Introduction: Data Communications, Internetworking: A Communications Model, Data Communications, Networks, The Internet, An Example Configuration. Protocol Architecture, The Need for a Protocol Architecture: The TCP/IP Protocol Architecture, The OSI Model, Traditional Internet-Based Applications, Characteristics of Data, Transmission: Concepts and Terminology, Analog and Digital Data Transmission, Transmission Impairments.

Learning Outcomes: At the end of this unit Students will be able to

1. Explain the Representations used for defining data communications with the state of art.

Data Communications

- Protocols and standards are vital to the implementation of data communications and networking. Protocols refer to the rules; a standard is a protocol that has been adopted by vendors and manufacturers.
- Network models serve to organize, unify, and control the hardware and software components of data communications and networking.

Data communications

- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.
- For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).
- The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

I**. Delivery**. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. **Timeliness**. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. Ifsome of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Definition of computer networks

A data network consists of a set of hosts connected by network devices. A host is any device that sends and receives information on the network. Peripherals are devices that are connected to hosts.

Some devices can act as hosts and peripherals. For example, a printer connected to a laptop that is on a network acts as a peripheral. If the printer is connected directly to a network device,such as a hub, a switch or a router, it acts as a host.

Computer networks are used globally in companies, homes, schools, and government agencies. Many of the networks connect through the Internet.

transmissions.

Networking benefits

The benefits of networking on computers and other devices include low costs and higher productivity. Thanks to networks, resource scan be shared, which reduces data duplication and corruption.

- ✓ Fewer peripherals are needed.

Every computer on the network does not need its printer, scanner, or backup device. It is possible to configure several printers in a central location and share them among network users. All network users send print jobs to a central print server that manages printr equests. The print server can distribute print jobs among the various printers, or it can queue jobs that require a particular printer.

- ✓ Greater communication capabilities

Networks offer various collaboration tools that can be used to establish communications between network users. Online collaboration tools include email, forums and chat, voice and video, and instant messaging. With these tools, users can communicate with friends,family, and colleagues.

- ✓ Duplication and file corruption are avoided

A server manages network resources. The servers store the data and share it with the users of a network. Confidential or essential data can be protected and shared with users who have permission to access such data. Document tracking software can be used toprevent users from overwriting or modifying files that other users are accessing at the same time.

- ✓ Lower cost in license acquisition

Acquiring application licenses can be expensive for individual computers. Many software providers offer site licenses for networks,which can significantly reduce the cost of the software. The site license allows a group of people or an entire organization to usethe application for a single fee.

- ✓ Centralized administration

Centralized administration reduces the number of people needed to manage devices and data on the network, allowing the company to save time and money.

Individual users of the network do not need to manage their data and devices. An administrator can control the data, devices, and permissions of network users. Creating backup copies of the data is more comfortable because of the data stored in a central location.

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

- In data communications, text is represented as a bit pattern, a sequence of bits
- Different sets of bit patterns have been designed to represent text symbols.
- Each set is called a code, and the process of representing symbols is called coding.
- Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.
- The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin. Appendix A includes part of the Unicode.

Numbers

- Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images

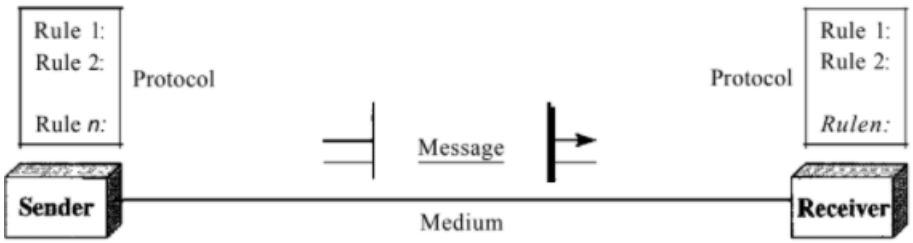
- Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand-white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

- Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we

Five components of data communication

Five components of data communication



-

Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

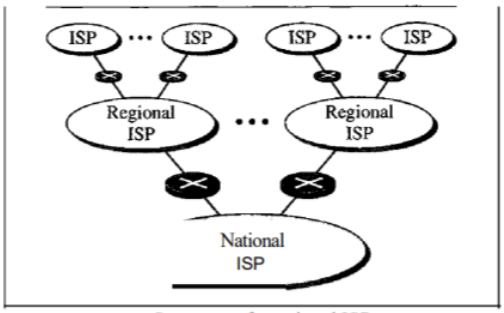
Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

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

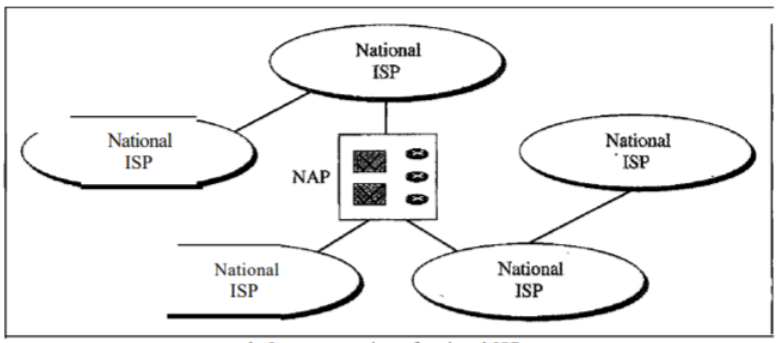
The Internet

- ✓ In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP).
- ✓ By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

- ✓ In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internet ting.
- ✓ The Internet has come a long way since the 1960s.
- ✓ The Internet today is not a simple hierarchical structure.
- ✓ It is made up of many wide- and local-area networks joined by connecting devices and switching stations.
- ✓ It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.
- ✓ Today most end users who want Internet connection use the services of Internet service providers (lSPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government.



a. Structure of a national ISP



b. Interconnection of national ISPs

International Internet Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called peering points. These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs.

Network Criteria:

The criteria that must be met by a computer network are:

1.Performance - It is measured in terms of transit time and response time.

- ✓ Transit time is the time for a message to travel from one device to another
- ✓ Response time is the elapsed time between an inquiry and a response.

Performance is dependent on the following factors:

- ✓ The number of users
- ✓ Type of transmission medium
- ✓ Capability of connected network
- ✓ Efficiency of software

2. Reliability - It is measured in terms of

- ✓ Frequency of failure
- ✓ Recovery from failures

3.Security - It means protecting data from unauthorized access.

Goals of Computer Networks

The following are some important goals of computer networks:

- **Resource Sharing** - Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, fax, modem, scanner etc.

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

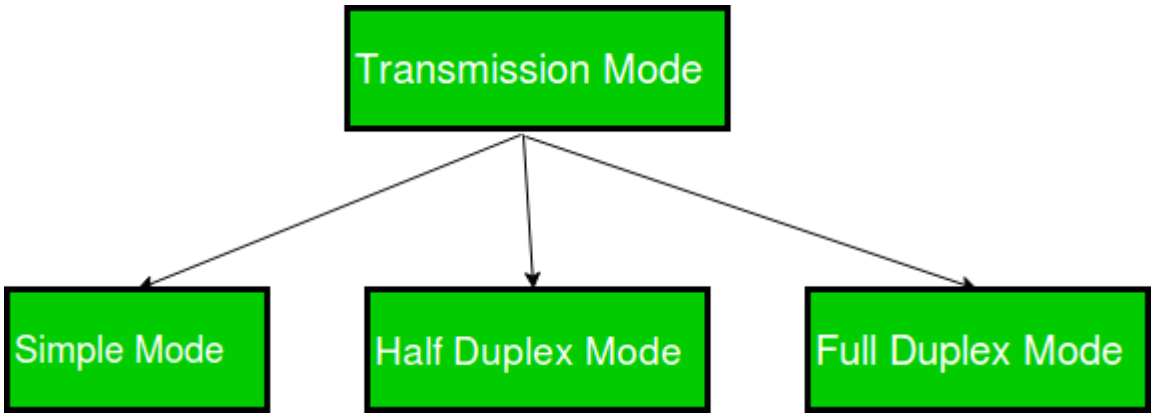
- **Inter-process Communication** - Network users, located geographically apart, may converse in an interactive session through the network. In order to permit this, the network must provide almost error-free communications.

- **Flexible access** - Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.

Other goals include Distribution of processing functions, Centralized management, and allocation of network resources, Compatibility of dissimilar equipment and software, Good network performance, Scalability, Saving money, Access to remote information, Person to person communication etc.,

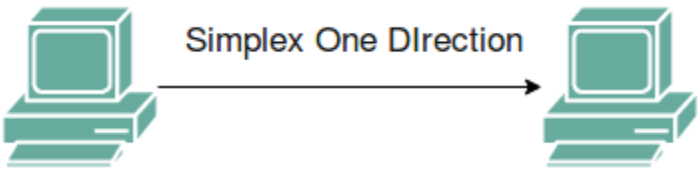
Data Flow

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:-



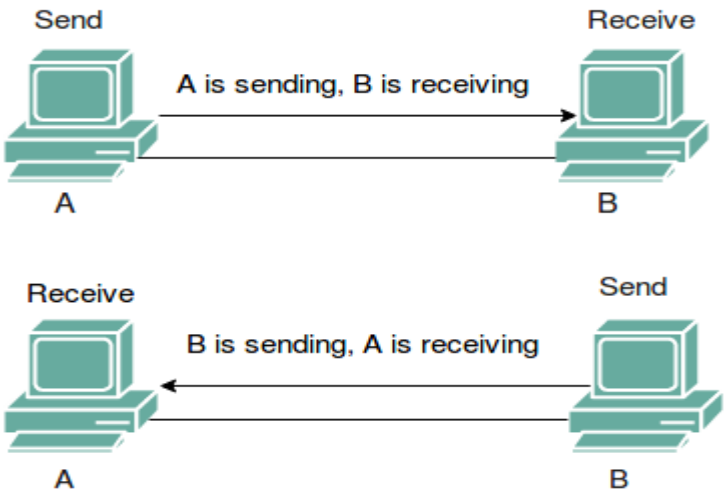
1. **Simplex Mode –**
   In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

   Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



2. Half-Duplex Mode –
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.
Channel capacity=Bandwidth * Propagation Delay



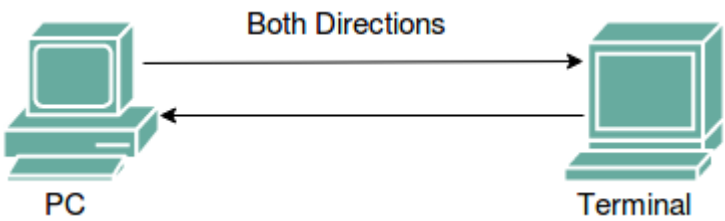
3. Full-Duplex Mode –
In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- Or the capacity is divided between signals travelling 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



Types of Connections

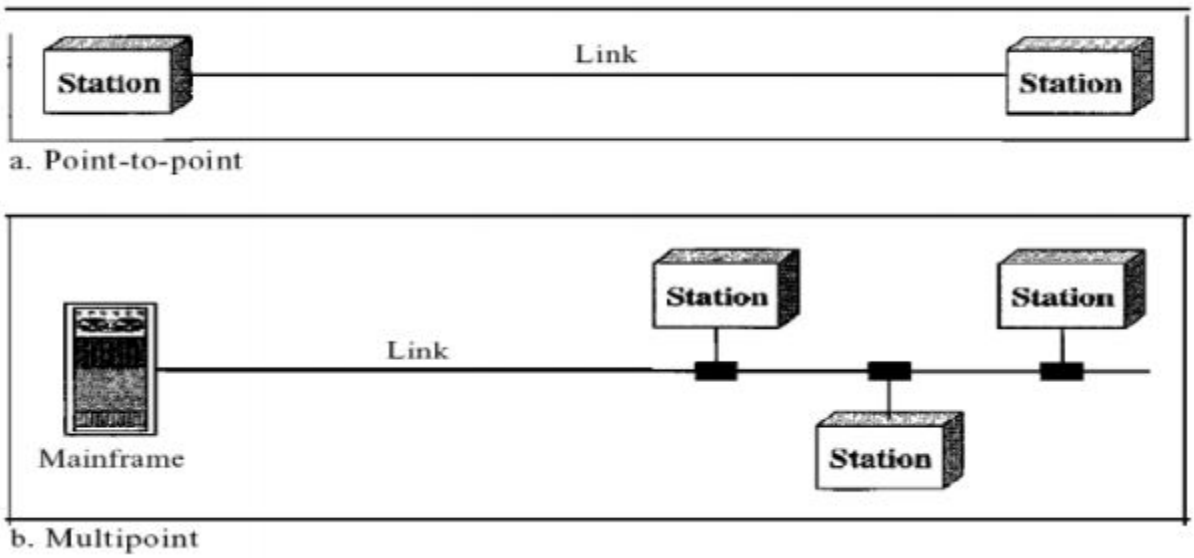
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

Point-to-Point

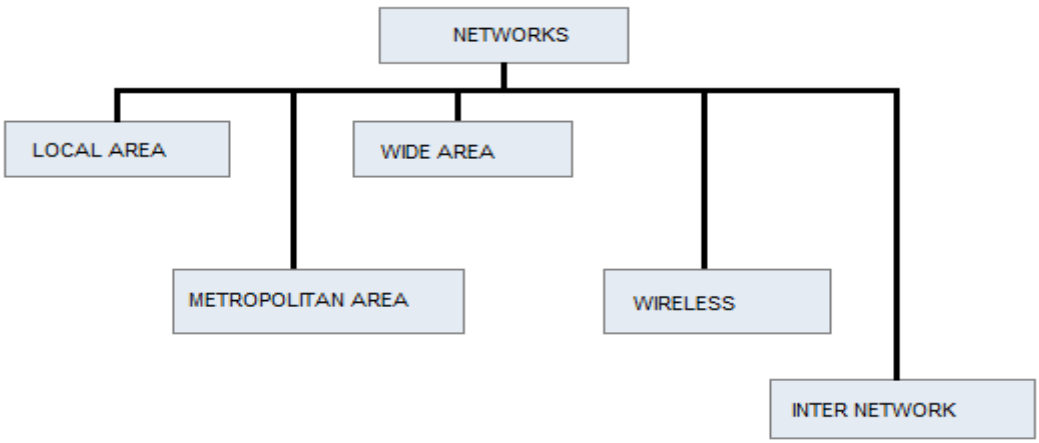
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

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



Types of Communication Networks

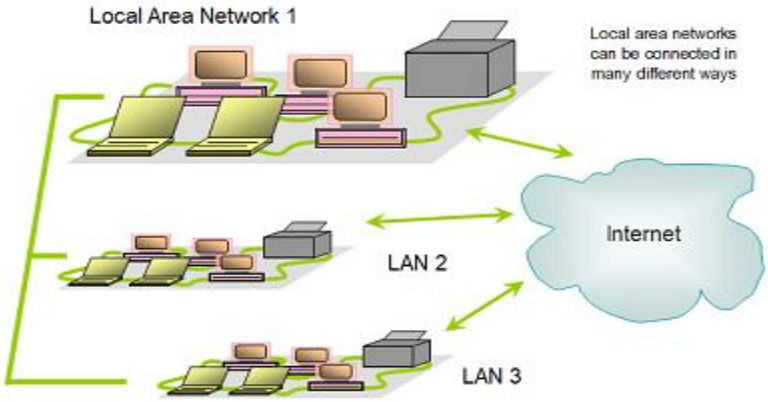


LANs and WANs

A network can be anything from two computers connected together, to millions of computers connected on the internet. There are many different types of networks such as LAN, WAN, VPN, WPAN and PAN.

LAN:

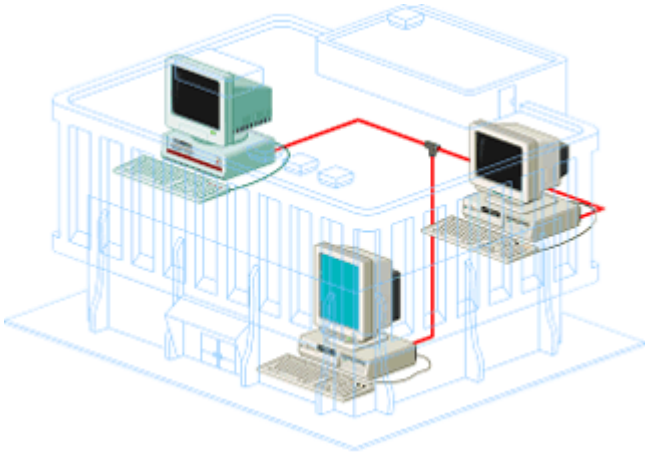
A LAN (local area network) is a network of computers within the same building, such as a school, home or business. A LAN is not necessarily connected to the internet.



Advantages and Disadvantages of LAN:

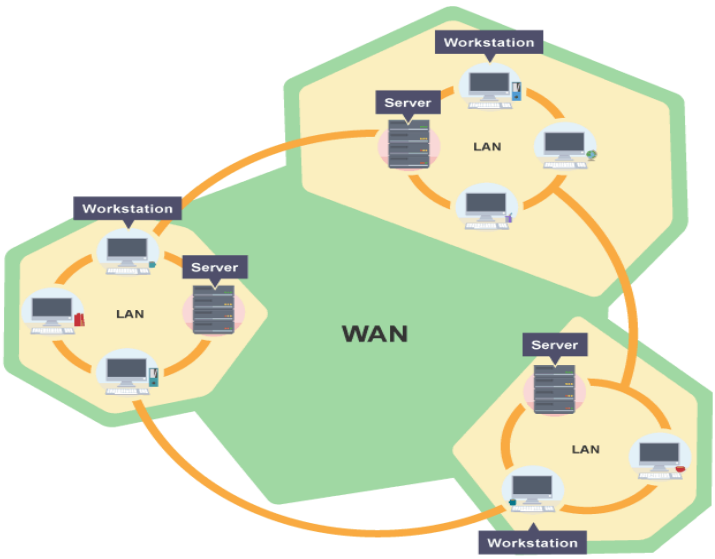
Advantages of LAN's	Disadvantages of LAN's
Saves money as each computer on the LAN can share resources. (For example - you only need to buy one printer because it can be shared between all the computers on the network)	**Viruses** can **spread** around LAN's very **quickly**. (This is because the computers are all joined together - if one computer gets infected, the other are at risk)
Files and data can be **shared** easily. (Like the shared drive on a school network)	**Security** can be an **issue**. (If one computer is hacked into, the other computers on the network can also be accessed)
Files and data can be **accessed** from **any computer** on the network. (For example - it doesn't matter which computer in the school you log onto, you can access your work files)	The network can become **unusable** if the main **server** computer **breaks down**. (You won't be able to log onto any of the client computers on the network)

LANS are confined to one room or small building.

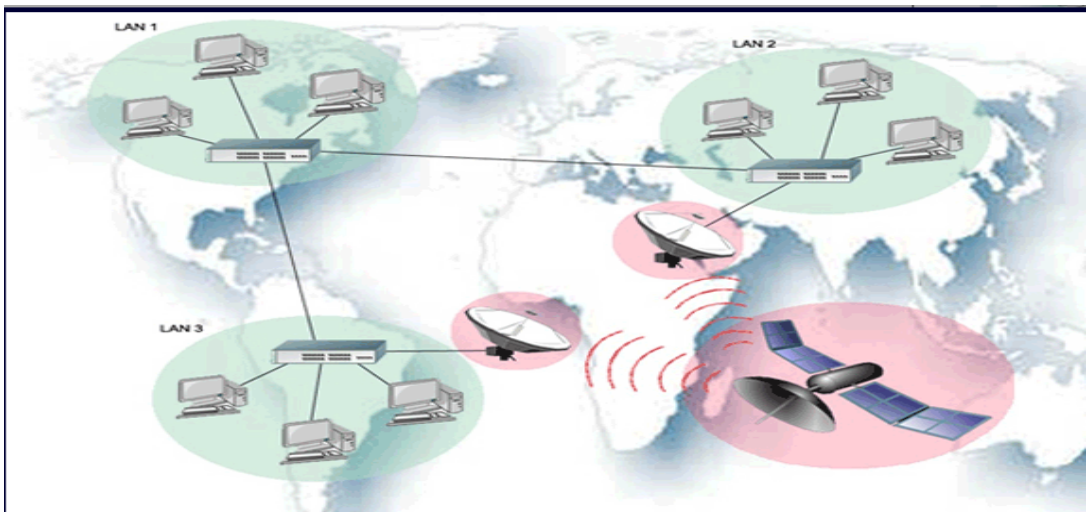


WAN

A WAN (wide area network) is created when LANs are connected. This requires media such as broadband cables, and can connect up organizations based in different geographical places. The internet is a WAN.



Advantages of WAN's	Disadvantages of WAN's
Computers can be **connected** over **wide areas**. (Across cities or even continents)	**Security** can be an **issue** as anyone with access to the internet can potentially access any of the computers on the network. (Computers on the network need to be secured with a firewall and important files should be encrypted)
Files and **data** can be **shared** over a **large area**.	It's very **easy** to accidentally **download viruses** from a WAN onto your computer. (You need to make sure that your computer is protected with up-to-date anti-virus)
People can use their computers/devices to **communicate** very quickly, over large areas. (Sending emails, discussion forums, video conferencing etc.)	Data is **transferred** across a WAN at a much **slower rate** than it is across a LAN. (Download speeds are limited)
E-Commerce (shopping) websites can be set up and accessed by people from all over the world.	**Monitoring** a WAN can be **difficult** because they have so many computers connected to them.



VPN:

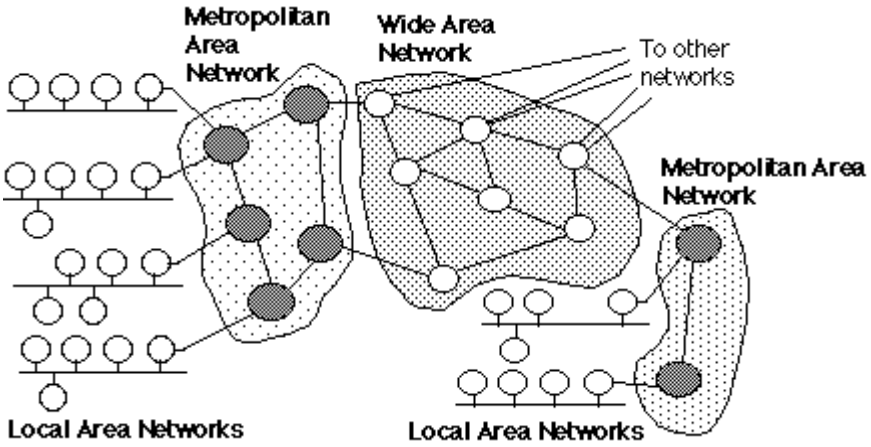
A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods -- including passwords, tokens and other unique identification methods -- to gain access to the VPN..

MAN:

- A Metropolitan Area Network (MAN) is one of a number of types of networks A MAN is a relatively new class of network, but for corporate users with large LANs.
- There are three important features which discriminate MANs from LANs or WANs:

1. The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.
2. A MAN is not generally owned by a single organisation. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a single network provider who sells the service to the users. This level of service provided to each user must therefore be negotiated with the MAN operator, and some performance guarantees are normally specified.
3. A MAN often acts as a high speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

A typical use of MANs to provide shared access to a wide area network is shown in the figure below:



Use of MANs to provide regional networks

(Or)

Types of area network

- The Network allows computers to connect and communicate with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover.
- There are some similarities and dissimilarities between them.
- One of the major differences is the geographical area they cover, i.e. LAN covers the smallest area; MAN covers an area larger than LAN and WAN comprises the largest of all.

There are other types of Computer Networks also, like :

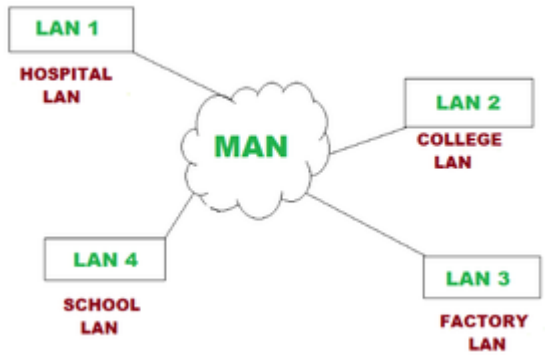
✓ PAN (Personal Area Network)
✓ SAN (Storage Area Network)
✓ EPN (Enterprise Private Network)
✓ VPN (Virtual Private Network)

Local Area Network (LAN) –

- LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs.
- The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol.
- Private addresses are unique in relation to other computers on the local network.
- Routers are found at the boundary of a LAN, connecting them to the larger WAN.
- Data transmits at a very fast rate as the number of computers linked is limited.
- By definition, the connections must be high speed and relatively inexpensive hardware (Such as hubs, network adapters, and Ethernet cables).
- LANs cover a smaller geographical area (Size is limited to a few kilometers) and are privately owned.
- One can use it for an office building, home, hospital, schools, etc. LAN is easy to design and maintain.
- A Communication medium used for LAN has twisted-pair cables and coaxial cables. It covers a short distance, and so the error and noise are minimized.
- Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. Propagation delay is very short in a LAN.
- The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers.
- A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN.
- The fault tolerance of a LAN is more and there is less congestion in this network.
- For example A bunch of students playing Counter-Strike in the same room (without internet).

Metropolitan Area Network (MAN)

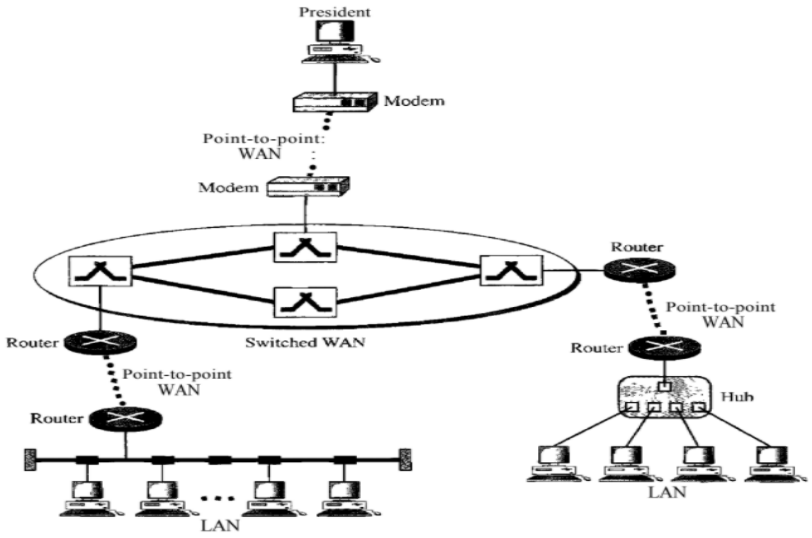
- MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN.
- It connects two or more computers that are apart but reside in the same or different cities.
- It covers a large geographical area and may serve as an ISP (Internet Service Provider).
- MAN is designed for customers who need high-speed connectivity.
- Speeds of MAN range in terms of Mbps.
- It’s hard to design and maintain a Metropolitan Area Network.
-



- The fault tolerance of a MAN is less and also there is more congestion in the network.
- It is costly and may or may not be owned by a single organization.
- The data transfer rate and the propagation delay of MAN are moderate.
- Devices used for transmission of data through MAN are Modem and Wire/Cable.
- Examples of a MAN are the part of the telephone company network that can provide a high-speed DSL line to the customer or the cable TV network in a city.

Wide Area Network (WAN)

- WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country.
- A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public.
- The technology is high speed and relatively expensive.
- There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain.
- Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network.
- A Communication medium used for WAN is PSTN or Satellite Link.
- Due to long-distance transmission, the noise and error tend to be more in WAN.
- WAN's data rate is slow about a 10th LAN's speed since it involves increased distance and increased number of servers and terminals etc.
- Speeds of WAN ranges from a few kilobits per second (Kbps) to megabits per second (Mbps).
- Propagation delay is one of the biggest problems faced here.
- Devices used for the transmission of data through WAN are Optic wires, Microwaves, and Satellites.

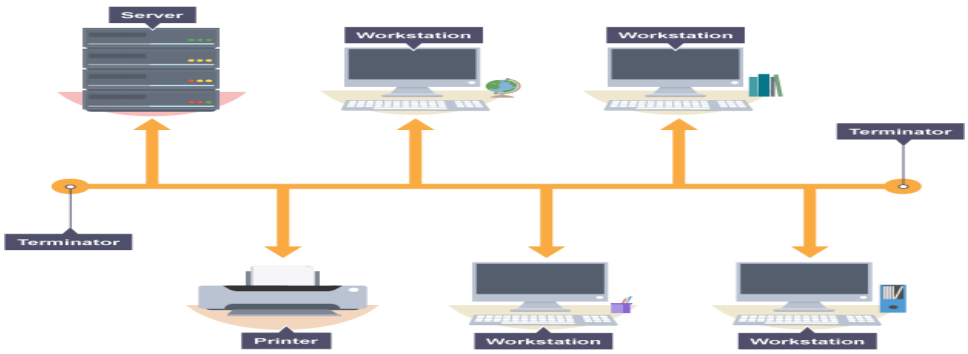


Network Topologies

Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.. Three of the main topologies include bus, star and ring.

Bus network

In a bus network all the workstations, servers and printers are joined to one cable - 'the bus'. At each end of the cable a terminator is fitted to stop signals reflecting back down the bus.



Advantages

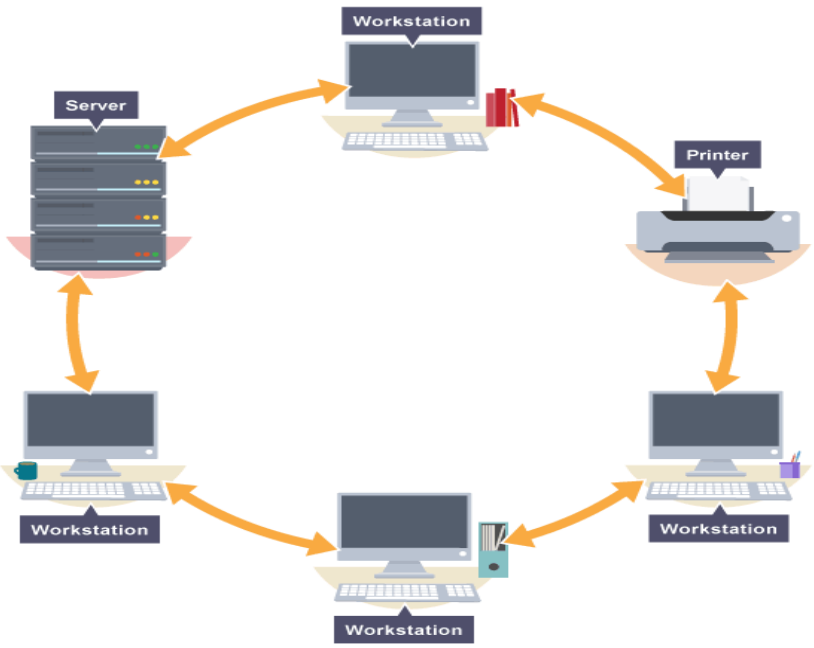
1. easy to install
2. cheap to install - it does not require much cabling
3. Used in small networks.
4. Easy to expand joining two cables together.

Disadvantages

1. if the main cable fails or gets damaged, the whole network will fail
2. Cable has a limited length.
3. as more workstations are connected, the performance of the network will become slower because of data collisions
4. Every workstation on the network 'sees' all of the data on the network, which can be a security risk.

Ring network

In a ring network, each device (e.g. workstation, server, and printer) is connected in a ring so each one is connected to two other devices. Each data packet on the network travels in one direction. Each device receives each packet in turn until the destination device receives it.



Advantages

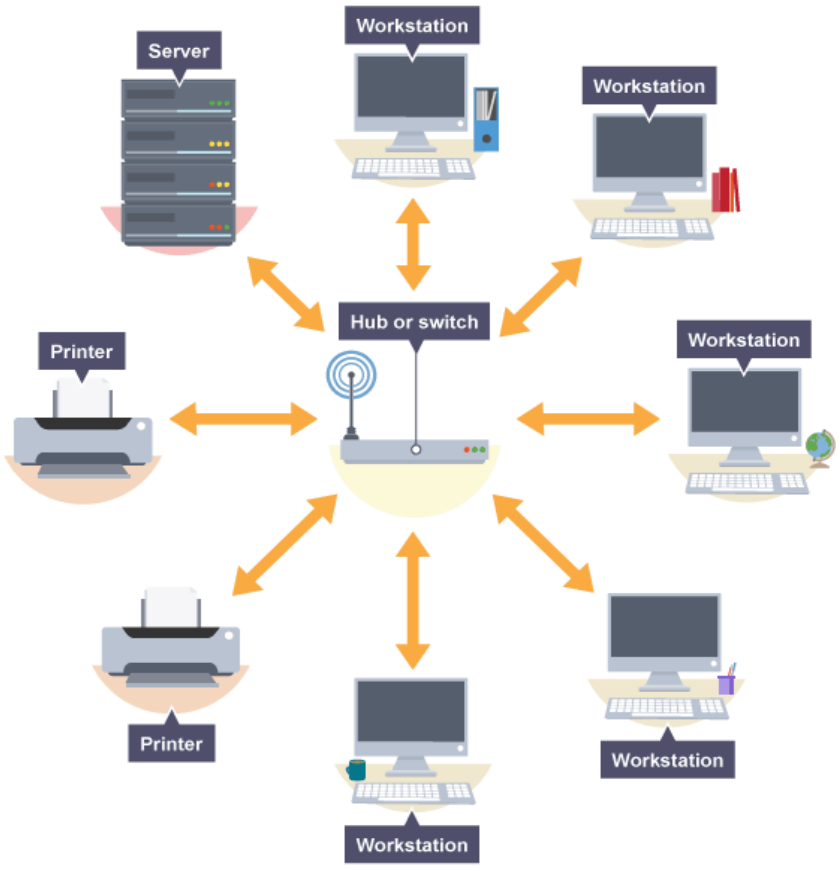
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand.

Disadvantages

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

Star network

In a star network, each device on the network has its own cable that connects to a switch or hub. This is the most popular way of setting up a LAN. You may find a star network in a small network of five or six computers where speed is a priority.



Advantages

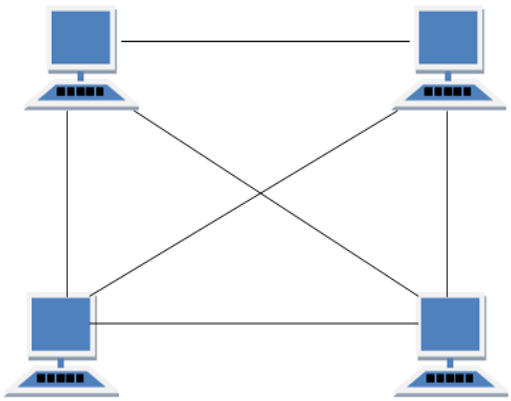
1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages

1. Expensive to install as this type of network uses the most cable, and network cable is expensive
2. Extra hardware is required - hubs or switches - which add to the cost
3. If a hub or switch fails, all the devices connected to it will have no network connection.

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n (n-2)/2 physical channels to link n devices.



Advantages of Mesh Topology

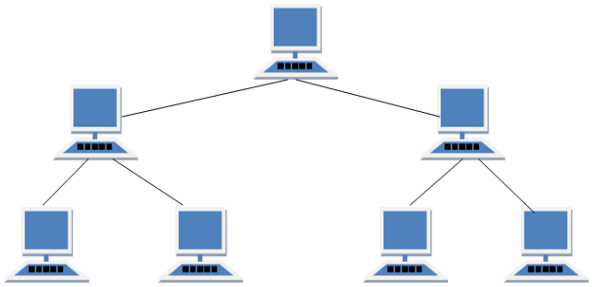
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology Heavily cabled.

a. Costly.
b. If more nodes are added maintenance is difficult.
c. Central hub fails, network fails.

Wired and wireless connections

Connections between computers on a network can be wired or wireless.

- Wired connection: Computers can be connected through Ethernet cables which connect to the Ethernet port. Connecting hardware such as a router has Ethernet ports.
- Wireless connection: Computers can make a wireless connection if they have a wireless NIC. A wireless router provides a connection with the physical network. A computer device needs to be within range of the router to get access. A wireless connection uses radio signals to send data across networks. The wireless adapter converts the data into a radio signal and the wireless receiver decodes it so that the computer can understand it.
- Wireless transmissions can be intercepted by anyone within range of the router. Access can also be restricted to specific MAC addresses, and transmissions are usually encrypted using a key that works with WPA (Wi-Fi protected access).

Advantages and disadvantages of wireless networks

Advantages

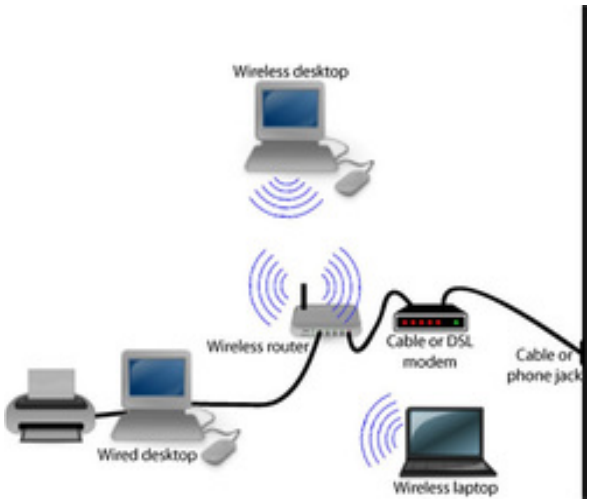
- Cheap set-up costs
- Not tied down to a specific location
- Can connect multiple devices without the need for extra hardware
- Less disruption to the building due to no wires being installed

Disadvantages

- interference can occur
- The connection is not as stable as wired networks and can 'drop off'
- It will lose quality through walls or obstructions
- More open to hacking
- Slower than wired networks

Wired and wireless connections

Connections between computers on a network can be wired or wireless.



Wired connection: Computers can be connected through Ethernet cables which connect to the Ethernet port. Connecting hardware such as a router has Ethernet ports.

Wireless connection: Computers can make a wireless connection if they have a wireless NIC. A wireless router provides a connection with the physical network. A computer device needs to be within range of the router to get access. A wireless connection uses radio signals to send data across networks. The wireless adapter converts the data into a radio signal and the wireless receiver decodes it so that the computer can understand it.

Wireless transmissions can be intercepted by anyone within range of the router. Access can also be restricted to specific MAC addresses, and transmissions are usually encrypted using a key that works with WPA (Wi-Fi protected access).

Advantages and disadvantages of wireless networks

Advantages

1. cheap set-up costs
2. not tied down to a specific location
3. can connect multiple devices without the need for extra hardware
4. less disruption to the building due to no wires being installed
5.

Disadvantages

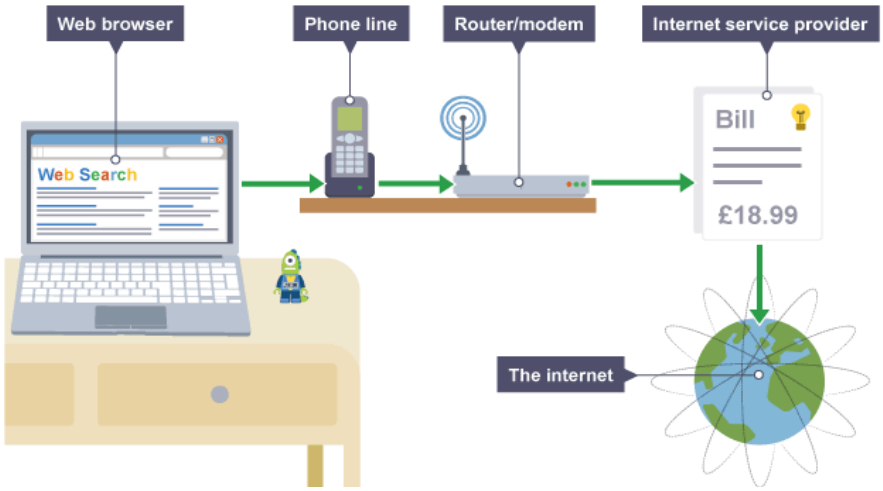
1. interference can occur
2. the connection is not as stable as wired networks and can 'drop off'

3. it will lose quality through walls or obstructions
4. more open to hacking
5. slower than wired networks

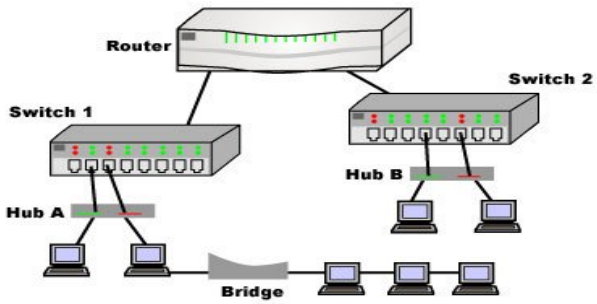
Networking hardware

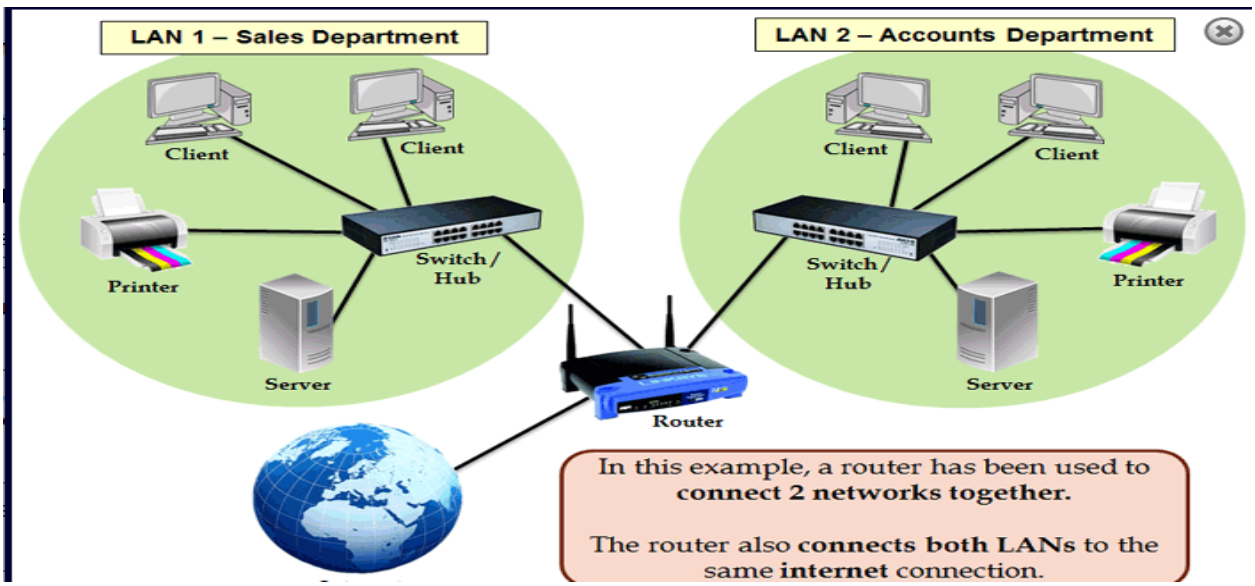
Computers need networking hardware in order to connect to each other. Routers, hubs, switches and bridges are all pieces of networking equipment that can perform slightly different tasks. A router can often incorporate hubs, switches and wireless access within the same hardware.

Routers



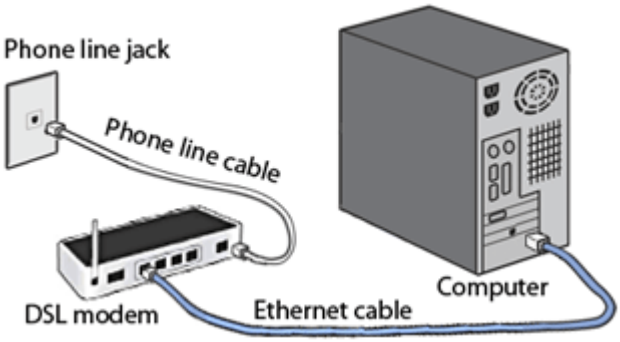
A router can form a LAN by connecting devices within a building. It also makes it possible to connect networks different Homes and businesses use a router to connect to the internet. A router can often incorporate a modem within the hardware.

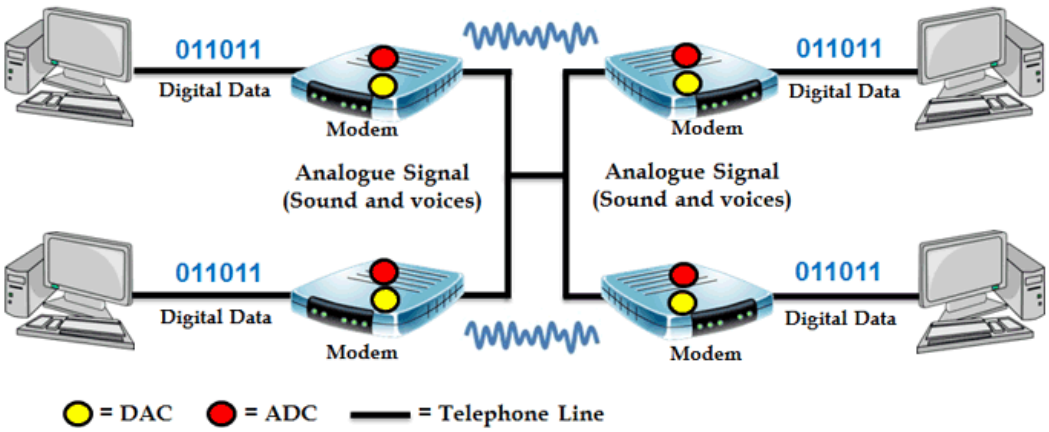




Modems

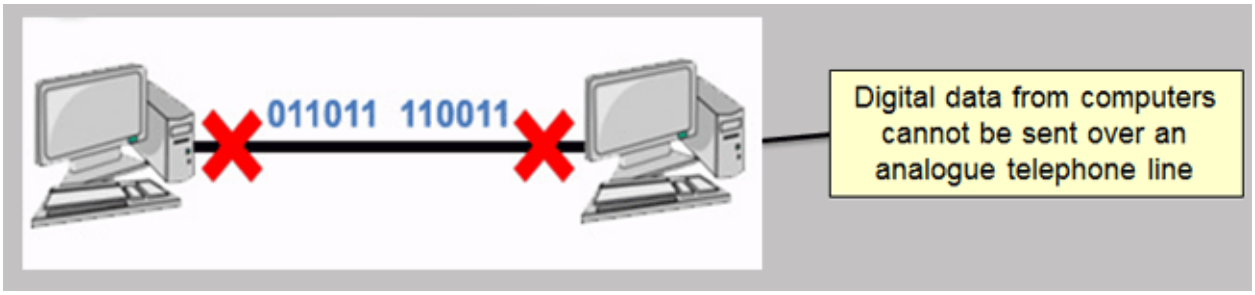
A modem enables a computer to connect to the internet over a telephone line. A modem converts digital signals from a computer to analogue signals that are then sent down the telephone line. A modem on the other end converts the analogue signal back to a digital signal which another computer can understand.



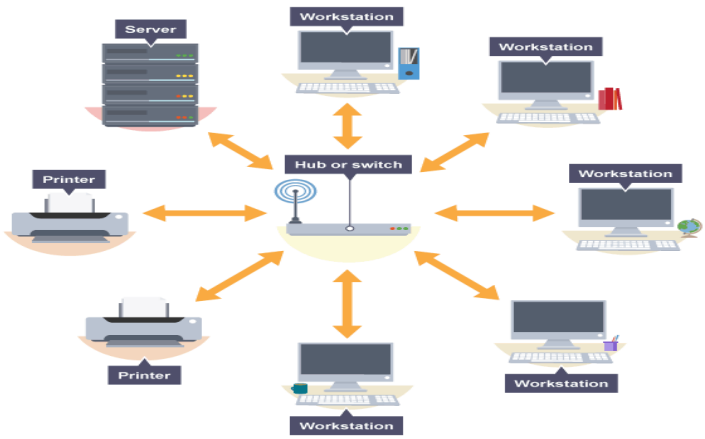


Modems with **DAC** and **ADC** which are converting data from **digital to analogue** to send down the telephone line and then from **analogue to digital** when the data arrives at the destination computer.

How do modem works?



Hubs, bridges and switches



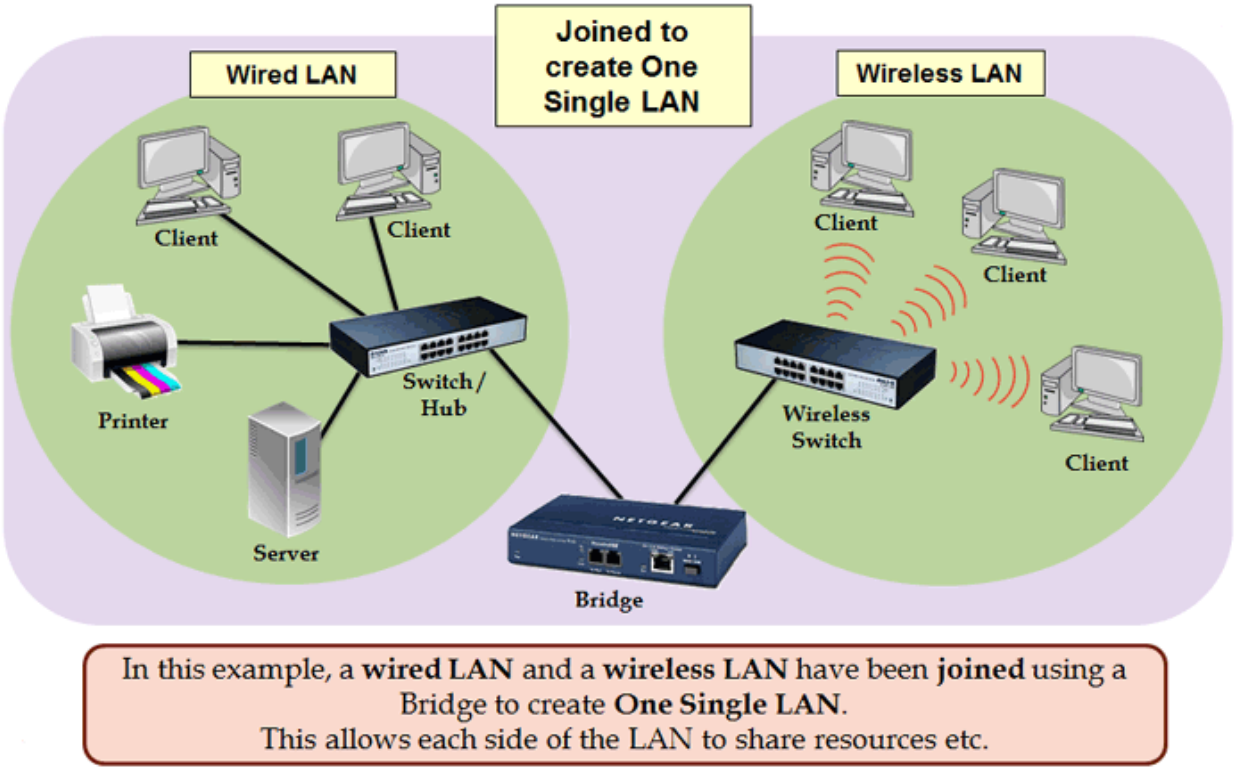
Hubs, bridges and switches allow multiple devices to connect to the router and they transfer data to all devices on a network. A router is a more complex device that usually includes the capability of hubs, bridges and switches.

Hubs

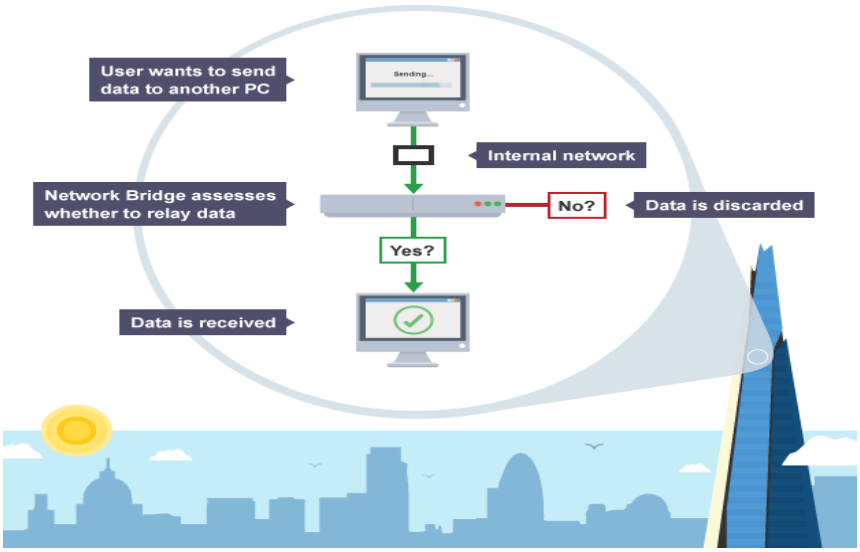
A hub broadcasts data to all devices on a network. This can use a lot of bandwidth as it results in unnecessary data being sent - not all computers might need to receive the data. A hub would be useful to link up a few games consoles for a local multiplayer game using a wired LAN.

Bridges

A bridge is used to connect two separate LAN networks. A computer can act as a bridge through the operating system. A bridge looks for the receiving device before it sends the message. This means that it will not send a message if the receiving computer is not there. It will check to see if the receiver has already had the message. This can help save unnecessary data transfers, which improves the performance of a network.



In this example, a **wired LAN** and a **wireless LAN** have been **joined** using a Bridge to create **One Single LAN**.
This allows each side of the LAN to share resources etc.



Switches

A switch performs a similar role to a hub and a bridge but is more powerful. It stores the MAC addresses of devices on a network and filters data packets to see which devices have asked for them. This makes a switch more efficient when demand is high. If, for example, a game involved lots of data being passed between machines, then a switch could reduce the amount of latency.

Networking Models

There are different networking models for how to connect computers over a network. Computers that request information are called clients and computers that provide information are servers. But the client and server relationship can be organized in different ways.

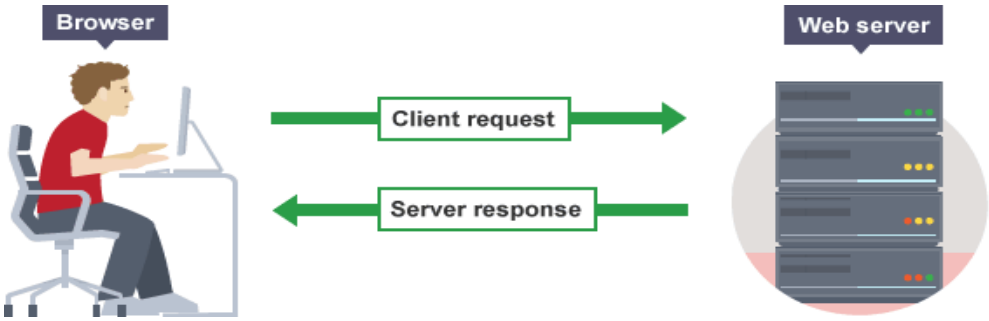
The most widely-used models are client-server or peer-to-peer (P2P).

Client-server

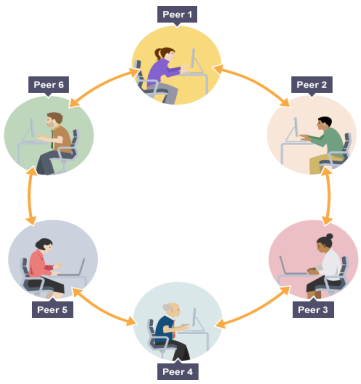
The client-server model is the relationship between two computers in which one, the client, makes a service request from another, the server. The key point about a client-server model is that the client is dependent on the server to provide and manage the information.

For example, websites are stored on web servers. A web browser is the client which makes a request to the server, and the server sends the website to the browser.

Popular websites need powerful servers to serve thousands or millions of clients, all making requests at the same time. The client side of a web application is often referred to as the front end. The server side is referred to as the back end.



Peer-to-peer (P2P)In a P2P network, no single provider is responsible for being the server. Each computer stores files and acts as a server. Each computer has equal responsibility for providing data.



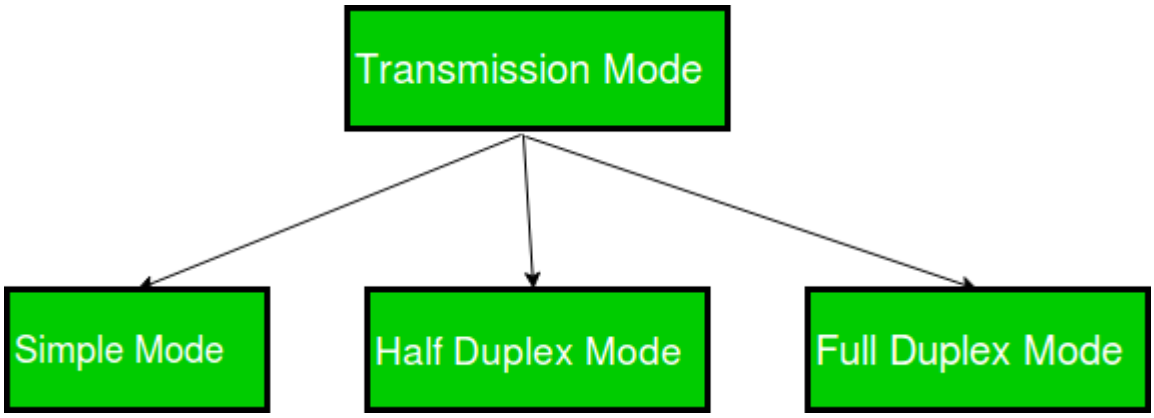
In the client-server model, many users trying to access a large file, such as a film, would put strain on one server. In the peer-to-peer model, many users on the network could store the same file. Each computer can then send sections of the file, sharing the workload. Each client can download and share files with other users.

P2P is ideal for sharing files. P2P would be unsuitable for a service such as booking tickets, as one server needs to keep track of how many tickets are left. Also, on P2P networks no single computer is responsible for storing a file - anyone can delete files as they wish.

Types of Transmission Modes:

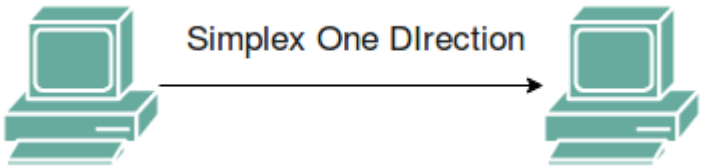
- Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur

between individual devices that are interconnected. There are three types of transmission mode:-



-

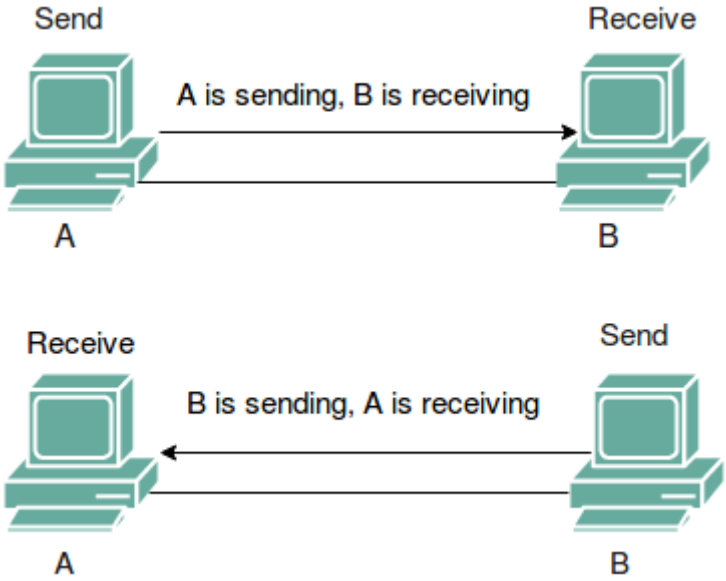
These are explained as following below.
1. Simplex Mode -
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.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

- 

2. Half-Duplex Mode -
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.
Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

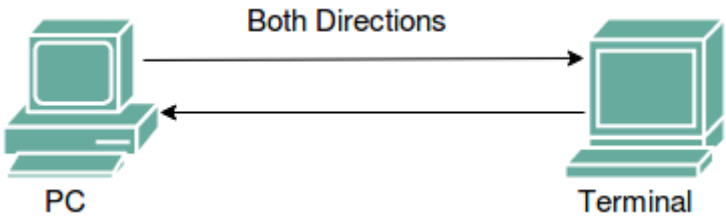
-

- Channel capacity=Bandwidth * Propagation Delay

- 

3. Full-Duplex Mode -
In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- 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
- 

Need of Protocol Architecture

- Layered structure of hardware and software that supports the exchange of data between systems as well as a distributed application (e.g. email or file transfer • Each protocol provides a set of rules.
- Typical task to be performed are as follows (E.g. File transfer) – Source must activate communications Path or inform network of desired destination system. – Source must check if destination is prepared to receive data. – File transfer application on source must

check if destination file management system will accept and store sender's file – May need file format translation

- Task broken into subtasks
- Implemented separately in layers in stack
- Each layer performs a related subset of functions needed in both systems
- Enable peer layers to communicate.
- The peer layers communicate by means of formatted blocks of data that obey a set of rules known as protocol.
- **Key Elements of a Protocol**

✓ Syntax – Creates a data block format understood by all
✓ Semantics – Control information for coordinating and error handling
✓ Timing – Synchronizes timing for functions such as speed matching and sequencing

- Task of communication broken up into modules

• For example file transfer could use three modules

– File transfer application

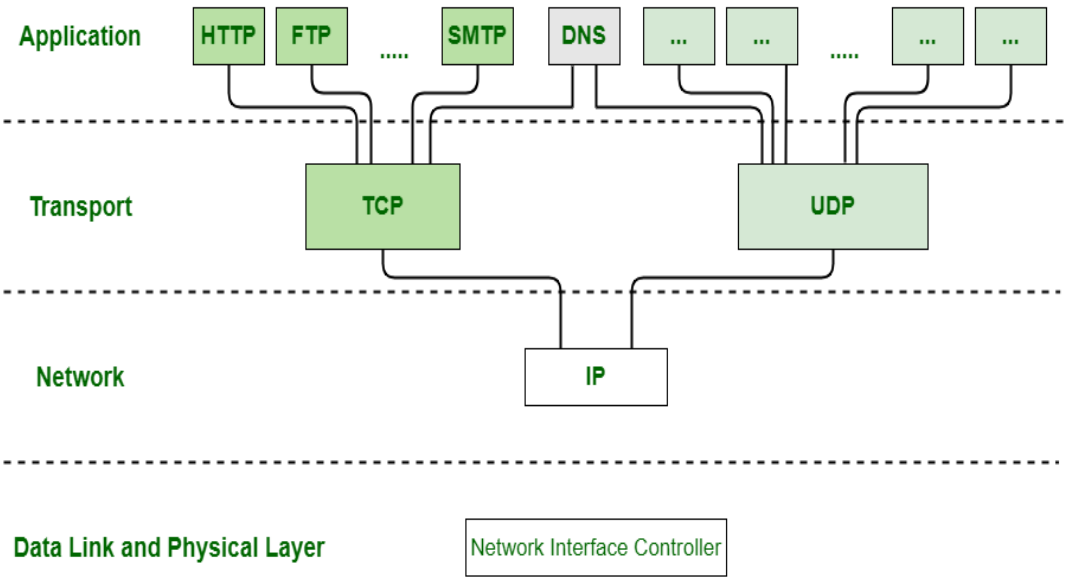
– Communication service module

– Network access module

TCP/IP Protocol Architecture Model

- The OSI model describes an idealized network communications with a family of protocols.
- TCP/IP does not correspond to this model directly.
- TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all.
- The table lists the layers from the topmost layer (application) to the lowest (physical network).

OSI Ref. Layer No.	OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
5,6,7	Application, session, presentation	Application	NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others
4	Transport	Transport	TCP, UDP
3	Network	Internet	IP, ARP, ICMP
2	Data link	Data link	PPP, IEEE 802.2
1	Physical	Physical network	Ethernet (IEEE 802.3) Token Ring, RS-232, others



Protocol Hierarchy, modified according to (BADACH et al. 2003)

The OSI Reference Model:

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983).

It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.

2. Each layer should perform a well-defined function.

3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

OSI Model Layer 1: The Physical Layer

1. Physical Layer is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

OSI Model Layer 2: Data Link Layer

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

OSI Model Layer 3: The Network Layer

1. Network Layer routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

OSI Model Layer 4: Transport Layer

1. Transport Layer decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer

3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

OSI Model Layer 5: The Session Layer

1. Session Layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

OSI Model Layer 6: The Presentation Layer

1. Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

OSI Model Layer 7: Application Layer

1. Application Layer is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model

OSI model distinguishes well between the services, interfaces and protocols.

Protocols of OSI model are very well hidden.

Protocols can be replaced by new protocols as technology changes.

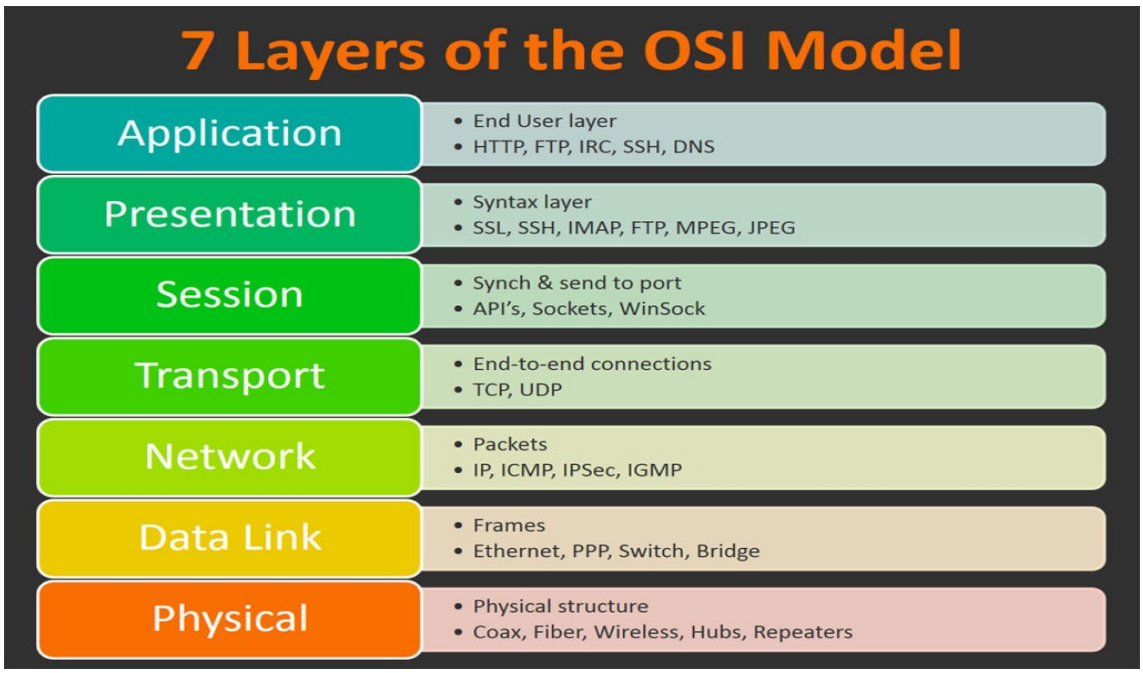
Supports connection oriented services as well as connectionless service.

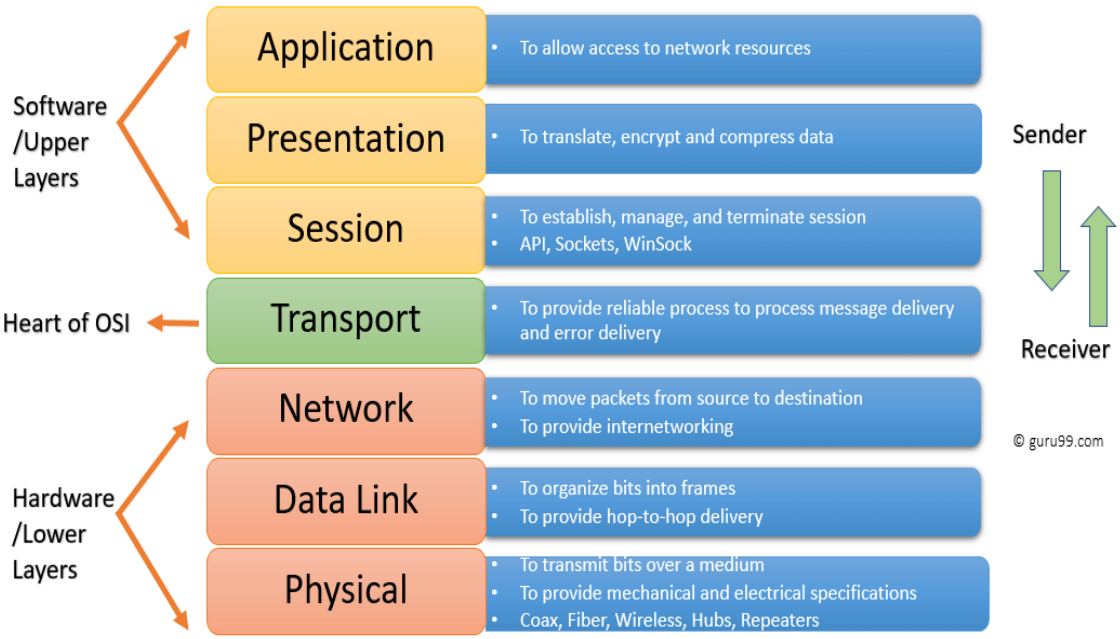
Demerits of OSI reference model

Model was devised before the invention of protocols.

Fitting of protocols is tedious task.

It is just used as a reference model.



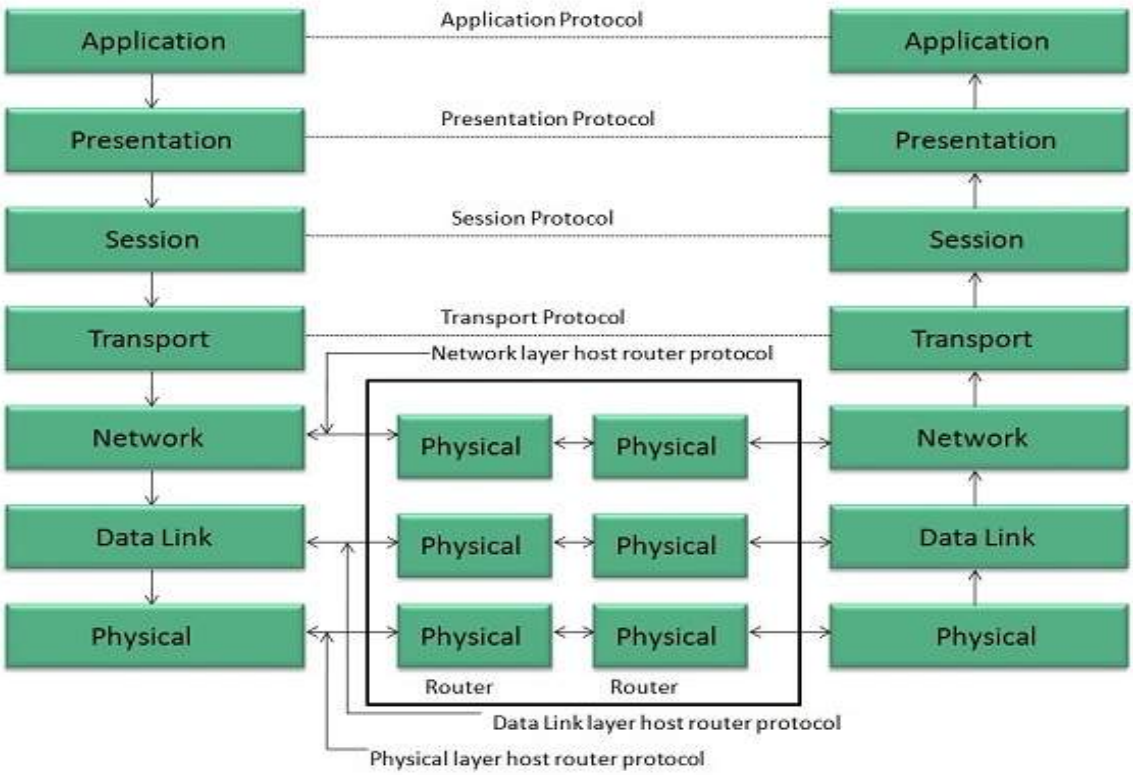


(or)

OSI Model

OSI is acronym of **Open System Interface**. This model is developed by the **International organization of Standardization (ISO)** and therefore also referred as **ISO-OSI** Model.

The OSI model consists of seven layers as shown in the following diagram. Each layer has a specific function, however each layer provide services to the layer above.



Physical Layer

The Physical layer is responsible for the following activities:

- Activating, maintaining and deactivating the physical connection.
- Defining voltages and data rates needed for transmission.
- Converting digital bits into electrical signal.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer

The data link layer performs the following functions:

- Performs synchronization and error control for the information which is to be transmitted over the physical link.
- Enables error detection, and adds error detection bits to the data which are to be transmitted.

Network Layer

Following are the functions of Network Layer:

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Transport Layer

The Transport layer performs the following functions:

- It decides if the data transmission should take place on parallel paths or single path.
- It performs multiplexing, splitting on the data.
- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

The Transport Layer guarantees transmission of data from one end to other end.

Session Layer

The Session layer performs the following functions:

- Manages the messages and synchronizes conversations between two different applications.
- It controls logging on and off, user identification, billing and session management.

Presentation Layer

The Presentation layer performs the following functions:

- This layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

Application Layer

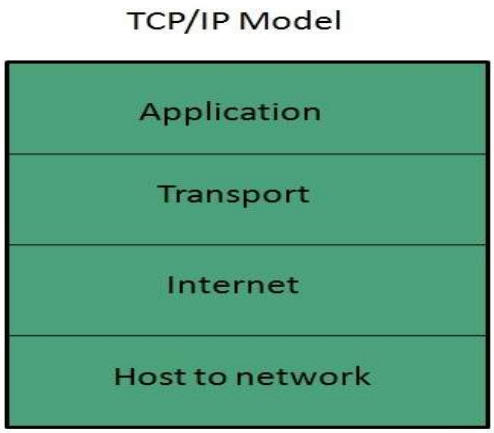
The Application layer performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

TCP/IP Model

TCP/IP model is practical model and is used in the Internet. TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.

The **TCP/IP** model combines the two layers (Physical and Data link layer) into one layer i.e. **Host-to-Network** layer. The following diagram shows the various layers of TCP/IP model:



Application Layer

This layer is same as that of the OSI model and performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.
- The functions such as LOGIN or password checking are also performed by the application layer.

Protocols used: TELNET, FTP, SMTP, DN, HTTP, NNTP are the protocols employed in this layer.

Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

- It uses **TCP** and **UDP** protocol for end to end transmission.
- TCP is reliable and **connection oriented protocol.**
- TCP also handles flow control.
- The UDP is not reliable and a **connection less protocol** also does not perform flow control.

Protocols used: TCP/IP and **UDP** protocols are employed in this layer.

Internet Layer

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent.

Protocols used: Internet Protocol (IP) is employed in Internet layer.

Host-to-Network Layer

This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

Protocols used: ARPANET, SATNET, LAN, packet radio are the protocols which are used in this layer.

TCP/IP VS OSI

- TCP/IP and OSI are reference models which divides the various responsibilities into a logical separation of layers. Practical implementations in devices are based on these 2 popular models. The difference amongst them lies in the no. of layers and their respective responsibilities:
-

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

-

Brief description of each model:

OSI Model It stands for Open Systems Interconnection. It comprises of 7 layers with the following responsibilites (starting from the lowest layer):

- Physical Layer: It is responsible for actual physical transmission of data (through channels). It recieves/transmits signals and then converts it to physical bits (0 & 1). It handles bit-synchronization (using clock), bit-rate control (no.of bits/sec), physical topology and transmission mode (simplex, half-duplex, full-duplex).
- Data-link Layer: It is responsible for Node-to-Node delivery of packets, Framing, Error control, Flow control, Physical Addressing (MAC). Upon recieving packets from network layer, it encapsulates it within a frame with the hardware (MAC) address of the reciever (obtained via ARP ~ Address Resolution Protocol).
- Network Layer: It is responsible for Logical Addressing (IPv4/v6) and Routing. Various routing algorithms are implemented at this layer, which determines the IP for the next hop in routing.
- Transport Layer: It is responsible for End-to-end delivery of packets. It also does Segmentation & Reassembly of packets(done if packet-size exceeds MTU ~ Max. Transmission Unit). It also does multiplexing/de-multiplexing of packets according to the application (using port no.). TCP/UDP (Connection vs. Connection-less) protocol is implemented at this layer.

- Session Layer: It is responsible for Session Management (Establishment, Maintenance, Termination), Authentication, Security, Synchronization & Restoration (check-points are established, such that upon re-connection state is resumed from the last saved point) and Dialog Control (synchronization when multiple parties are interacting ~ conference).
- Presentation Layer: It is responsible for Translation (e.g. ASCII to EBCDIC), Encryption/Decryption and Compression.
- Application Layer: Implements application-specific protocols (HTTP, HTTPS, FTP, SMTP etc.) They produce the data, interacts with the user (input and display of data). e.g. Browsers, Skype, Messaging Apps.
- TCP/IP Model It comprises of 4 layers with the following responsibilities (starting from the lowest layer):

- Network Access Layer: It is a combination of the Physical and Data-Link Layer, and is responsible for data transmission and hardware addressing (MAC).
- Internet Layer: It is the counterpart of OSI's Network layer, and is responsible for routing and logical addressing. (IP, ICMP, ARP).
- Transport Layer: Maintains End-to-end connectivity. It is a counterpart of the OSI's transport layer, and has the same responsibilites (TCP vs. UDP).
- Application Layer: Application-specific protocols are implemented here. (HTTP, HTTPS, FTP, SMTP etc.)
- The differences amongst these two is tabulated as:

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.

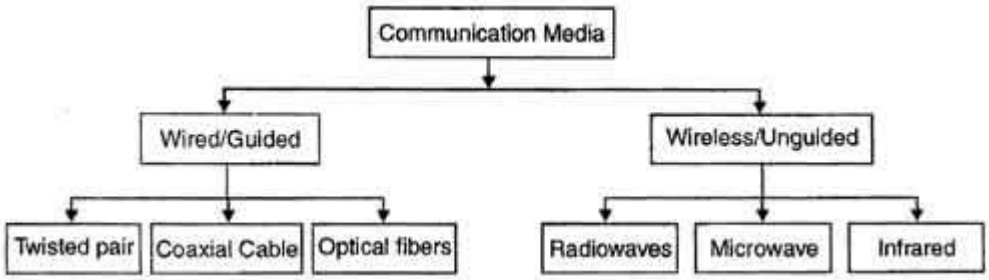
Transimission Medias

Wired or Guided Media or Bound Transmission Media : Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Popular bound transmission media 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.



Twisted Pair Cable

- This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :
- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.
- A twisted pair consists of two conductors(normally copper), each with its own plastic insulation, twisted together.
- One of these wires is used to carry signals to the receiver, and the other is used only as ground reference.
- The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference(noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources.
- This results in a difference at the receiver.

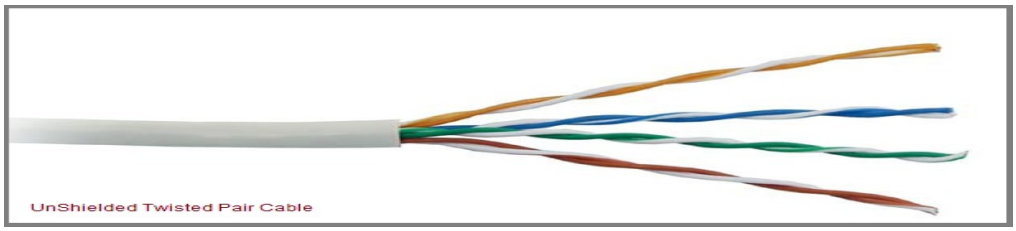
Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

- It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.
- UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector

and 4 pair cable use RJ-45 connector.



Advantages

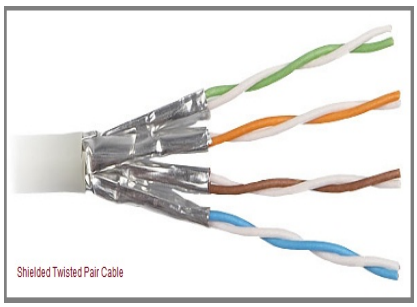
- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.
- It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

- This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).
- It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Advantages

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate

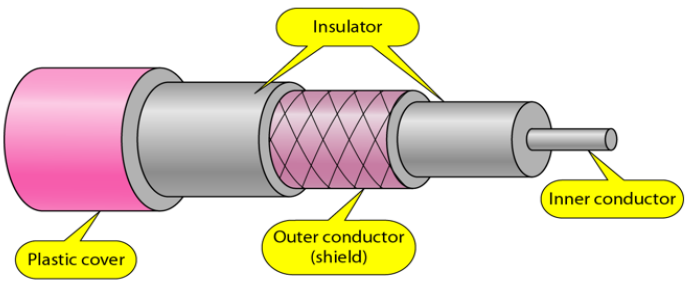
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages

- Difficult to manufacture
- Heavy

Coaxial Cable

- Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one.
- It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit.
- The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.
- Here the most common coaxial standards.
- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



Fiber optics:

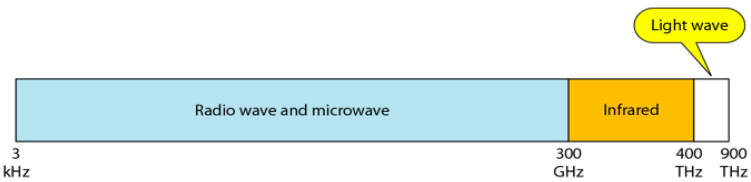
- fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long distance, high-performance data networking, and telecommunications.
- Compared to wired cables, fiber optic cables provide higher bandwidth and can transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.
- Fiber optic cables carry communication signals using pulses of light generated by small lasers or light-emitting diodes.
- How Fiber Optic Cables Work
- A fiber optic cable consists of one or more strands of glass, each only slightly thicker than a human hair. The center of each strand is called the core, which provides the pathway for

light to travel. The core is surrounded by a layer of glass called cladding that reflects light inward to avoid loss of signal and allow the light to pass through bends in the cable.

- The two primary types of optical fiber cables are single mode and multi-mode. Single-mode fiber uses extremely thin glass strands and a laser to generate light, while multi-mode optical fiber cables use LEDs.
- Advantages of Fiber Optic Cables
- Fiber cables offer several advantages over long-distance copper cabling.
- Fiber optics support a higher capacity. The amount of network bandwidth a fiber cable can carry easily exceeds that of a copper cable with similar thickness. Fiber cables rated at 10 Gbps, 40 Gbps, and 100 Gbps are standard.
- Because light can travel for much longer distances over a fiber cable without losing its strength, the need for signal boosters is lessened.
- A fiber optic cable is less susceptible to interference. A copper network cable requires shielding to protect it from electromagnetic interference. While this shielding helps, it is not sufficient to prevent interference when many cables are strung together in proximity to one another. The physical properties of fiber optic cables avoid most of these problems.

UnBounded/UnGuided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



Unguided signals can travel from the source to the destination in several ways: **Gound propagation**, **Sky propagation** and **Line-of-sight propagation** as shown in below figure.
Propagation Modes

- **Ground Propagation:** In this, radio waves travel through the lowest portion of the atmosphere, hugging the Earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
- **Sky Propagation:** In this, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to Earth. This type of transmission allows for greater distances with lower output power.
- **Line-of-sight Propagation:** in this type, very high-frequency signals are transmitted in straight lines

directly from antenna to antenna.

We can divide wireless transmission into three broad groups:

1. Radio waves
2. Micro waves
3. Infrared waves

Radio Waves

- Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.
- Radio waves are omnidirectional.
- When an antenna transmits radio waves, they are propagated in all directions.
- This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna send waves that can be received by any receiving antenna.
- The omnidirectional property has disadvantage, too.
- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signal suing the same frequency or band.
- Radio waves, particularly with those of low and medium frequencies, can penetrate walls.
- This characteristic can be both an advantage and a disadvantage. It is an advantage because, an AM radio can receive signals inside a building.
- It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Applications

- The omnidirectional characteristics of radio waves make them useful for multicasting in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Micro Waves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. Micro waves are unidirectional.
- When an antenna transmits microwaves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- The unidirectional property has an obvious advantage.
- A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Advantages of Microwave Transmission

- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another, a short-range communication system in on room cannot be affected by another system in the next room.

Transmission impairment

Transmission impairment occurs when the received signal is different from the transmitted signal. As we know, a signal can be transmitted as Analog signal or it can be transmitted as a digital signal. In Analog signals due to transmission impairment the resulting received signal gets different amplitude or the shape. In the case of digitally transmitted signals at the receiver side we get changes in bits (0's or 1's).

Causes

There are various causes of transmission impairments −

Noise

Distortion

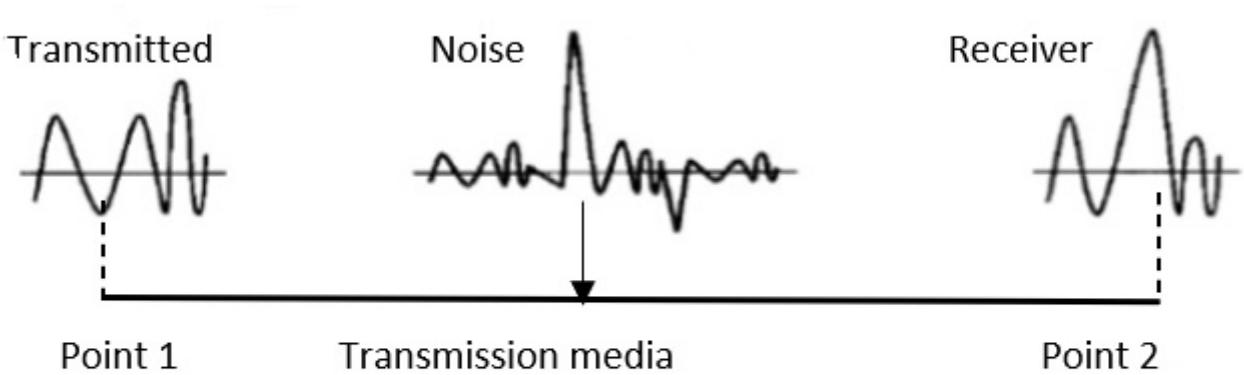
Attenuation

Let us understand them one by one.

Noise

Noise is the major factor for the transmission distortion as any unwanted signal gets added to the transmitted signal by which the resulting transmitted signal gets modified and at the receiver side it is difficult to remove the unwanted noise signal. These noises are various kinds like shot noise, impulse noise, thermal noise etc.

Noise is diagrammatically represented as follows −

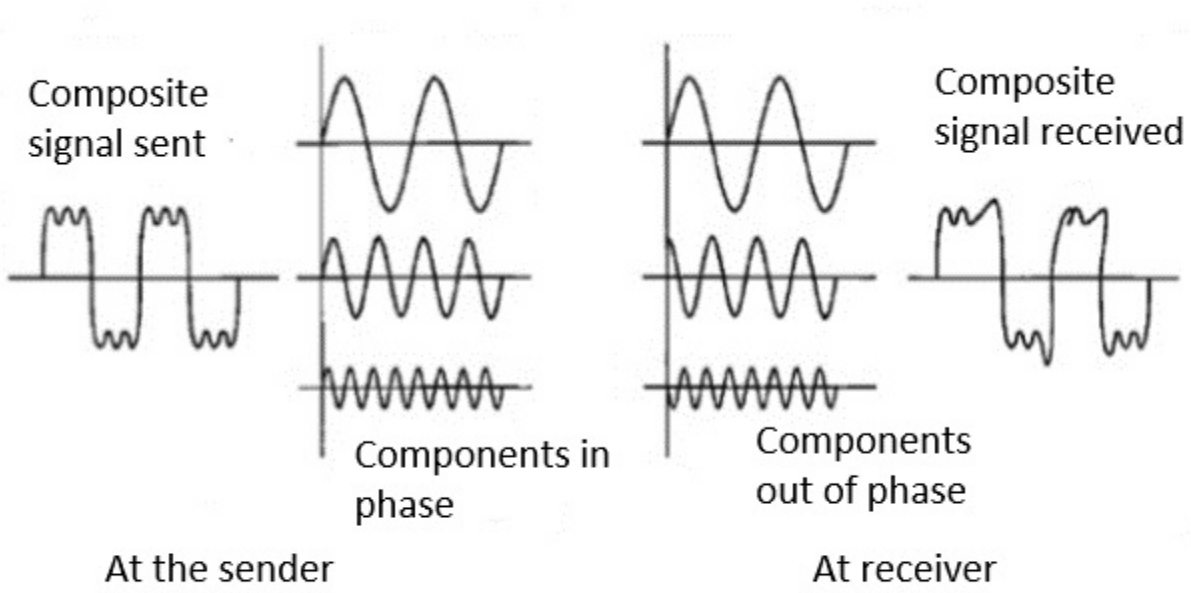


Distortion

This kind of distortion is mainly appearing in case of composite signals in which a composite signal has various frequency components in it and each frequency component has some time constraint which makes a complete signal.

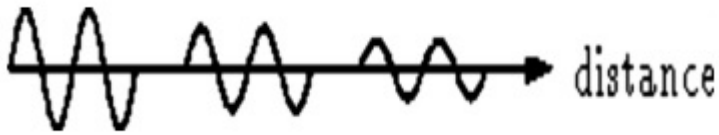
But while transmitting this composite signal, if a certain delay happens between the frequencies components, then there may be the chance that the frequency component will reach the receiver end with a different delay constraint from its original which leads to the change in shape of the signal. The delay happens due to environmental parameters or from the distance between transmitter and receiver etc.

Distortion is diagrammatically represented as follows −



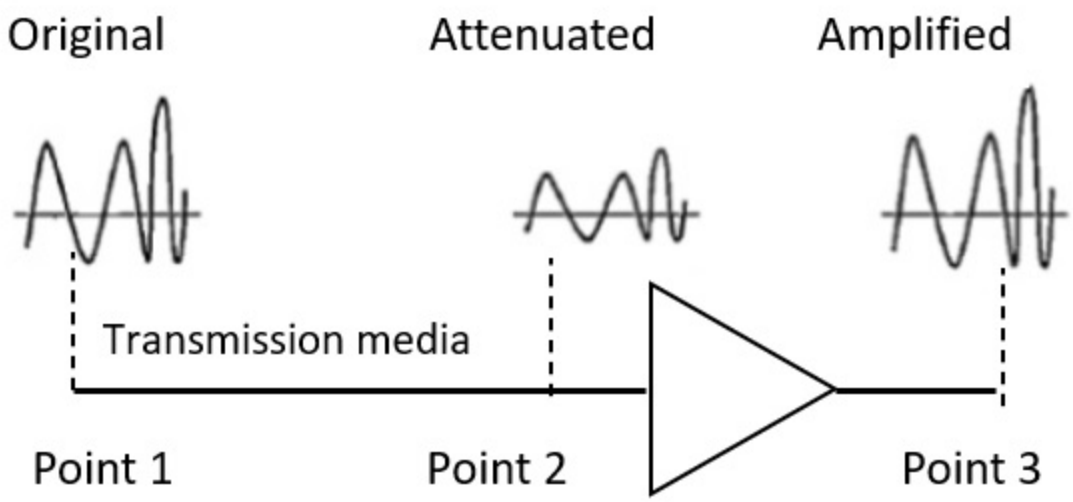
Attenuation

Attenuation is generally decreased in signal strength, by which the received signal will be difficult to receive at the receiver end. This attenuation happens due to the majority factor by environment as environment imposes a lot of resistance and the signal strength decreases as it tries to overcome the resistance imposed.



The above picture shows that the signal loses power at its travels time.

Attenuation is diagrammatically represented as follows −


Original
Attenuated
Amplified
Transmission media
Point 1
Point 2
Point 3