**Unit-I Networking Fundamentals and Physical Layer 04 Hours**

**Network Organizations and Architectures:** What is computer Networks, Network Topologies: Mesh, Star and Hierarchical, Types of Computer Networks: LAN, MAN, WAN, PAN, Internet, internet and Intranet. Client-Server; Peer To Peer.

**Network Architecture Modes:** Infrastructure and Ad-hoc mode. Reference Models: OS and TCP/IP. Design Issues for Layers.

**Physical Layer:** Transmission Mediums: Air, Vacuum, Cat5, Cat5e, Cat6, Cat6a, Cat7, Cat8, OFC - Single and Multicore.

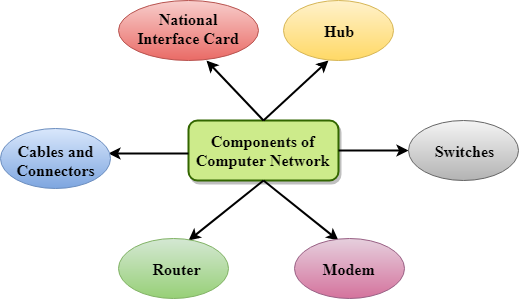
**Networking Devices Wired and Wireless:** NIC, Repeater, Bridge, Switch, Modem, Router, Gateways and Access Point.

**1. What is a Computer Network?**

* Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
* The aim of the computer network is the sharing of resources among various devices.
* In the case of computer network technology, there are several types of networks that vary from simple to complex level.

**1.1. Components Of Computer Network:**

Major components of a computer network are:



**1.2 Uses Of Computer Network**

* **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
* **Server-Client model:** Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
* **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
* **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

**1.4 Features Of Computer network**

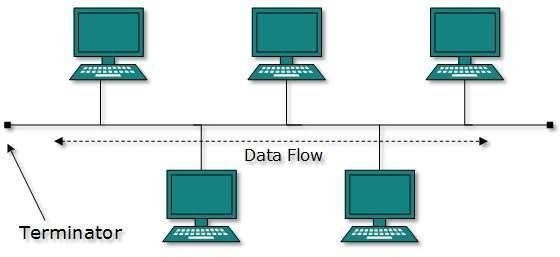
* **Communication speed:** Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.
* **File sharing:** File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.
* **Back up and Roll back is easy:** Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.
* **Software and Hardware sharing:** We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.
* **Security:** Network allows the security by ensuring that the user has the right to access the certain files and applications.
* **Scalability:** Scalability means that we can add the new components on the network. Network must be scalable so that we can extend the network by adding new devices. But, it decreases the speed of the connection and data of the transmission speed also decreases, this increases the chances of error occurring. This problem can be overcome by using the routing or switching devices.
* **Reliability:** Computer network can use the alternative source for the data communication in case of any hardware failure.

**2. Network Topology**

Computers in a network have to be connected in some logical manner. The layout pattern of the interconnections between computers in a network is called **network topology**.

**2.1 Bus topology**

**Bus topology** uses one main cable to which all nodes are directly connected. The main cable acts as a backbone for the network. One of the computers in the network typically acts as the computer server. The first advantage of bus topology is that it is easy to connect a computer or peripheral device. The second advantage is that the cable requirements are relatively small, resulting in lower cost. One of the disadvantages is that if the main cable breaks, the entire network goes down. This type of network is also difficult to troubleshoot. For these reasons, this type of topology is not used for large networks.



**Fig. Bus topology**

**2.1.1 Advantages of Bus Topology**

* It is easy to set up, handle, and implement.
* It is best-suited for small networks.
* It costs very less.

**2.1.2 Disadvantages of Bus Topology**

* The cable length is limited. This limits the number of network nodes that can be connected.
* This network topology can perform well only for a limited number of nodes. When the number of devices connected to the bus increases, the efficiency decreases.
* It is suitable for networks with low traffic. High traffic increases load on the bus, and the network efficiency drops.
* It is heavily dependent on the central bus. A fault in the [bus](https://instrumentationtools.com/ethernet-bus-animation/) leads to network failure.
* It is not easy to isolate faults in the network nodes.
* Each device on the network “sees” all the data being transmitted, thus posing a security risk.

**2.2 Star topology**

In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible. Star topology is very popular because the startup costs are low. It is also easy to add new nodes to the network. The network is robust in the sense that if one connection between a computer and the hub fails, the other connections remain intact. If the central hub fails, however, the entire network will fail.



**Fig.** **Star topology**

**2.2.1 Advantages of Star Topology**

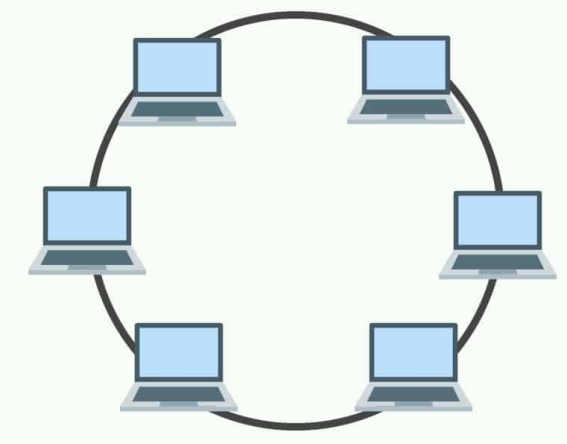
* Due to its centralized nature, the topology offers simplicity of operation.
* It also achieves isolation of each device in the network.
* Adding or removing network nodes is easy, and can be done without affecting the entire network.
* Due to the centralized nature, it is easy to detect faults in the network devices.
* As the analysis of traffic is easy, the topology poses lesser security risk.
* Data packets do not have to pass through many nodes, like in the case of a ring network. Thus, with the use of a high-capacity central hub, traffic load can be handled at fairly decent speeds.

**2.2.2 Disadvantages of Star Topology**

* Network operation depends on the functioning of the central hub. Hence, [central hub](https://instrumentationtools.com/difference-between-router-switch-and-hub/) failure leads to failure of the entire network.
* Also, the number of nodes that can be added, depends on the capacity of the central hub.
* The setup cost is quite high.

**2.3 Ring topology**

In ring topology, the computers in the network are connected in a circular fashion, and the data travels in one direction. Each computer is directly connected to the next computer, forming a single pathway for signals through the network. This type of network is easy to install and manage. If there is a problem in the network, it is easy to pinpoint which connection is defective. It is also good for handling high-volume traffic over long distances since every computer can act as a booster of the signal. On the downside, adding computers to this type of network is more cumbersome, and if one single computer fails, the entire network goes down.



**Fig. Ring topology:**

**2.3.1 Advantages of Ring Topology**

* The data being transmitted between two nodes passes through all the intermediate nodes. A central server is not required for the management of this topology.
* The traffic is unidirectional and the data transmission is high-speed.
* In comparison to a bus, a ring is better at handling load.
* The adding or removing of network nodes is easy, as the process requires changing only two connections.
* The configuration makes it easy to identify faults in network nodes.
* In this topology, each node has the opportunity to transmit data. Thus, it is a very organized network topology.
* It is less costly than a star topology.

**2.3.2 Disadvantages of Ring Topology**

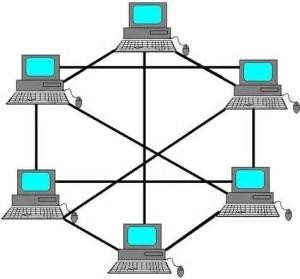
* The failure of a single node in the network can cause the entire network to fail.
* The movement or changes made to network nodes affect the entire network’s performance.
* Data sent from one node to another has to pass through all the intermediate nodes. This makes the transmission slower in comparison to that in a [star topology](https://instrumentationforum.com/t/star-topology-principle/3749). The transmission speed drops with an increase in the number of nodes.
* There is heavy dependency on the wire connecting the network nodes in the ring.

**2.4 Mesh topology**

In mesh topology, every node has a direct point-to-point connection to every other node. Because all connections are direct, the network can handle very high-volume traffic. It is also robust because if one connection fails, the others remain intact. Security is also high since data travels along a dedicated connection.

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



**Fig. Mesh topology**

**2.4.1 Advantages of Mesh Topology**

* The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.
* The failure of a single node does not cause the entire network to fail as there are alternate paths for data transmission.
* It can handle heavy traffic, as there are dedicated paths between any two network nodes.
* Point-to-point contact between every pair of nodes, makes it easy to identify faults.

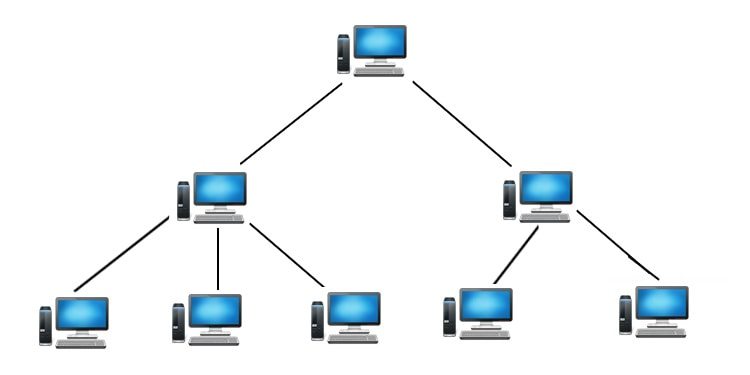
**2.4.2 Disadvantages of Mesh Topology**

* The arrangement wherein every network node is connected to every other node of the network, many connections serve no major purpose. This leads to redundancy of many network connections.
* A lot of cabling is required. Thus, the costs incurred in setup and maintenance are high.
* Owing to its complexity, the administration of a mesh network is difficult.

**2.5 Tree topology**

A **tree topology** is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate [network](https://www.computerhope.com/jargon/n/network.htm), or the information in a [database](https://www.computerhope.com/jargon/d/database.htm).

In a tree topology, there can be only one connection between any two connected nodes. Because any two nodes can have only one mutual connection, tree topologies create a natural [parent and child](https://www.computerhope.com/jargon/p/parechil.htm) hierarchy.



**2.5.1 Advantages of Tree Topology**

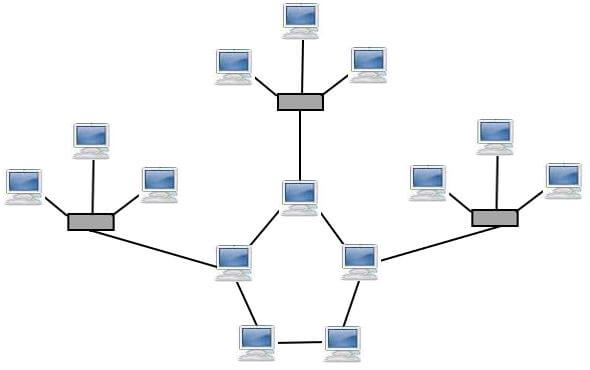
* The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
* The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
* Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
* Fault identification is easy.
* The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

**2.5.2 Disadvantages of Tree Topology**

* As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.
* Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to that in other topologies.
* Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

**2.5 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.



**Fig.** **Hybrid Topology**

**2.5.1 Advantages of Hybrid Topology :**

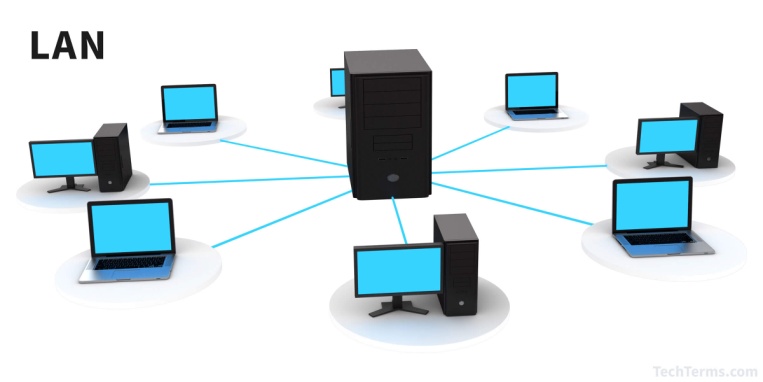
* This type of topology combines the benefits of different types of topologies in one topology.
* Can be modified as per requirement.
* It is extremely flexible.
* It is very reliable.
* It is easily scalable as Hybrid networks are built in a fashion which enables for easy integration of new hardware components.
* Error detecting and trouble shooting is easy.
* Handles large volume of traffic.
* It is used for create large network.

**2.5.2 Disadvantages of Hybrid Topology :**

* It is a type of network expensive.
* Design of a hybrid network is very complex.
* There is change hardware in order to connect topology with another topology.
* Usually hybrid architectures are usually larger in scales so they requires a lot of cables in installation process.
* Hubs which are used to connect two distinct networks, are very costly. And hubs are different from usual hubs as they need to be intelligent enough to work with different architectures.
* Installation is a difficult process.

**3. Types of Computer Networks**

**3.1 Local Area Network**



A **L**ocal **A**rea **N**etwork (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.

**3.1.1 Characteristics of LAN**

Here are 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.
* There are various kinds of media access control methods like token ring and ethernet.

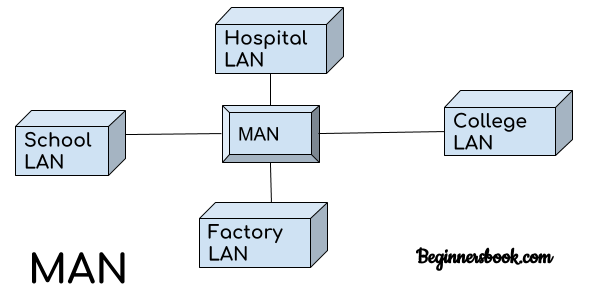
**3.1.2 Advantages of LAN**

* 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.

**3.1.3 Disadvantages 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

**3.2 What is MAN?**



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.

**3.2.1 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
* Data rates adequate for distributed computing applications.

**3.2.2 Advantages of MAN**

Here are pros/benefits of using MAN system:

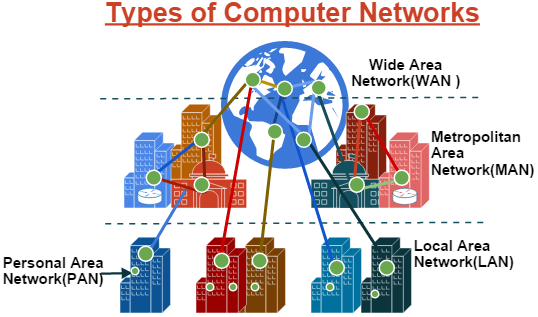
* It offers fast communication using high-speed carriers, like fiber optic cables.
* It provides excellent support for an extensive size network and greater access to WANs.
* The dual bus in MAN network provides support to transmit data in both directions concurrently.
* A MAN network mostly includes some areas of a city or an entire city.

**3.2.3 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

**3.3 What is WAN?**



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.

**3.3.1 Characteristics of LAN:**

* 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.

**3.3.2 Advantages of WAN**

Here are the benefits/ pros of using 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.

**3.3.3 Disadvantage of WAN**

Here are drawbacks/cons of using WAN:

* 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.
* Offers lower security compared to other types of networks.

**3.4 PAN**



* PAN (Personal Area Network) is a small-scale network used for connecting devices within the range of a few meters, typically around a single person.
* It allows personal devices to communicate with each other — such as smartphones, tablets, laptops, printers, headphones, etc.
* Bluetooth connections, infrared communication, Wi-Fi Direct, USB connections.

**3.4 1 Characteristics of PAN:**

* Short Range: Typically covers 1 to 10 meters.
* Personal Use: Designed for individual users to connect personal devices.
* Wireless or Wired: Can be both wireless (Bluetooth, Infrared) or wired (USB).
* Low Power Consumption: Consumes less power due to short range and small number of devices.
* Simple Setup: Easy to configure and use, often with minimal technical knowledge.
* Low Cost: Requires minimal hardware and infrastructure.

**3.4.2 Advantages of PAN:**

* Convenience: Easy to connect and manage personal devices.
* Portability: Can be used anywhere (home, office, travel).
* Cost-effective: Inexpensive to set up and maintain.
* Low Power Usage: Energy-efficient for devices like smartphones and wearables.
* Quick Data Transfer: Enables fast sharing of data between nearby devices.

**3.4.3 Limitations of PAN:**

* Limited Range: Effective only within a few meters.
* Limited Devices: Supports only a few devices at a time.
* Low Data Transfer Rate (in some cases): Slower compared to larger networks for heavy data transfer.
* Security Risks: Vulnerable to unauthorized access if not properly secured (e.g., open Bluetooth).
* Interference: Wireless PANs can be affected by interference from other devices or obstacles.

**4. Internet and Intranet**

**4.1 Internet**

A global network that connects millions of computers and devices worldwide, allowing public access to information and communication.

* + 1. **Key Features:**
* Public network
* Unlimited access
* Global connectivity
* Uses standard protocols like TCP/IP
* Examples: Websites, Emails, Social Media

**4.1.2 Advantages:**

* + Access to vast information
  + Global communication (Email, Chat, Video Calls)
  + Online services (Banking, Shopping, Education)
  + Social networking

**4.1.3 Limitations:**

* + Security risks (hacking, malware)
  + Privacy concerns
  + Dependence on internet service providers (ISPs)
  + Misinformation and data overload

**4.2 Intranet**

A private network used within an organization for internal communication and information sharing.

* + 1. **Key Features:**
  + Private and restricted access
  + Used within an organization
  + Controlled by organization’s IT department
  + Often requires login credentials

**4.2.2 Advantages:**

* Secure internal communication
* Centralized data management
* Improves collaboration and efficiency
* Protects sensitive information

**4.2.3 Limitations:**

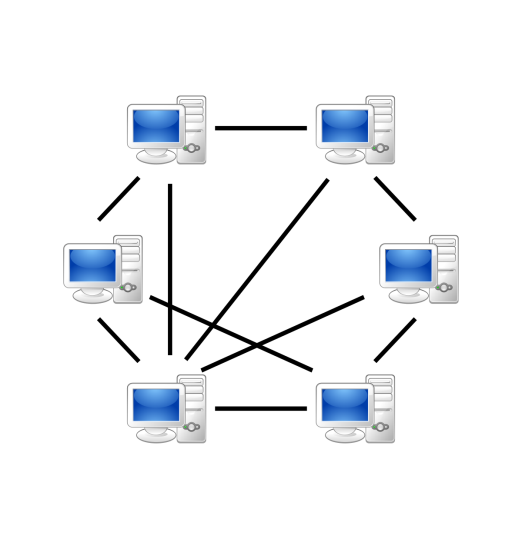
* + Limited to organization’s users
  + High setup and maintenance cost
  + Requires internal management and security
  + Limited external access

**4.3 Comparison table of Internet vs Intranet**

| **Feature** | **Internet** | **Intranet** |
| --- | --- | --- |
| **Definition** | Global network connecting millions of devices worldwide. | Private network used within an organization. |
| **Access** | Public, open to everyone. | Restricted, only authorized users can access. |
| **Ownership** | No single owner; multiple organizations manage parts. | Owned and managed by a specific organization. |
| **Users** | General public, anyone with internet access. | Employees or authorized members of an organization. |
| **Security** | Less secure, exposed to threats. | More secure, controlled by internal IT policies. |
| **Purpose** | Share information, communication, services globally. | Share internal information, documents, and tools. |
| **Cost** | Lower cost for users (mostly subscription fees). | Higher cost for setup and maintenance. |
| **Examples** | Google, Facebook, YouTube, Email services. | Company internal HR portal, internal chat, company documentation systems. |

**5. Peer-To-Peer network**

* Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
* Peer-To-Peer network is useful for small environments, usually up to 10 computers.
* Peer-To-Peer network has no dedicated server.
* Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



**5.1 Advantages Of Peer-To-Peer Network:**

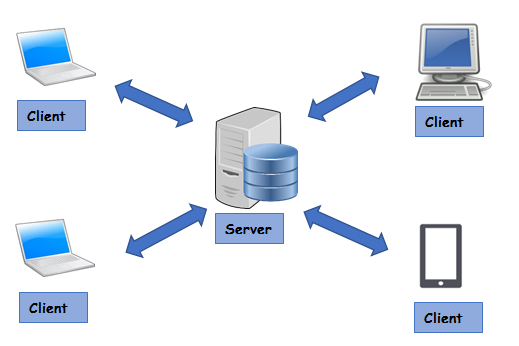
* It is less costly as it does not contain any dedicated server.
* If one computer stops working but, other computers will not stop working.
* It is easy to set up and maintain as each computer manages itself.

**5.2 Disadvantages Of Peer-To-Peer Network:**

* In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
* It has a security issue as the device is managed itself.

**6. Client/Server Network**

* Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
* The central controller is known as a **server** while all other computers in the network are called **clients**.
* A server performs all the major operations such as security and network management.
* A server is responsible for managing all the resources such as files, directories, printer, etc.
* All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



**6.1 Advantages Of Client/Server network:**

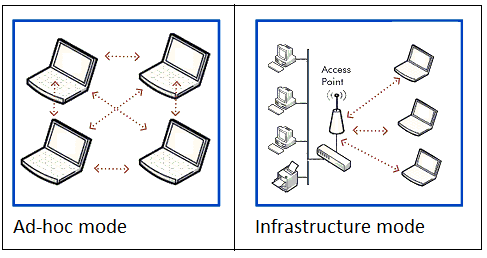
* A Client/Server network contains the centralized system. Therefore we can back up the data easily.
* A Client/Server network has a dedicated server that improves the overall performance of the whole system.
* Security is better in Client/Server network as a single server administers the shared resources.
* It also increases the speed of the sharing resources.

**6.2 Disadvantages Of Client/Server network:**

* Client/Server network is expensive as it requires the server with large memory.
* A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
* It requires a dedicated network administrator to manage all the resources.

**7. Network Architecture Modes:**

**7. 1. Infrastructure Mode**



* A network mode where all devices (clients) communicate through a central device such as an Access Point (AP) or Router.
* Devices don’t communicate directly; instead, they send data to the AP, which forwards it to the destination device.
  + 1. **Key Features:**
  + Centralized control
  + Better management and security
  + Supports larger networks
  + Easier to scale

**7.1.2 Examples:**

* + Home Wi-Fi with router
  + Office wireless networks
  + Public Wi-Fi hotspots

**7.1.3 Advantages:**

* + Centralized management
  + Stronger security controls
  + Better range and stability
  + Supports many devices
    1. **Limitations:**
  + Needs hardware (AP/Router)
  + Single point of failure (if AP fails, whole network is affected)
  + Higher setup cost

**7.2. Ad-hoc Mode**

* A network mode where devices communicate directly with each other without any central device.
* Each device connects peer-to-peer, forming a temporary network.

**7.2.1 Key Features:**

* + Decentralized
  + Temporary and quick setup
  + No dedicated infrastructure
    1. **Examples:**
  + File sharing between two laptops using Wi-Fi Direct
  + Bluetooth connections
  + Emergency networks in disaster areas

**7.2.3 Advantages:**

* + Easy and quick to set up
  + No need for extra hardware
  + Flexible and portable

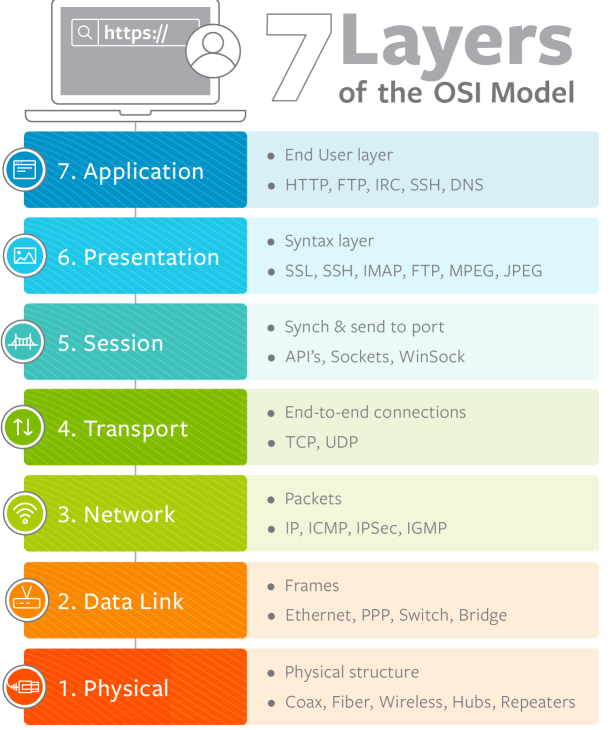
**7.2.4 Limitations:**

* + Limited range and scalability
  + Less secure
  + Difficult to manage in large networks
  + Lower performance compared to infrastructure mode

**8. Reference Models**

**8.1 Open Systems Interconnection**

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



**8.1.1. Physical Layer (Layer 1) :**

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

The functions of the physical layer are :

* **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
* **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
* **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
* **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Hub, Repeater, Modem, Cables are Physical Layer devices.  
Network Layer, Data Link Layer and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

**8.1.2. Data Link Layer (DLL) (Layer 2) :**

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.  
**Data Link Layer is divided into two sub layers :**

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the data Link layer are :

* **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
* **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
* **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
* **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
* **Access control:**When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

*\* Packet in Data Link layer is referred as****Frame****.  
\*\* Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.  
\*\*\* Switch & Bridge are Data Link Layer devices.*

**8.1.3. Network Layer (Layer 3) :**

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

* **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
* **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver’s IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

*\* Segment* in Network layer is referred as **Packet**.

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

**8.1.4. Transport Layer (Layer 4) :**

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

**At sender’s side:**

Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.  
Note: The sender need to know the port number associated with the receiver’s application.  
Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

**At receiver’s side:**

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

* **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
* **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include  
   – Connection Establishment  
   – Data Transfer  
   – Termination / disconnection  
   In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

*\* Data in the Transport Layer is called as****Segments****.  
\*\* Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.  
Transport Layer is called as****Heart of OSI****model.*

**8.1.5. Session Layer (Layer 5) :**

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.  
The functions of the session layer are :

* **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
* **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
* **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

*\*\*All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as “Application Layer”.  
\*\*Implementation of these 3 layers is done by the network application itself. These are also known as****Upper Layers****or****Software Layers****.*

**8.1.6. Presentation Layer (Layer 6) :**

Presentation layer is also called the **Translation layer**.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.  
The functions of the presentation layer are :

* **Translation :** For example, ASCII to EBCDIC.
* **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
* **Compression:** Reduces the number of bits that need to be transmitted on the network.

**7. Application Layer (Layer 7) :**

At the very top of the OSI Reference Model stack of layers, we find 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.  
Ex: Application – Browsers, Skype Messenger etc.  
*\*\*Application Layer is also called as Desktop Layer.*

The functions of the Application layer are :

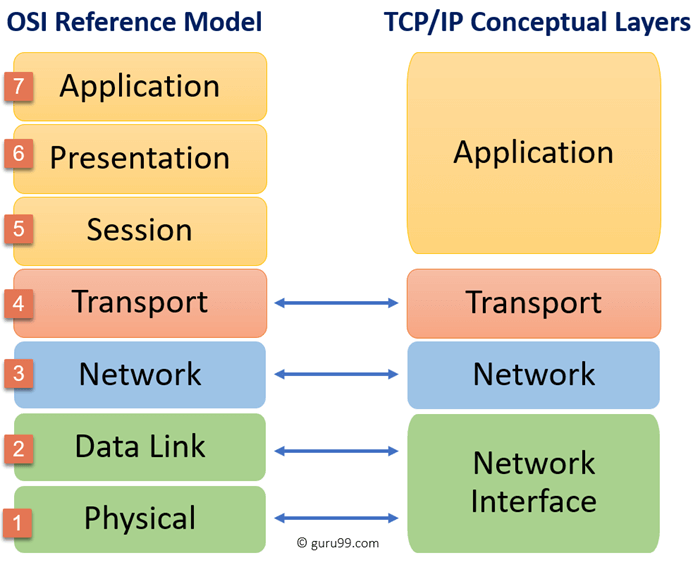
1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in the Internet because of its late invention. Current model being used is the TCP/IP model.

**8.2 TCP/IP model**

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

* Process/Application Layer
* Host-to-Host/Transport Layer
* Internet Layer
* Network Access/Link Layer



The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

**8.2.1. Network Access Layer –**

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

**8.2.2. Internet Layer –**

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

* **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
* IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
* **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
* **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

**8.2.3. Host-to-Host Layer –**

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

* **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
* **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

**8.2.4. Application Layer –**

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

* + - **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
    - **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    - **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

**8.3 OSI vs TCP/IP**

|  |  |
| --- | --- |
| **TCP/IP** | **OSI** |
| TCP refers to Transmission Control Protocol. | OSI refers to Open Systems Interconnection. |
| TCP/IP has 4 layers. | OSI has 7 layers. |
| TCP/IP is more reliable | OSI is less reliable |
| TCP/IP does not have very strict boundaries. | OSI has strict boundaries |
| TCP/IP follow a horizontal approach. | OSI follows a vertical approach. |
| TCP/IP uses both session and presentation layer in the application layer itself. | OSI uses different session and presentation layers. |
| TCP/IP developed protocols then model. | OSI developed model then protocol. |
| Transport layer in TCP/IP does not provide assurance delivery of packets. | In OSI model, transport layer provides assurance delivery of packets. |
| TCP/IP model network layer only provides connection less services. | Connection less and connection oriented both services are provided by network layer in OSI model. |
| Protocols cannot be replaced easily in TCP/IP model. | While in OSI model, Protocols are better covered and is easy to replace with the change in technology. |

**9. Transmission Media**

On any network, the various entities must communicate through some form of media. Just as humans can communicate through telephone wires or sound waves in the air, computers can communicate through cables, light, and radio waves. Transmission media enable computers to send and receive messages but do not guarantee that the messages will be understood.

Most common network transmission media are coaxial cable, shielded twisted-pair cable, and unshielded twisted-pair cable, fiber-optic cable and wireless communications.

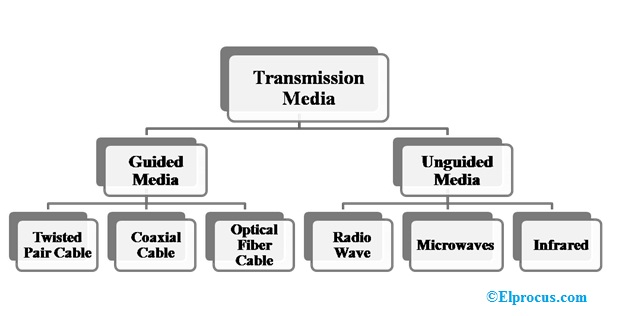
Select the appropriate media for various situations. Media choices include the following:

* Twisted-pair cable
* Coaxial cable
* Fiber-optic cable

Wireless communications Situational elements include the following:

* Cost
* Distance limitations
* Number of nodes

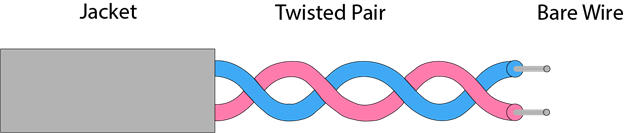
**9.1. Types of transmission media**

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.

**Fig. Types of transmission media**

**9.1.1 Twisted pair**

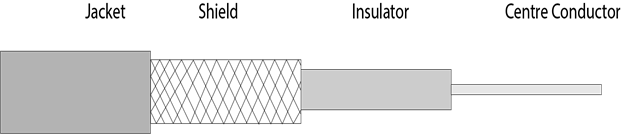
* Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.
* 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.



**Fig. Twisted pair**

**9.1.2 Coaxial cable**

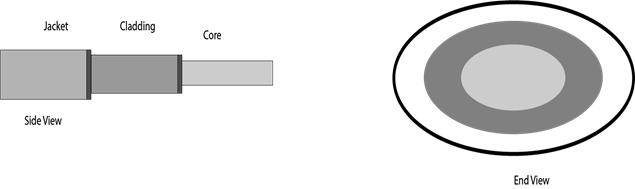
* Coaxial cable gets its name because it contains two conductors that are parallel to each other. The center conductor in the cable is usually copper. The copper can be either a solid wire or stranded martial.
* Outside this central Conductor is a non-conductive material. It is usually white, plastic material used to separate the inner Conductor form the outer Conductor. The other Conductor is a fine mesh made from Copper. It is used to help shield the cable form EMI.



**Fig. Coaxial cable**

**9.1.3 Fiber Optic Cable**

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates. In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield



**Fig. Fiber Optic Cable**

**9.2 Unguided Media (Wireless Media)**

**9.2.1 Air**

* **Medium:** Natural medium used for wireless communication.
* **Used in:** Radio, Wi-Fi, Bluetooth, Satellite, Cellular networks.
* **Advantages:**
  + No physical cables.
  + Easy to install and expand.
* **Limitations:**
  + Signal interference.
  + Limited range and security.

**9.2.2 Vacuum**

* **Medium:** Space devoid of matter (used in satellite and space communication).
* **Used in:** Space communication (NASA, satellites).
* **Advantages:**
  + No attenuation due to air resistance.
* **Limitations:**
  + Expensive equipment.
  + Limited to special applications.

**9.3 Guided Media (Wired Media)**

**9.3.1 Twisted Pair Cables (Ethernet Cables)**

**9.3.1.1 Cat5 (Category 5)**

* **Speed:** Up to 100 Mbps (Fast Ethernet).
* **Frequency:** 100 MHz.
* **Usage:** Older LAN networks.
* **Distance:** Up to 100 meters.
* **Limitation:** Not suitable for Gigabit Ethernet.

**9.3.1.2 Cat5e (Category 5 Enhanced)**

* **Speed:** Up to 1 Gbps (Gigabit Ethernet).
* **Frequency:** 100 MHz.
* **Usage:** Common in home/office LANs.
* **Improved:** Reduced crosstalk compared to Cat5.

**9.3.1.3 Cat6 (Category 6)**

* **Speed:** Up to 10 Gbps (short distances).
* **Frequency:** 250 MHz.
* **Usage:** Enterprise LANs.
* **Distance:** 55 meters for 10 Gbps.

**9.3.4 Cat6a (Augmented Cat6)**

* **Speed:** 10 Gbps.
* **Frequency:** 500 MHz.
* **Distance:** Up to 100 meters.
* **Better shielding:** Less interference.

**9.3.1.5 Cat7**

* **Speed:** 10 Gbps.
* **Frequency:** 600 MHz.
* **Shielded:** STP (Shielded Twisted Pair).
* **Usage:** Data centers, high-speed LANs.

**9.3.1.6 Cat8**

* **Speed:** Up to 40 Gbps.
* **Frequency:** 2000 MHz.
* **Distance:** Up to 30 meters.
* **Usage:** Short-range data centers and high-speed backbone.

**9.4 Optical Fiber Cable (OFC)**

* Uses light signals for data transmission.
* Very high bandwidth and long-distance transmission.

**9.4.1 Single-core (Single-Mode Fiber - SMF)**

* **Core Diameter:** ~8-10 microns.
* **Light Source:** Laser.
* **Distance:** 40-100 km.
* **Speed:** Very high (up to Tbps).
* **Usage:** Long-distance telecom, backbone networks.

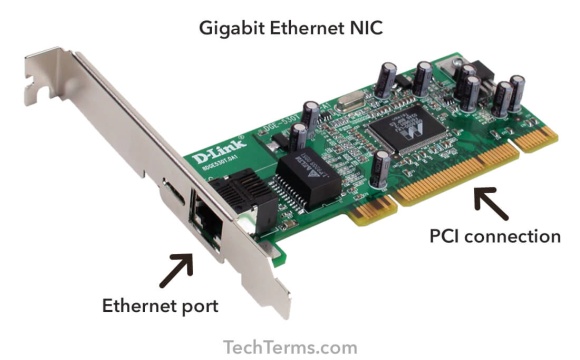
**9.4.2 Multicore (Multi-Mode Fiber - MMF)**

* **Core Diameter:** 50-62.5 microns.
* **Light Source:** LED.
* **Distance:** Up to 2 km.
* **Speed:** High but less than SMF.
* **Usage:** LANs, short-distance data centers.
  1. **Summary Table**

| **Medium** | **Speed** | **Max Distance** | **Use Case** |
| --- | --- | --- | --- |
| Air | Variable | Depends on technology | Wi-Fi, Mobile |
| Vacuum | High | Space distances | Satellite |
| Cat5 | 100 Mbps | 100 m | Older LANs |
| Cat5e | 1 Gbps | 100 m | Home/Office LAN |
| Cat6 | 10 Gbps | 55 m | Enterprise |
| Cat6a | 10 Gbps | 100 m | Enterprise |
| Cat7 | 10 Gbps | 100 m | Data Centers |
| Cat8 | 40 Gbps | 30 m | High-speed DC |
| Single-Core OFC | Tbps | 40-100 km | Telecom Backbone |
| Multi-Core OFC | Gbps | 2 km | LAN/Data Centers |

**10. Devices**

* 1. **NIC(Network interface card)**



NIC is a device that helps the computer to communicate with another device. The network interface card contains the hardware addresses, the data-link layer protocol use this address to identify the system on the network so that it transfers the data to the correct destination.

There are two types of NIC: wireless NIC and wired NIC.

* Wireless NIC: All the modern laptops use the wireless NIC. In Wireless NIC, a connection is made using the antenna that employs the radio wave technology.
* Wired NIC: Cables use the wired NIC to transfer the data over the medium.

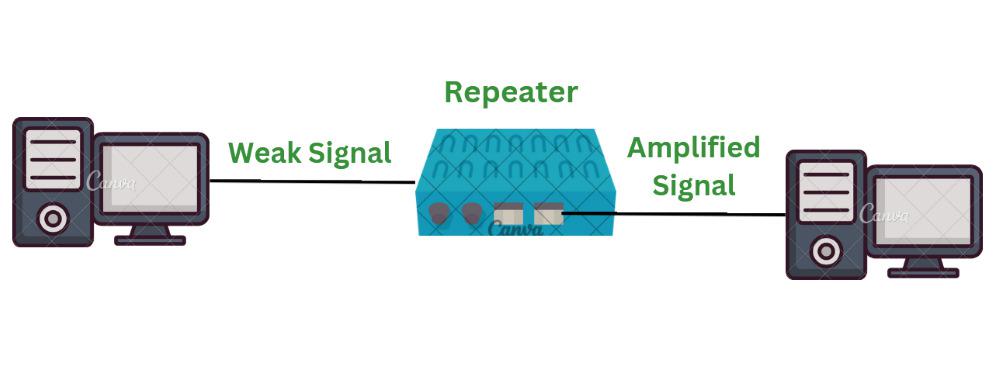
**Advantages:**

* Enables physical connection to the network.
* Supports high-speed data transfer.
* Plug-and-play; easy to install.

**Limitations:**

* Requires proper driver/software.
* Failure results in loss of network connectivity.

**10.2 Repeater**



**Features:**

* Operates at Physical Layer.
* Amplifies and regenerates weak signals.
* Extends distance of data transmission.

**Capacity:**

* Depends on underlying network (up to 10 Gbps for modern repeaters).

**Advantages:**

* Extends network range.
* Simple and inexpensive.
* No configuration needed.

**Limitations:**

* Cannot filter traffic.
* Only amplifies signals; also amplifies noise.
* Cannot connect different network types.

**10.3 Bridge**

A Bridge is a kind of networking device that interconnects two or more networks together by dividing LAN into different segments. For this purpose it uses forwarding database or a bridge table. Unlike hubs, bridges does not simply broadcast traffic it effectively manages and it broadcasts traffic to network segments. Moreover it functions at datalink layer of the OSI model.

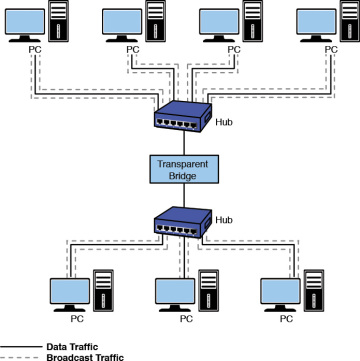
A bridge can be used in computer networks to interconnect two LANs together and separate network segments. Recall that a *segment* is a section of a network separated by bridges, switches, and routers. The **bridge** is a layer 2 device in the OSI model, meaning that it uses the MAC address information to make decisions regarding forwarding data packets. Only the data that needs to be sent across the bridge to the adjacent network segment is forwarded. This makes it possible to isolate or segment the network data traffic

**Features:**

* Operates at Data Link Layer.
* Connects two LAN segments.
* Uses MAC addresses to forward frames.
* Reduces network collisions.

**Advantages of Bridges**

* + **Network Extend:** Sometimes bridges act as repeaters to extend a network. Networks with different architectures can be connected together using bridges.
  + **Increased Bandwidth** : Few of the nodes present on a network share a separate collision domain. For these individual nodes, bridges increases bandwidth.
  + **High Reliability** : Overall the network reliability is basically high in a bridge which makes it easier to maintain the network. And also network congestion can be reduced by dividing LAN into small segments.
  + **Frame Buffering** : Different segments uses different MAC protocols. As a result it creates frame buffers. Therefore, bridges works to interconnect different segments.
  + **Protocol Transparency** : Bridges generally functions at the MAC layer. This makes higher levels of protocol transparent.



**Disadvantages of Bridges**

* + **Cost**: On average a bridge costs more than the hub and repeaters. That is the reason why it is only preferred when there is LAN network traffic load. In other situations of variable data load it is advisable to use either a hub or a repeater.
  + **Speed** : A bridge does more buffering of frames and introduce more relays. This makes them slower compare to a repeater.
  + **Network Performance** :Since bridges make extra processing by viewing all of the MAC addresses, they can potentially downgrade network performance.
  + **Broadcast Filtering :**Bridges cannot individually filter the broadcast traffic. They simply forward broadcast packets.
  + **Broadcast Storms** : Another downfall of simply forwarding broadcast traffic is that they can situation known as broadcast storms. Broadcast storms are nothing but high amount of broadcast traffic.

**10.4 Switches**



Switch is a networking device that groups all the devices over the network to transfer the data to another device. A switch is better than Hub as it does not broadcast the message over the network, i.e., it sends the message to the device for which it belongs to. Therefore, we can say that switch sends the message directly from source to the destination.

It is networking device which transfers data only to the host where it is being addressed. It checks the destination address to route the packet appropriately.

Following are features of the network switches.  
• It operates at layer-2 (data link layer).  
• It is available in various configurations and as per data transfer speeds such as 10/100/1000 Mbps or 10/100 Gbps.  
• Operates in full duplex mode  
• Packet collision is avoided due to port to port data transmission.

**Advantages of Switches**

Following are the benefits or **advantages of Switches**:

* They increase the available bandwidth of the network.
* They help in reducing workload on individual host PCs
* They increase the performance of the network.
* Networks which use switches will have less frame collisions. This is due to the fact that switches create collision domains for each connection.
* Switches can be connected directly to workstations.

**Disadvantages of Switches**

Following are the **disadvantages of Switches**:

* They are more expensive compare to network bridges.
* Network connectivity issues are difficult to be traced through the network switch.
* Broadcast traffic may be troublesome.
* If switches are in promiscuous mode, they are vulnerable to security attacks e.g. spoofing IP address or capturing of ethernet frames.
* Proper design and configuration is needed in order to handle multicast packets.
* While limiting broadcasts, they are not as good as routers.

**10.5 Modem (Modulator-Demodulator)**



**Features:**

* Converts digital data to analog and vice versa.
* Enables internet access over telephone lines or coaxial cables.

**Capacity:**

* DSL Modem: Up to 100 Mbps.
* Cable Modem: Up to 1 Gbps or more (DOCSIS 3.1).

**Advantages:**

* Essential for ISP connection.
* Simple setup.
* Supports both upload and download.

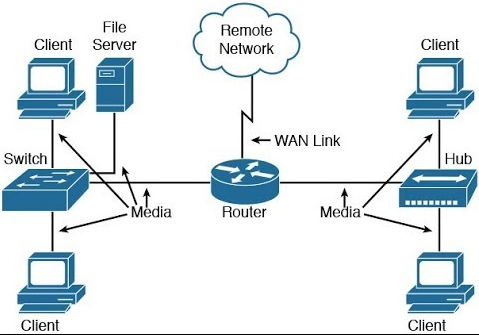
**Limitations:**

* Not useful inside LAN.
* Speed depends on ISP and line quality.
* Only converts signals; cannot route or switch.

**10.6 Router**

This networking device provides interconnection between two dissimilar networks. It operates at layer-3 of OSI stack and takes care of routing of packets based on routing table. It uses IP addressing for routing the packets. The IP address of each hosts contain two parts viz. network address and host address. The router checks destination host address, source host address and network address in order to route IP packet appropriately. Refer [TCP-IP Packet format](https://www.rfwireless-world.com/General/TCP-IP-packet-format.html) to know about various fields and their purpose in the networking system.

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.



**Benefits or advantages of Routers**

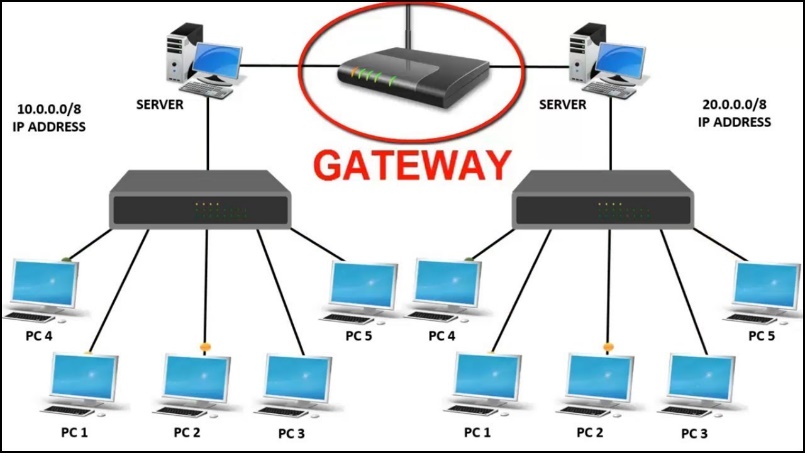
Following are the benefits or **advantages of Routers**:

* It provides connection between different network architectures such as ethernet & token ring etc.
* It can choose best path across the internetwork using dynamic routing algorithms.  
  It can reduce network traffic by creating collision domains and also by creating broadcast domains.
* It provides sophisticated routing, flow control and traffic isolation.
* They are configurable which allows network manager to make policy based on routing decisions.

**Drawbacks or disadvantages of Routers**

* Following are the drawbacks or **disadvantages of Routers**:
* They operate based on routable network protocols.
* They are expensive compare to other network devices.
* Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
* They are slower as they need to analyze data from layer-1 through layer-3.
* They require considerable amount of initial configurations.
* They are protocol dependent devices which must understand the protocol they are forwarding.

**10.7 Gateway**



**Features:**

* Operates across all layers (mainly Application Layer).
* Converts protocols between different networks.
* Acts as entry/exit point for different networks.

**Capacity:**

* Varies widely based on application.

**Advantages:**

* Enables communication between different architectures.
* Supports protocol translation (TCP/IP ↔ IPX/SPX, VoIP, Email, etc.).
* Essential for hybrid networks.

**Limitations:**

* High cost.
* Complex configuration.
* Requires skilled technical expertise.

**10.8 Access Point (AP)**

**Features:**

* Operates at Data Link Layer (Layer 2).
* Connects wireless devices to wired LAN.
* Supports multiple wireless standards (Wi-Fi 4/5/6/6E).

**Capacity:**

* Wi-Fi 5 (802.11ac): Up to 3.5 Gbps.
* Wi-Fi 6 (802.11ax): Up to 9.6 Gbps.

**Advantages:**

* Provides wireless coverage.
* Easy network expansion.
* Supports many simultaneous users.

**Limitations:**

* Limited coverage area (~30-50 meters indoors).
* Signal interference from walls, devices.
* Security issues if not properly secured.

**10.9 Summary Table**

| **Device** | **Layer** | **Capacity** | **Key Advantage** | **Key Limitation** |
| --- | --- | --- | --- | --- |
| NIC | Data Link | Up to 10 Gbps | Enables device connection | Hardware dependent |
| Repeater | Physical | Up to 10 Gbps | Extends signal range | Amplifies noise too |
| Bridge | Data Link | ~1 Gbps | Segments network | Limited scalability |
| Switch | Data Link | Up to 100 Gbps | Efficient LAN traffic | Complex in large LANs |
| Modem | Physical | Up to 1 Gbps | ISP connectivity | No LAN management |
| Router | Network | Up to Tbps | Inter-network routing | Complex configuration |
| Gateway | All Layers | Application Dependent | Protocol translation | High cost & complexity |
| Access Point | Data Link | Up to 9.6 Gbps | Wireless access | Limited range |