UNIT-I Computer Networks & Internet

Computer Network

- A computer network is a system in which multiple computers are connected to each other to share information and resources.
- The physical connection between networked computing devices is established using either cable media or wireless media.
- The best-known computer network is the Internet.

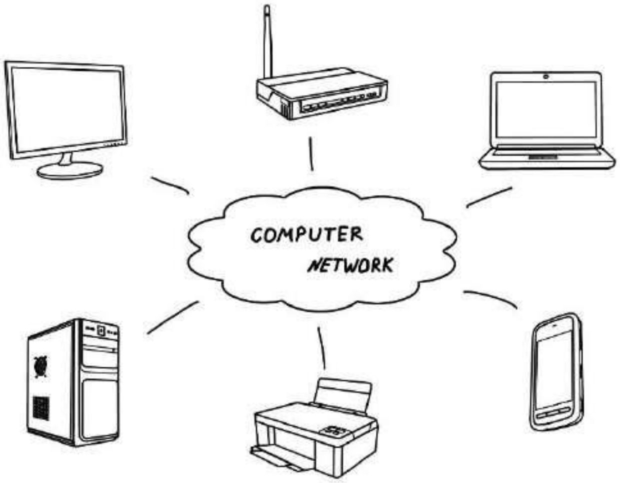


Figure 1: Computer Network

Advantages of Computer Networks

- **File sharing**
  The major advantage of a computer network is that allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so.
- **Resource sharing**
  All computers in the network can share resources such as printers, fax machines, modems, and scanners.
- **Better connectivity and communications**
  It allows users to connect and communicate with each other easily. Various communication applications included e-mail and groupware are used. Through e-mail, members of a network can send a message and ensure safe delivery of data to other members, even in their absence.
- **Internet access**
  Computer networks provide internet service over the entire network. Every single computer attached to the network can experience the high-speed internet.
- **Entertainment**
  Many games and other means of entertainment are easily available on the internet. Furthermore, Local Area Networks (LANs) offers and facilitates other ways of enjoyments, such as many players are connected through LAN and play a particular game with each other from a remote location.

- **Inexpensive system**
  Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means a reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.
- **Flexible access**
  A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine.
- **Instant and multiple access**
  Computer networks are multiple processes. Many users can access the same information at the same time. Immediate commands such as printing commands can be made with the help of computer networks.

Disadvantages of Computer Networks

- **Lack of data security and privacy**
  Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.
- **Presence of computer viruses and malware**
  If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply.
- **Lack of Independence**
  Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.
- **Lack of Robustness**
  As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill.
- **Need an efficient handler**
  For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

Use (Applications) of Computer Networks

- **Financial services**
  Nowadays, almost all the financial services depend on the computer network. You can access the financial services across the world. For example, a user can transfer money from one place to another by using the electronic fund transfer feature. You can use networking in various financial areas such as ATM, foreign exchange and credit history search.
- **Business**

Nowadays, most of the works of businesses are done over the computers. To exchange the data and ideas, you need effective data and resources sharing features. To do this, you need to connect the computer with each other through a network. For example, a person of one department of an organization can share or access the electronic data of other departments through a network.

- **Email services**
  A computer network provides you the facility to send or receive emails across the globe in few seconds.
- **Mobile applications**
  By using mobile applications, such as cellular or wireless phones, you can communicate (exchange your views and ideas) with one other.
- **Directory services**
  It provides you the facility to store files on a centralized location to increase the speed of search operation worldwide.
- **Teleconferencing**
  It contains voice conferencing and video conferencing which are based on networking. In teleconferencing, the participants need not be presented at the same location.

Types of Computer Networks

LAN (Local Area Network)

- It is privately-owned networks within a single building or campus of up to a few kilometers in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are easy to design and troubleshoot
- In LAN, all the machines are connected to a single cable.
- Different types of topologies such as Bus, Ring, Star, and Tree are used.
- The data transfer rates for LAN is up to 10 Gbits/s.
- They transfer data at high speeds. The high transmission rate is possible in LAN because of the short distance between various computer networks.
- They exist in a limited geographical area.
- **Advantages**
  - ➢ LAN transfers data at high speed.
  - ➢ LAN technology is generally less expensive.

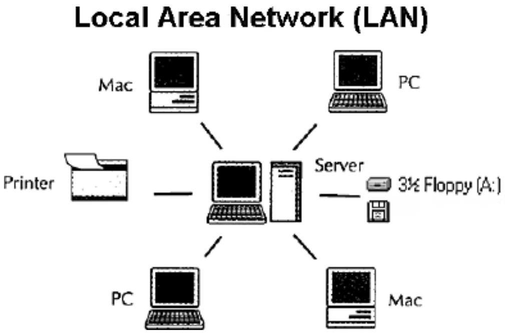


Figure 2: Local Area Network

MAN (Metropolitan Area Network)

- MAN is a larger version of LAN which covers an area that is larger than the covered by LAN but smaller than the area covered by WAN.
- A metropolitan area network or MAN covers a city. The best-known example of a MAN is the cable television network available in many cities.
- MAN connects two or more LANs.
- At first, the companies began jumping into the business, getting contracts from city governments to wire up an entire city.
- The next step was television programming and even entire channels designed for cable only.

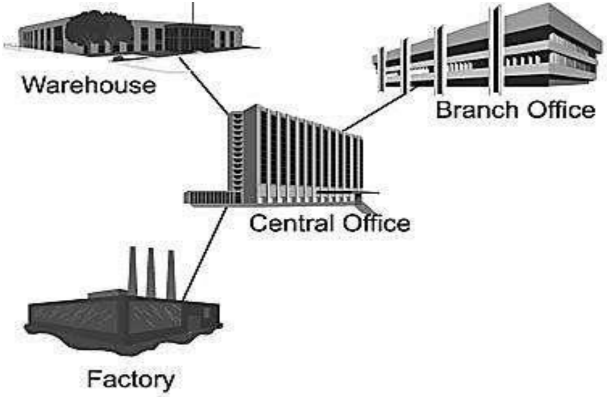


Figure 3: Metropolitan Area Network

WAN (Wide Area Network)

- WAN spans a large geographical area, often a country or region.
- WAN links different metropolitan's countries and national boundaries thereby enabling easy communication.
- It may be located entirely within a state or a country or it may be interconnected around the world.
- It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
- The communication between different users of WAN is established using leased telephone lines or satellite links and similar channels.

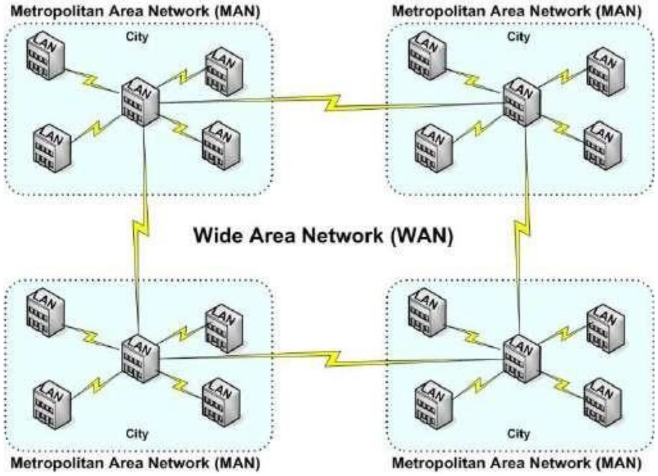

Metropolitan Area Network (MAN)
City
LAN
LAN
LAN
LAN
LAN
Metropolitan Area Network (MAN)
City
LAN
LAN
LAN
LAN
LAN
Wide Area Network (WAN)
LAN
LAN
LAN
LAN
LAN
City
Metropolitan Area Network (MAN)
LAN
LAN
LAN
LAN
LAN
City
Metropolitan Area Network (MAN)

Figure 4: Wide Area Network

UNIT-I Computer Networks & Internet

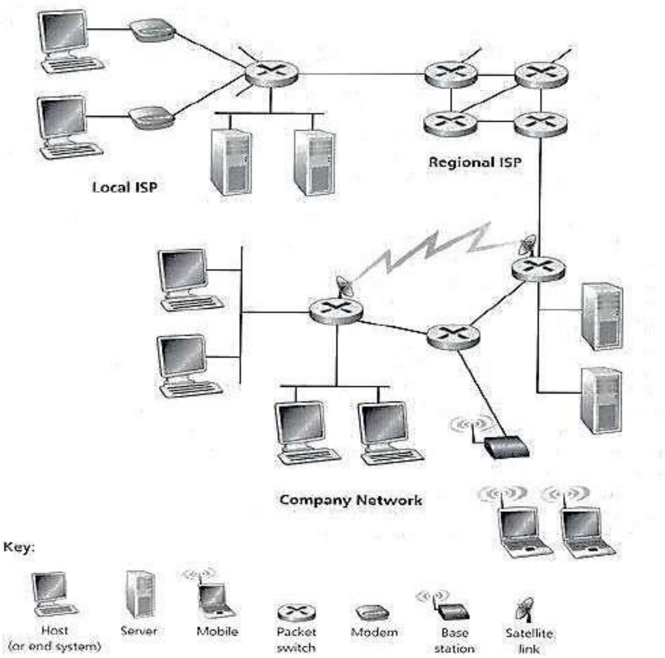
Difference between LAN, MAN, and WAN.

Parameter	LAN	MAN	WAN
Area covered	Covers a small area. i.e. within building	Covers larger than LAN & smaller than WAN	Covers large area
Error rates	Lowest	Moderate	Highest
Transmission speed	High speed	Moderate speed	Low speed
Equipment cost	Inexpensive	Moderate-expensive	Most expensive
Design & maintenance	Easy	Moderate	Difficult

Internet

- The internet is a type of world-wide computer network.
- The internet is the collection of infinite numbers of connected computers that are spread across the world.
- We can also say that the Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.
- It is established as the largest network and sometimes called a network of a network that consists of numerous academic, business and government networks, which together carry various information.
- The Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
- When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

Figure 5: Some pieces of the Internet



Protocol

- A protocol is a set of rules that govern (manages) data communications.
- Protocols define methods of communication, how to communicate when to communicate etc.
- A protocol is an agreement between the communicating parties on how communication is to proceed.
- Important elements of protocols are
  1. Syntax
  2. Semantics
  3. Timing
- **Syntax**:- Syntax means format of data or the structure how it is presented e.g. first eight bits are for sender address, next eight bits are for receiver address and rest of the bits for message data.
- **Semantics**:- Semantics is the meaning of each section of bits e.g. the address bit means the route of transmission or final destination of a message.
- **Timing**:- Timing means, at what time data can be sent and how fast data can be sent.
- Some protocols also support message acknowledgment and data compression designed for reliable and/or high-performance network communication.
- Example: HTTP, IP, FTP etc…

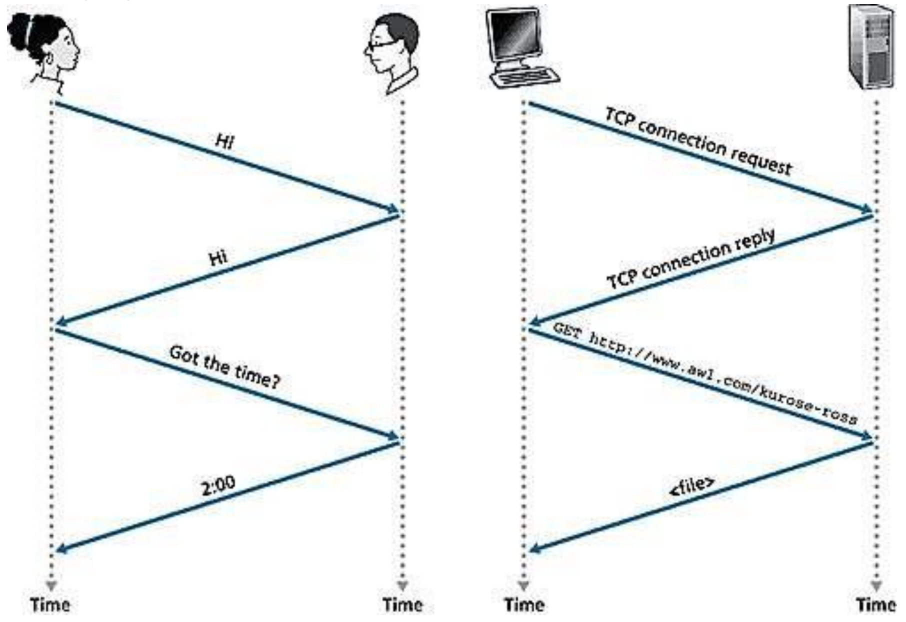


Figure 6: A human protocol and a computer network protocol

The Network Edge

- It defines those computers of the network used at the edge (end) of the network. These computers are known as hosts or end system.
- A host can be classified into the following two types:
  - **Clients**: Refer to the computer systems that request servers for the completion of a task. The clients are generally called desktop PCs or workstations.
  - **Servers**: Refer to the computer systems that receive requests from the clients and process them. After the processing is complete, the servers send a reply to the clients who sent the request.

- The concept of clients and servers is essential in the network design. The various networks design models are as follows:
  1. Peer to Peer network 2. Client-Server network

Peer to Peer network

- In this network group of computers is connected together so that users can share resources and information.
- There is no central location (server) for authenticating users, storing files, or accessing resources and each of them works as both client and server.
- This means that users must remember which computers in the workgroup have the shared resource or information that they want to access.
- **Advantage**:
  - ➢ It is easy to set up.
  - ➢ There is no need for any committed server as each peer acts as both server and client.
  - ➢ The network implementation is quite cheap.
  - ➢ The resources of a peer can be shared with other peers very easily in the network.
- **Disadvantage:**
  - ➢ The speed of the network decreases due to heavy usage.
  - ➢ It is not easy to keep track of information on each computer.
  - ➢ There is no central backup of files and folders.
  - ➢ Network and data security are weak.

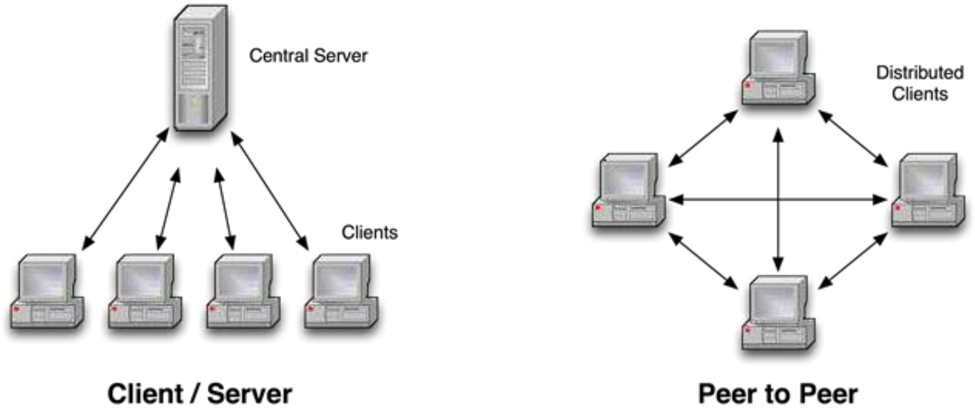


Figure 7: Network Edge - Client/Server Network and Peer to Peer

Client/Server network

- A client/server network is a system where one or more computers called clients to connect to a central computer named as a server to share or use resources.
  - The client requests a service from a server, which may include running an application, querying a database, printing a document, performing a backup or recovery procedure. The request made by the client is handled by a server.
  - A client/server network is that in which the files and resources are centralized. This means that the server can hold them and other computers (Client) can access them.

  - **Advantage**:
    - ➢ The server system holds the shared files.
    - ➢ The server system can be scheduled to take the file backups automatically.

- ➢ Network access is provided only to authorized users through user security at the server.
- ➢ The server system is a kind of central repository for sharing a printer with clients.
- ➢ Internet access, e-mail routing, and such other networking tasks are quite easily managed by the server.
- ➢ The software applications shared by the server are accessible to the clients.

- **Disadvantage:**
  - ➢ The implementation of the network is quite expensive.
  - ➢ An NOS (Network Operating System) is essential.
  - ➢ If a server fails, the entire network crashes.
  - ➢ There may be congestion if more than one client requests for a service at the same time.

Techniques used in data communications to transfer data

1. Connection-oriented method
2. Connectionless method

Connection-oriented method

- Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call.
- However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network.
- Connection-oriented communication is done in one of two ways over a packet switched network:
  1. Without virtual circuits
  2. With virtual circuits.

Without virtual circuits:

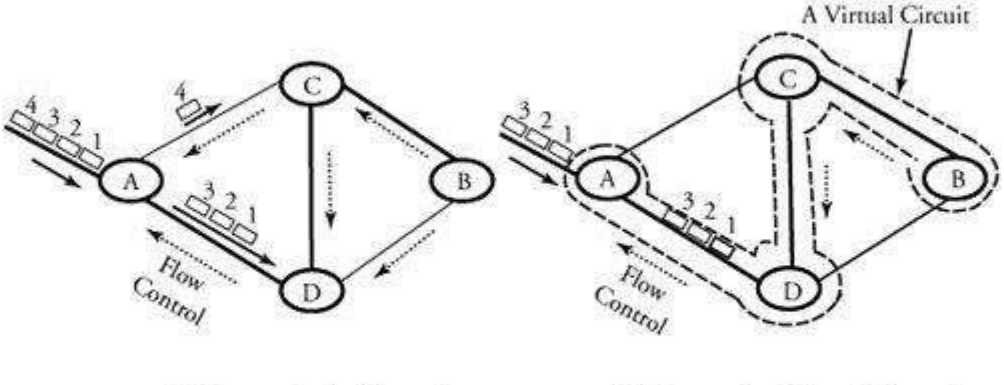
- This is what TCP does on the Internet.
- The only two machines on the Internet are aware of the connection which is established between the two computers at the endpoints.
- The Internet itself, its routers and links have no information about the presence of a connection between the two computers.
- This means that all of the packets flowing between the two computers can follow different routes.
- One benefit of establishing the connection is that the flow of packets from the source to the destination can be slowed down if the Internet is congested and speeded up when congestion disappears.
- Another benefit is that the endpoints can anticipate traffic between them, and agree to cooperate to ensure the integrity and continuity of the data transfers. This allows the network to be treated as a "stream" of data.

With virtual circuit:

- This is not used on the Internet, but is used in other types of networks (eg. the "X.25" protocol, still popular in Europe).
- The routers within the network route all packets in one connection over the same route. The advantage is that video and voice traffic is easier to carry because routers can reserve memory space to buffer the transmission.

Connectionless method

- Connectionless communication is just packet switching where no call establishment and release occur.
- A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel a different route to the destination since there is no connection.
- Connectionless service is typically provided by the UDP (User Datagram Protocol). The packets transferred using UDP are also called datagrams.



(a) Connectionless Network (b) Connection-Oriented Network

Feature	Connectionless	Connection-oriented
How is data sent?	One packet at a time	Continuous stream of packets
Do packets follow the same route?	No	Virtual circuit: yes Without virtual circuit: no
Are resources reserved in the network?	No	Virtual circuit: yes Without virtual circuit: no
Are resources reserved in communicating hosts?	No	Yes
Is connection establishment done?	No	Yes
Is state information stored at network nodes?	No	Virtual circuit: yes Without virtual circuit: no
What is the impact of node/switch crash?	Only packets at a node are lost	All virtual circuits through node fail
What addressing information is needed on each packet?	Full source and destination address	Virtual circuit: virtual circuit number Without virtual circuit: full source and destination address

Transmission Media

- A transmission media can be defined as anything that can carry information from a source to a destination.
- On the basis of transmission of data, the transmission media can be classified into two categories:
    1. Guided (Physical) transmission media
    2. Unguided (Wireless) transmission media

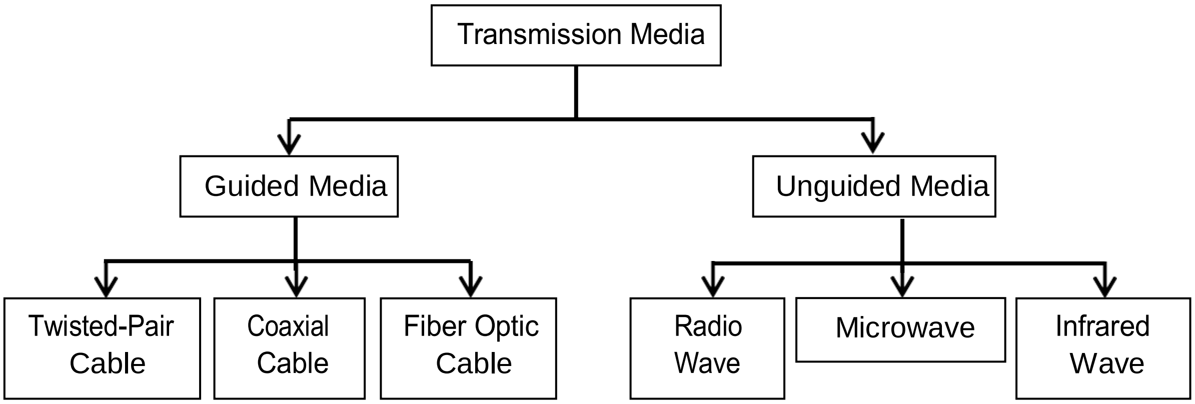


Figure 8: Classification Transmission Media

Guided Transmission Media

- Guided media are those that provide a channel from one device to another.
- The three Guided (Physical) media commonly used for data transmission are:

1. Twisted-Pair 2. Coaxial 3. Fiber Optics

1. Twisted Pair

- A twisted pair consists of two insulated copper wires, typically about 1 mm thick.
- The wires are twisted together in a helical form, just like a DNA molecule.
- Twisting is done because two parallel wires constitute a fine antenna.
- When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively.

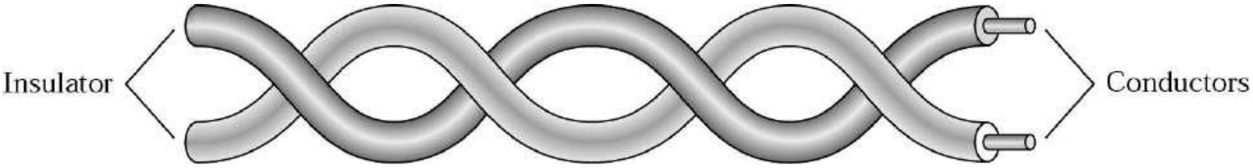


Figure 9: Twisted Pair Cable

Why cable is twisted?

- 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 relatives to the noise or crosstalk sources.
- This results in a difference at the receiver.
- By twisting the pair, a balance is maintained.

Types of Twisted-Pair Cable

1) **Unshielded twisted-pair (UTP)**

- Twisted pair cabling comes in several varieties, two of which are important for computer networks.
- **Category 3** twisted pairs consist of two insulated wires gently twisted together.
- Most office buildings had one category 3 cable running from a central wiring closet on each floor into each office.
- **Category 5** is the more advanced twisted pairs were introduced.
- They are similar to category 3 pairs, but with more twists per centimeter, which results in less crosstalk and a better-quality signal over longer distances, making them more suitable for high-speed computer communication.
- Up-and-coming categories are 6 and 7, which are capable of handling signals with bandwidths of 250 MHz and 600 MHz, respectively (versus a mere 16 MHz and 100 MHz for categories 3 and 5 respectively).

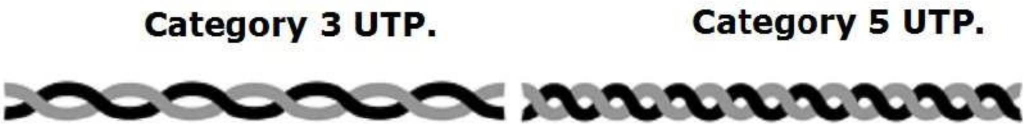


Figure 10: Unshielded twisted-pair

2) **Shielded twisted-pair (STP).**

- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.
- It is bulkier and more expensive.
- **Applications:**
  - Used in telephone lines to provide voice and data channels.
  - The DSL lines use by telephone companies use the high-bandwidth capability of UTP cables.
  - LANs, such as 10Base-T, 100Base-T also uses twisted-pair cables.

2. **Coaxial Cable**

- It has better shielding than twisted pairs, so it can span longer distances at higher speeds.
- Two kinds of the coaxial cable are widely used. One kind is a 50-ohm cable which is commonly used when it is intended for digital transmission from the start.
- The other kind is a 75-ohm cable which is commonly used for analog transmission and cable television but is becoming more important with the advent of the Internet over cable.
- A coaxial cable consists of stiff copper wire as the core surrounded by an insulating material.
- The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh.
- The outer conductor is covered in a protective plastic sheath.
- The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.
- The bandwidth possible depends on the cable quality, length, and signal-to-noise ratio of the data signal. Modern cables have a bandwidth of close to 1 GHz.

- Coaxial cables used is widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on long-haul routes.

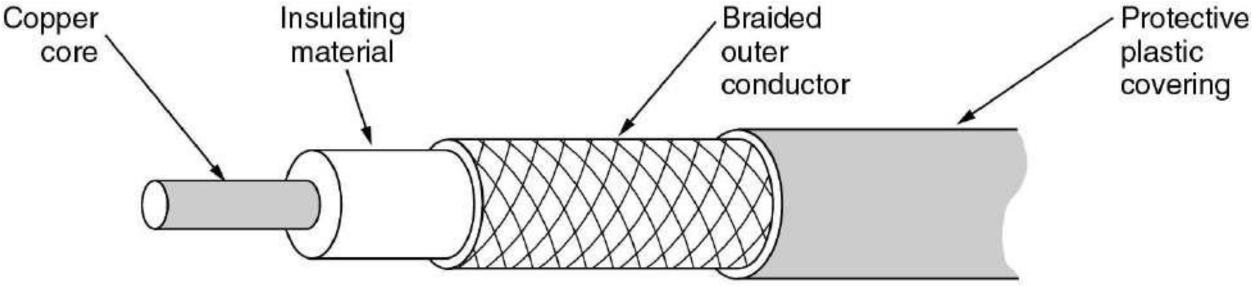


Figure 11: Coaxial Cable

3. Fiber Optics

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through a core is reflected off the cladding instead of being refracted into it.

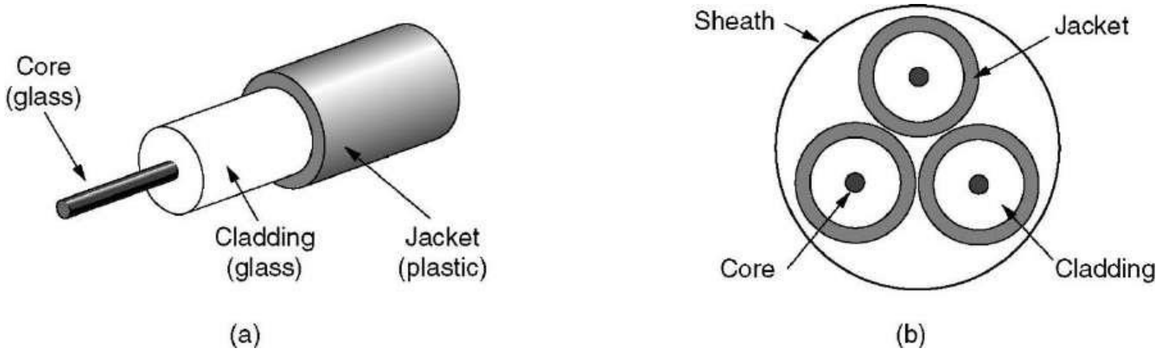


Figure 12: Fiber Optic Cable

- Fiber optic cables are similar to coax, except without the braid.
- The figure shows a single fiber viewed from the side. At the center is the glass core through which the light propagates.
- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.
- Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath. The figure shows a sheath with three fibers.

Unguided (Wireless) transmission media

- Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.
  1. Radio Transmission
  2. Microwave Transmission
  3. Infrared
  4. Lightwave Transmission

1. **Radio Transmission**
   - Radio waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
   - Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.
   - The properties of radio waves are frequency dependent.
   - At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source, roughly as $1/r^2$ in the air.
   - At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain.
   - At all frequencies, radio waves are subject to interference from motors and other electrical equipment.

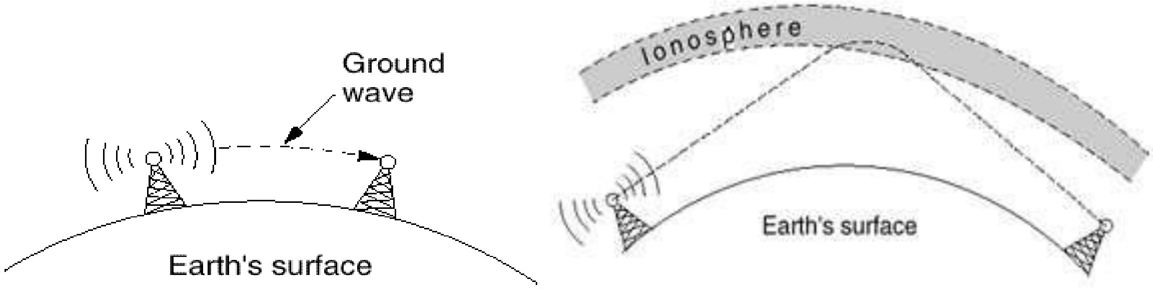


Figure 13: Ground wave

   - In the VLF, LF, and MF bands, radio waves follow the curvature of the earth.
   - In the HF they bounce off the ionosphere.
2. **Microwave Transmission**
   - Since the microwaves travel in a straight line, if the towers are too far apart, the earth will get in the way. Consequently, repeaters are needed periodically.
   - Unlike radio waves at lower frequencies, microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space.
   - Above 100 MHz, the waves **travel in straight lines** and can, therefore, be narrowly focused. Concentrating all the energy into a small beam using a **parabolic antenna** gives a much higher signal to noise ratio.
   - **Advantages:**
     - No right way is needed (compared to wired media).
     - Relatively inexpensive.
     - Simple to install.
   - **Disadvantages:**
     - Do not pass through buildings well.
     - Multipath fading problem (the delayed waves cancel the signal).
     - Absorption by rain above 8 GHz.
     - A severe shortage of spectrum.
3. **Infrared**
   - Unguided infrared and millimetre waves are widely used for short-range communication.
   - The remote controls used on televisions, VCRs, and stereos all use infrared communication.

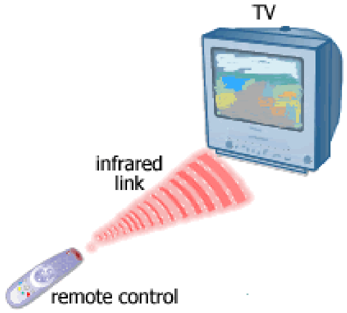


Figure 14: Infrared wave connection

- They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects (try standing between your remote control and your television and see if it still works).
- In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like a radio.
- On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus.
- It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.
- Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason.
- Therefore, no government license is needed to operate an infrared system, in contrast to radio systems, which must be licensed outside the ISM bands.

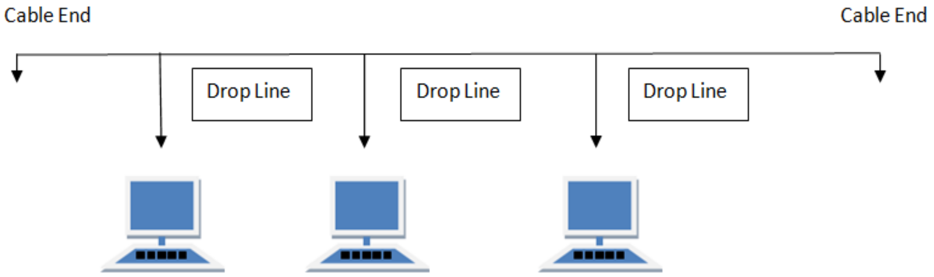
Topologies (Network Topologies)

- Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other.
- Types of network topologies :

1. Bus	3. Star	5. Tree
2. Ring	4. Mesh	6. Hybrid

Bus Topology

- Bus topology is a network type in which every computer and network device is connected to a single cable.



Features:

- It transmits data only in one direction.
- Every device is connected to a single cable.

Advantages:

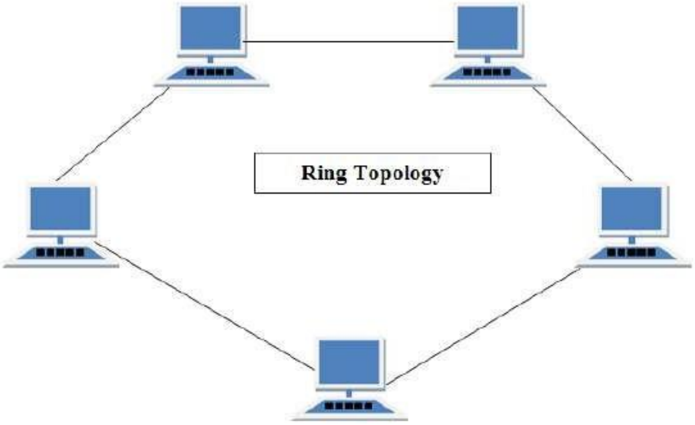
- It is cost effective (cheaper).
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages:

- Cables fail then the whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.

Ring Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.



Features:

- A number of repeaters are used and the transmission is unidirectional.
- A date is transferred in a sequential manner that is bitten by bit.

Advantages:

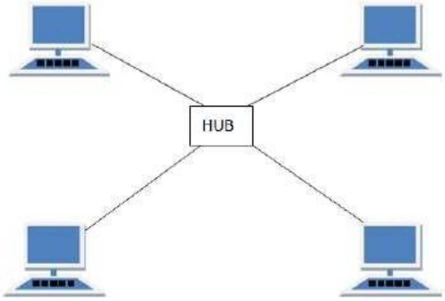
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Disadvantages:

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

Star Topology

- In this type of topology, all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features:

- Every node has its own dedicated connection to the hub.
- Acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages:

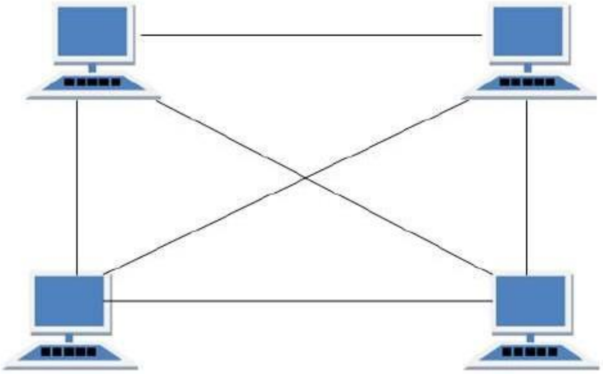
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to set up and modify.
- Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive to use.
- If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the.

Mesh Topology

- It is a point-to-point connection to other nodes or devices.
- Traffic is carried only between two devices or nodes to which it is connected.



Features:

- Fully connected.
- Robust.
- Not flexible.

Advantages:

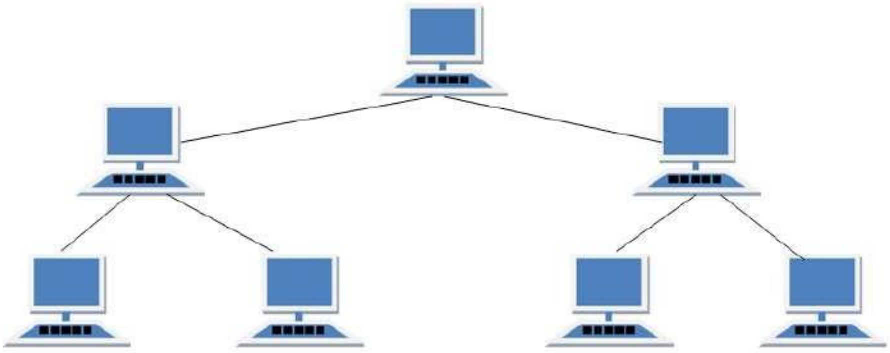
- Each connection can carry its own data load.
- It is robust.
- A fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration are difficult.
- Cabling cost is more.
- Bulk wiring is required.

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.



Features:

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages:

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

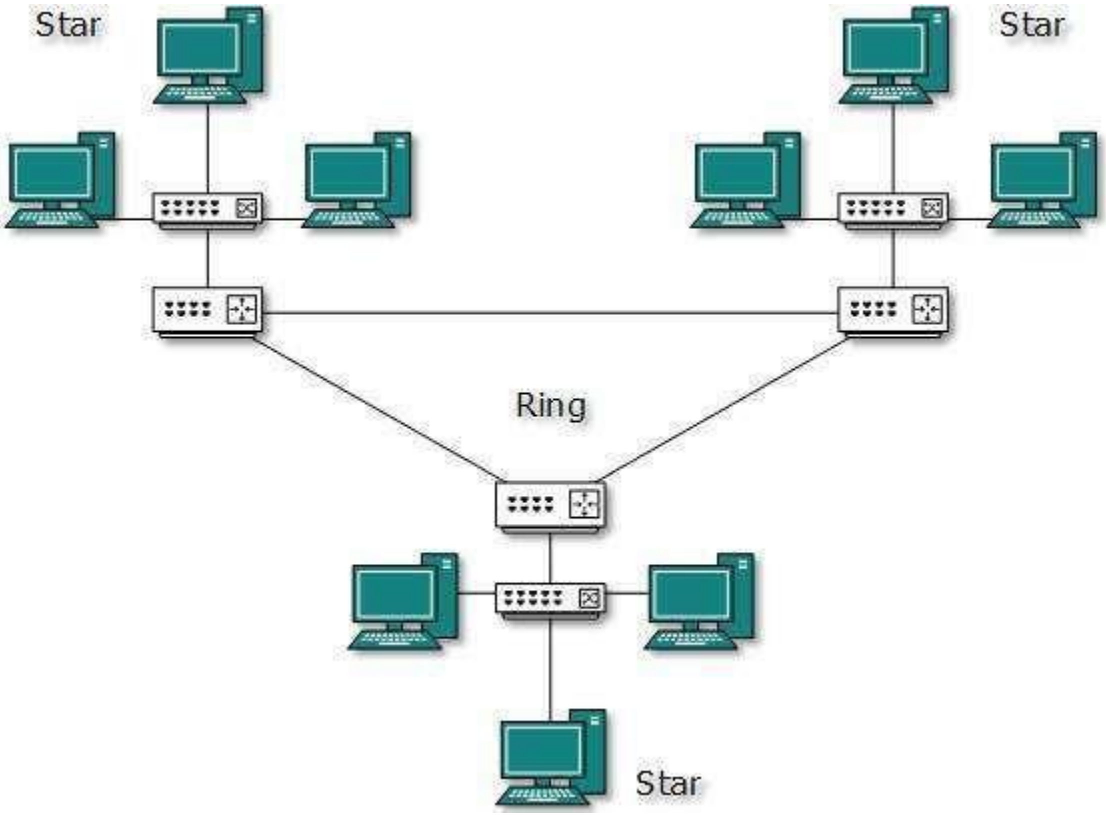
Disadvantages:

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails then network fails.

Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.

- For example, if in an office in one department ring topology is used and in another star, topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features:

- It is a combination of two or more topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages:

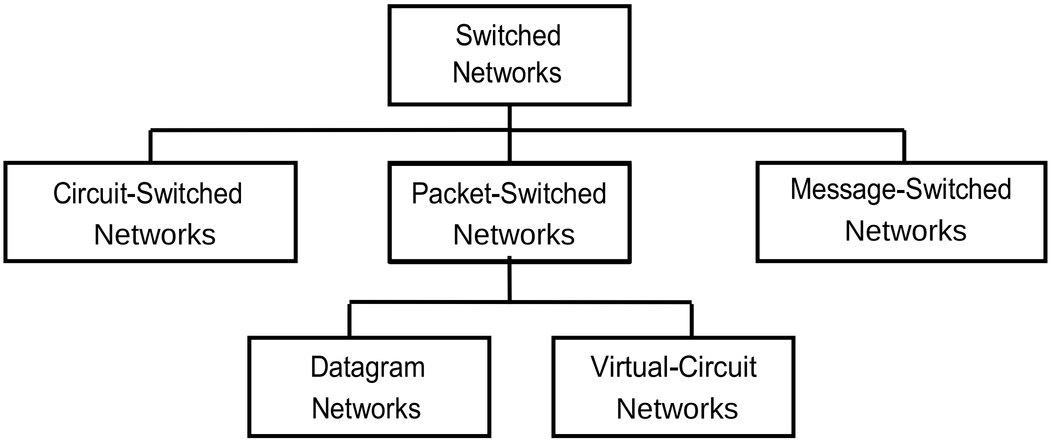
- Reliable as error detecting and troubleshooting is easy.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages:

- Complex in design.
- Costly.

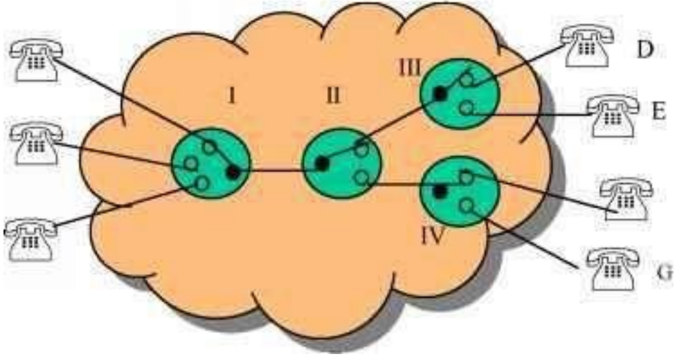
The Network Core

- Network core defines the connection of different network segments together and the process to transmit the data packets across the network.
- The network core is implemented through the use of switching techniques.
- The classification of a switching network is shown below:

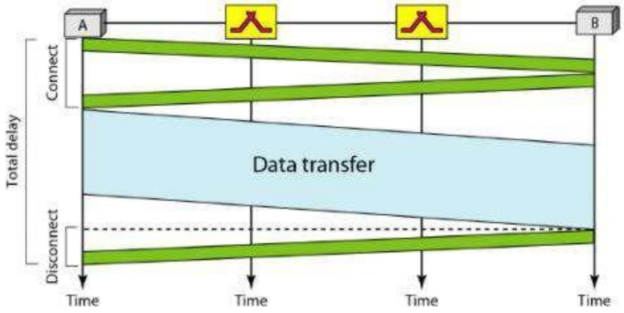


Circuit Switching

- Circuit switching is used in public telephone networks and is the basis for private networks built on leased-lines.
- Circuit switching was developed to handle voice traffic but also digital data (although inefficient)
- With circuit switching a dedicated path is established between two stations for communication.



- Switching and transmission resources within the network are reserved for the exclusive use of the circuit for the duration of the connection.
- The connection is transparent: once it is established, it appears to attach devices as if there were a direct connection.
- Communication via circuit switching involves three phases:
    1. Circuit Establishment
    2. Data Transfer
    3. Circuit Disconnect



- Connection path must be established before data transmission begins. Nodes must have switching capacity and channel capacity to establish a connection.
- Circuit switching is inefficient
    1. Channel capacity dedicated for a duration of a connection
    2. If no data, capacity wasted
- Set up (connection) takes time
- Once connected, a transfer is transparent to the users
    1. Data is transmitted at a fixed data rate with no delay (except for the propagation delay)
- Developed for voice traffic (phone)
    1. May also be used for data traffic via modem
- Interconnection of telephones within a building or office.
- In circuit switching, a direct physical connection between two devices is created by space-division switches, time-division switches, or both OR Circuit switching use any of below two technologies:

Space Division Switching

- In a space-division switch, the path from one device to another is spatially separate from other paths.
- Developed for the analogue environment.
- A crossbar is the most common space-division switch. It connects n inputs to m outputs via n × m cross points.
- Crossbar switch.

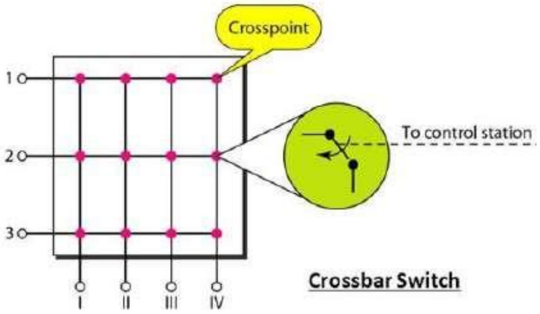
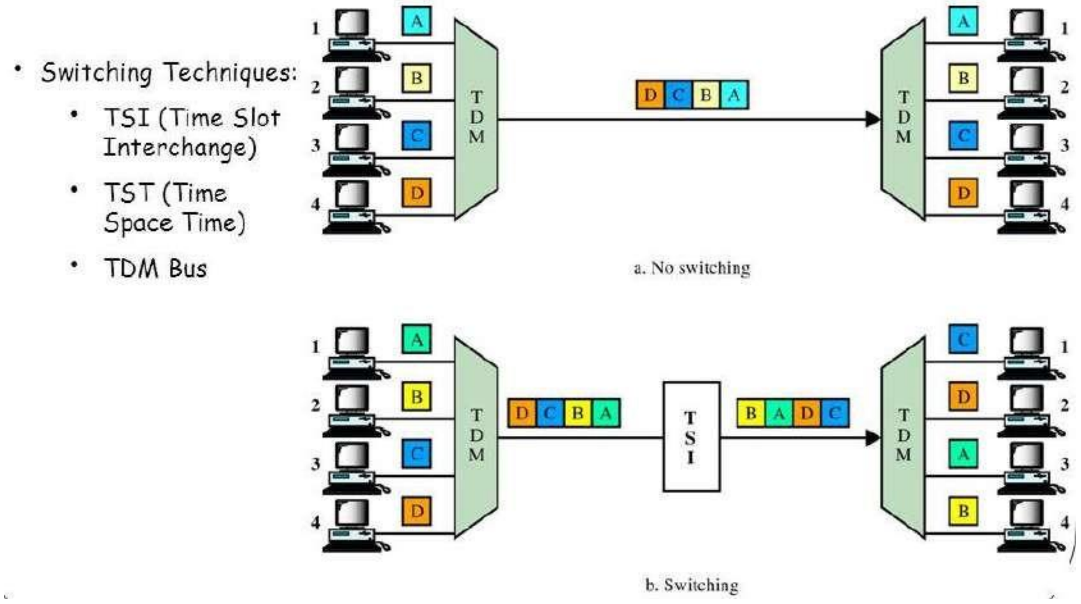


Figure 15: Space Division Switching

Time Division Switching

- In a time-division switch, the inputs are divided in time, using TDM. A control unit sends the input to the correct output device.
- Use digital time division techniques to set up and maintain virtual circuits.



- Switching Techniques:
  - TSI (Time Slot Interchange)
  - TST (Time Space Time)
  - TDM Bus

a. No switching

b. Switching

Figure 16: Time Division Switching

Packet Switching

- Packet switching was designed to provide a more efficient facility than circuit-switching for burst data traffic.
- With packet switching, a station transmits data in small blocks, called packets.
- At each node, packets are received, stored briefly (buffered) and passed on to the next node.
  1. Store and forward mechanism
- Each packet contains some portion of the user data plus control info needed for proper functioning of the network.
- A key element of packet-switching networks is whether the internal operation is datagram or virtual circuit (VC).
  1. With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.
  2. With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.
- Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- Station breaks a long message into packets. Packets sent one at a time to the network.
- Packets handled in two ways:
  1. **Datagram**
     - Each packet treated independently
     - Packets can take any practical route
     - Packets may arrive out of order
     - Packets may go missing
     - Up to receiver to re-order packets and recover from missing packets
  2. **Virtual Circuit**
     - Pre-planned route established before any packets sent.

- Once the route is established, all the packets between the two communicating parties follow the same route through the network
- Call request and call accept packets to establish a connection (handshake)
- Each packet contains a Virtual Circuit Identifier (VCI) instead of a destination address
- No routing decisions required for each packet
- Clear request to drop circuit
- Not a dedicated path

Message Switching

- This technique was somewhere in the middle of circuit switching and packet switching.
- In message switching, the whole message is treated as a data unit and is transferred in its entirety.
- A switch working on message switching first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

Protocols layers and their service model

OSI Layer Architecture

- OSI model is based on a proposal developed by the International Standards Organization (ISO) as the first step toward international standardization of the protocols used in the various layers.
- It was revised in 1995.
- The model is called the 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.
  1. Physical Layer
  2. Data Link Layer
  3. Network Layer
  4. Transport Layer
  5. Session Layer
  6. Presentation Layer
  7. Application Layer

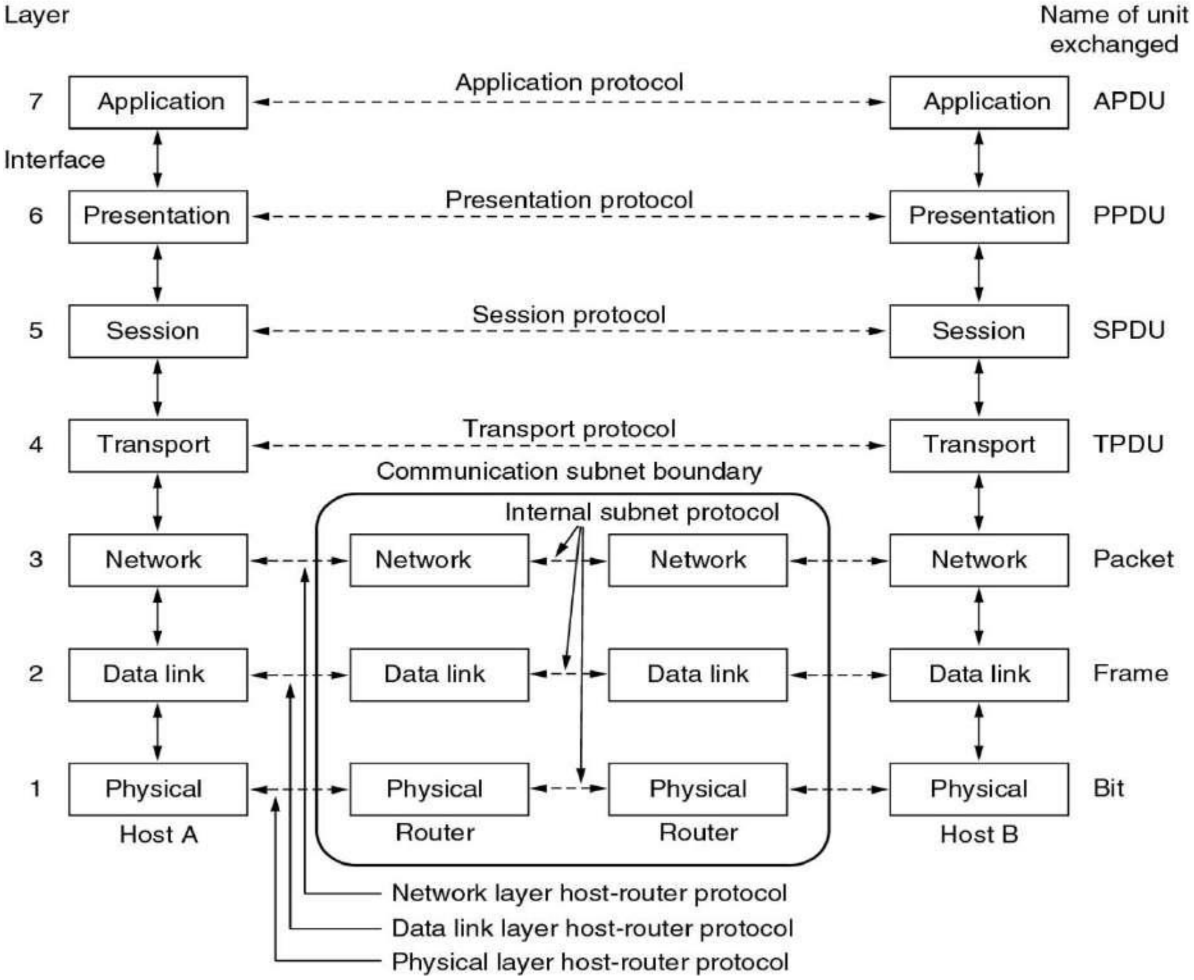


Figure 17: OSI Reference Model

Physical Layer

- The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium.
- It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:
- **Data encoding**: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in a bit and frame synchronization.
- **Transmission technique**: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signalling.
- **Physical medium transmission**: transmits bits as electrical or optical signals appropriate for the physical medium.

Data link Layer

- The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.
- To do this, the data link layer provides:
- **Link establishment and termination**: establishes and terminates the logical link between two nodes.
- **Frame traffic control**: tells the transmitting node to "back-off" (stop) when no frame buffers are available.
- **Frame sequencing**: transmits/receives frames sequentially.
- **Frame acknowledgment**: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame delimiting**: creates and recognizes frame boundaries.
- **Frame error checking**: checks received frames for integrity.
- **Media access management**: determines when the node "has the right" to use the physical medium.

Network Layer

- The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, a priority of service, and other factors.
- To do this, the data link layer provides:
- **Routing**: routes frames among networks.
- **Subnet traffic control**: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- **Frame fragmentation**: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re- assembly at the destination station.
- **Logical-physical address mapping** translates logical addresses or names, into physical addresses.
- **Subnet usage accounting**: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Transport Layer

- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves (release) the higher layer protocols from any concern with the transfer of data between them and their peers.
- The size and complexity of a transport protocol depend on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.
- The transport layer provides:
- **Message segmentation**: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- **Message acknowledgment**: provides reliable end-to-end message delivery with acknowledgments.

- **Message traffic control**: tells the transmitting station to "back-off" when no message buffers are available.
- Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.
- The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.
- In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

Session Layer

- The session layer allows session establishment between processes running on different stations. It provides:
- **Session establishment, maintenance, and termination**: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- **Session support**: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

- The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
- The presentation layer provides:
- **Character code translation**: for example, ASCII to EBCDIC.
- **Data conversion**: bit order, CR-CR/LF, integer-floating point, and so on.
- **Data compression** reduces the number of bits that need to be transmitted on the network.
- **Data encryption**: encrypt data for security purposes. For example, password encryption.

Application Layer

- The application layer serves as the window for users and application processes to access network services.
- This layer contains a variety of commonly needed functions:
  1. Resource sharing and device redirection
  2. Remote file access
  3. Remote printer access
  4. Inter-process communication
  5. Network management
  6. Directory services
  7. Electronic messaging (such as mail)
  8. Network virtual terminals

TCP/IP Reference Model (Internet Protocol Stack layers)

- Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide.
- TCP/IP either combines several OSI layers into a single layer or does not use certain layers at all.

- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
- The TCP/IP model has five layers.
    1. Application Layer
    2. Transport Layer
    3. Internet Layer
    4. Data Link Layer
    5. Physical Network

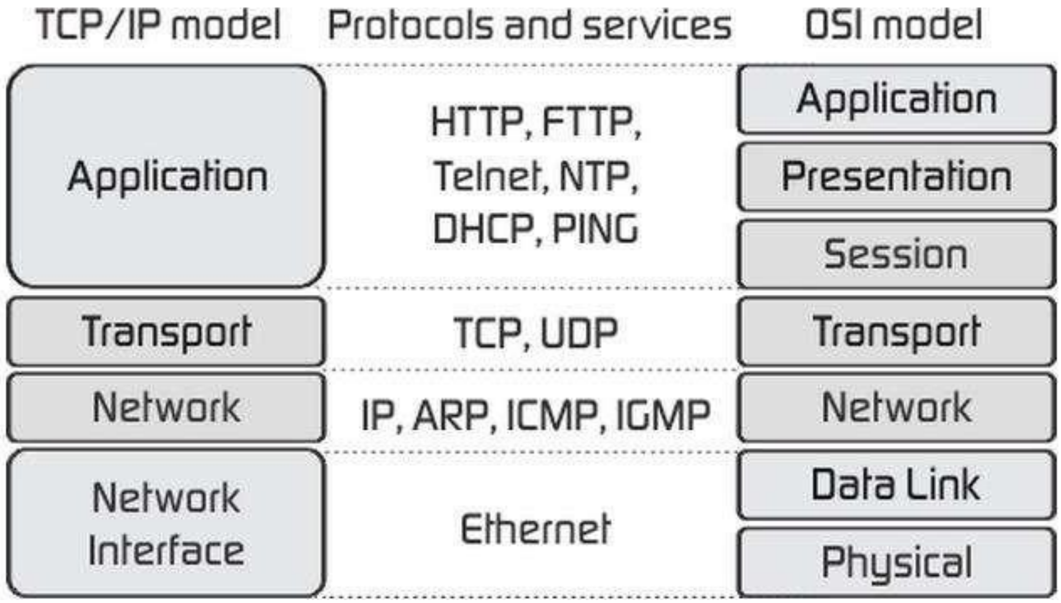


Figure 18: TCP/IP Reference Model

- As we can see from the above figure, the presentation and session layers are not there in the TCP/IP model. Also, note that the Network Access Layer in the TCP/IP model combines the functions of Data link Layer and Physical Layer.

Application Layer

- The application layer is the topmost layer of the four-layer TCP/IP model.
- The application layer is present on the top of the Transport layer.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer

- The purpose of the Transport layer is to permit devices on the source and destination hosts to carry on a conversation.

- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
  - ➢ Reliable delivery data
  - ➢ Duplicate data suppression
  - ➢ Congestion control
  - ➢ Flow control

- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
  - ➢ Connectionless
  - ➢ Unreliable
  - ➢ Best-effort service
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

Network Layer (Internet Layer)

- The internet layer also called the network layer.
- Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The Internet layer is also responsible for the routing of IP datagrams.
- Internet Protocol (IP) is the most important protocol in this layer.
- It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram.
- Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer (Network Access Layer)

- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

OSI (Open System Interconnection)	TCP/IP (Transmission Control Protocol / Internet Protocol)
• It has 7 layers	• It has 4 layers
• OSI provides layer functioning and also defines functions of all the layers.	• TCP/IP model is more based on protocols and protocols are not flexible with other layers.

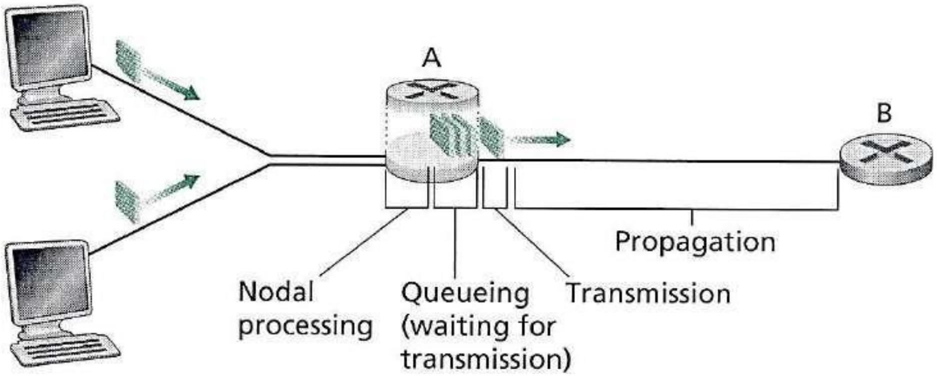
In the OSI model, the transport layer guarantees the delivery of packets	In the TCP/IP model, the transport layer does not guarantee delivery of packets.
Follows horizontal approach	Follows a vertical approach.
OSI model has a separate presentation layer	TCP/IP doesn't have a separate presentation layer

OSI is a general model.	TCP/IP model cannot be used in any other application.
The network layer of the OSI model provides both connection-oriented and connectionless service.	The Network layer in the TCP/IP model provides connectionless service.
OSI model has a problem of fitting the protocols in the model	TCP/IP model does not fit any protocol
Protocols are hidden in the OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces, and protocols very clearly and makes a clear distinction between them.	In TCP/IP, it is not clearly separated its services, interfaces, and protocols.

Understanding of Delay, Loss, and Throughput in the Packet Switching Network

Basics

- Recall that a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination).
- As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.
- The most important of these delays are the
  - Nodal processing delay
  - Queuing delay
  - Transmission delay
  - Propagation delay
- Together, these delays accumulate to give a total nodal delay.
- The performance of many Internet applications—such as search, Web browsing, email, maps, instant messaging, and voice-over-IP—are greatly affected by network delays.



Processing Delay

Figure 19: Delay in Packet Switched Network

- The time required to examine the packet's header and determine where to direct the packet is part of the processing delay.

- The processing delay can also include other factors, such as the time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream node to the router.
- It is typically on the order of microseconds or less.

Queuing Delay

- At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link.
- The length of the queuing delay of a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.
- If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay will be zero.
- On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.
- Queuing delays can be on the order of microseconds to milliseconds in practice.

Transmission Delay

- Assuming that packets are transmitted in a first-come-first-served manner like packet-switched networks.
- Now packet can be transmitted only after all the packets that have arrived before it have been transmitted.
- Denote the length of the packet by L bits, and denote the transmission rate of the link from a router to a router by R bits/sec.
- The transmission delay is L/R.
- Transmission delays are typically on the order of microseconds to milliseconds in practice.

Propagation Delay

- Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay.
- The bit propagates at the propagation speed of the link.
- The propagation speed depends on the physical medium of the link.
- Propagation delays are on the order of milliseconds.
- Propagations delay=d (Length of Physical Link) /s (Propagation speed in medium).

Packet Loss

- Packet loss is the failure of one or more transmitted packets to arrive at their destination.
- This event can cause noticeable effects on all types of digital communications.
- The loss of data packets depends on the switch queue. The loss of data packets increases with the increases in the traffic intensity.
- It affects the performance of the network.

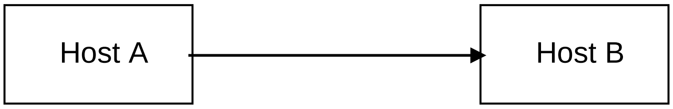
Throughput

- Throughput or Network Throughput is the rate of successful message delivery over a communication channel.
- The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node.
- Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

Problem:

In this problem, we consider sending real-time voice from Host A to Host B over a packet- switched network (VoIP). Host A converts analog voice to a digital 64 kbps bit stream on the fly. Host A then groups the bits into 56-byte packets. There is one link between Hosts A and B; its transmission rate is 2 Mbps and its propagation delay is 10 msec. As soon as Host A gathers a packet, it sends it to Host B. As soon as Host B receives an entire packet, it converts the packet's bits to an analog signal. How much time elapses from the time a bit is created (from the original analog signal at Host A) until the bit is decoded (as part of the analog signal at Host B)?

Given
:



- Analog to Digital conversion rate = 64 kbps
- Packet size = 56 bytes (Convert into bits so 56 bytes = 56 * 8 = 448 bits).
- Transmission rate = 2 Mbps
- Propagation delay = 10 msec

- Since this is a packet switched network, the data will be transmitted packet by packet.
- A packet is 56 byte and the analog to digital conversation rate is 64 kbps, thus the preparing time
  PT for a packet is 448/(64*1000)= 0.007 sec = 7 msec
- The transition delay TD for a packet is (Size or Length of packet) / (Speed or Transmission rate)
  So, TD = (56*8) / (2*1000*1000) =0.000224 s = 0.224msec.
- Propagation delay PD = 10msec (Given in sum)
- Finally, the total time elapses from the time a bit is create until the bit is decoded is PT+TD+PD= 7+0.224+10 = 17.224 msec.