**Local Area Network (LAN)**

### Characteristics of LAN

Here are the important characteristics of a LAN network:

* It is a private network, so an outside regulatory body never controls it.
* LAN operates at a relatively higher speed compared to other WAN systems.

### Advantages of LAN

Here are the pros/benefits of LAN:

* Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
* You can use the same software over the network instead of purchasing the licensed software for each client in the network.
* Data of all network users can be stored on a single hard disk of the server computer.
* You can easily transfer data and messages over networked computers.
* It will be easy to manage data at only one place, which makes data more secure.
* Local Area Network offers the facility to share a single internet connection among all the LAN users.

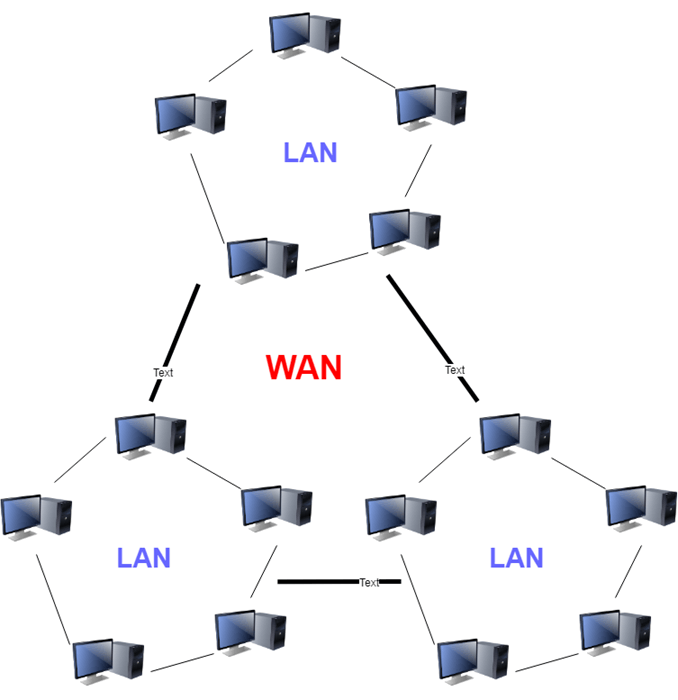
### Disadvantages of LAN

Here are the cons/drawbacks of LAN:

* LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
* The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
* Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
* Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

## What is WAN (Wide Area Network)?

**WAN** (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN’s using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.



**Wide Area Network (WAN)**

### Characteristics of WAN

Below are the characteristics of WAN:

* The software files will be shared among all the users; therefore, all can access to the latest files.
* Any organization can form its global integrated network using WAN.

### Advantages of WAN

Here are the benefits/pros of WAN:

* WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
* Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
* WLAN connections work using radio transmitters and receivers built into client devices.

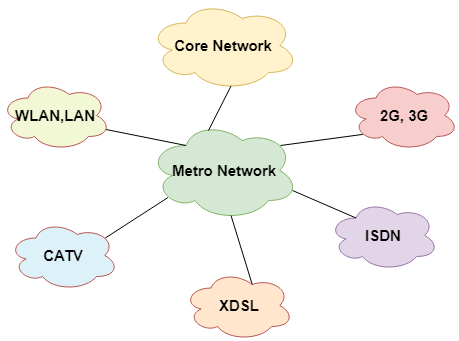
### Disadvantages of WAN

Here are the drawbacks/cons of WAN network:

* The initial setup cost of investment is very high.
* It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
* There are more errors and issues because of the wide coverage and the use of different technologies.
* It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.

## What is MAN (Metropolitan Area Network)?

A **Metropolitan Area Network** or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.



Metropolitan Area Network (MAN)

### Characteristics of MAN

Here are important characteristics of the MAN network:

* It mostly covers towns and cities in a maximum 50 km range
* Mostly used medium is optical fibers, cables

### Advantages of MAN

Here are the pros/benefits of MAN network:

* It offers fast communication using high-speed carriers, like [fiber optic cables](https://www.guru99.com/ethernet-cables-types.html).
* It provides excellent support for an extensive size network and greater access to WANs.
* The dual bus in MAN network provides support to transmit data in both directions concurrently.
* A MAN network mostly includes some areas of a city or an entire city.

### Disadvantages of MAN

Here are drawbacks/cons of using the MAN network:

* You need more cable to establish MAN connection from one place to another.
* In MAN network it is tough to make the system secure from hackers

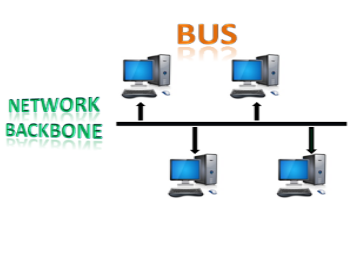
# What is Network Topology?

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

## Types of Network Topology

Physical topology is the geometric representation of all the nodes in a network. There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.

## 1) Bus Topology



* The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
* Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

**CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

* **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
* **CSMA CA:** **CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

### Advantages of Bus topology:

* **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
* **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
* **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
* **Limited failure:** A failure in one node will not have any effect on other nodes.

### Disadvantages of Bus topology:

* **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

## 2) Ring Topology



* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction.
* The most common access method of the ring topology is **token passing**.
  + **Token passing:** It is a network access method in which token is passed from one node to another node.
  + **Token:** It is a frame that circulates around the network.

### Working of Token passing

* A token move around the network and it is passed from computer to computer until it reaches the destination.
* The sender modifies the token by putting the address along with the data.
* The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
* In a ring topology, a token is used as a carrier.

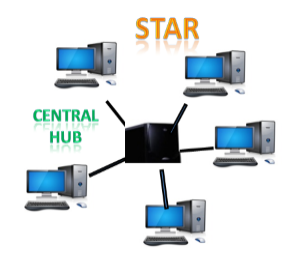
### Advantages of Ring topology:

* **Network Management:** Faulty devices can be removed from the network without bringing the network down.
* **Product availability:** Many hardware and software tools for network operation and monitoring are available.
* **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
* **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

### Disadvantages of Ring topology:

* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Failure:** The breakdown in one station leads to the failure of the overall network.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

## 3) Star Topology



* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a **physical star topology**.
* Star topology is the most popular topology in network implementation.

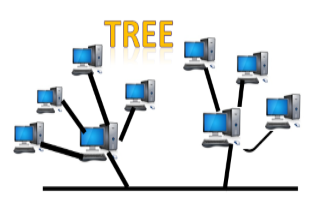
### Advantages of Star topology

* **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
* **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
* **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
* **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
* **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
* **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
* **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

### Disadvantages of Star topology

* **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.

## 4) Tree topology



* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

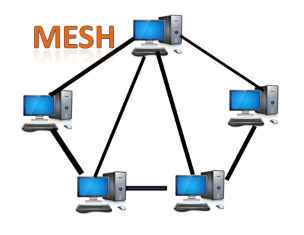
### Advantages of Tree topology

* **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
* **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
* **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
* **Error detection:** Error detection and error correction are very easy in a tree topology.
* **Limited failure:** The breakdown in one station does not affect the entire network.
* **Point-to-point wiring:** It has point-to-point wiring for individual segments.

### Disadvantages of Tree topology

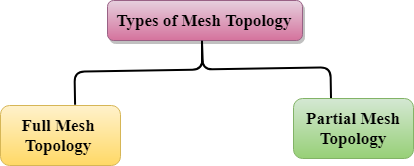
* **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
* **High cost:** Devices required for broadband transmission are very costly.
* **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
* **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

## 5) Mesh topology



* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point of communication.
* The Internet is an example of the mesh topology.
* Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
* Mesh topology is mainly used for wireless networks.
* Mesh topology can be formed by using the formula:  
  **Number of cables = (n\*(n-1))/2;**

Where n is the number of nodes that represents the network.



* **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
* **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

### Advantages of Mesh topology:

**Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

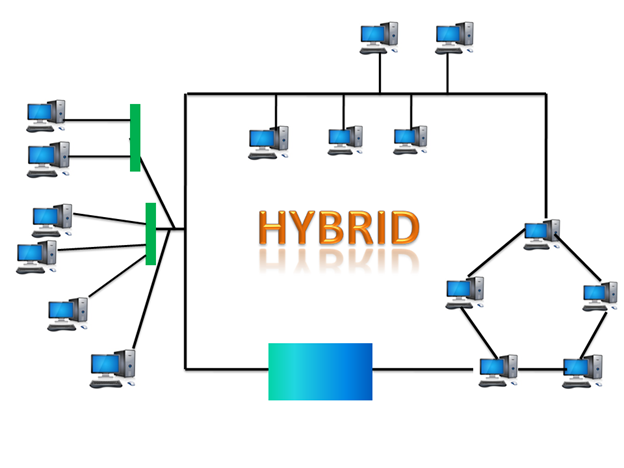
**Fast Communication:** Communication is very fast between the nodes.

**Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

### Disadvantages of Mesh topology

* **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
* **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
* **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

## 6) Hybrid Topology



* The combination of various different topologies is known as **Hybrid topology**.
* A Hybrid topology is a connection between different links and nodes to transfer the data.
* When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

### Advantages of Hybrid Topology

* **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
* **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
* **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
* **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

### Disadvantages of Hybrid topology

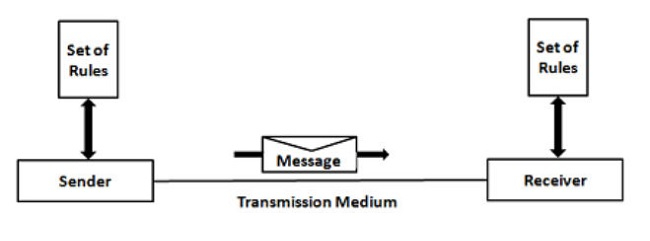
* **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
* **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
* **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

# What are the components of the Data Communication System?

**Data communication** is nothing but the exchange of data between any two devices via transmission media.

**Components**

There are five main components of data communication and they are explained below −



### Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:**It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium / Communication Channels:**Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Set of rules (Protocol):**When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.

Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:

* **TCP (Transmission Control Protocol)**: It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.
* **IP (Internet Protocol)**: Do you ever wonder how does computer determine which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

**TRANSMISSION MEDIUM**

**Transmission media**is a pathway that carries the [information](https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals.

An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called **Communication** **channel.**

## Types of Transmission Media

**Transmission media is broadly classified into two groups.**

**Wired or Guided Media or Bound Transmission Media:**

[Bound transmission media](https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-bound-transmission-media-type-of-bound-transmission-media-explain) are the cables that are tangible or have physical existence and are limited by the physical geography. Popular [bound transmission media](https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-bound-transmission-media-type-of-bound-transmission-media-explain) in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

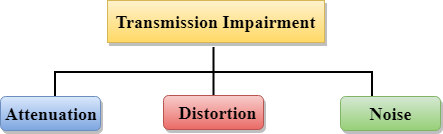
**Wireless or Unguided Media or Unbound Transmission Media:**

Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless **communication.** Nowadays wireless communication is becoming popular. Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infra red are some of popular unbound transmission media.

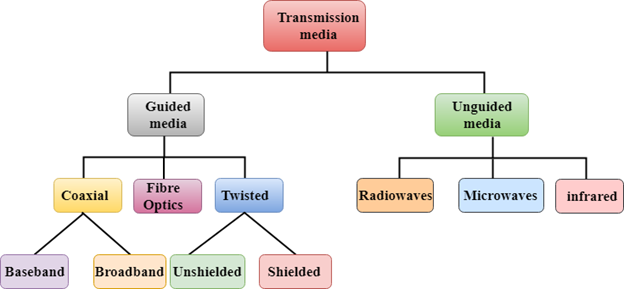
### Some factors need to be considered for designing the transmission media:

* **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:** Interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

## Causes of Transmission Impairment:



* **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
* **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
* **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.



# Guided Media

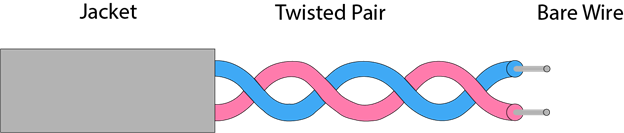
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

**Types of Guided media:**

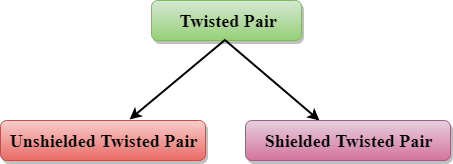
## Twisted pair:

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

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.

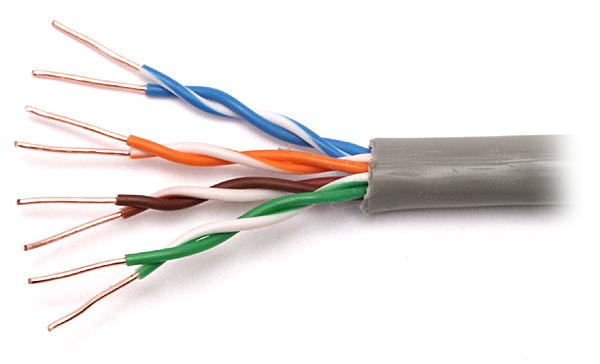


**Types of Twisted pair:**



### Unshielded Twisted Pair:

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



* **Category 1:** Category 1 is used for telephone lines that have low-speed data.
* **Category 2:** It can support upto 4Mbps.
* **Category 3:** It can support upto 16Mbps.
* **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
* **Category 5:** It can support upto 200Mbps.

**Advantages of Unshielded Twisted Pair:**

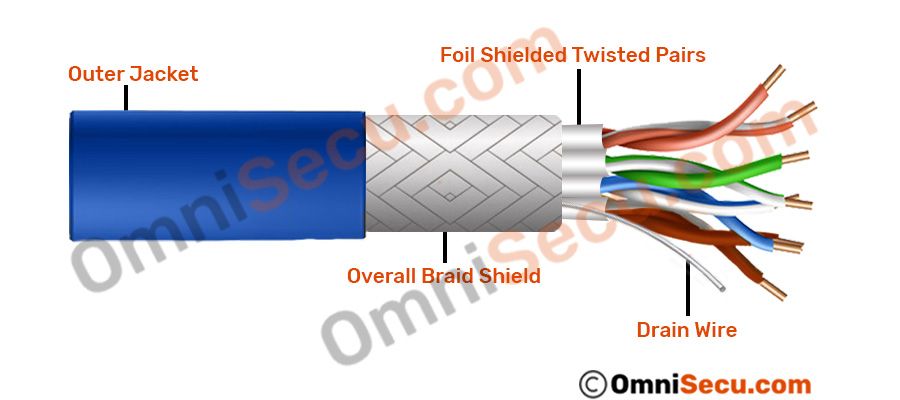
* It is cheap.
* Installation of the unshielded twisted pair is easy.
* It can be used for high-speed LAN.

**Disadvantage:**

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

### Shielded Twisted Pair

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



**Characteristics of Shielded Twisted Pair:**

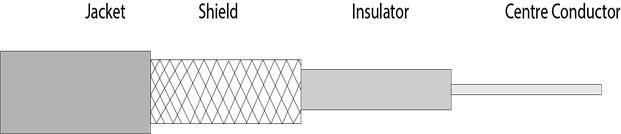
* The cost of the shielded twisted pair cable is not very high and not very low.
* An installation of STP is easy.
* It has higher capacity as compared to unshielded twisted pair cable.
* It has a higher attenuation.
* It is shielded that provides the higher data transmission rate.

**Disadvantages**

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

## Coaxial Cable

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



**Coaxial cable is of two types:**

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

**Advantages of Coaxial cable:**

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

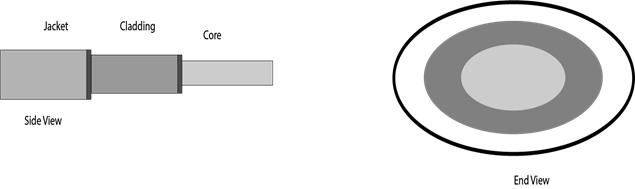
**Disadvantages of Coaxial cable:**

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

## Fibre Optic

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

**Diagrammatic representation of fibre optic cable:**



**Basic elements of Fibre optic cable:**

* **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
* **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
* **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

**Following are the advantages of fibre optic cable over copper:**

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

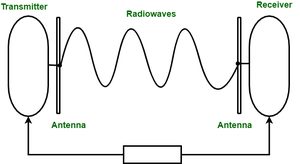
**2. Unguided Media:**   
It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

**Features:**

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

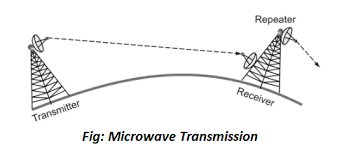
There are 3 types of Signals transmitted through unguided media:

**(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.



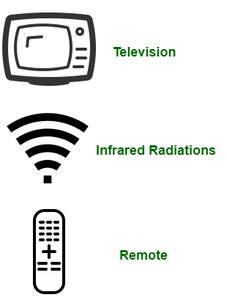
Further Categorized as (i) Terrestrial and (ii) Satellite.

**(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 in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

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

* 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.

**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.
  1. **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 simplex 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.
  1. **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.

### Comparison Chart

|  |  |  |  |
| --- | --- | --- | --- |
| **Basis for Comparison** | **Simplex** | **Half Duplex** | **Full Duplex** |
| Direction of Communication | Unidirectional | Two-directional, one at a time | Two-directional, simultaneously |
| Send / Receive | The sender can only send data | The sender can send and receive data, but one a time | The sender can send and receive data simultaneously |
| Performance | Worst performing mode of transmission | Better than Simplex | Best performing mode of transmission |
| Example | Keyboard and monitor | Walkie-talkie | Telephone |

**Network Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

### Hub

A hub is a centralized device that connects multiple devices in a single LAN network. When a hub receives a data signal from a connected device on one of its ports, except for that port, it forwards those signals from the remaining ports to all other connected devices. Typically, a hub has one or more uplink ports that are used to connect it to another hub.

**There are two types of the Hub.**

**Passive Hub**: - A passive hub forwards data signals as it receives them. It does not change data signals in any manner.

**Active Hub**: - An active hub also forwards data signals. But, before forwarding them, it amplifies them. Due to this added feature, an active Hub is also called a repeater.

The following image shows an active hub and a passive hub.



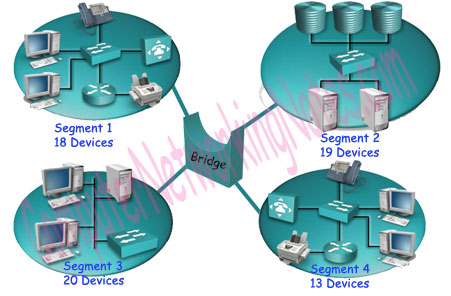
Hubs are no longer used in computer networks.

### Bridge

A bridge is used to divide a large network into smaller segments. The basic functions of a bridge are the following: -

* Breaking a large network into smaller segments.
* Connecting different media types such as UTP and fiber optic.
* Connecting different network architectures such as Ethernet and the Token ring.

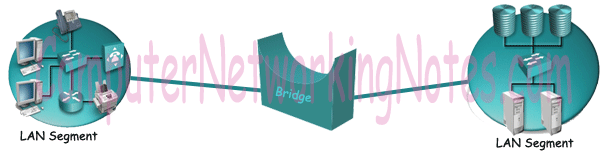
The following image shows an example of a bridge.



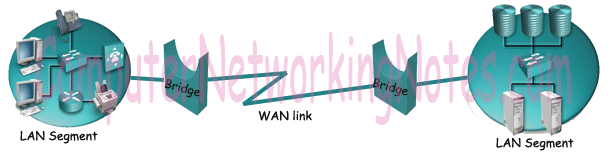
A bridge can connect two different types of media or network architecture, but it cannot connect two different types of network layer protocols such as TCP/IP or IPX. It requires the same network-layer protocols across all segments.

**There are three types of bridge:-**

**Local Bridge**: - The Bridge directly connects two LAN segments. In Ethernet implementations, this is known as a transparent bridge. In the Token Ring network, this is called a source-routed bridge.



**Remote Bridge**: - This Bridge connects with another Bridge over the WAN link.



**Wireless Bridge**: - This Bridge connects with another Bridge without using wires. It uses radio signals for connectivity.



In networking models such as the OSI layers model and TCP/IP model, the functionalities of Bridges are defined in the physical layer and data link layer.

Just like a Hub, a Bridge is also no longer used in the computer network. Bridges have been replaced by switches.

### Switch

Just like a hub and a bridge, a switch is also used to connect multiple devices in a LAN segment. A switch is the upgraded version of the bridge. Besides providing all the functionalities of a bridge, it also offers several additional features.

The biggest advantage of a switch is that it makes switching decisions in hardware by using application-specific integrated circuits (ASICs).

Unlike the generic processors that we use in our PC, ASICs are specialized processors built only to perform particular tasks. Usually, the ASICs in switches have a single task and that is switching the frames as fast as they can.

An ASIC occupied switch performs this task blazingly fast. For example, an entry-level 2960 Catalyst Switch can process 2.7 million frames per second.

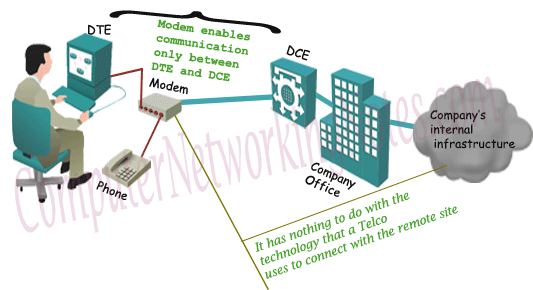


### Modem

In simple language, a modem is a device that is used to connect to the Internet. Technically, it is the device that enables digital data to be transmitted over telecommunication lines.

A Telco company uses entirely different data transmission technology from the technology that a PC uses for data transmission. A modem understands both technologies. When it receives signals from the PC, it converts them into the format that the Telco company understands. When it receives signals from the Telco company, it converts them into a format that the PC understands.

It enables communication between the PC (Known as the DTE device) and the Telecom company's office (Known as the DCE device).



The following image shows some common types of modems.



### Gateway

Gateway is used to forward packets that originate from a local host or a local network and are intended for remote networks. If a data packet does not get its destination address in the local network then it takes the help of the gateway device to find the destination address in the remote network. The gateway device knows the path to the remote destination address. If necessary, it also encapsulates the packet so that it can travel through other networks to reach its destination address.

**The following image shows a gateway device.**



Examples of the Gateway

**Email Gateway**: - An email gateway translates SMTP e-mails in standard X.400 format before forwarding.

**GSNW Gateway**: - A GSNW gateway allows Windows clients to access resources from the NetWare server.

**PAD Gateway**: - A PAD gateway provides connectivity between a LAN network and an X.25 network.

### Router

A router connects different network segments. It switches data packets between networks that are either located in different logical segments or constructed with different network-layer protocols.

When a router receives a data packet on any of its interfaces, it checks the destination address of that packet, and based on that destination address, forwards that data packet to the interface that is associated with the destination address.

To forward data packets to their destination, the router keeps a record of the connected network. These records are maintained in a database table known as the routing table. Routing tables can be created statically or dynamically.

The following image shows two routers.



**The main functions of routers are the following: -**

* To connect different network segments.
* To connect different network protocols such as IP and IPX.
* To connect several smaller networks into a large network.
* To break a large network into smaller networks.
* To connect two different media types such as UTP and Fiber optical.
* To connect two different network architectures such as Token Ring and Ethernet.
* To connect LAN network with Telco company's office.
* To access DSL services.

### Proxy

A proxy is used to hide the internal network from the outside world. It may be a dedicated device or maybe application software. Once it is configured, all communication goes through it. Since external devices cannot directly access internal equipment, they cannot tamper with internal equipment.

The following image shows an example of a proxy.

