1... Introduction to Computer Network

Objectives...

- To learn basics of Computer Network.
- To understand various Network topologies and Network types.
- To know about Modes of communication.
- To get information of Server based and Peer to Peer LANs.
- To study about Protocols and standards and Network Software.

1.1 BASICS OF COMPUTER NETWORK (W-18, S-19, S-22, S-23)

- Today every business in the world needs a computer network for smooth operations, flexibly, instant communication and data access. Just imagine if there is no network communication in the university campuses, hospitals, multinational Organizations and educational institutes then how difficult are to communicate with each other.
- A computer network is comprised of connectivity devices and components. To share data and resources between two or more computers is known as Networking.

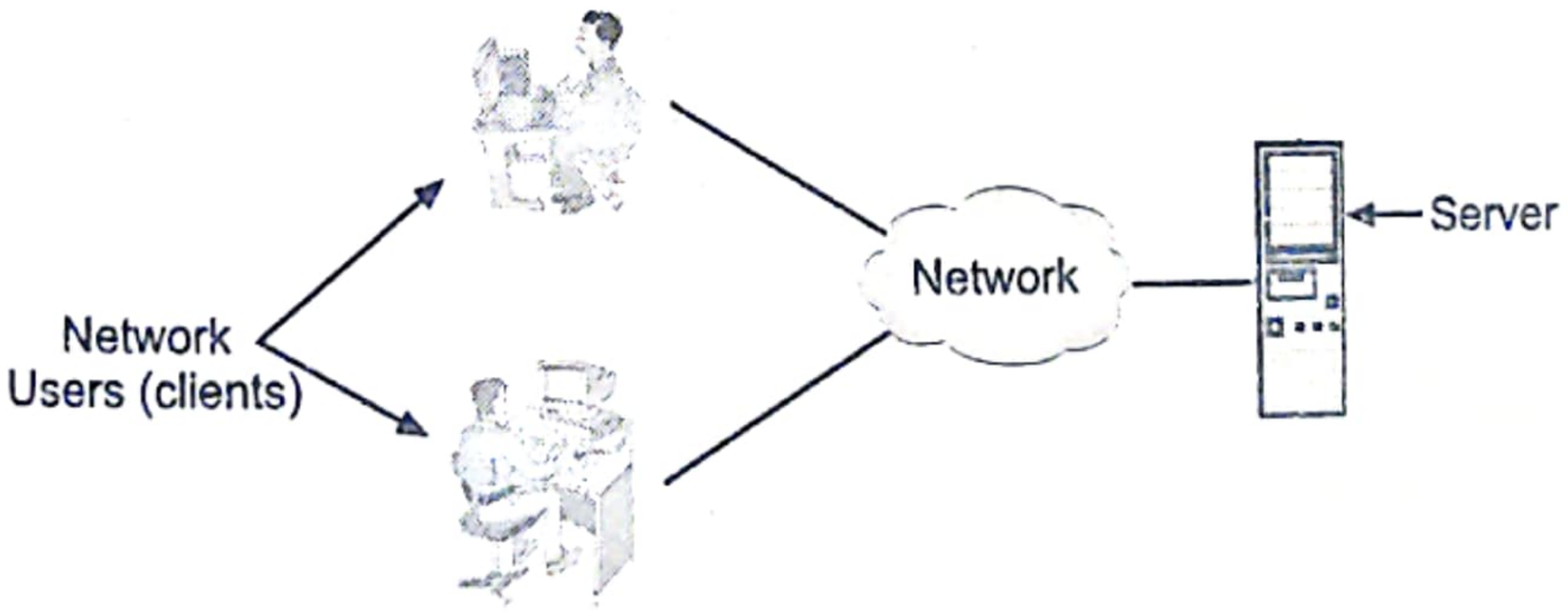


Fig. 1.1: A Typical Computer Network

- The purpose of a computer network is to link two or more "clients" together in order to exchange information.

1.1.1 Definition

(W-22, S-23)

- A computer network is a system for communication among two or more computers.

OR

- A computer network is defined as two computers that are linked together through either a physical cable, or a wireless device. This link then allows the computers on the network to share resources such as an Internet connection, printers, files, and programs.

OR

- A computer network is a collection of computer systems which can communicate or interact with each other.

OR

- Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

1.1.2 Goals

(W-22, S-23)

- The computer networks are playing an important role in providing services to large or small or medium organizations as well as to the individual common man.
- Network services are the things that a network can do.

Like human being computer network provides following goals:

1. **Resource Sharing:**

- It is the main goal of the computer network. The goal is to provide data and hardware to all programs on network regardless of physical location of resources and users.
- In computer network, one of the machines can work as a server. So whatever important data we want, can be stored on server. This data (files, documents) can be shared by users. One hard disk will fulfill the need of all users.
- This allows us to extract co-relation about the whole network. For example, we can manage all the users from server. We can copy data of one user to other user. We can send similar information to all users and so on.
- In short, Networks used to provide sharing of resources such as information or processors.

2. **High Reliability:**

- Network provides high reliability by having alternative sources of data.
- For example, all files could be replicated on more than one machines, so if one of them is unavailable due to hardware failure or any other reason, the other copies can be used.

3. **Minimize Cost:**

- Small computers have a much better price to performance ratio as compared to large ones. So it is always minimizing the cost to set up a network of large or small number of computers than the large ones.

- As well as by sharing the resources like printer, we can save the cost. While designing cost of a network is an important factor.

4. **High Performance:**

- Computer network provides the network user with maximum performance at minimum cost. The network performance can be measured by its transit time and response time.
  (i) Transit time is the amount of time required for a message to travel from one device to another device in network.
  (ii) Response time is the time elapsed between an inquiry and a response.
- Network performance depends on a number of factors including, network transmission medium, network hardware, network software and traffic load. Computer network have provided means to increase system performance as the work load increases.

5. **Scalability:**

- We can easily extend computer network just by adding more computers, printers or any other devices without disturbing others and affecting overall performance.

6. **Powerful Communication Medium:**

- A computer network provides a powerful communication medium.
- Computer network helps people who live or work apart to report together. So, when one user prepared some documentation, he can make the document online enabling other to read and convey their opinions.
- From the server, we can send same information to all users and users can also communicate with the server. For this reason, computer network is a powerful communication medium.

7. **Distribution of Workload:**

- By using computer network, large work can be distributed among different network users.

8. **Security:**

- Network security issues comprise of prevention from virus attacks and protecting data from unauthorized access. Only authorized user can access resource in a computer network.

9. **Backups:**

- Similarly, in computer network taking backup is very easy. Because data is stored on server. By using a single floppy drive or CD writer we can take backups.

1.1.3 Network Structure

- In any network, there are collections of machines intended for application user programs.

- Any network should have following elements:
  1. **Hosts:** Hosts are the machines intended for running user application. They are also called end systems because they are the end users.
  2. **Communication subnet:** Hosts are connected with each other by communication subnet. The job of the subnet is to carry messages from host to host. The subnet plays an important role in network addressing which is needed in internetworking.
- In most WANs, subnet consists of two different elements:
  - **Transmission lines:** These are also referred as circuits, channels or trunks. These move bits between machines. For communication these lines are very important.
  - **Switching element:** This is also called as IMP i.e. Interface Message Processors. IMPs are specialized computers used to connect two or more transmission lines. Some may called them packet switched node, Intermediate system and data switching exchange, routers.

Components of Network:

- A computer network comprises the following components:
  1. Computers (at least two).
  2. Cables that connect the computers to each other.
  3. A network interface device on each computer (This is called a Network Interface Card or NIC).
  4. A switch (Note: hubs are no longer recommended).
  5. Network operating system software.
  6. Uninterruptible power supply (optional).

1.1.4 How Does a Computer Network Work ?

- Following figure shows how simple network to send information from one computer send to another:

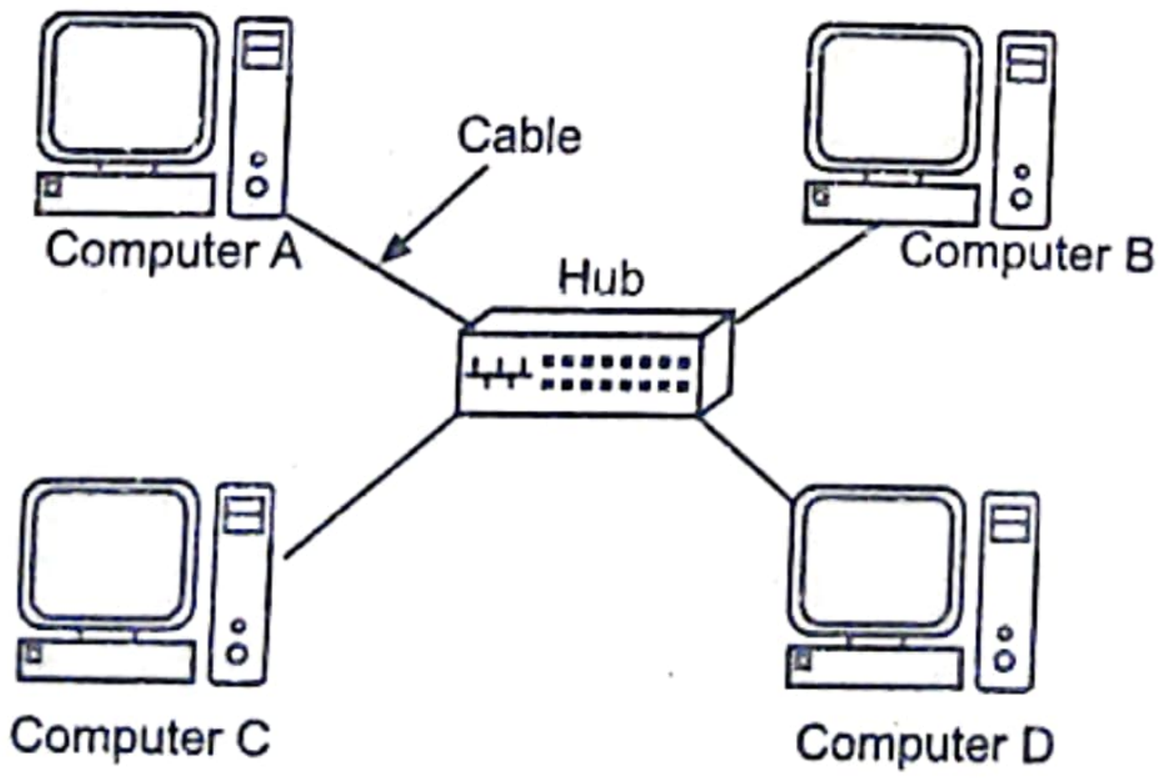


Fig. 1.2: A Typical Network

- If Computer A wants to send a file to Computer B, the following would take place:
  1. Based on a protocol that both computers use, the NIC in Computer A translates the file, (which consists of binary data 1's and 0's) into pulses of electricity.
  2. The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
  3. The hub takes in the electric pulses and shoots them out to all of the other cables.
  4. Computer B's NIC interprets the pulses and decides if the message is for it or not. In this case, it is so Computer B's NIC translates the pulses back into the 1's and 0's that make up the file.
- If Computer A sends the message to the network using NetBEUI, a Microsoft protocol, but Computer B only understands the TCP/IP protocol, it will not understand the message; no matter how many times Computer A sends it. Computer B also would not get the message if the cable is getting interference from the fluorescent lights or if the network card has decided not to turn on today etc.

1.1.5 Applications

A computer network has of following applications:

1. **Resource Sharing:** Enables users to share hardware like scanners and printers. This reduces costs by reducing the number of hardware items bought. Resources are available to anyone on the network without regard to the physical location of the resource and the user.

   For example: Printers, scanners, CD burners, etc.
2. **Information Sharing:** Allows users access to data stored on others computers. This keeps everyone up-to-date on the latest data, since it's all in the same file, rather than having to make copies of the files, which are immediately out-of-date.

   For example: Files, database, records etc.
3. **Person-to-Person Communication:** For example, e-mail (electronic mail). Voice and Video conferencing is also available to perform virtual meetings.

- Online reservations for airlines, railways and online examination systems are available because of network.
- We can access remote information for bank transaction, MSEB bill paying, by reading newspapers.
- **For example:** GIS [Geographical Information System] is available from which we can get the information of soil details, water detail, rivers, oceans maps, area wise details of our earth.

4. **Electronic Business:** Users can place orders electronically as needed. In the industries or Organizations, management can keep track of all inventories, sales, production, personnel information through network. By using electronic mail facility, messages, documents, memos can be send to different people and immediately get the delivery report.

5. **Interactive Entertainment:** Users can play real-time simulation games, like flight simulators, Age of empires etc. Also allows user to chat, watch movies, solve quiz, etc.
6. **Manufacturing**: Computer network is used in manufacturing and in manufacturing process also.

   For example: CAD (Computer Aided Design) and CAM (Computer Aided Manufacturing).
7. **Marketing and Sales**: Sales application-teleshopping is one of the computer network's applications. This application uses order-entry computers or the telephones are connected to an order processing network. The network is used to transmit and receive critical sales, administrator and research data by the travelling salesman and remote employees.
8. **Banking:** Computers are instrumental to the way the banking industry performs its business. This technology allows banks to be able to take banking transactions and update accounts in real time.
9. **Financial services**: It include credit history searches, foreign exchange and investment services and Electronic Fund Transfer (EFT) which allows a user to transfer money without going to bank.
10. **Insurance:** The world of insurance relies on computers to the same extent as banks. With the use of the Internet, insurance companies are able to access information which will determine whether they accept clients or not.

1.1.6 Network Hardware - Broadcast and Point to Point

- Network hardware structure is a design required for developing any computer network.
- For classification of computer network, transmission technology is important.
- Transmission technology refers how two devices are connected and how they are communicating. In transmission technology, a link is the physical communication pathway that transfers data from one device to another.
- For communication to occur, two devices must be connected in same way to the same link at the same time.
- The transmission technology can be broadly categorized into two types:
  1. Broadcast networks (multipoint)
  2. Point-to-Point networks

1.1.6.1 Broadcast Network

- The networks having multipoint configuration are called as Broadcast Network.
- Broadcast network has single communication channel that is shared by all the machines on the network. Short messages called packets in certain contexts, sent by any machine, are received by all the others.

- An address field within the packet specifies for whom it is intended. After receiving a packet, a machine checks the address field.
- If the packet is intended for itself, it processes the packet; if packet is intended for some other machine, it is just ignored. Example: LAN
- It is normally a connection of hosts and repeaters. Here if packet is not responded, then it will be lost.
- A broadcast network is an organization, such as a corporation or other association, that provides live or recorded content, such as movies, newscasts, sports, and public affairs programs for broadcast over a group of radio or television stations.
- They are generally primarily either a television network or a radio network, although some organizations run both types of networks.
- A broadcast network avoids the complex routing procedures of a switched network by ensuring that each node's transmissions are received by all other nodes in the network.
- Therefore, a broadcast network has only a single communications channel.
- A wired Local Area Network (LAN), for example, may be set up as a broadcast network, with one user.

Modes of operations:

- Broadcast network supports two modes of operations:

1. **Broadcasting:** Broadcast systems generally use a special code in the address field for addressing a packet to all the concerned computers. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called Broadcasting.
2. **Multicasting:** Some broadcast systems also support transmission to a subset of the machines known as Multicasting. When a packet is sent to a certain group, it is delivered to all machines of that group. Examples of this network are Ethernet and Bus topology based on LAN.

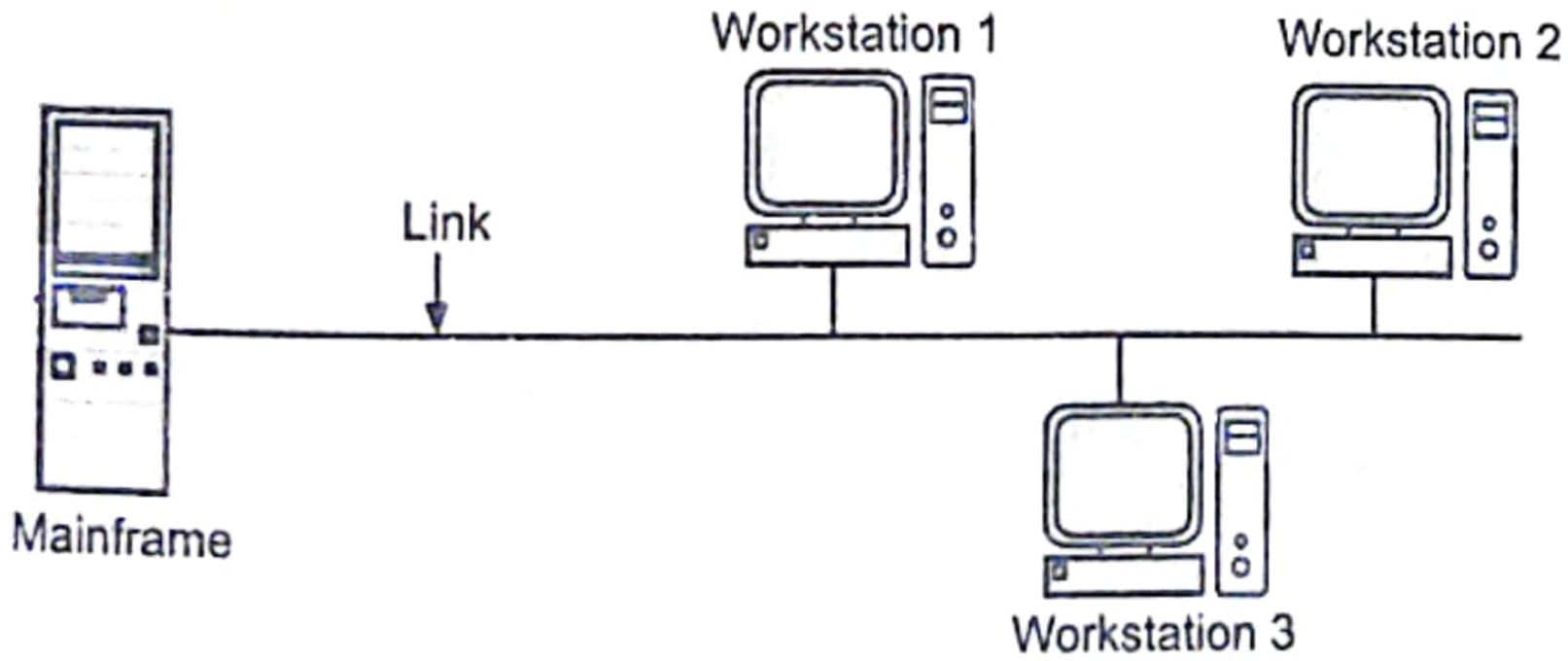


Fig. 1.3: Broadcast Network

1.1.6.2 Point-to-Point Network

- In contrast, Point-to-Point network consists of many connections between individual pairs of machines to go from the source to destination.

- A packet on this type of network may have to visit one or more intermediate machine. Often multiple routes of different lengths are possible.
- So routing algorithms play an important role in Point-to-Point communication. Example: WAN
- It is normally a connection of routers, called as Subnet.
- If two routers, that are not connected by a direct cable and wish to communicate, they must do it via other routers. A packet is sent from one to another via. Intermediate router.
- The packet is stored until there required output line is free and then forwarded.
- A subnet using this principle is called as point to point store and forward or packet switched network.
- A Point-to-Point network with one sender and one receiver is sometimes called Unicasting.
- Examples of Point-to-Point networks are LAN (Local Area Networks), MAN (Metropolitan Area Network), WAN (Wide Area Network), Internet, etc.

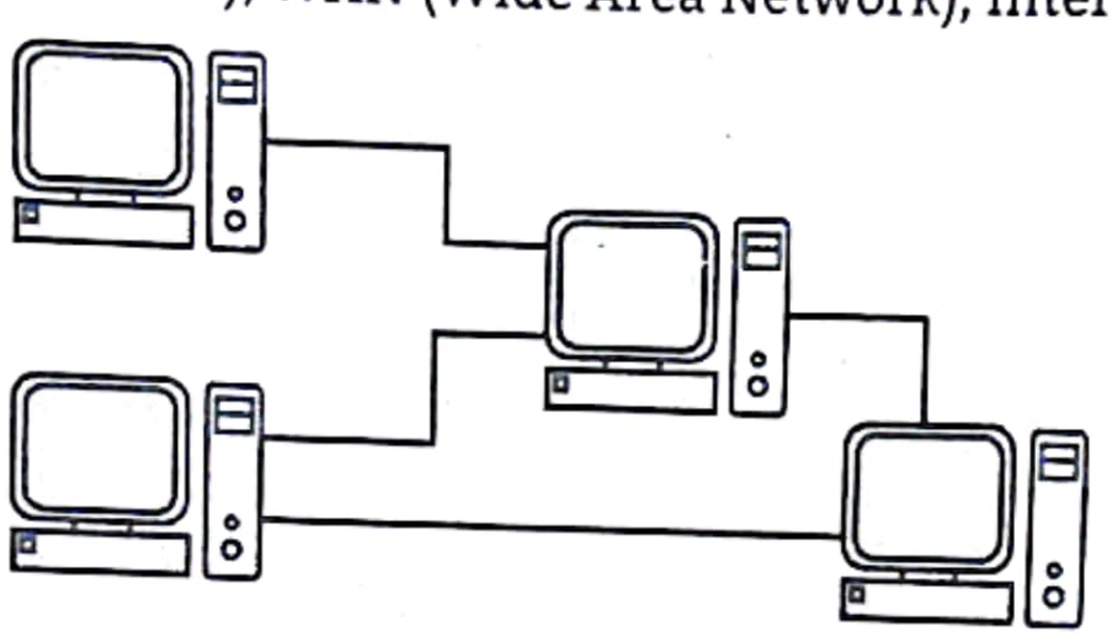


Fig. 1.4: Point-to-Point Network

Advantages:

1. **Simple:** A Point-to-Point network is one of the simplest networks because it only involves two nodes.
2. **Cheapest and effective:** This is one of the cheapest and most effective network architectures because it doesn't involve the cost of redundancies.
3. **Less Complex:** It does not add the complexity of needing several nodes functioning to make a connection.

Disadvantages:

1. **Lack of security:** You have limited number of concurrent connections and anyone with access to the network can access all shared files/folders. You open yourself up to viruses/spyware/adware/rootkits and lots of other 'malware'.
2. **More expensive:** As it requires lots of transmission lines and switching elements to connect remote hosts. It also requires a lot of bandwidth.

1.1.7 Components of Data Communication (W-18)

- The five components of data communication are:

1. **Message/Data:** The message is nothing but the data or information which is to be communicated. It may have texts, numbers, pictures, sound or video or combination of anything from these.
2. **Sender:** This is the device which sends the data message. It can be a computer, workstation, telephone handset, video camera and so on. Data is in human readable form, gets converted into machine form i.e. 0's and 1's.
3. **Receiver:** The receiver is the device which receives the message. Again it can be a computer, workstation, telephone handset, television and so on.

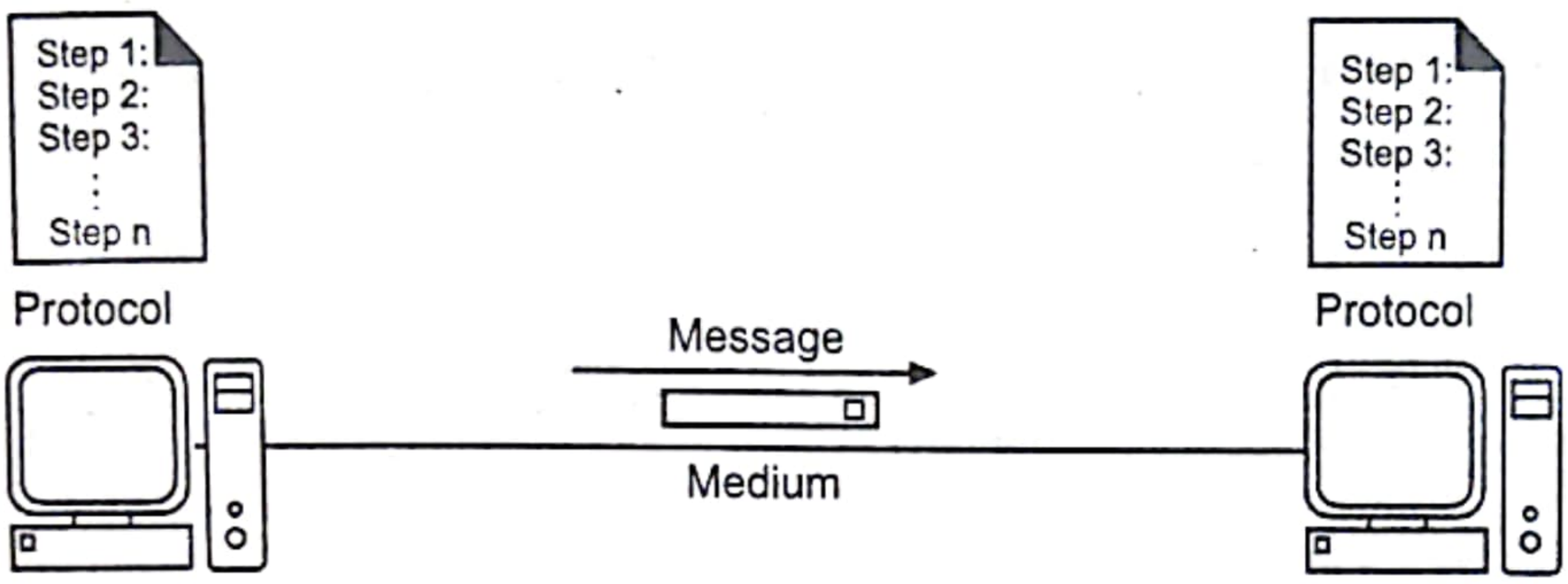


Fig. 1.5: Components of Data Communication

4. **Transmission Medium:** The transmission medium is the physical path by which a message travels from sender to receiver. It may be twisted-pair wire, coaxial cable, fiber-optic cable, laser or radio waves and so on. The radio waves may be terrestrial or satellite microwave.
5. **Protocol:** A protocol is a set of rules required for data communication. It represents the agreement between the two communicating devices. Without protocol, we can connect two devices but they cannot communicate with each other. For example, without a translator, a Japanese cannot communicate with a French person. The job of protocol is similar to the translator.

1.1.8 Advantages and Disadvantages of Network

- Computer Network consist of following Advantages:

1. **Speed:** Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, than carrying or sending the disks from one computer to another. This method of transferring files (referred to as Sneaker-net) is very time-consuming.
2. **Cost:** Networkable versions of many popular software programs are available at considerable savings when compared to buying individually licensed copies. Besides monetary savings, sharing a program on a network allows for easier upgrading of the

program. The changes have to be done only once, on the file server, instead of on all the individual workstations.

3. **Security:** Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.
4. **Centralized Software Management:** One of the greatest benefits of a network is the fact that all of the software can be loaded on one computer (the *file server*). This eliminates the need to spend time and energy installing updates and tracking files on independent computers throughout the building or campus.
5. **Resource Sharing:** Sharing resources is another area in which a network exceeds stand-alone computers. Most organizations cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.
6. **Sharing Software:** Users can share software within the network easily. Networkable versions of software are available at considerable savings compared to individually licensed version of the same software. Therefore large companies can reduce the cost of buying software by networking their computers.
7. **Easy Communication:** It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. Person to person communication became easy due to e-mail systems, instant messaging, telephony, video conferencing, chat rooms etc.
8. **Flexible Access:** Some organization's networks allow authorized users to access their files from computers throughout the network of organization.
9. **Workgroup Computing:** Workgroup software (such as *Microsoft BackOffice*) allows many users to work on a document or project concurrently. For example, educators located at various schools within a state could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

Disadvantages of Network:

- A computer network consist of following disadvantages:

1. **Expensive to Install:** Although a network will generally save money over time, the initial costs of installation can be prohibitive. Cables, network cards and software are expensive, and the installation may require the services of a technician.
2. **Requires Administrative Time:** Proper maintenance of a network requires considerable time and expertise.
3. **Breakdowns and Possible Loss of Resources:** Although a file server is no more susceptible to failure than any other computer in the network. When the files server "goes down," the entire network may come to a halt. When this happens, the entire organization may lose access to necessary programs and files.

4. **Security Threats:** Security threats are always problems with large networks. There are hackers who are trying to steal valuable data of large companies for their own benefit. So it is necessary to take utmost care to facilitate the required security measures.
5. **Bandwidth Issues:** In a network, there are users who consume a lot more bandwidth than others. Because of this some other people may experience difficulties.

1.2 NETWORK TOPOLOGIES

(S-18, W-18, W-22, S-23)

- Topology is the physical layout of computers, cables, switches, routers and other components of a network. This term can also refer to the underlying network architecture such as Ethernet or Token Ring.
- The word "topology" comes from "topos", which is Greek word for "place". When you design a network, your choice of topology will be determined by the size, architecture, cost and management of the network.
- A node is an active device connected to the network, such as a computer or a printer. It can be a piece of networking equipment such as a hub, switch or a router.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices, (usually called *nodes*) to one another.

Note: The term "topology" can refer to either a network's physical topology, which is the actual physical layout or pattern of the cabling or its logical topology, which is the path that signals actually take around the network. This difference is most evident in Token Ring networks, whose cabling is physically arranged in a star, but whose signal flows in a ring from one component to the next. The term "topology" without any further description is usually assumed to mean the physical layout.

Types of Network Topologies:

- Fig. 1.6 shows different categories of topologies in computer network. In the following section we will see description of some of them.

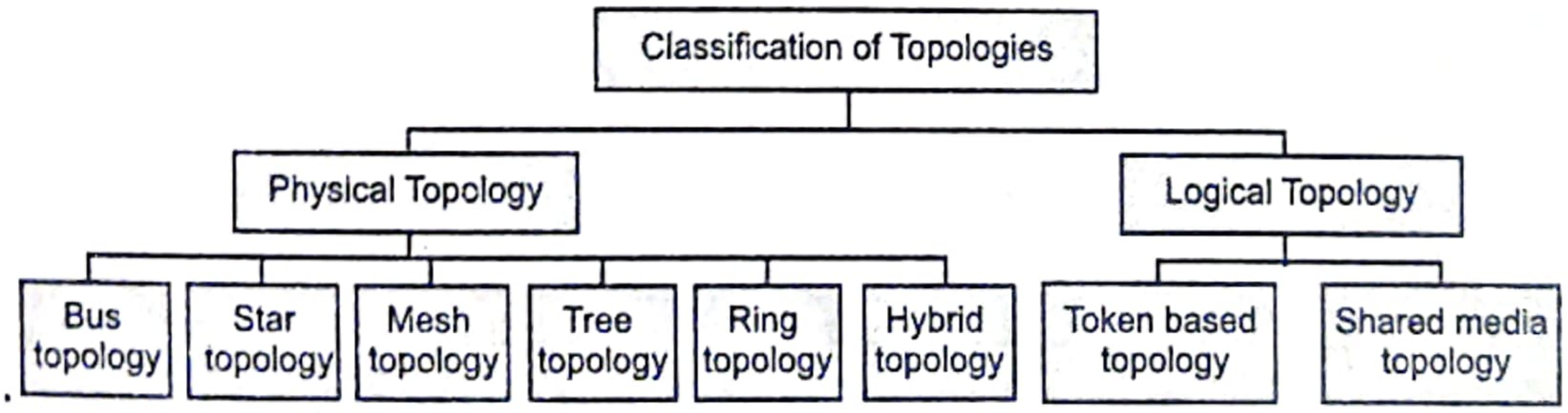


Fig. 1.6: Types of Network Topologies

- Topology defines the physical or logical arrangement of links in a network.
- The **Physical Topology** of a network refers to the configuration of cables, computers and other peripherals. This includes the arrangement and location of network nodes and how they are connected.

- The **Logical Topology** refers to the paths that messages take to get from one user on the network to another.
- Now let us see types of Physical Topology of a network.

1.2.1 Mesh Topology

- Each device in mesh topology has a dedicated point-to-point link to every other device. Dedicated means that link carries traffic only between the two devices it connects.
- The mesh topology connects each computer on the network to the complex in a redundant pattern.
- This topology is generally used only in Wide Area Networks (WANs) in which different networks are connected using routers.

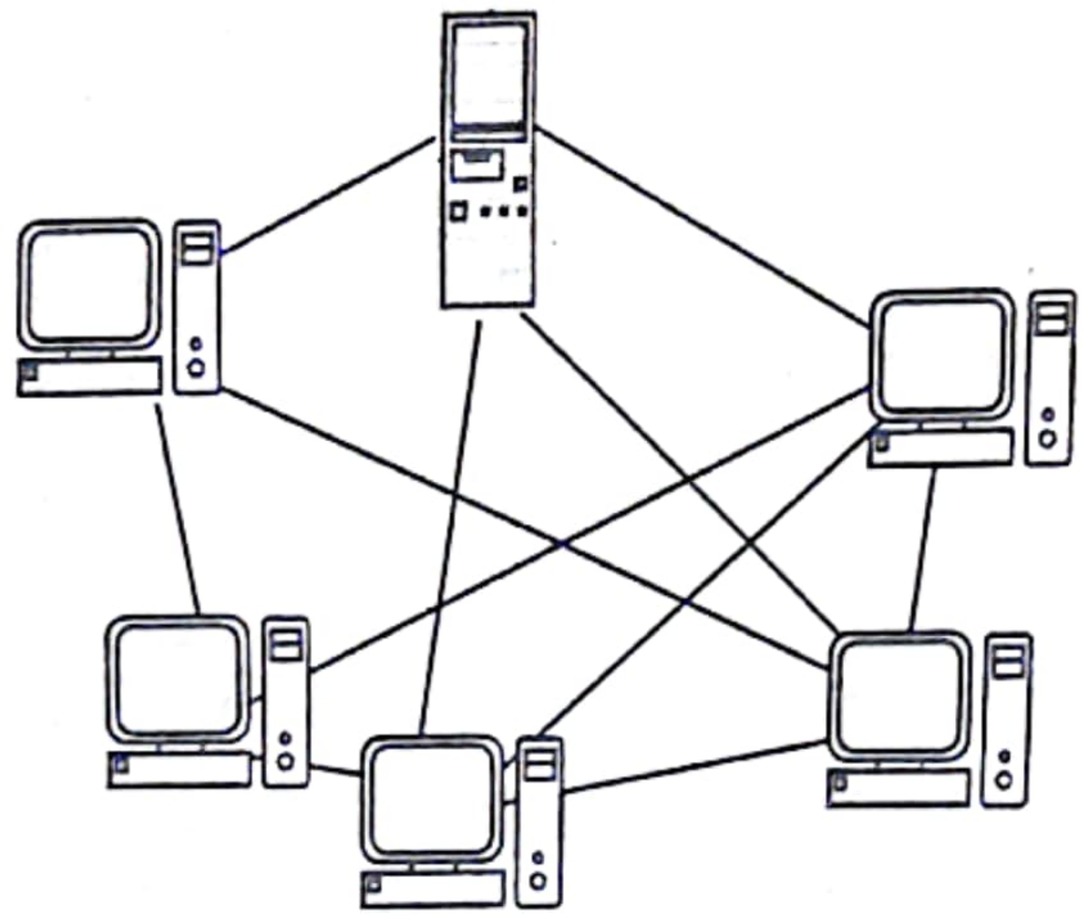


Fig. 1.7: Mesh Topology

- Fully connected mesh network has **n(n – 1)/2** links for **n** devices. To accommodate n(n-1)/2 links, every device on the network must have **n – 1** input/output (I/O) ports. Meshes use a significantly larger amount of network cabling than do the other network topologies, which makes it more expensive. The mesh topology is highly fault tolerant.
- That is, every computer has multiple possible connection paths to the other computers on the network, so a single cable break will not stop network communications between any two computers.
- A network topology in which every device is connected by a cable to every other device on the network. Multiple links to each device are used to provide network link redundancy.

Advantages:

1. Each connection can carry its own data load due to dedicated link.
2. Eliminates traffic problem.

3. Mesh topology is robust. If one link becomes unusable, it does not affect other systems.
4. Privacy or Security because of dedicated line.
5. Point-to-point link make fault identification easy.

Disadvantages:

1. More cables are required than other topologies.
2. Installation and reconfiguration is very difficult because each device must be connected to every other device.
3. Expensive due to hardware requirements such as cables and input/output ports.

1.2.2 Star Topology

- Each device in star topology has a dedicated point-to-point link to central controller, usually called a **hub** or **switch.**
- The controller acts as an exchange that means if one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- At the center of the star is a wiring hub or concentrator and the nodes or workstations are arranged around the central point representing the points of the star.
- The hub manages and controls all functions of the network. It also acts as a repeater for the data flow.

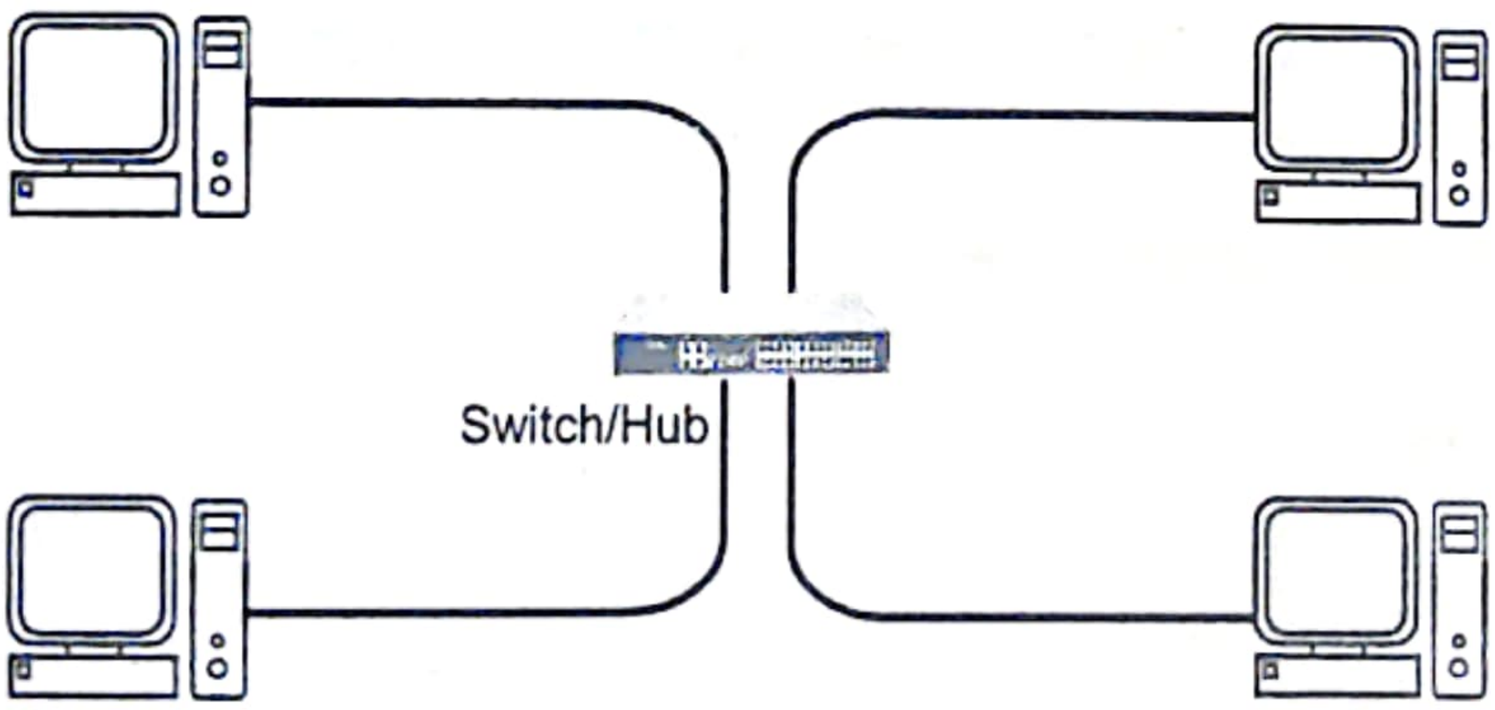
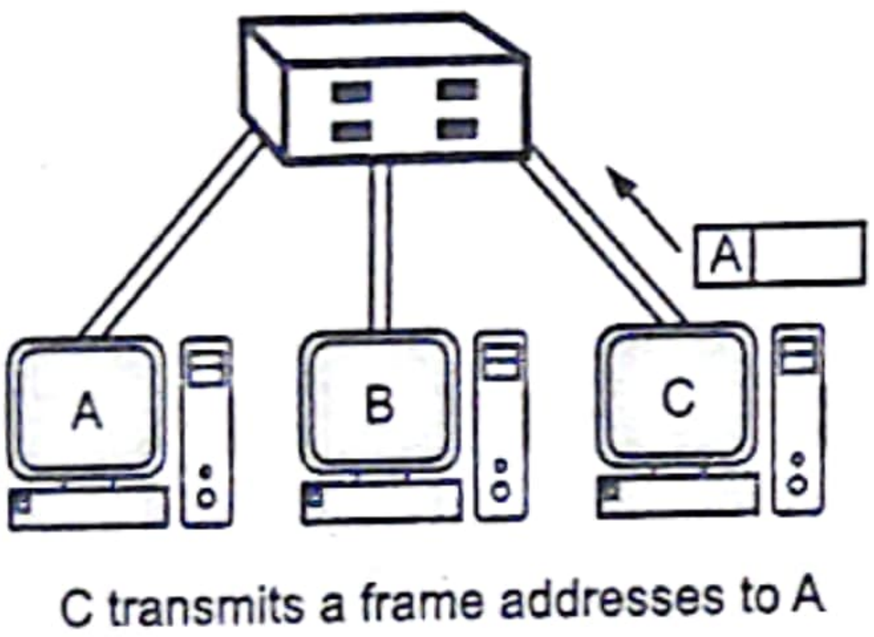


Fig. 1.8(a): Star Topology

- The devices are not directly linked to one another in star topology.
- Wiring costs tend to be higher for star networks than for other configurations, because each node requires its own individual cable.
- This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.
- The protocols used with star configurations are usually *Ethernet* or *LocalTalk*. Computers are connected by cable segments to a centralized hub.
- Signal travels through the hub to all other computers. Star topology requires more cable.

- **Illustration of Star topology:** In star topology, each station or node attached to central node (may be hub or switch) (Ref. Fig. 1.8(b)). Suppose node "C" wants to transfer data to node "A". If hub is use as a central node then it will broadcast packet to each every other node but only station/node "A" copies the packet and all other nodes discard the packet. But if switch is used as a central node then it will directly sent the packet only to node "A".



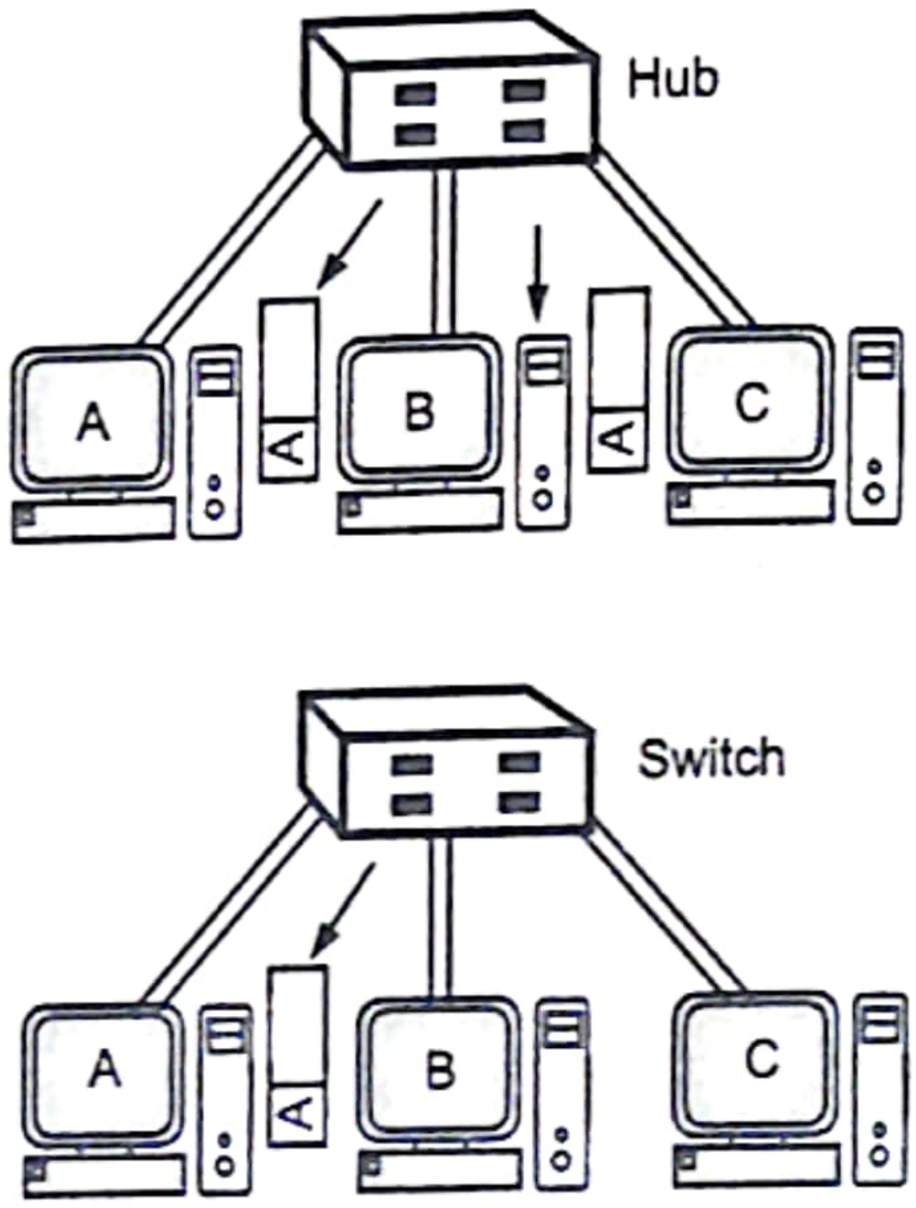


Fig. 1.8(b): Example of Star Topology

Advantages:

1. Easy to install, reconfigure and wire.
2. Robustness i.e. if one link fails, only that link is affected.
3. Fast as compare to ring topology.
4. Multiple devices can transfer data without collision.
5. Eliminates traffic problem.
6. No disruptions to the network then connecting or removing devices.
7. Easy to detect faults and to remove parts.
8. Supported by several hardware and software venders.

Disadvantages:

1. If central node (hub or switch) goes down then entire network goes down.
2. More cabling is required than bus topology, so expensive than bus topology.
3. Performance is depending on capacity of central device.

1.2.3 Bus Topology

- In networking, a topology that allows all network nodes to receive the same message through the network cable at the same time is called as bus topology.

- In this topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it is also referred to as Backbone cable.
- Trunk cable is then connected to the branch cables which were further connected to the PCs. Every network device communicates with the other device through this Bus.
- Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- A node (computer) that wants to send data, it puts the data on the bus which carries it to the destination node.
- When one computer sends a signal on the wire, all the computers on the network receive the information, but only one accepts the information. The rest regrets the message. One computer can send a message at a time. A computer must wait until the bus is free before it can transmit.

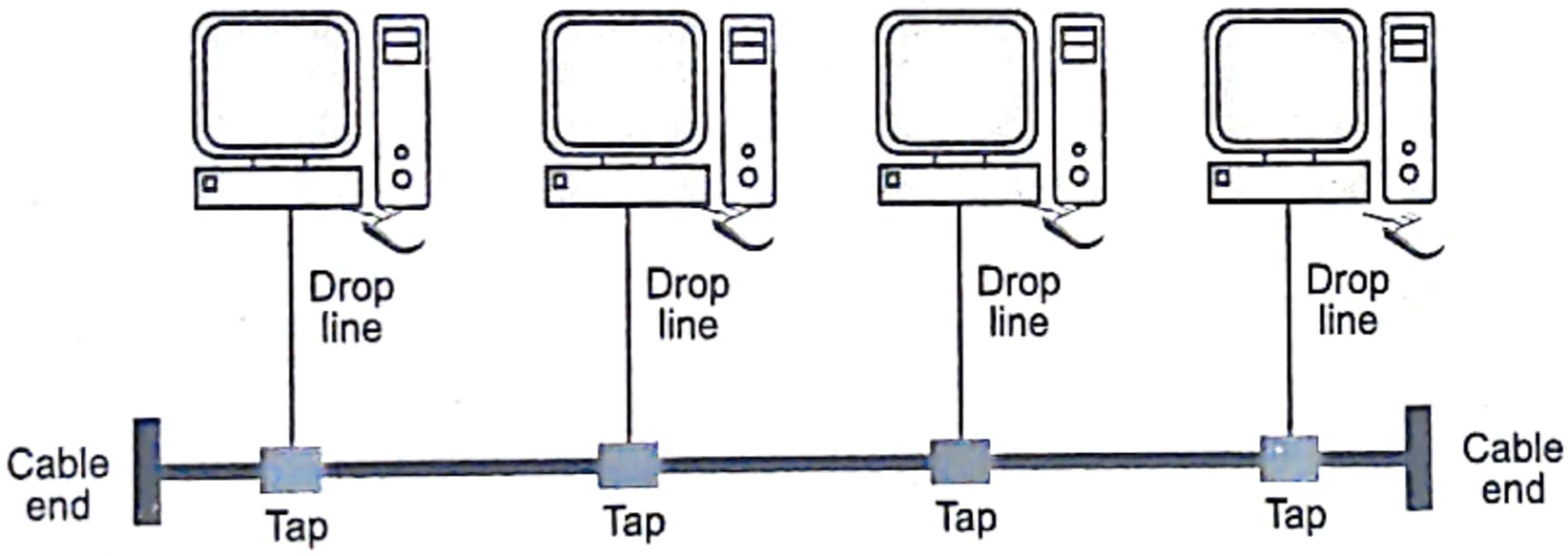


Fig. 1.9(a): Bus Topology

- In bus topology, communications goes both directions along the line. It is a multipoint configuration.
- Examples: Ethernet and LocalTalk networks use a linear bus topology.
- A network that uses a bus topology is referred to as a "Bus Network".

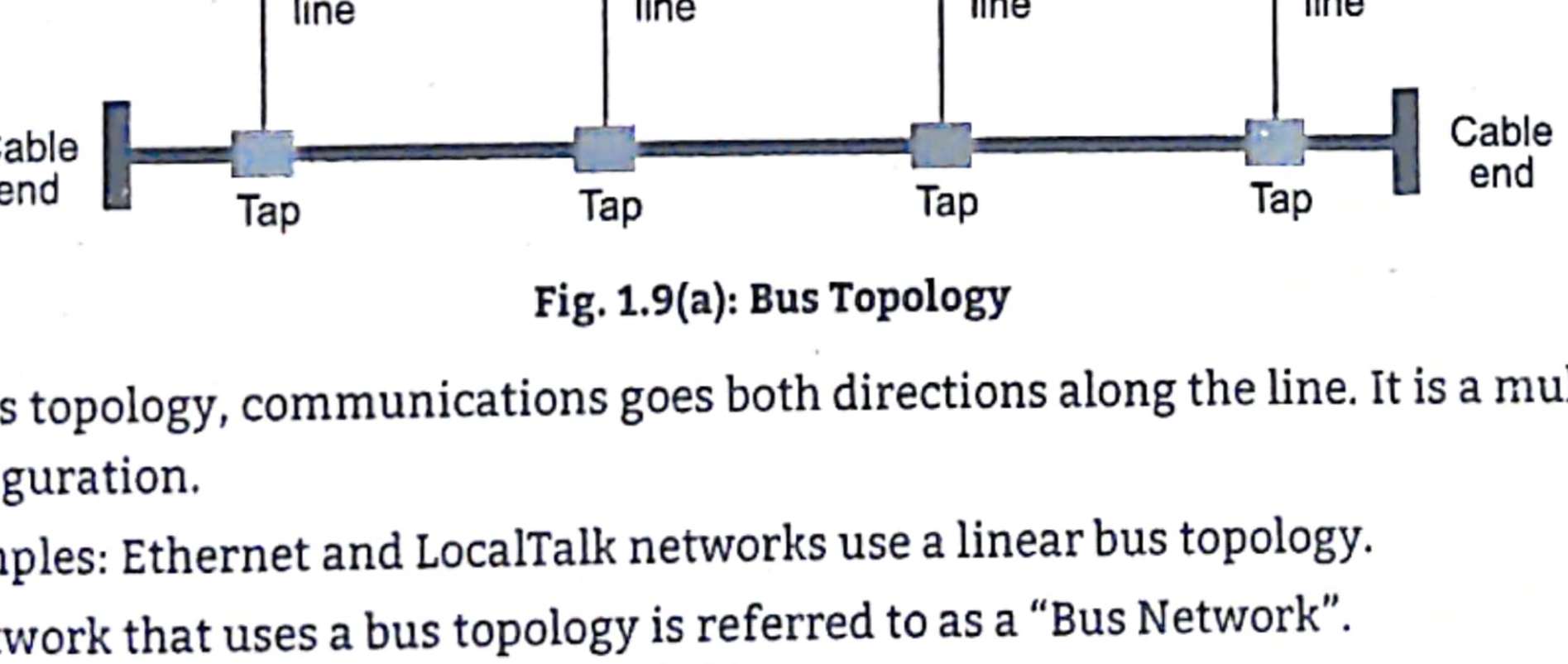


Fig. 1.9(b): A Bus Network

- **Illustration of Bus Topology:** Suppose node "A" wants to transfer data to node "D" as shown in Fig. 1.9(c). In bus topology all nodes will receive the packet sent by node "A" to node "D" because of common/same medium/link used by all nodes. Node "B" and node "C" will reject the packet while node "D" will accept the packet.

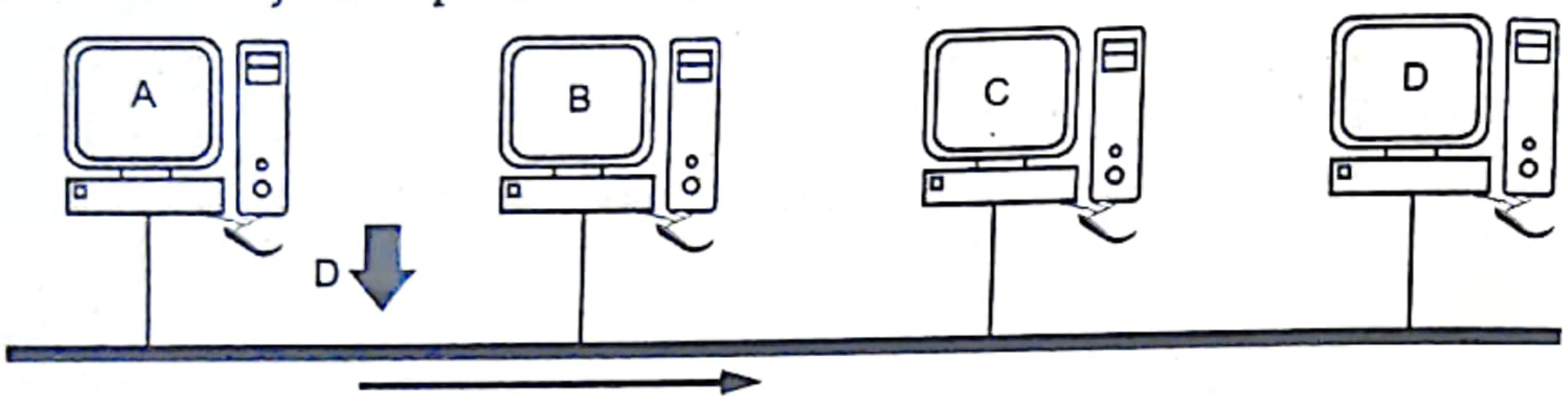


Fig. 1.9 (c): Example of Bus Topology

Advantages:

1. Easy to install. It's very easy to connect a computer or peripheral to a bus.
2. Bus topology is the cheapest way of connecting computers to form a workgroup or departmental LAN because it requires less cabling length.
3. Any one computer or device being down does not affect the others.
4. Fast as compare to ring topology.

Disadvantages:

1. Can not connect a large number of computers.
2. A fault or break in the bus cable stops all transmission.
3. Difficult to identify the problem if the entire network shuts down.
3. Collision may occur.
4. Signal reflection at the taps can cause degradation in quality.
5. Used for only small network.
6. Heavy network traffic can slow a bus considerably.

1.2.4 Ring Topology

- Each device in Ring topology has a dedicated point-to-point line configuration only with the two devices on either side of it, (Dedicated means that the link carries traffic only between the two devices is connects.)
- In ring topology, the computers in the network are connected in circular fashions which form of a ring.
- In other words, in ring topology, each computer is connected to the next computer, with the last one connected to the first, or we can say each device is connected to other two devices with dedicated link in one direction, from device to device.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. Computers are connected on a single circle of cable.
- Ring networks normally use some form of token-passing protocol to regulate network traffic. The token is passed from one computer to the next, only the computer with the token can transmit.
- The receiving computer strips the data from the token and sends the token back to the sending computer with an acknowledgment.
- After verification, the token is regenerated. Ring topology is a network topology in the form of a closed loop or circle, with each node in the network connected to the next. Messages move in one direction around the system.
- When a message arrives at a node, the node examines the address information in the message. If the address matches the node's address, the message is accepted; otherwise, the node regenerates the signal and places the message back on the network for the next node in the system.
- This regeneration allows a ring network to cover greater distances than star networks or bus networks.
- The failure of a single node can disrupt network operations; however, fault tolerant techniques have been developed to allow the network to continue to function in the event one or more nodes fail.

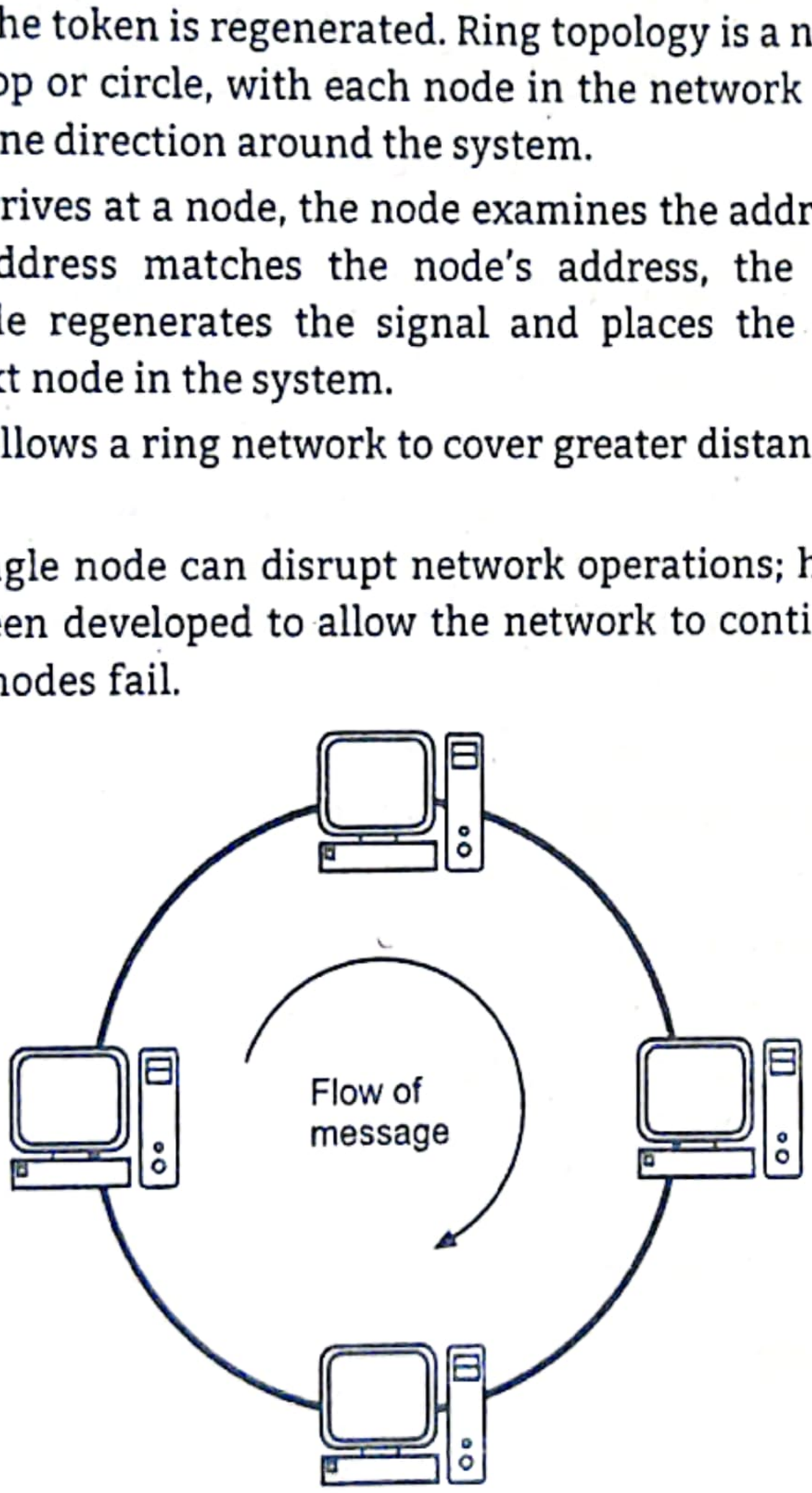


Fig. 1.10(a): Ring Topology

- **Examples:** Ring topology usually seen in a Token Ring or FDDI (Fiber Distributed Data Interface) network.

Illustration of Ring Topology:

- In ring topology, each node functions as a repeater. Suppose, in Fig 1.10(b) ring operates in clockwise direction i.e. data is transferred from one node to another in

clockwise direction and node "B" wants to transmit data to node "A". Node "B" wil first prepare the frame, and then forward it towards node "C". Node "C" examines the frame and ignores it. Node "C" simply forwards it to node "A". Node "A" accepts the frame, because its intended for it.

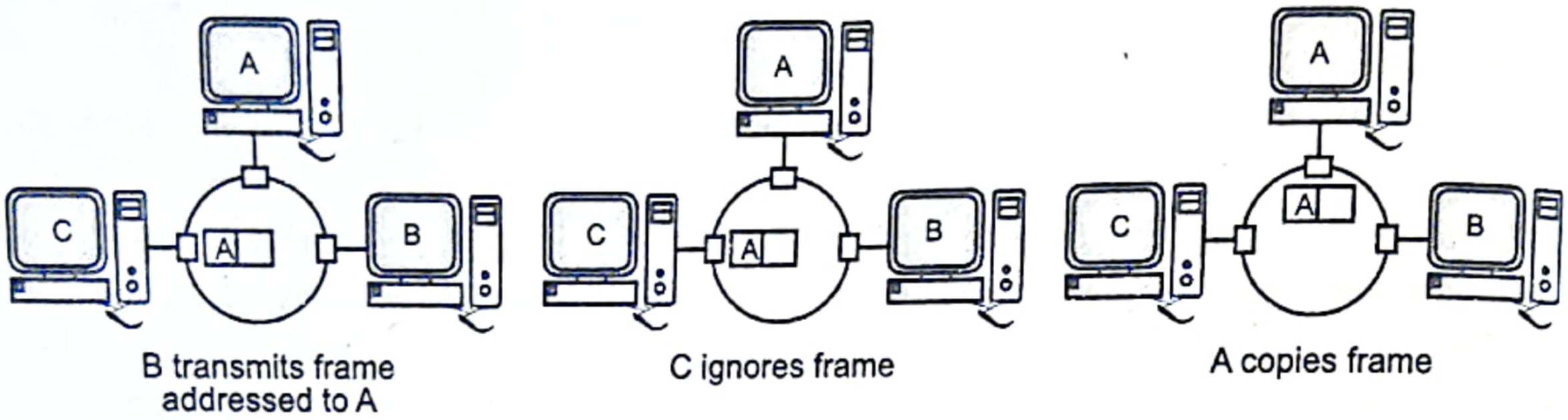


Fig. 1.10 (b): Example of Ring topology

Advantages:

1. Require less cabling so is less expensive.
2. Fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.
4. Reduces chances of collision.
5. Each computer has equal access to resources.
6. There is no need for network server to control the connectivity between workstations.

Disadvantages:

1. The major disadvantage of a physical ring topology is its sensitivity to single link failure. If one connection between two stations fails or a bypass for a particular inactive station is malfunctioning, the ring traffic is down.
2. Traffic is unidirectional.
3. Slow in speed.
4. Reconfiguration is required i.e. to add one node, whole network must be down first.

1.2.5 Tree Topology

- **A tree topology** is variation of a star topology. In tree topology not every device plugs to the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub.
- A tree topology can also combines characteristics of linear bus and star topologies.
- It consists of groups of star-configure workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network and enable schools to configure a network to meet their needs.

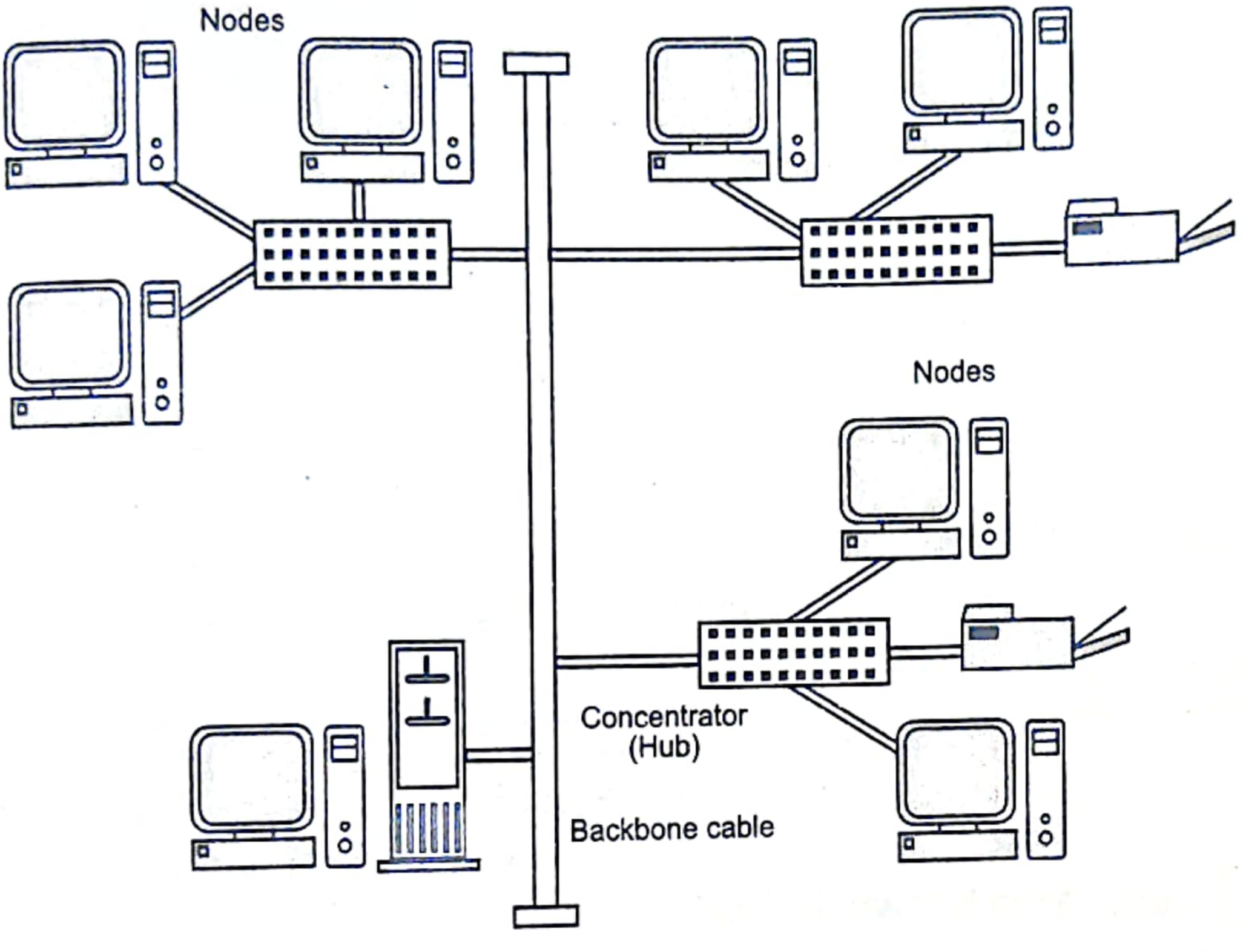


Fig. 1.11: A Tree Network

Advantages:

1. Easy to install, reconfigure and wire.
2. Robustness: If one link fails, only that link is affected.
3. Fast as compare to ring topology.
4. Multiple devices can transfer data without collision.
5. Eliminates traffic problem.
6. No disruptions to the network then connecting or removing devices.
7. Easy to detect faults and to remove parts.
8. Supported by several hardware and software venders.

Disadvantages:

1. If central node (hub or switch) goes down then entire network goes down.
2. More cabling is required than bus topology, so expensive than bus topology.
3. More expensive than bus topologies because of the cost of the concentrators (hub or switch).

1.2.6 Hybrid Topology

- A hybrid topology is combination of two or more network topologies. Fig. 1.12 shows a hybrid star and Bus topologies.

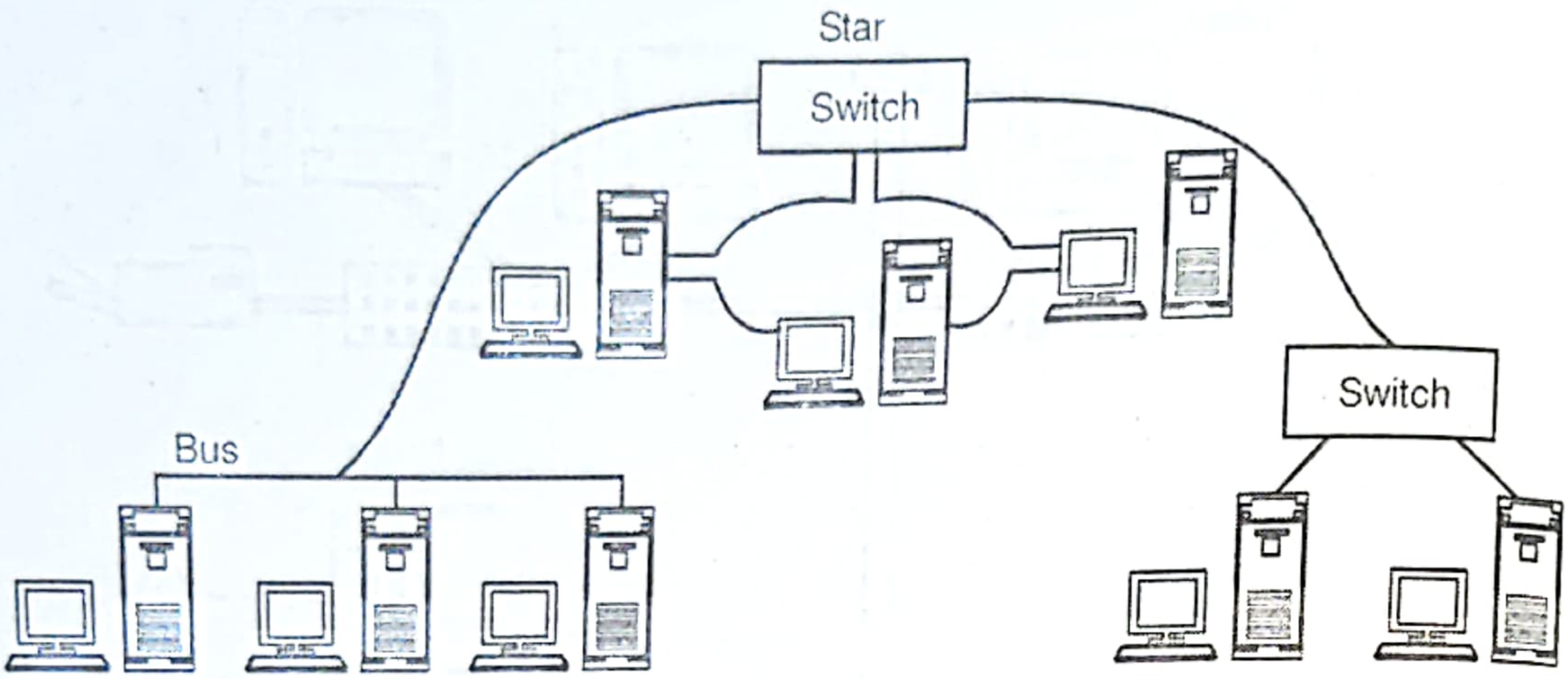


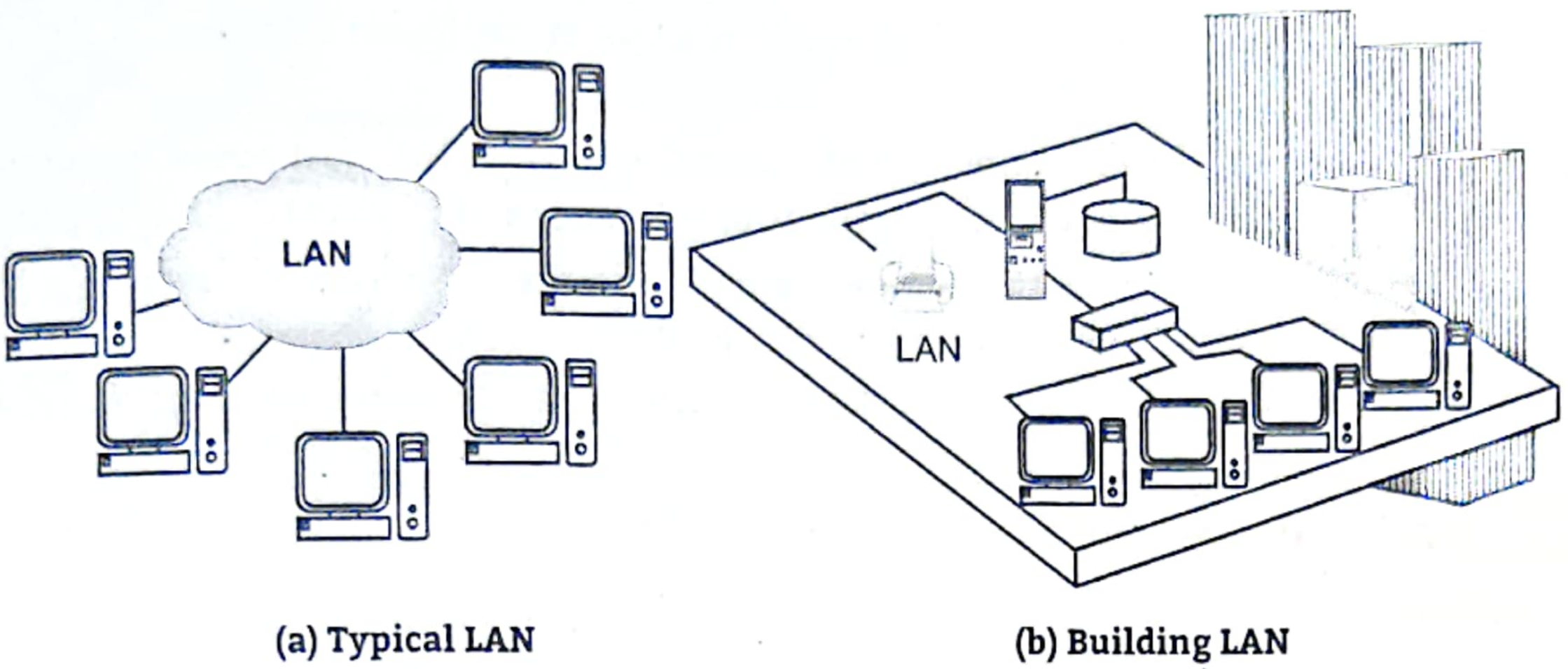
Fig. 1.12: Hybrid Topology

1.3 TYPES OF NETWORK (S-22)

- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

1.3.1 Local Area Network (LAN) (S-19)

- LAN is a group of computers and associated peripheral devices connected by a communications channel, capable of sharing files and other resources among several users.
- Local area networks are privately-owned networks covering a small geographical area, (less than 1 km) like a home, office, or groups of buildings.
- Depending on the needs of the organization and the type of technology used, a LAN can be as simple as two PCs and a printer or it can extend throughout an organization.
- LANs are widely used to connect personal computers and workstations to share resources like printers and exchange information.
- LANs are distinguished from other kind of networks by three characteristics i.e., their size, their transmission technology and their topology.
- Generally, LAN will use only one type of transmission medium wired or wireless. The most common LAN topologies are bus, ring or star.
- Early LAN had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 to 1000 mbps. Wireless LANs are the newest evolution in LAN technology.
- At present, LANs are being installed using wireless technologies. Such a system makes use of access point or APs to transmit and receive data. One of the computers in a network can become a server serving all the remaining computers called clients.
- For example, a library will have a wired or wireless LAN network for users to interconnect local networking devices. For example, Printers and Servers to connect to the Internet.



(a) Typical LAN (b) Building LAN

Fig. 1.13

1.3.1.1 Components of LAN [W-18]

- LAN components are configurable in a variety of ways, but a LAN always requires the same basic components.
- PCs/workstations and servers.
- Network Interface Card (NIC): A network card is a component that allows the computer to communicate across a network. This component is frequently built into the motherboard of today's computers, but it can also be a separate card for use in a PCI slot, or part of an external unit that connects to the computer via a USB port.
- Cabling and connectors, for example, coaxial cable and BNC connector, Unshielded Twisted Pair (UTP) and RJ-45 connector.
- Hub, concentrator, and more complicated network devices such as Bridge, LAN Switch and Router.

1.3.1.2 Working of LAN [S-18; W-19]

- Before you can link computers into a LAN, you must install a network-aware operating system on them to enable them to share resources.
- The choice of operating system depends on whether the network will be a peer-to-peer network or a server-based network.
- Microsoft Windows 98 is a good choice for peer-to-peer workgroup LANs, while Windows NT and Windows 2000 offer the security and scalability needed to support a server-based network.
- Next, you choose a networking architecture. Then you must install a suitable Network Interface Card (NIC) in an available slot on the motherboard of each node (computer) in the network.
- You must also install a software driver to control the card's functions. You use cabling to join the NICs in order to enable the computers to communicate with each other.

- The most common type of cabling used in LANs is unshielded twisted-pair (UTP) cabling.
- The cabling is installed in some kind of topology or layout, the most popular of which is the cascaded star topology used in the 10BaseT version of Ethernet.
- You then choose a protocol to enable the nodes on the network to speak a common "language"; the most popular protocol is TCP/IP, especially for Internet connectivity, although for small stand-alone workgroup LANs that use Windows 95 or Windows 98/Me, NetBEUI is still popular.

1.3.1.3 Advantages and Disadvantages of LAN

Advantages:

1. The reliability of network is high because the failure of one computer in the network does not effect the functioning for other computers.
2. Addition of new computer to network is easy.
3. High rate of data transmission is possible.
4. Peripheral devices like magnetic disk and printer can be shared by other computers.
5. Less expensive to install.

Disadvantages:

1. Used for small geographical Areas.
2. Limited computers are connected in LAN.
3. Special security measures are needed to stop users from using programs and data that they should not have access to network.
4. Networks are difficult to set up and need to be maintained by skilled technicians.
5. If the file server develops a serious fault, all the users are affected, rather than just one user in the case of a stand-alone machine.

1.3.1.4 Uses of LAN

- Following are the major areas where LAN is normally used:
  1. File transfers and Access
  2. Word and Text processing
  3. Electronic message handling
  4. Remote database access
  5. Personal computing
  3. Digital voice transmission and Storage
  7. Office automation
  8. Factory automation
  9. Distributed computing

10. Fire and Security systems
11. Process control
12. Document distribution.

1.3.2 Metropolitan Area Network (MAN)

- If a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city then this network is called Metropolitan Area Network (MAN).
- MAN is an extended face of LAN, in which computing devices spread over a city are interconnected with communication mediums to form a network.
- Geographical area for MAN lies between 16 km to 50 km generally covers towns and cities. In this type of networks data is transmitted over one or two cables.

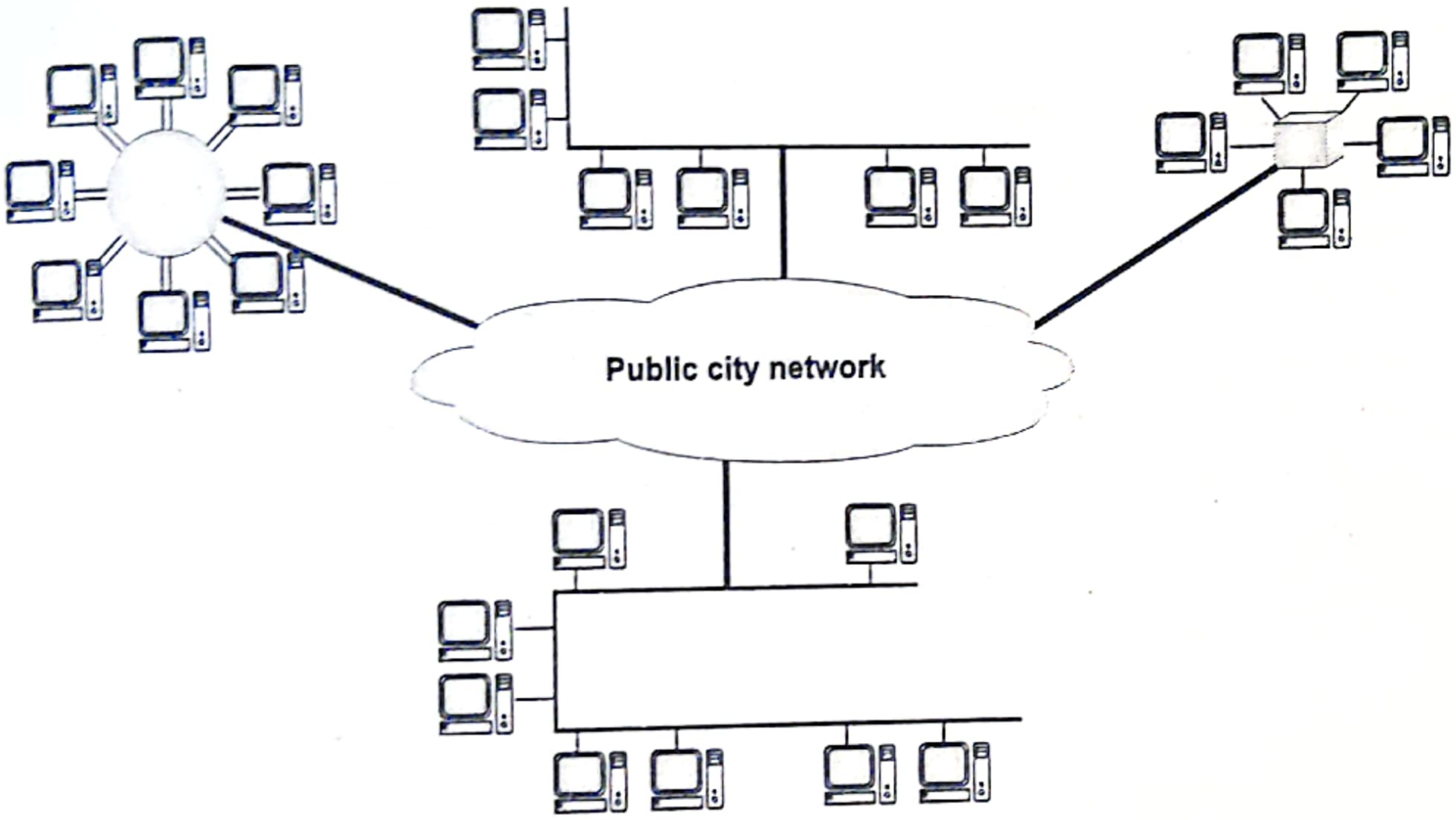


Fig. 1.14: Metropolitan Area Network

- Multiple networks that are connected within the same city to form a citywide network for a specific government or industry.
- By interconnecting smaller networks within a large geographic area, information is easily disseminated throughout the network. Local libraries and government agencies often use a MAN to connect to citizens and private industries. ATM (Asynchronous Transfer Modes), FDDI (Fiber Distributed Data Interface) etc. are the technologies used in MAN.
- A MAN may be wholly owned and operated by a private company. Number of LANs connected so that resources may be shared LAN-to-LAN as well as device-to-device. For example, cable television network.

1.3.2.1 Advantages and Disadvantages of MAN

Advantages:

1. MAN spans large geographical area than LAN.
2. MAN falls in between the LAN and WAN therefore, increases the efficiency of handling data.
3. MAN saves the cost and time attached to establish a wide area network.
4. MAN offers centralized management of data.
5. MAN enables us to connect many fast LANs together.

Disadvantages:

1. Cost is high.
2. Speed is slow.

1.3.3 Wide Area Network (WAN)

- A network that connects users across large distances, often crossing the geographical boundaries of cities or states.
- WANs utilize public, leased, or private communication devices.
- A WAN provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, or even whole world.
- A geographically distributed network composed of Local Area Networks (LANs) joined into a single large network using services provided by common carriers.
- WANs are commonly implemented in enterprise networking environments in which company offices are in different cities, states, or countries or on different continents.

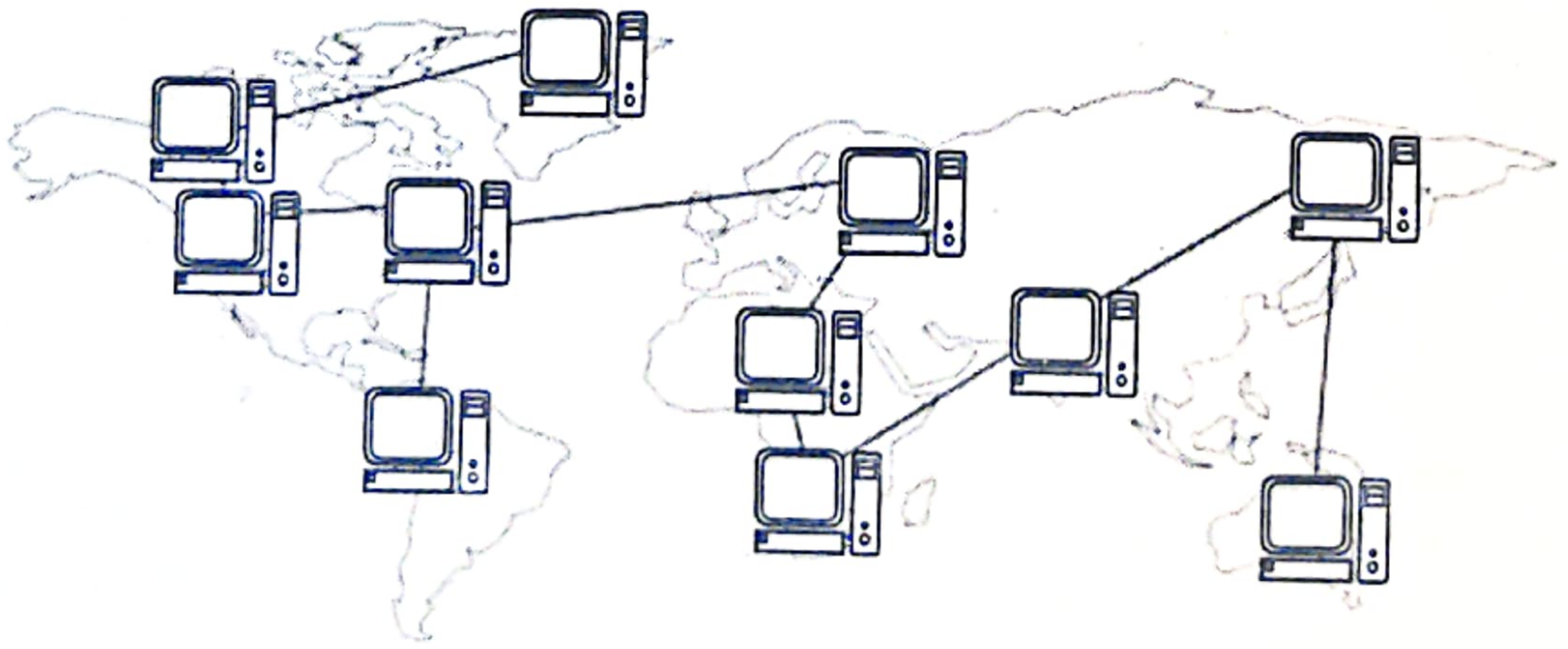


Fig. 1.15: Wide Area Network

- A WAN that is entirely owned and used by a single company is often referred to as an enterprise network.

- Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the different LANs using services such as dedicated leased phone lines, dial-up phone lines (both synchronous and asynchronous), satellite links, and data packet carrier services.
- Wide area networking can be as simple as a modem and remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked using special routing protocols and filters to minimize the expense of sending data sent over vast distances.
- A WAN is a geographically dispersed collection of LANs. A wide area network is simply a LAN of LANs or Network of Networks.
- WAN are characterized by the slowest data communication rates and the largest distances.
- Wide Area Networks are commonly connected either through the Internet or special arrangements made with phone companies or other service providers.
- WAN may use advanced technologies like Asynchronous Transfer Mode (ATM), Frame Relay and SONET.
- Internet, Indian Railway Reservation System, Bank Networks that supported core banking, etc. are some good examples of WAN. The Internet is the largest WAN, spanning the World today.
- LAN's and WAN's come in many different flavors. The most popular type of network is Ethernet. Ethernet networks have speeds of 10 Mbps, 100 Mbps, or 1 Gbps.

1.3.3.1 Architecture of Wide Area Network

- WAN contains a collection of machines used for running user (i.e. application) programs. All the machines called hosts are connected by a communication subnet.

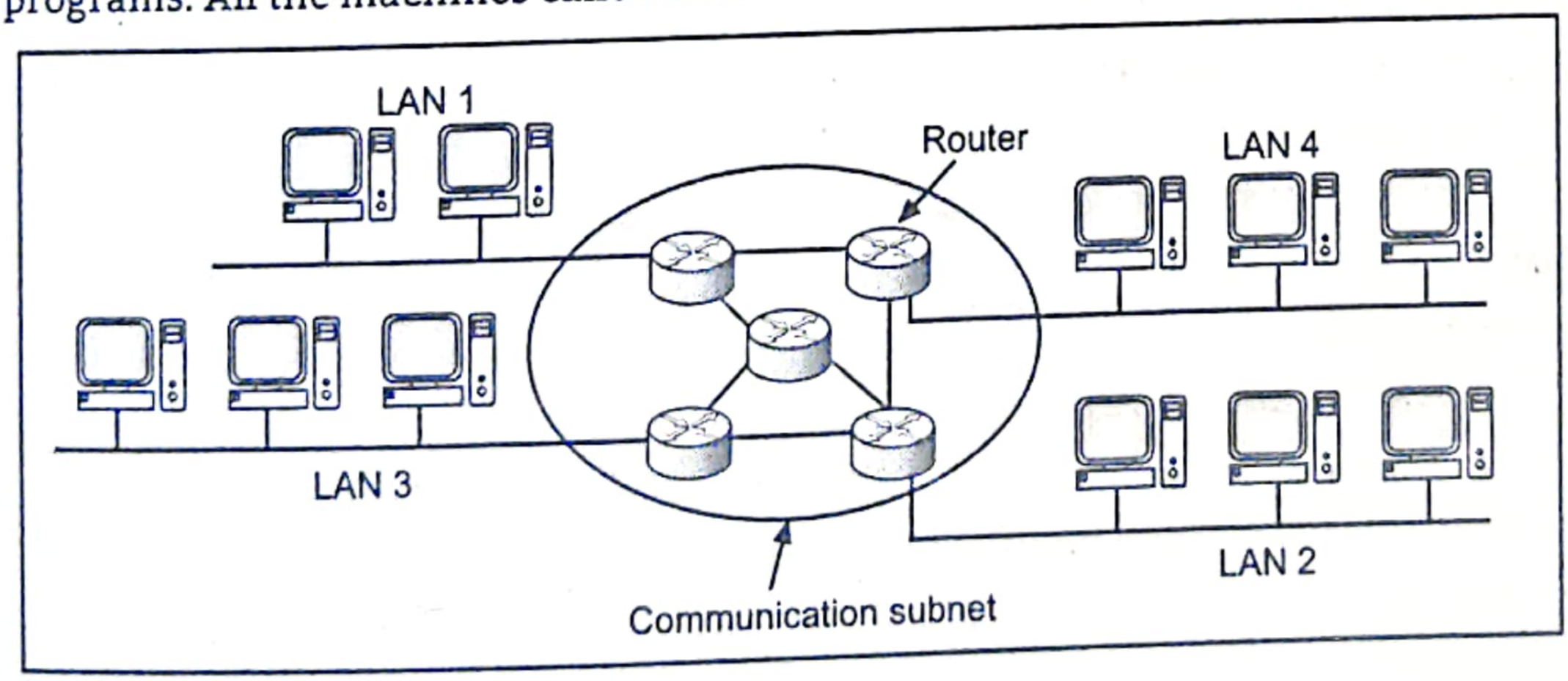


Fig. 1.16: Communication Subnet in WAN

- The function of the subnet is to carry messages from host to host. The subnet consists of two important components; transmission lines and switching elements.

- Transmission lines move bits from one machine to another. The switching elements are specialized computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line to forward them.
- The switching elements are either called as packet switching nodes, intermediate systems, data switching exchanges or routers.
- When a packet is sent from one router to another via one or more intermediate routers, the packet is received at intermediate router. It is stored in the routers until the required output line is free and then forwarded. A subnet using this principle is called a Point to Point, store-forward or Packet Switched Subnet.
- WAN's may use public, leased or private communication devices, and can spread over a wide geographical area. A WAN that is entirely owned and used by a single company is often called as an Enterprise Network.

1.3.3.2 Characteristics of WAN

- Followings are the major characteristics of WAN.

1. **Communication Facility:**
   - For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas communications.
   - Computer conferencing is another use of WAN where users communicate with each other through their computer system.
2. **Remote Data Entry:**
   - Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities.
   - For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.
3. **Centralized Information:**
   - In modern computerized environment you will find that big organizations go for centralized data storage.
   - This means if the organization is spread over many cities, they keep their important business data in a single place.
   - As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site.

Advantages:

1. Allows many people to use the same network from many different locations.

2. Used for Large Geographical Area.
3. Expensive devices (like printers or phone lines to the internet etc.) can be shared by all the computers on the network.
4. Adds fluidity to user's information communication.

Disadvantages:

1. Protection against hackers and viruses adds more complexity and expense.
2. Setting up a network can be time consuming.
3. Can be expensive.
4. Slow in speed than LAN and MAN.
5. WANs need a good firewall to restrict outsiders from entering and disrupting the network.

Difference between various types of Networks:

Table 1.1: Difference between LAN, MAN and WAN

Sr. No.	Parameters	LAN	WAN	MAN
1.	Stands for	Local Area Network.	Wide Area Network.	Metropolitan Area Network.
2.	Area covered	Covers small area i.e. within the building (less than 1 km).	Covers large geographical area, like country, state etc.	Covers larger area than LAN and smaller than WAN like city, campus.
3.	Error rates	Lowest.	Highest.	Moderate.
4.	Transmission speed	High.	Low.	Moderate.
5.	Equipment cost	Uses inexpensive equipment.	Uses most expensive equipment.	Uses moderately expensive equipment.
6.	Example	Offices, Cyber Café.	Internet.	ATM, FDDI etc.
7.	Data transfer rate	High.	Low.	Moderate.
8.	Setup cost	Low.	High.	Moderate.

1.3.4 Internetwork (S-19)

- Today, it is very rare to see a LAN, a MAN in isolation, they are connected to one another. When two or more networks are connected, they become an Internetwork or Internet.

- An internetwork is formed when distinct networks are interconnected. The Internet is a structured organized system.
- Internetworking started as a way to connect different types of computer networking technology.
- Computer network term is used to describe two or more computers that are linked to each other. When two or more computer networks or computer network segments are connected using devices such as a router then it is called as Computer Internetworking.
- Internetworking is a term used by Cisco. Any interconnection among or between public, private, commercial, industrial, or governmental computer networks may also be defined as an internetwork or Internetworking.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks.
- 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.

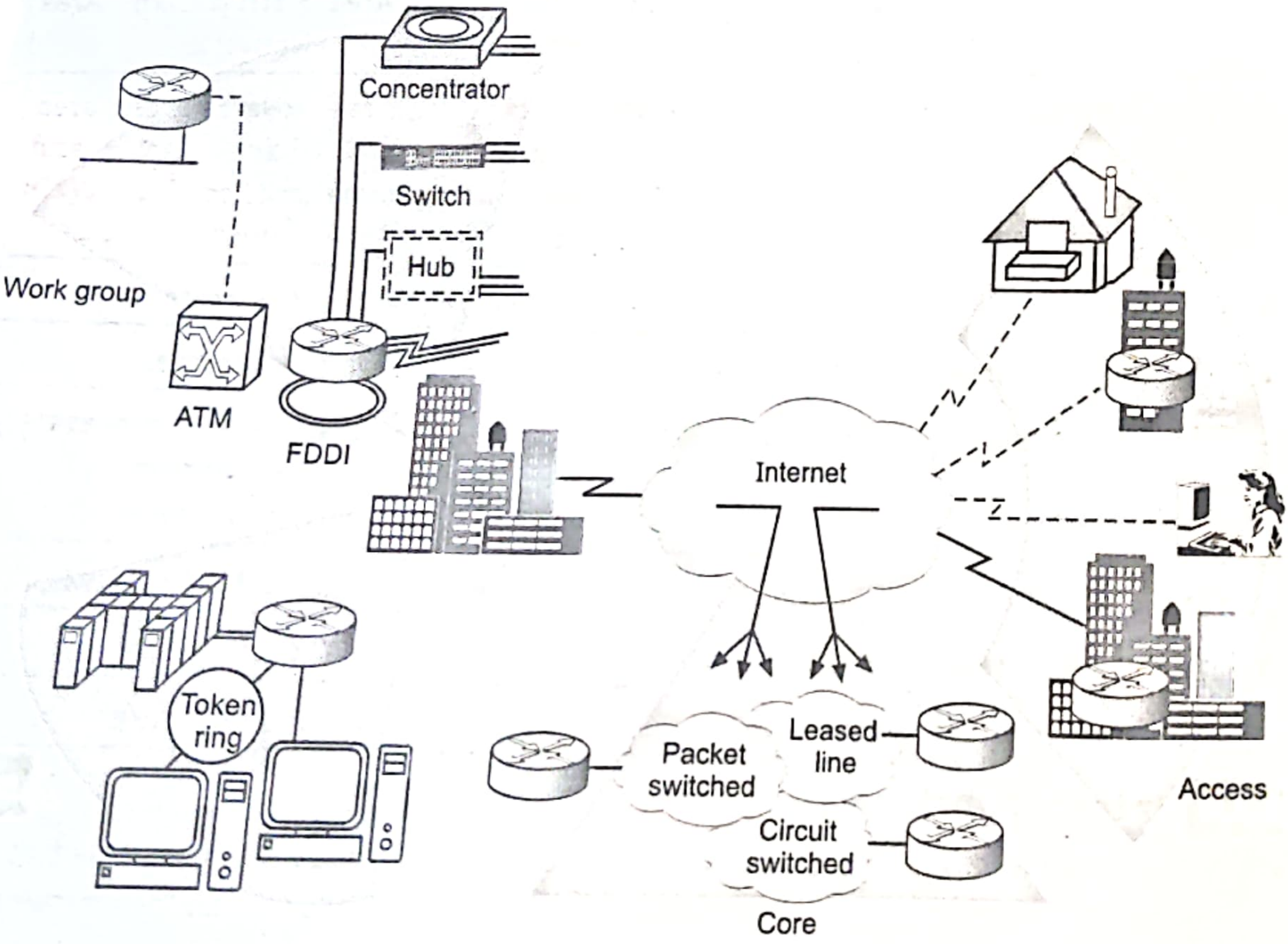


Fig. 1.17: Internetworking

- Today, most end users who want Internet connection use the services of Internet Service Providers (ISPs). There are international, national, regional and local service providers.
- There are following variants of Internetwork or Internetworking:

1. **Intranet:** An intranet is a set of interconnected networks or Internetworking, using the Internet Protocol and uses IP-based tools such as web browsers and FTP tools that are under the control of a single administrative entity.
2. **Extranet:** An extranet is a network of internetwork or Internetworking, that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities.
3. **Internet:** It is a network of networks based on many underlying hardware technologies, but unified by an internetworking protocol standard, the Internet Protocol Suite. It is often also referred as TCP/IP.

Advantages of Internetworking:

1. Internetworks reduce network traffic.
2. The benefit of reduced traffic is optimized performance.
3. Network problems can be more easily identified and isolated in smaller networks, as opposed to one large network.
4. We can more efficiently span long distance by connecting multiple smaller networks.

1.3.5 Wireless Network

- Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.
- The word wireless is dictionary defined as "having no wires".
- In networking terminology, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but rather the network is connected by radio waves and/or microwaves to maintain communications.
- The basis of wireless systems is radio waves, an implementation that takes place at the physical level of network structure.

1.3.5.1 Types of Wireless Network

- Wireless networks can be divided into three main categories as System Interconnection, Wireless LANs, and Wireless WANs.

1. System Interconnection:

- System interconnection means connecting the components of computer using short range radio.
- All components can also be connected by a short range wireless network called Bluetooth. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer.

- The system interconnection networks use the Master-Slave paradigm as shown in Fig. 1.18.

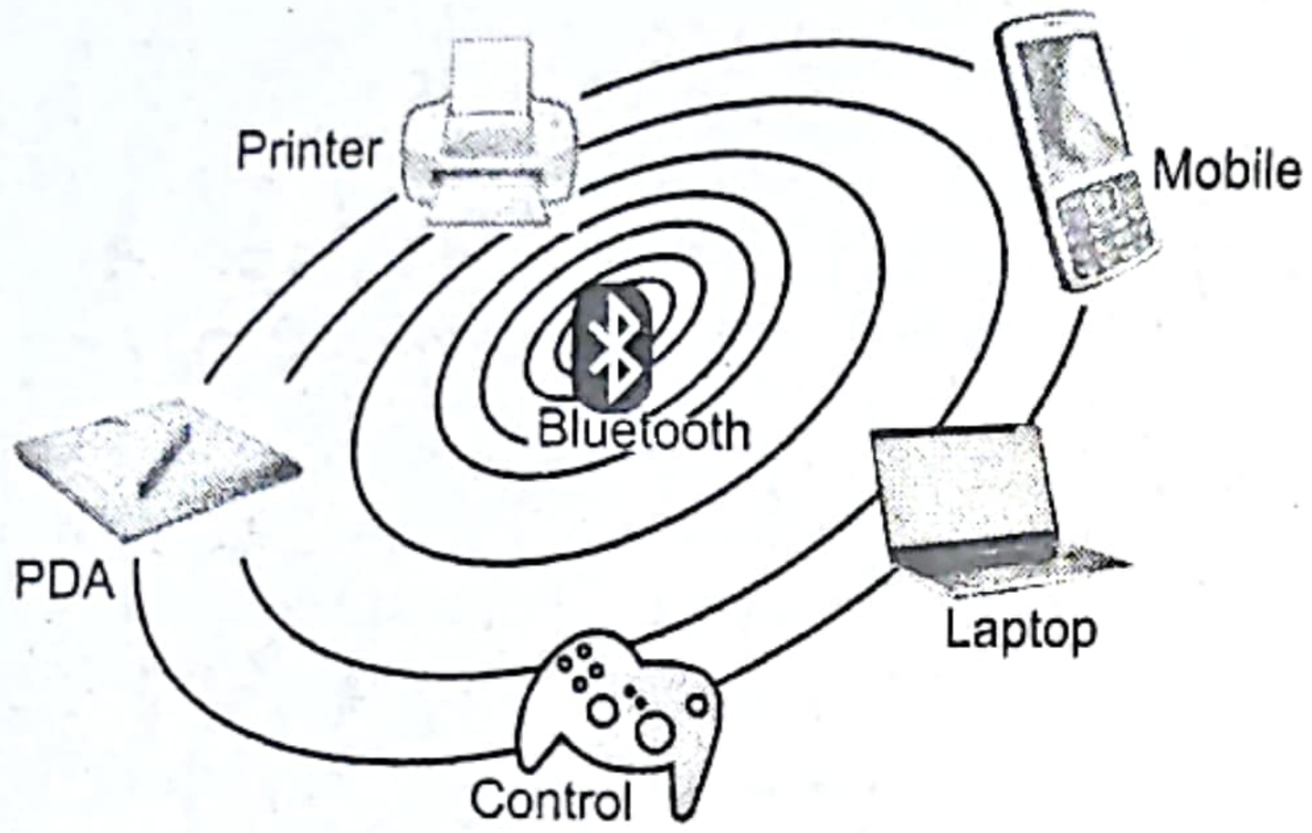


Fig. 1.18: Bluetooth Configuration

2. Wireless LANs:

- The next step in wireless networking is the wireless LANs. WLANs are systems in which every computer has a radio modem and antenna with which it can communicate with other system.
- Wireless LANs are becoming increasingly common in small offices and homes.
- IEEE 802.11 is a standard for wireless LANs.

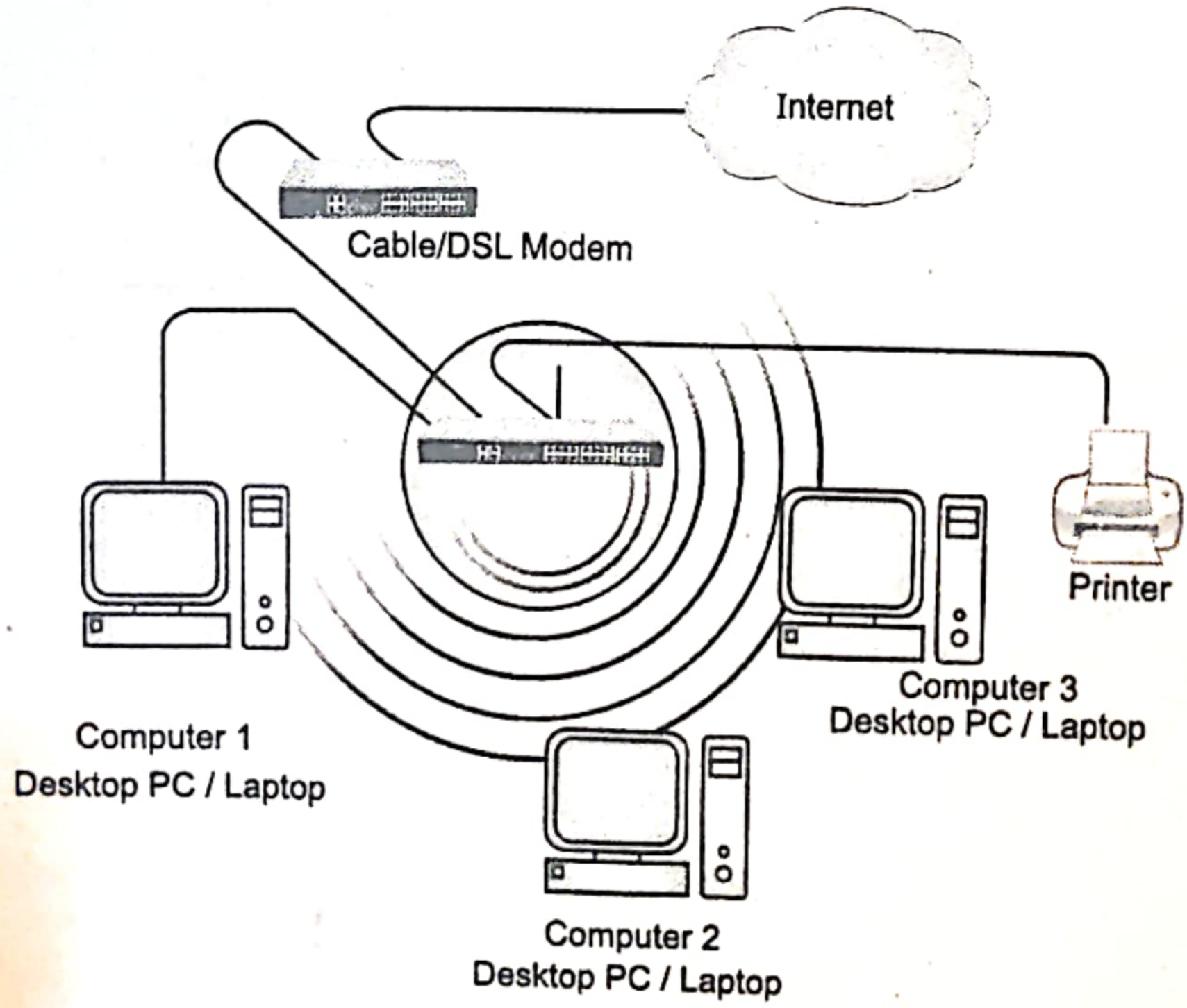


Fig. 1.19: Wireless LAN

- A Wireless Local Area Network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access.

3. Wireless WANs:

- The third kind of wireless network is used in wide area system.
- The radio network used for cellular telephones is an example of a low-bandwidth wireless system.
- Cellular wireless networks are like wireless LANs except that the distances involved are much greater and the bit rates are much lower.
- In addition to low-speed networks, high bandwidth wide area wireless networks are also being developed. The initial use is high speed wireless internet access from homes and business bypassing the telephone system.
- Wireless Wide Area Networks (WWANs) are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system.

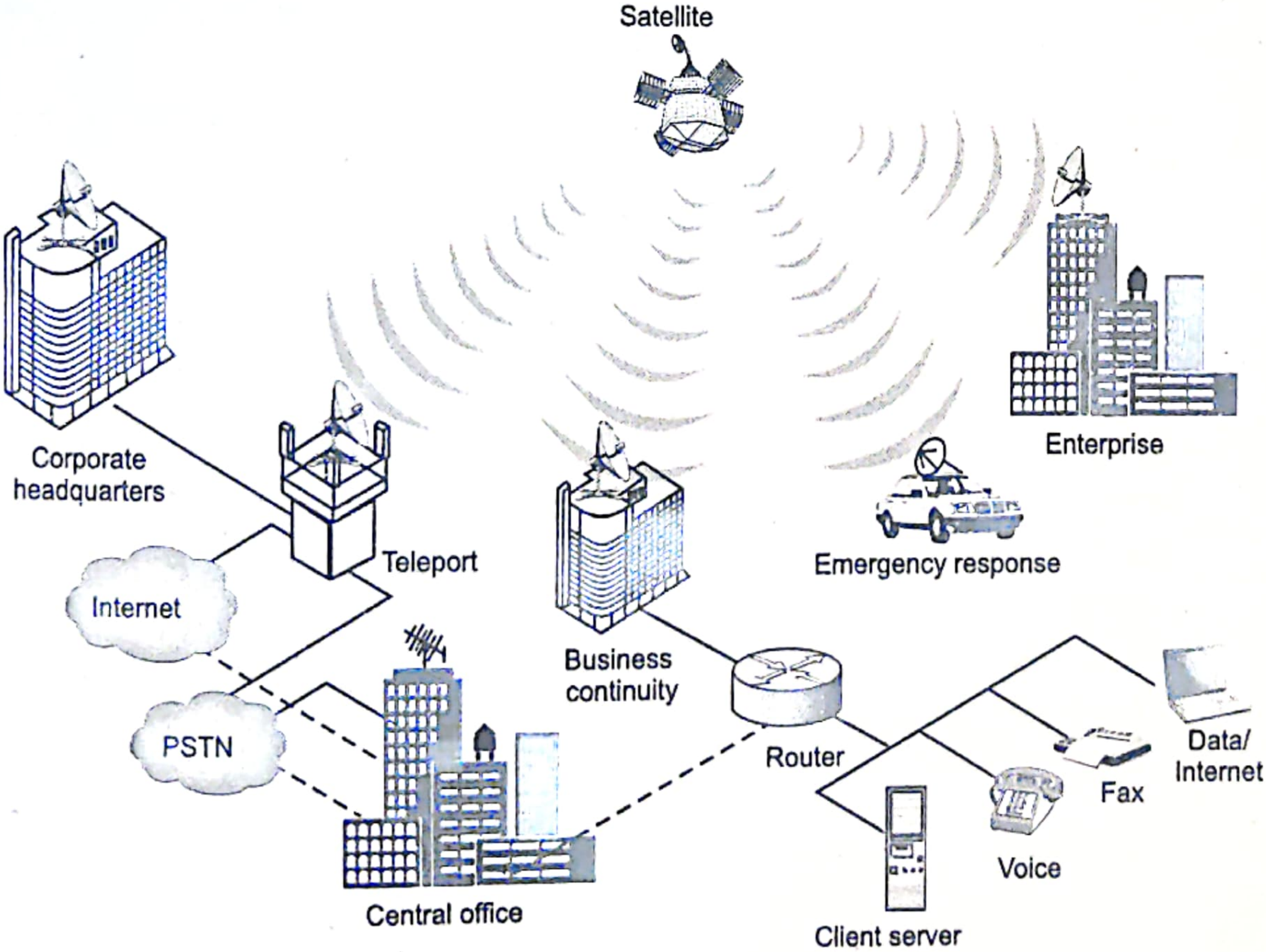


Fig. 1.20: WWAN

1.4 MODES OF COMMUNICATION (S-18, S-19, W-18, S-22, W-2

- In data communication, the exchange of information takes place throug transmission modes which defines the direction of the flow of information betwee two communication devices i.e. it tells the direction of signal flow between the tw devices.
- Communication between two devices can be Simplex, Half-duplex or Full duple transmission modes..

1.4.1 Simplex

- 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.

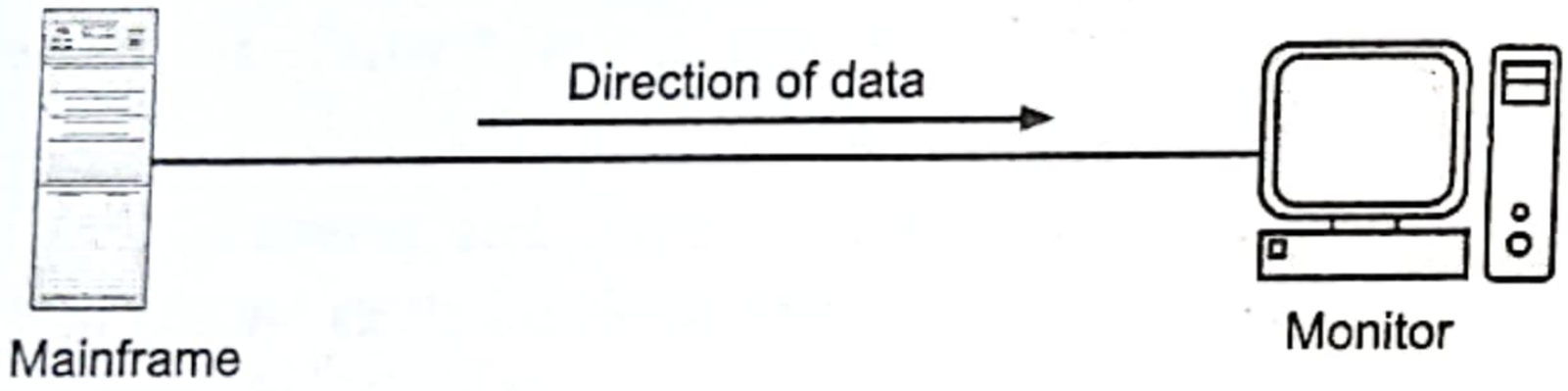


Fig. 1.21: Simplex Mode

- Simplex means communication runs in one direction. The examples includes:
  (i) TV and radio broadcasting or pager.
  (ii) Keyboards and traditional monitors are both examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
- Simplex transmission occurs in many common communication applications, the most obvious being broadcast and cable television.
- It is not used in true network communication because stations on a network generally need to communicate both ways.
- Some forms of network communication might seem to be simplex in nature, such as streaming audio or video, but the communication actually takes place using bidirectional network traffic, usually Transmission Control Protocol (TCP) traffic.

1.4.2 Half Duplex

- In half-duplex mode, each station can both transmit and receive, but not at the same time. For half-duplex, both end devices can send and receive, (they must alternate). When one device is sending, the other can only receive, and vice versa.

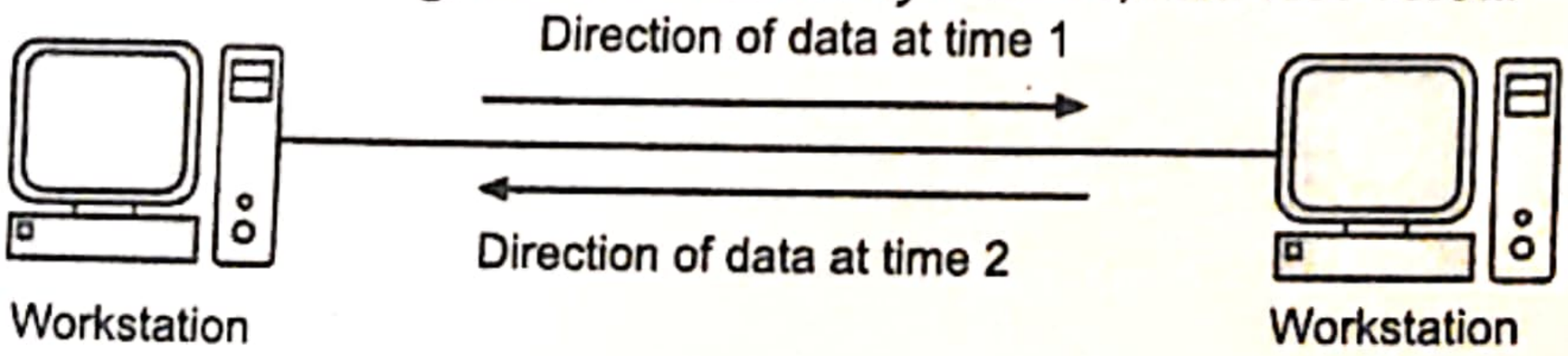


Fig. 1.22: Half-duplex Mode

- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- The simplest example is a walkie-talkie: You have to press a button to talk and release the button to listen. When two people use walkie-talkies to communicate, at any given moment, only one of them can talk while the other listens. If both try to talk simultaneously, a collision occurs and neither hears what the other says.
- Communication through traditional Ethernet networks is another example of half-duplex communication. When one station on an Ethernet transmits, the other stations detect the carrier signal and listen instead of transmitting. If two stations transmit signals simultaneously, a collision occurs and both stations stop transmitting and wait random intervals of time before retransmitting.

1.4.3 Full Duplex

- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously. The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
- In full-duplex mode, signals going in either direction share the capacity of the link.

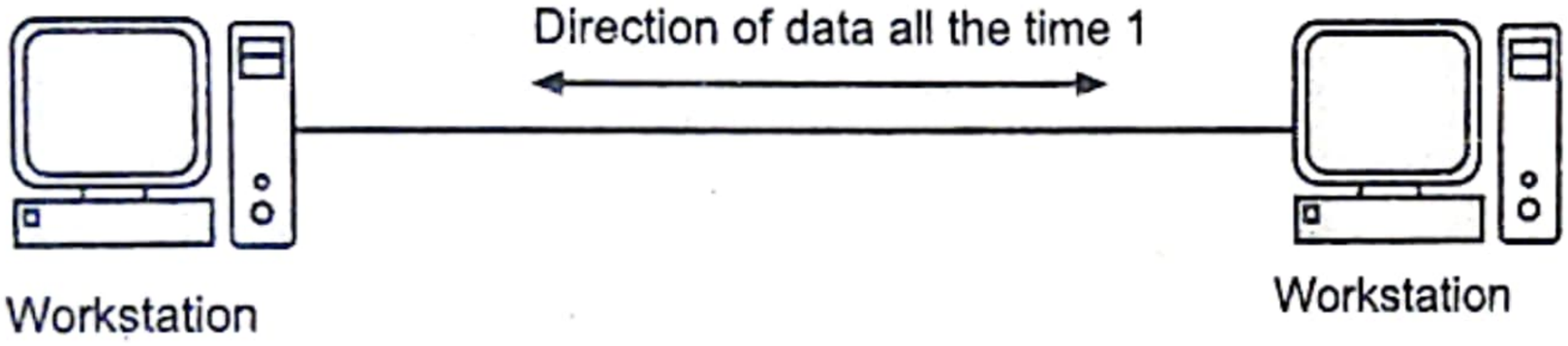


Fig. 1.23: Full-duplex Mode

- Sharing of link 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 of the channel is divided between signals travelling in both directions.
- For example, mobile phones operate in full-duplex mode when two persons talk on mobile phone, both can listen and speak simultaneously.
- In full-duplex communication, both stations send and receive at the same time, and usually two communication channels are required. However, you can also achieve full-duplex communication using a multiplexing technique whereby signals travelling in different directions are placed into different time slots.
- The disadvantage of this technique is that it cuts the overall possible transmission speed by half.

1.5 SERVER BASED LANS & PEER-TO-PEER LANS (S-18, 19 W-18)

- The PC requires operating system to manage the files and hardware. Similarly, LAN needs the NOS (Network Operating System) which controls the transmission of data and messages between workstations.

- In the simplest case, the NOS makes the disk drive on the server appear to be an extra drive (F:) on each workstation.
- The NOS also make a LAN printer appears as a locally attached printer at your workstation.
- They are of two types:
  1. Server-based LAN.
  2. Peer-to-peer LAN.
- The server-based LAN, a separate, unattended computer acts as a file server whereas in peer-to-peer LAN, a workstation may acts as a workstation and file server simultaneously.

1.5.1 Server-Based LAN (S-22)

- These LANs offer better performance and increased the reliability.
- Network operating system such as Novell network is installed on a file server which replaces the DOS completely.
- The file server organizes the disk in a way that performs well for large files. This is referred as dedicated server LAN.
- Companies that offer server based LANs are Apple Talk, Wrap Server, Vines, Netware, and Windows NT Server.
- The diagrammatic representation of Server based LAN is as shown in Fig. 1.24.

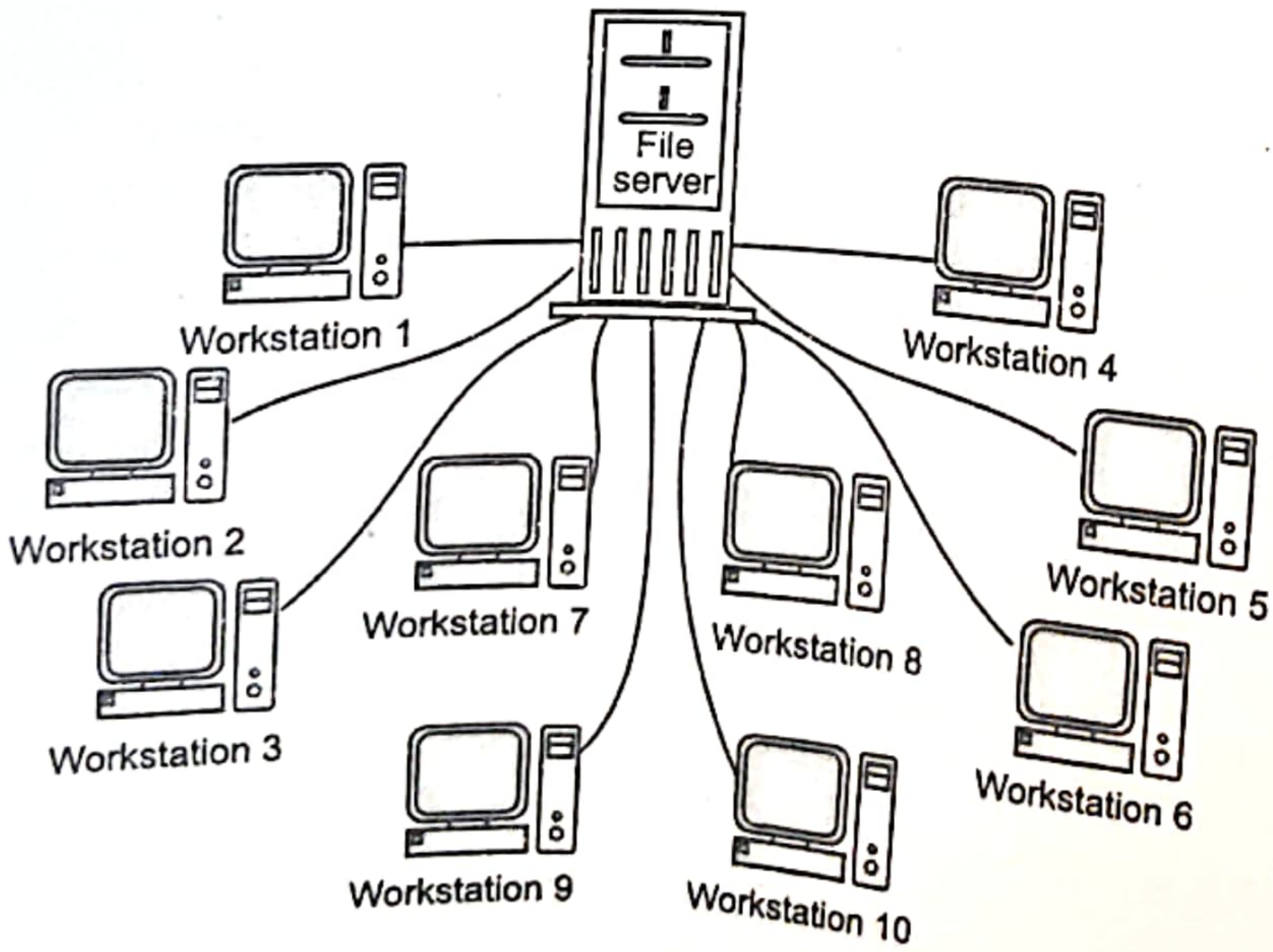


Fig. 1.24: Server Based LANs

1.5.2 Peer-to-Peer LAN (S-22)

- In this LAN, only one machine will work as workstation and a file server.
- This is not a dedicated machine. Fig. 1.25 shows Peer-LAN environment, in which three desktop computers acts as both file server and workstation.
- In a peer LAN, the disk space and files on your computer become communal property. Peer LANs are cost effective for small, lightly loaded networks.
- The advantage of this LAN is that user don't have to remember to copy files from their computers be a separate file server for other people to access.
- Obviously this access is depends upon the security and rights given to the users.

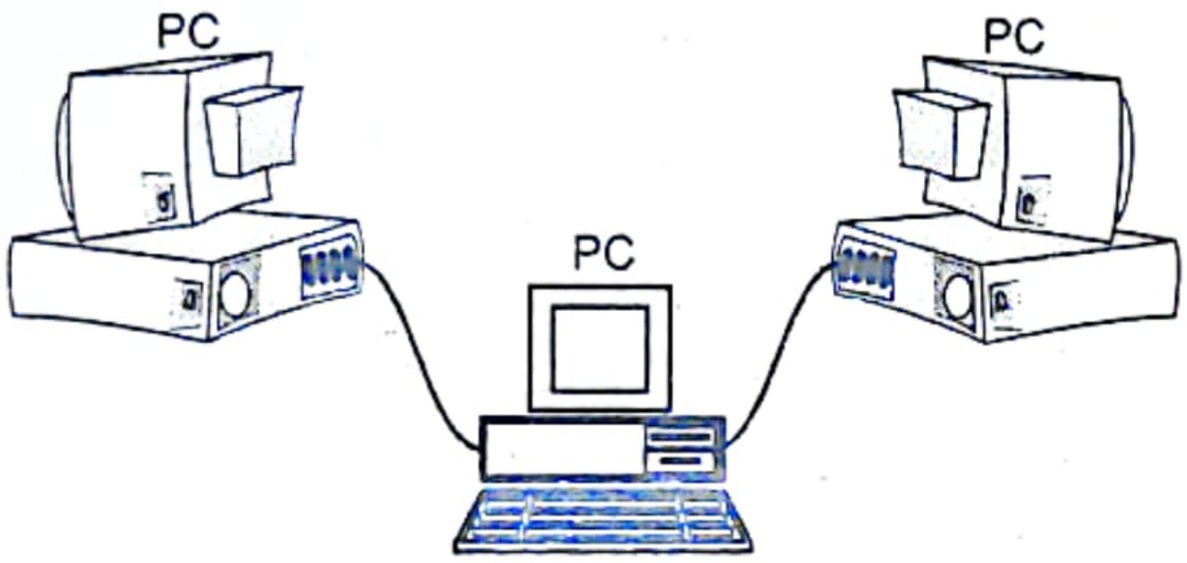


Fig. 1.25: Peer-to-Peer LAN

- The companies that offer peer LAN's are 10NETplus, EasyNet, AppleTalk, GVLANOS, Ready Link, NET/30 etc.
- The NOS is installed on a file server machine and this network software is installed on each machine. They communicate through protocol.
- A list of NOS is given below in Table. But most popular NOS is Novell Netware.

Table 1.2: List of Various Network Operating Systems

Operating system	Manufacturer
AppleTalk	Apple
LANtastic	Artisoft
Netware	Novell
Network File System (NFS)	Sun microsystem
Wrap server	IBM
Wrap connect	IBM
Vines	Banyan
Window NT server	Microsoft
Windows for workgroup	Microsoft

1.5.3 Comparison of Server-based LAN and Peer-to-Peer LAN (S-19)

Table 1.3: Difference between Server-based LAN and Peer-to-Peer LAN

Sr. No.	Server-based LAN	Peer-to-Peer LAN
1.	Server-based LAN a separate, unattended computer acts as a file server.	Peer-to-peer LAN, a workstation may acts as a workstation and file server.
2.	Server-based LAN also referred as dedicated server LAN.	Peer-to-peer LAN is not dedicated machine.
3.	High performance.	Low performance.
4.	More reliable.	Less reliable.
5.	Costly for small network.	Cost effective for small networks.
6.	Examples: (i) Apple Talk, (ii) WrapServer	Examples: (i) EasyNet, (ii) 10NetPlus

1.6 PROTOCOLS AND STANDARDS (S-18, W-18, S-23)

- Protocol is very important for networking without a protocol network is meaningless. The sender and the receiver, the two parties in data communication must agree on a common set of rules, i.e. protocols before they can communicate with each other.
- A protocol is a set of rules that governs the communications between computers on a network. The sender and the receiver, the two parties in data communication must agree these rules before they can communicate with each other.
- These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.
- In networking many protocols are available, some of which are more popular than others.
- Two networking devices wishing to communicate with each other cannot just begin data transmission arbitrarily, i.e. one device cannot simply start sending bit streams to the other. The two networking devices must agree on a set of rules before this transmission can begin.

Terms:

- A protocol defines the following terms:
  1. **Timing:** Timing refers to an agreement between the sender and the receiver about the data transmission rates and duration.

2. **Syntax:** The syntax of protocol defines the structure or format of data. This means that the order in which it is to be sent is decided. A protocol could define that the first 16 bits of a data transmission must always contain the receiver's address.
3. **Semantics:** Protocol semantics defines the interpretation of the data that is being sent. For example: The semantics could define that if the last two bits of the receiver's address field contain a 00, it means that the sender and the receiver are on the same network.

1.6.1 Examples of Protocols

- The most common protocols are:
  1. Ethernet
  2. LocalTalk
  3. Token Ring
  4. FDDI
  5. ATM

1. Ethernet:

- The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection).
- This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear.
- Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs.
- Each computer then backs off and waits a random amount of time before attempting to retransmit.
- With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.
- The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.
- To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called **Fast Ethernet**.
- Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary.
- Fast Ethernet is becoming common in organizations that have been recently wired.

2. LocalTalk:

- LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers.
- The method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- It is similar to CSMA/CD except that a computer signals its intention to transmit before it actually does so.
- LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software.
- With the addition of the server version of AppleShare software, a client/server network can be established.
- The LocalTalk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk is speed. Its speed of transmission is only 230 Kbps.

3. Token Ring:

- The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing.
- In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring.
- A single electronic token moves around the ring from one computer to the next.
- If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token.
- The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer.
- The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring has decreased.

4. FDDI:

- Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances.
- The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology.
- Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring.
- A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

5. **ATM:**

- Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher.
- ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets.
- ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable.
- ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients.
- As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

Table 1.4: Summary of Protocols

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	0.23 Mbps (or 230 Kbps)	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

- Protocols also define procedures for handling lost or damaged transmissions or "packets." TCP/IP (for UNIX, Windows NT, Windows 95 and other platforms), IPX (for Novell NetWare), DECnet (for networking Digital Equipment Corp. computers), AppleTalk (for Macintosh computers), and NetBIOS/NetBEUI (for LAN Manager and Windows NT networks) are the main types of network protocols in use today.

1.6.2 Protocol Standards

- Standards are necessary in daily life. Everything that we use in our daily life has some common features, some standards. In the absence of standards, every manufacturer can theoretically manufacture a set of goods or services that are incompatible with other manufactures.
- To avoid such anomalies or problems a set of standards is established which governs the rules that manufactures must obey. In exactly the same way standards for data communications have been set or developed.

- A lot of incompatibility issues have no place in data communications, which is highly desirable.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Setting standards, rules that all manufacturers of hardware and software will follows, are important for a number of reasons:
  - Standards describe accurately and unambiguously how information is transmitted.
  - A manufacturer's products will work successfully with other manufacturer's products if they all follow the same standards.
  - By defining a set of standards, you are providing a framework within which all manufacturers can design new, successful products.
  - Standards break down complex ideas into smaller, methodical, and easier to understand components.
- Data communications standards can be classified into two types: De facto (i.e., meaning "by fact" or "by convention") and De jure (meaning "by law" or "by regulation").

1. **De facto:**

- The standards that have not been approved by an organized body but have been adopted as standards through widespread use are De facto standards. De facto standards are often established originally by manufactures who seek to define the functionality of a new product of technology.
- De facto data communication standards can be further divided into **proprietary** and **non-proprietary** standards. The proprietary standards are invented and owned by an organization who first uses them, and which gain popularity.
- Proprietary standards are closed, because they close-off communication with devices/systems of other vendors. Non-proprietary standards are those that are developed by an organization/ committee/group, which become popular and vendors start supporting them.
- Non-proprietary standards are open standards because anybody adhering to those automatically gains access to all others following those standards.

Examples:

1. *The most important De facto organization involved in establishing communication standards and protocols is CCITT (Consultative Committee for International Telegraph and Telephone) is United Nations agency responsible for defining standards for Telegraph and Telephone. X.25 is most common standard for WAN.*

2. IBM (International Business Machines): SNA (System Network Architecture) protocol is example of De facto protocol. The IBM developed this protocol in 1974 for its mainframe computers, still being used by large number of organizations all over the world.

2. De jure:

- These standards have been legislated by an official body. These are usually led by governments or government-appointed agencies.

Examples:

- For example, the IEEE (Institute of Electrical and Electronic Engineers) has the authority to create electrical standards such as wireless communication.
- On a global level ISO, the International Standards Organization was setup to create standards. They have produced over 18,500 formal standards covering everything from quality control to making tractors.

1.6.3 Standards Organizations

(S-22)

- Standards organizations can be classified into three categories:
  1. Standards creation committees
  2. Forums
  3. Regulatory agencies
- There is lot of organizations serving as standards creation committees.

1. American National Standards Institute (ANSI):

- ANSI is a private non-profit organization that does not have any direct ties with the US federal government. Generally, all ANSI projects are undertaken for the social benefit of the US citizens. Professional groups, regulatory bodies, government, and consumer groups represent ANSI.

2. Electronic Industries Association (EIA):

- EIA is a non-profit organization that is aligned with ANSI. EIA focus is public awareness and lobbying for standards. The main contributions to the data communications technology are the development of interfaces for physical connections and electronic signal specifications for data communications.

3. International Telecommunications Union-Telecommunications Standards Sector (ITU-T):

- ITU-T was earlier known as the Consultative Committee for International Telegraphy and Telephony (CCITT). ITU-T was formed by the United Nations in response to the demands from some nations who were developing their own national standards for data communications in the early 1970s and which led to issues of incompatibility with each other.

4. Institute of Electrical and Electronics Engineers (IEEE):

- IEEE is the biggest professional engineering body in the world. IEEE focus areas are developments in the areas of electric and electronic engineering and radio sciences. IEEE also covers the development and adoption of international computer and communications standards.

5. International Standards Orgnisation (ISO):

- ISO is a well-known multi-national standards body. Open Systems Interconnection (OSI) model as a networking protocol is a major contribution of the ISO to the data communications world. Most members of ISO are their respective government representatives. ISO created in 1947, the ISO is a non-profitable standards creation organisation. Members from over eighty developed nations actively represent the ISO.

Forums:

- The main drawback of standards committees is notorious for the slow speed of developments and decision-making.
- Forums generally concentrate on a particular technology, and this specialization helps them to achieve a great amount of throughput with contributions from a variety of forum members.
- User groups, industry representatives, university students, and experts come together and set up forums to address the various issues and concerns of data communications technology, and come up with standards from time to time.
- **Examples:**
  1. Internet Society (ISOC)
  2. Internet Engineering Task Force (IETF)
  3. Frame Relay Forum
  4. ATM Forum
- These are Government appointed agencies. For example, Federal Communications Commission (FCC) of the US are always involved in regulating standards.
- These agencies help to protect the interests of the general public in areas such as radio, television and wired communications.
- Every portion of communications technology must be approved by FCC before it can be sold in the market.
- FCC periodically reviews the rates changed by service providers, technical specifications of communication hardware and divides and allocates ratio frequencies, etc.

1.7 NETWORK SOFTWARE

- Network software interacts, increases and faciliates the functions of a computer network. It has become integral part of today's computing world where shared information, effective communication and reliable productivity is needed.

1.7.1 Protocol Hierarchies, Layers, Peers, Interfaces

Protocol Hierarchy:

- Networks are set up with a protocol hierarchy that divides the communication task into several layers. A protocol is a set of rules for communication within a layer.
- Design of protocols should be simple. To reduce the design complexity of a protocol, most of the networks are organized as a series of **layers** or levels. Each layer is built upon its predecessor i.e. previous layer.
- The number of layers used, name of each layer, contents of each layer and function of each layer are different from one network to other network. But the purpose of each layer is to offer services to the higher layers is same in all networks.
- Layer n on one machine communicates with its corresponding layer n of another machine. That is layer 1 communicates with layer 1 of other machine. The rules and the conventions which are used for this conversation/communication are known as layer 'n' protocol. Fig. 1.26 illustrates 7-layer network.

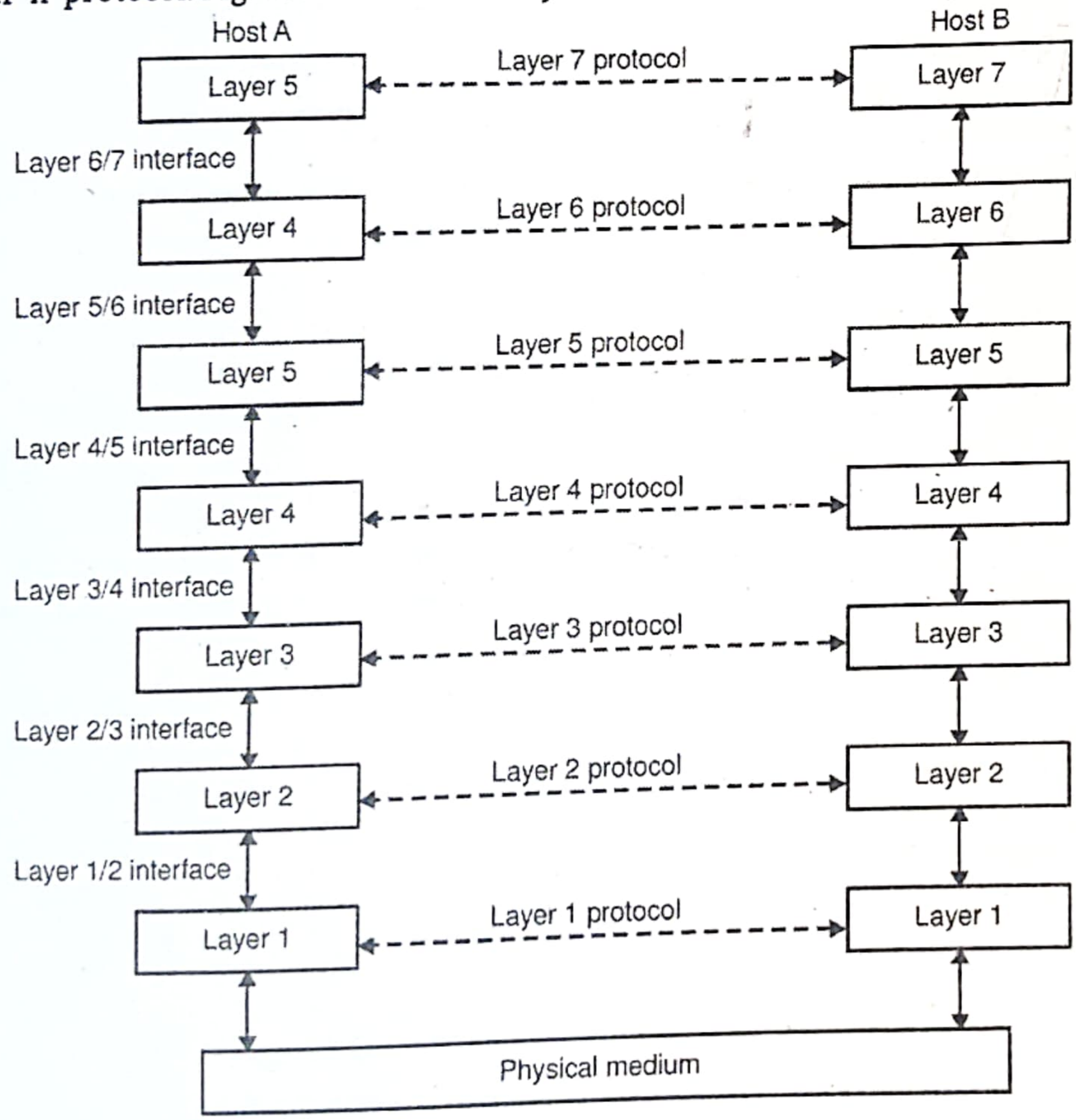


Fig. 1.26: Layers, Protocols and Interfaces

- **Peers:** The corresponding layer entities on different machines are called peer processes. We can say that each peer communicates through protocol.
- Actually, speaking, no data can directly transfer from layer n of one machine to layer n of another machine. Each layer passes data and control information to the lower level. For example, layer 6 passes data to layer 5.
- When it reaches to lowest layer i.e. layer 1 it transfers data to the physical medium which is the medium through which actual communication occurs. We can say that layer 5 of one machine has virtual communication with layer 5 of another machine.
- This virtual communication is shown by dotted lines and physical communication, [occurs in layer 2 and layer 1] is shown by solid lines.

Interface:

- The physical communication between each pair of adjacent layers is known as **Interface**. The interface defines the primitive operations and services which a lower layer offer to the upper one.
- Most important considerations are defining clean interfaces between the layers. So that if we want to replace a layer with different implementation, it must be possible. For example, all telephone lines we replaced by satellite channels. The amount of information passed between layers should be smallest.
- The set of layers and protocol together is called the **Network Architecture**. The architecture must have enough information. So that the software and hardware can be designed to follow the protocols.
- But the details of the implementation and specification of interfaces are not considered as a part of architecture. It is because these are not visible from outside and are within the machines.

Multi-layer Communication:

- Let's consider the idea of multi-layer communication. Two persons (layer 3), one speaking French and other speaking Japanese want to communicate. As they have to common language they require a translator (layer 2) who translates their messages into the respective language (English).
- The translators contact with engineers (layer 1) for transmission by telegram, telephone, computer network etc. And the message is passed across 2/3 interface to second person.
- Here, the protocol is completely independent of the other ones. If both translators switch from English to German, it will not affect the other protocol.

Example:

- Now let's consider the technical example of 7-layer network. A message M is produced by host A in layer 7. The message is passed from layer 7 to layer 6 according to the definition of layer 6/7 interface. Layer 6 transforms the message in certain ways for example text compression. Then it passes the new message M to layer 5 across layer 5/6 interface. Layer 5 just regulates the direction of flow.

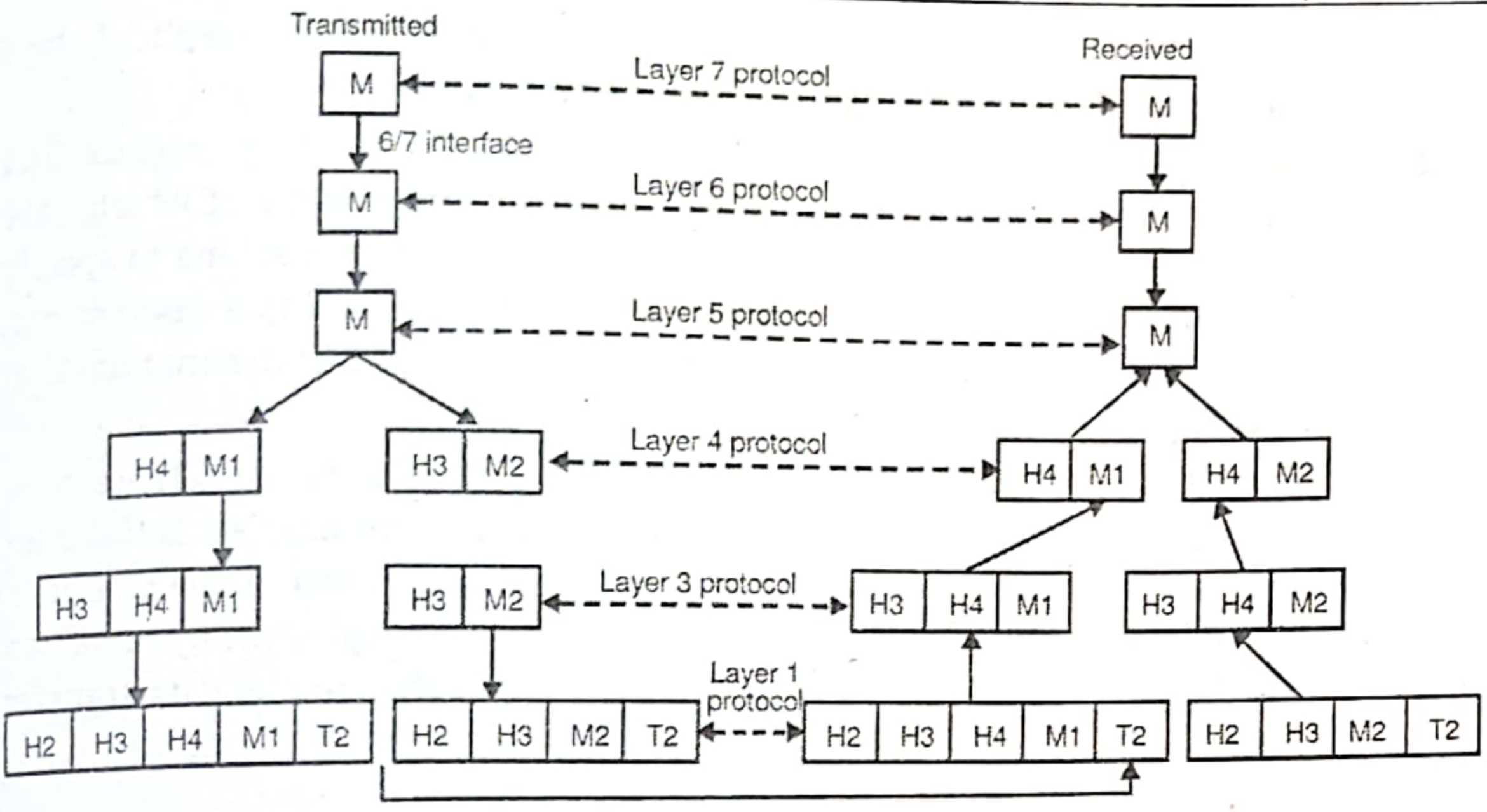


Fig. 1.27: Information Flow in 7 Layer Network

- In many networks, layer 4 does not have restrictions or limits to the size of the message. But layer 3 may have limits. So layer 4 breaks up the message into smaller units, by writing a header to each unit. Header allows reconnecting the message in the original form at destination machine. Header contains the sequence number. Sometime, in many layers header contains sizes, times and other control fields with the sequence number.
- Layer 3 decides about the outgoing line and attaches its own header and then passes the data to layer 2.
- Layer 2 adds a header to each piece and a trailer and then gives this resulting message in the form of unit to layer 1 for physical transmission. This message is converted back again into the original message with the same procedure from lower layer to upper layer.
- The peer process abstraction is very crucial to all network design. This abstraction technique allows partitioning the design at complete network i.e. unmanageable problem into several smaller and manageable layers.

(W-18)

1.7.2 Design Issues of the Layers

- Some of the key design issues that occur in computer netoworking are present in severeal layers. Below, we will briefly mention some of the more important ones.

1. **Connection Establishment and Termination:** In a network, there are many computers available. Each machine has multiple processes. A process of one machine specifies with which computer connection is established. Therefore every layer must have a mechanism for connection establishment. When the

connection is not needed, it should be terminated. That is why there should be a mechanism available to terminate the connection.

2. **Addressing:** Every layer needs a mechanism for identifying senders and receivers. Since a network normally has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify with whom it wants to talk. As a consequence of having multiple destinations, some form of addressing is needed in order to specify a specific destination. That is the facility of acknowledgement can be provided.
3. **Direction of Data Transfer:** There are some rules for data transfer. These rules should be present in the design issue. Data transfer may be simplex, half-duplex or full-duplex. Simplex communication means the data travels in one direction. For example: data transfer from CPU to monitor. Half-duplex means data can transfer in either direction but not simultaneously. For example: data transfer from one workstation to other workstation. Full-duplex means data transfer is possible in both directions at once.
4. **Error Control:** The physical communication circuits are not perfect. So control is an important issue. The receiver and sender, both ends of the connection must agree upon the error-detecting and error-correcting code. The receiver can gives acknowledgement to the sender about which message has been received or not.
5. **Avoid loss of sequencing:** Proper sequencing must be allowed. This is needed because in the communication channels the messages are not delivered in the same order as they were sent. So by providing sequence number provision, a receiver can put them back in order.
6. **Ability of receiving Long Messages:** Several layers cannot accept very long messages. So there should be a mechanism to disassemble that message, transmit it and reassemble it again. Similarly, if the message is very small or a data unit is very small, it is inefficient to transmit them separately. So several small messages to the same destination are gathered into a single message, transmitted and then afterwards separated at last end.
7. **To use Multiplexing and De-multiplexing:** There are various processes available; it is very expensive or inconvenient to set up a separate connection for each pair of communicating process. So it is necessary to have multiplexing and de-multiplexing. This is needed to share a single communication channel among several unrelated conversations. For example: Client/ Server model.
8. **Routing:** It is a network structure. So for reaching a particular destination, multiple paths are available. One or two layers can be split up and have a routing technique. A route can be chosen for communication. For example, if we want to go to ShivajiNagar, we can go from Fergusson college Road or from Jangali Maharaj Road etc.

Layers:

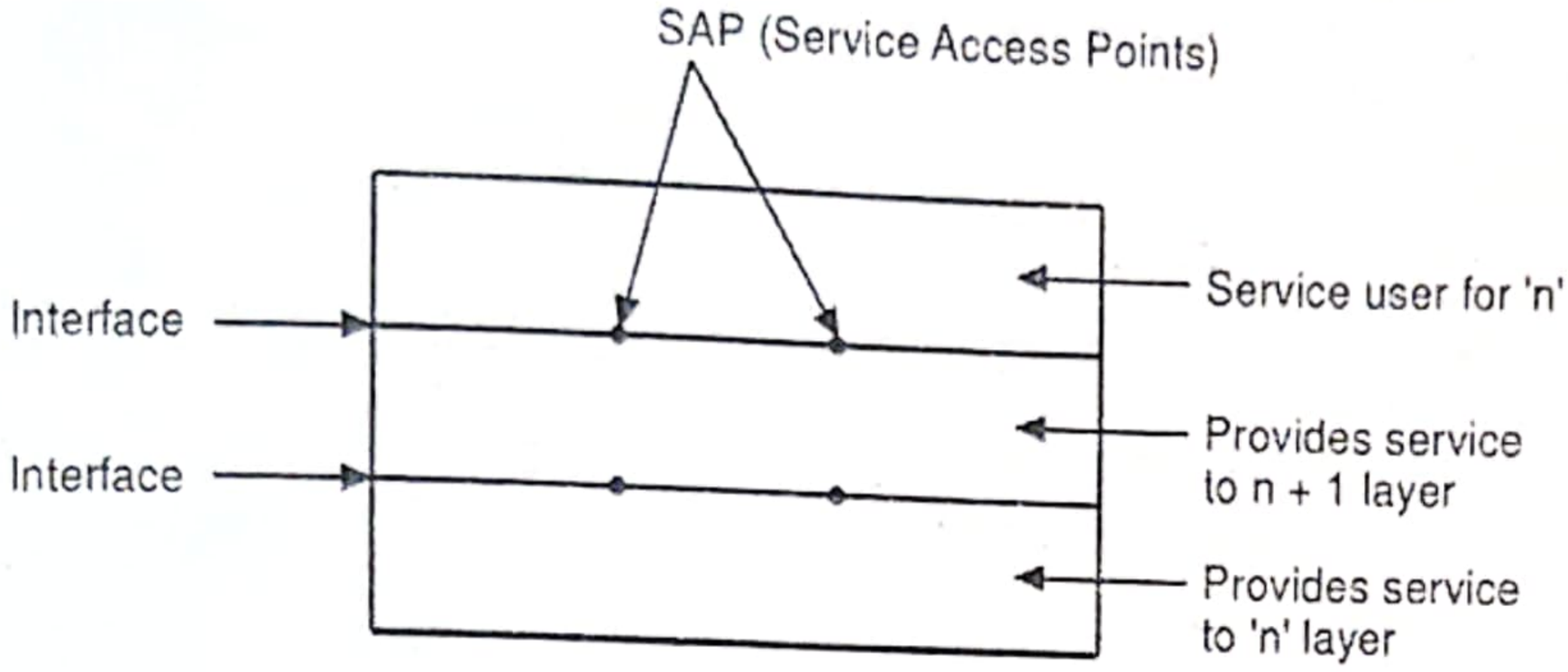


Fig. 1.28: Layers to Reduce Design Complexity

- To reduce design complexity, most networks are to achieve as a series of layers or levels. Each one built upon the one below it.
- **SAP (Service Access Points):** SAP is generally used as an identifier label for endpoints of network in OSI networking or model. It is a data structure and identifier also for a buffer area in memory of system. It is a point in a layer of a layered architecture where a network is usually provided and where layer just above layer that provides service can probably have access to it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differs from network to network. However, in all networks, the purpose of each layer is to offer certain services to the higher layer.
- The function of each layer is to provide services to the layer above it. The active elements in each layer are often called entities. Entity can be software entity or hardware entity.
- The layered architecture concept redefines the way networks are conceived and creates significant cost savings and managerial benefits.
- Instead of building a separate network for each service, user can have multiple services sharing a common core network.
- Adding new services and managing the network infrastructure must be easy.
- That is why the layered architecture concept will become increasingly important for user.
- It offers opportunities to reduce capital and operating expenditure by offering a smooth step-by-step migration to IP.
- Key advantage is that network resources can be used more effectively in terms of simplicity and fewer equipment sites leading to lower total cost of ownership.
- Also, the need for transmission connections in the network can, in many cases, be reduced by more than 50 %.

1.7.2.1 Advantages and Disadvantages of Layered Designs

Advantages:

- Layered designs issues consist of following advantages:

1. Segmentation of high-level from low-level issues. Complex problems can be broken into smaller more manageable pieces.
2. Since, the specification of a layer says nothing about its implementation, the implementation details of a layer are hidden, (abstracted) from other layers.
3. Easier exchange of parts at a later date.
4. Development by teams is aided because of the logical segmentation.
5. Many upper layers can share the services of a lower layer. Thus layering allows us to reuse functionality.

Disadvantages:

- Layered designs consist of following disadvantages:

1. Layering can lead to poor performance. To avoid this penalty, in situations where an upper layer can optimize its actions by knowing what a lower layer is doing, we can reveal information that would normally be hidden behind a layer boundary.
2. The layers must be engineered at the outset, before the system is built.
3. Layering is a form of information hiding. A "layering violation" occurs in situations where a layer uses knowledge of the implementation details of another layer in its own operations. At the limit this leads to changes to one layer resulting in changes to every other layer, which is an expensive and error prone proposition.
4. The trouble with layers of computer software is that sooner or later you loose touch with reality. Layers are abstraction boundaries and the more they encapsulate their works the more one is unaware of the application's inner works.

1.7.3 Connection Oriented and Connectionless Services [S-19, W-22]

- Layers can offer two different types of service to the layers are:
  1. Connection-oriented
  2. Connectionless

1.7.3.1 Connection-oriented Services

- In general, transport protocols can be characterized as being either connection-oriented or connectionless.
- Connection-oriented services must first establish a connection with the desired service before passing any data.
- A connectionless service can send the data without any need to establish a connection first.

Phases in Connection-oriented service:

- Connection-oriented service involves three phases: Connection Establishment, Data Transfer, and Connection Termination.

- **Connection Establishment:** During connection establishment phase, the end nodes may reserve resources for the connection.
- The end nodes also may negotiate and establish certain criteria for the transfer, such as a window size used in TCP connections. This resource reservation is one of the things exploited in some denial of service (DOS) attacks.

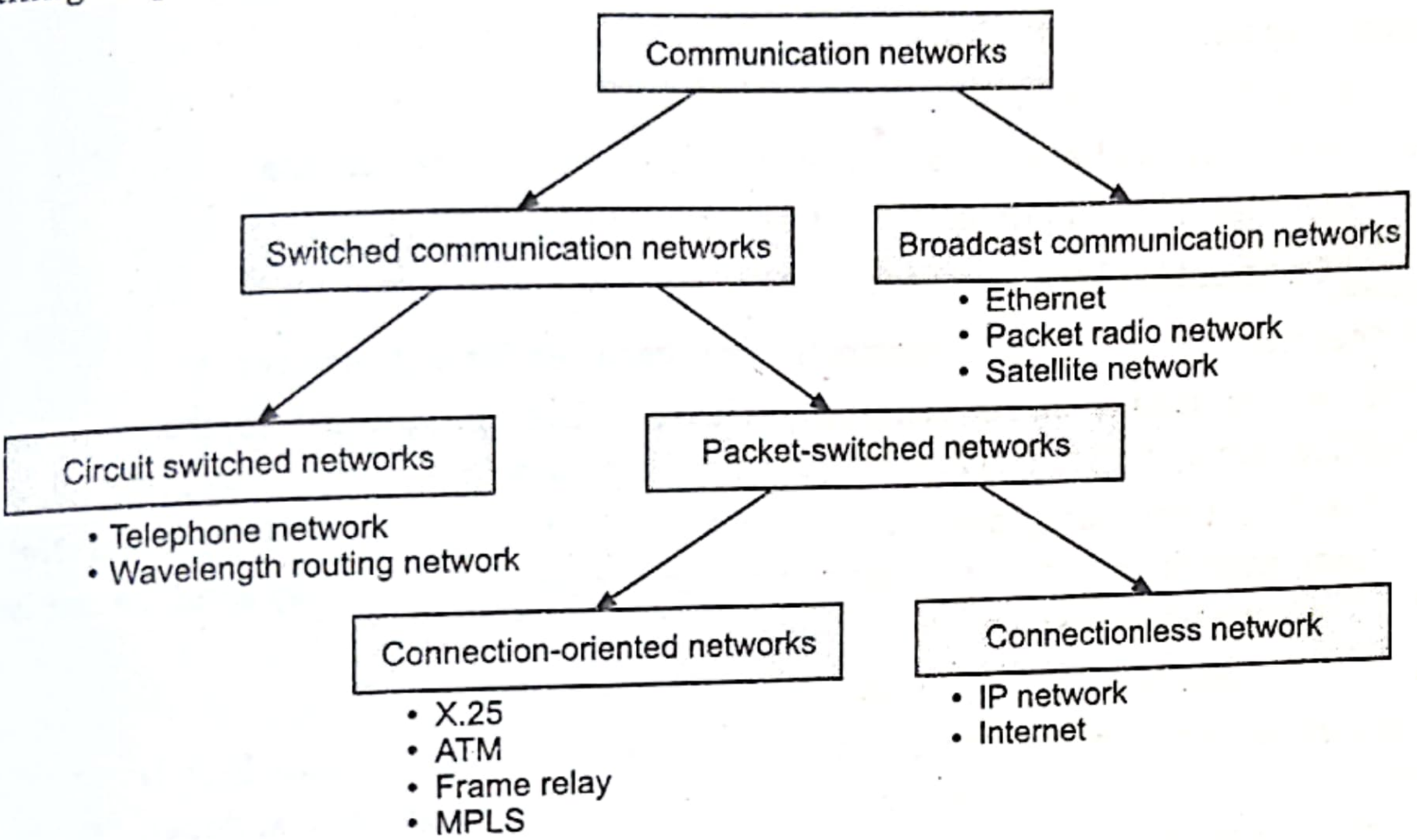


Fig. 1.29: Types of Communication Networks

- An attacking system will send many requests for establishing a connection but then will never complete the connection. The attacked computer is then left with resources allocated for many never-completed connections. Then, when an end node tries to complete an actual connection, there are not enough resources for the valid connection.
- **Data Transfer:** The data transfer phase occurs when the actual data is transmitted over the connection. During data transfer, most connection-oriented services will monitor for lost packets and handle resending them.
- **Connection Termination:** The protocol is generally also responsible for putting the packets in the right sequence before passing the data up the protocol stack. When the transfer of data is complete, the end nodes terminate the connection and release resources reserved for the connection.
- **Session connection:** A Connection-oriented service requires a session connection be established before any data can be sent with a direct physical connection between the sessions. This often considered being a more reliable network service than the alternative connectionless service.

Advantages:

1. These services provide guarantee delivery of data.
2. This service is more reliable then connectionless services.
3. Some connection oriented services will monitor for lost packets and handl resending them.

Disadvantages:

1. A connection must require.
2. These services have more overhead than connectionless service.
3. Complex method for data transferring.

1.7.3.2 Connectionless Services

- It does not require a session connection between sender and receiver.
- The sender simply starts sending packets, (called datagrams) to the destination. TCP(Transmission Control Protocol) is a connection-oriented transport protocol.
- While UDP(User Datagram Protocol) is a connectionless network protocol. Neither system must maintain state information for the systems that they send transmission to or receive transmission from.
- A connectionless network provides minimal services.
- Connection-oriented methods may be implemented in the data link layers of the protocol stack and/or in the transport layers of the protocol stack, depending on the physical connections in place and the services required by the systems that are communicating.
- This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Both operate over IP.
- The physical, data link, and network layer protocols have been used to implement guaranteed data delivery. For example, X.25 packet-switching networks perform extensive error checking and packet acknowledgment because the services were originally implemented on poor-quality telephone connections.
- Today, networks are more reliable. It is generally believed that the underlying network should do what it does best, which is deliver data bits as quickly as possible.
- Therefore, connection-oriented services are now primarily handled in the transport layer by end systems, not the network. This allows lower-layer networks to be optimized for speed.
- LANs operate as connectionless systems. A computer attached to a network can start transmitting frames as soon as it has access to the network.
- It does not need to set up a connection with the destination system ahead of time. However, a transport-level protocol such as TCP may set up a connection-oriented session when necessary.

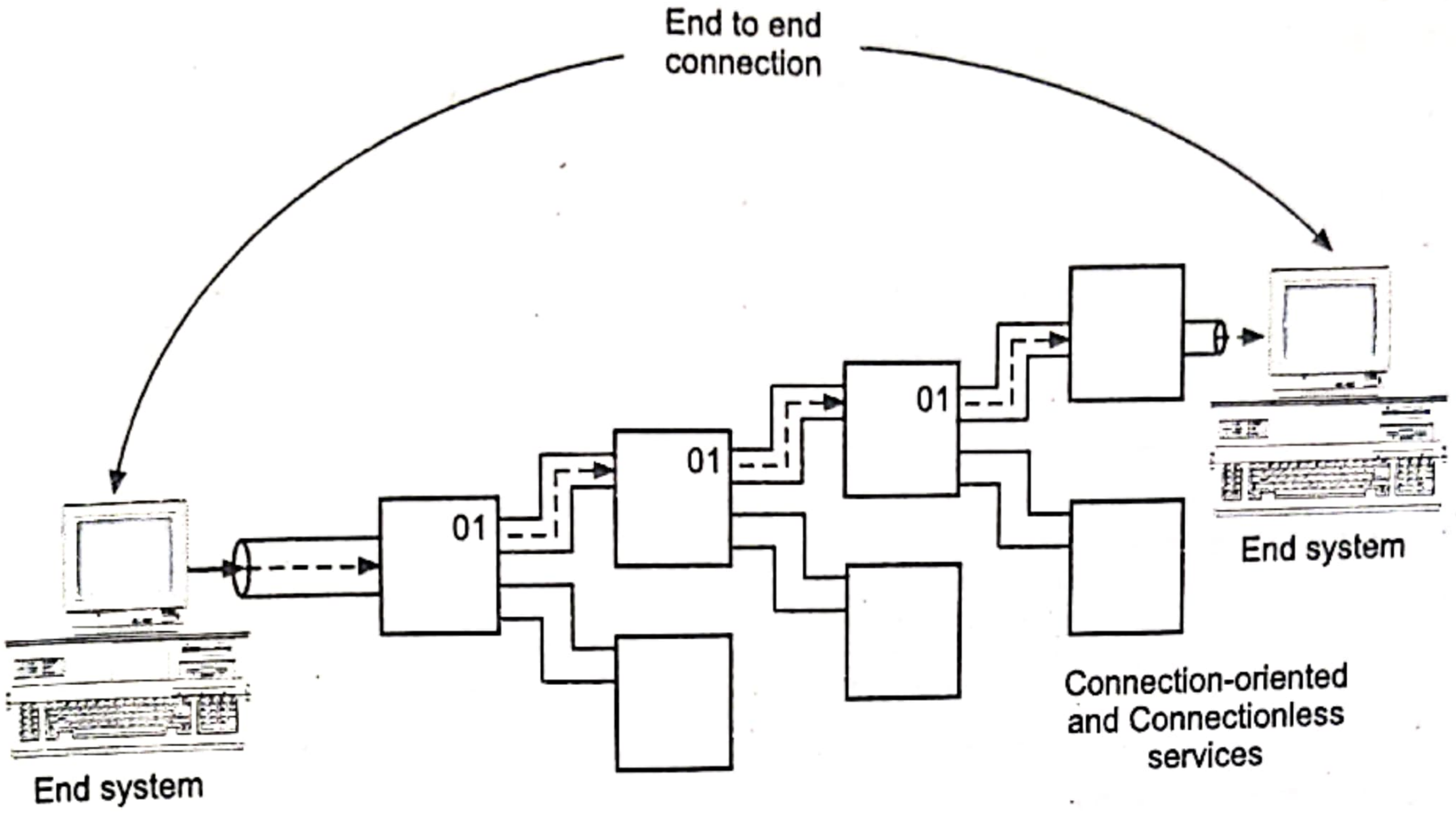


Fig. 1.30: Connection Services

- The internet is one big connectionless packet network in which all packets delivers are handled by IP.
- However, TCP adds connection-oriented services on top of IP. TCP provides all the upper-level connection-oriented session requirements to ensure that data is delivered properly.
- MPLS is a relatively new connection-oriented networking scheme for IP networks that sets up fast label-switched paths across routed or layer 2 networks.
- A WAN service that uses the connection-oriented model is frame relay. The service provider sets up PVCs (Permanent Virtual Circuits) through the network as required or requested by the customer.
- ATM is another networking technology that uses the connection-oriented virtual circuit approach.

Advantages:

1. Does not require any connection.
2. These services are very simple and easy for data transfer.
3. Used for periodic burst data transfer.
4. Less overhead then connection oriented services.

Disadvantages:

1. Less reliable than connection-oriented services.
2. No guarantee for delivery of data.
3. It provides minimal services.

Examples of Services:

Table 1.5: Different types of Services and Example

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

- Observe that each layer in the OSI model may offer different kinds of service. Often there is datagram service on the lower layers while e.g. the transport layer offers a reliable message stream.

Service Primitives:

- A service is formally specified by a set of primitives (operations) available to a user process to access the service.

Table 1.6: Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection.
CONNECT	Establish a connection with a waiting peer.
RECEIVE	Block waiting for an incoming message.
SEND	Send a message to the peer.
DISCONNECT	Terminate a connection.

Table 1.7: Comparison between Connection-oriented and Connectionless services

Sr. No.	Connection-oriented Service	Connectionless Services
1.	Connection-oriented services must first establish a connection with the desired service before passing any data.	A connectionless service can send the data without any need to establish a connection first.
2.	Connection - oriented services provide some level of delivery guarantee.	Connectionless services do not provide some level of delivery guarantee.

Contd...

3.	Connection-oriented network services have more overhead.	Connectionless network have less overhead.
4.	TCP (Transmission Control Protocol) is a connection-oriented transport protocol,	While UDP (User Datagram Protocol) is a connectionless network protocol.
5.	This method is often called a "reliable" network service.	This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers.
6.	**Examples:** MPLS is a relatively new connection - oriented networking scheme for IP networks that sets up fast label-switched paths across routed or layer 2 networks. A WAN service that uses the connection-oriented model is frame relay. ATM is another networking technology that uses the connection-oriented virtual circuit approach.	**Examples:** LANs operate as connectionless systems. The Internet is one big connectionless packet network in which all packet deliveries are handled by IP.

Summary

- Computer network is a set or collection of computing devices that are linked to each other in order to communicate and share their resources with each other.
- The interconnected computers can share resources, which called networking.
- Computer network is divided into wired and wireless network. A wired network is simply a collection of two or more computers, printers, and other computing devices linked by cables like Ethernet, coaxial cables. A wireless network, which uses high-frequency radio waves or micro wave rather than wires to communicate between nodes.
- Nowadays, computer networks have become an essential part of industry, entertainment world, business as well as our daily lives. Some of the applications of computer network in different fields are: Business applications, Home applications and Mobile application.
- Remote access is the ability to get access to a computer or a network from a remote distance. For example, Home users get access to the Internet through remote access to an Internet Service Provider (ISP).
- Transmission Technology refers how two devices are connected and how they are communicating.

- The transmission technology can be categorized broadly into two types i.e. Point-to-Point networks and Broadcast networks (multipoint).
- Communication between two directly interconnected devices is referred to as point-to-point communication.
- Point-to-point networks consist of many connections between individual pairs of computers or machines.
- Point-to-point transmission with one sender and one receiver is sometime called unicasting.
- The networks having multipoint configuration are called Broadcast Networks.
- A collection of interconnected networks is called an internetwork or internet. The Internet is a global network connecting millions of computers.
- Network topology defines the geographic arrangement of computer networking devices.
- Topology defines the physical (describes the placement of network nodes and the physical connections between them) or logical (the paths that take messages to get from one place on the network to another place) arrangement of links in a network.
- Network topology is defined as, "the physical interconnection between various elements on computer network, such as links and nodes".
- There are number of different network topologies in networking like star, ring, mesh, tree, bus etc.
- In bus topology, all nodes are connected to a central cable which is called a bus. This bus is also called as a Trunk or sometimes it was also referred to as Backbone cable.
- In ring topology, the computers in the network are connected in a circular fashion which forms of a ring.
- In star topology all the cables run from the computers to a central location, where they are all connected by a device called a hub/switch.
- Computer networks fall into three classes regarding the size, distance and the structure namely LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
- Local Area Network (LAN) is a privately-owned network covering a small geographic area (10 m to 1 km), like a home, office, building or group of buildings (For example: campus).
- Metropolitan Area Network (MAN) covers a larger geographical area than a LAN (1 km to 10 km), ranging from several blocks of buildings to entire cities.
- Wide Area Networks (WAN) covers a large geographical area (100 km to 1000 km), often a country. IT can be divided into three main categories system interconnection (connecting the components of computer using short range radio like Bluetooth.

- The word wireless is dictionary defined as "having no wires". The computer networks that are not connected by cables of any kind are called as Wireless networks.
- Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system.
- An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.
- A protocol is a set of rules that governs the communications between computers on a network.
- Networks are set up with a protocol hierarchy that divides the communication task into several layers. A protocol is a set of rules for communication within a layer.
- Connection-oriented services must first establish a connection with the desired service before passing any data.
- A connectionless service can send the data without any need to establish a connection first.

Check Your Understanding

1. Which topology requires a central controller or hub ?
   (a) Star (b) Mesh
   (c) Bus (d) Ring
2. Which topology requires a multipoint connection?
   (a) Mesh (b) Star
   (c) Ring (d) Bus
3. Which of the following is NOT a key element of a protocol?
   (a) Semantics (b) Signal
   (c) Syntax (d) Timing
4. In a network with 25 computers, which topology would require the most extensive cabling?
   (a) Star (b) Mesh
   (c) Bus (d) Ring
5. In a _____ connection, more than two devices can share a single link.
   (a) Point-to-point (b) Primary
   (c) Multipoint (d) Secondary
6. Which of the following topology is most susceptible to failure following a cable break?
   (a) Star (b) Mesh
   (c) Bus (d) Tree

7. Communication channel is shared by all the machines on the network in _____.
   (a) broadcast network (b) unicast network
   (c) multicast network (d) none of the mentioned
8. _____ is the technology that connects the machines and people within a site in a small area .
   (a) LAN (b) MAN
   (c) WAN (d) None of these
9. _____ is a network that covers geographic areas that are larger, such as districts or cities.
   (a) LAN (b) MAN
   (c) WAN (d) None of these

ANSWERS

1. (a)	2. (c)	3. (b)	4. (b)	5. (c)	6. (c)	7. (a)
8. (a)	9. (b)					

Practice Questions

Q.I Answer the following questions in short.

1. Define Computer Network.
2. How are networks classified?
3. State applications of computer networks.
4. Enlist various advantages and disadvantages of network.
5. What is topology?
6. What is Protocol?
7. What are the modes of communications? Explain with example.

Q.II Answer the following questions.

1. What is Computer Network? What are its goals?
2. Define topology. Explain any one topology with its advantages and disadvantages.
3. Write a note on point-to-point and broadcast transmission.
4. What are the applications of computer networks?
5. How are networks classified?
6. What is an internetwork? Explain its structure in brief.
7. Write a short note on: (a) WAN, and (b) MAN.
8. What are standards? What is their need? What are the two types of standards?
9. Define protocol.

10. Compare WAN and MAN.
11. Compare peer-to-peer LAN and server-based LAN.
12. With suitable diagram describe network components
13. Explain the layered network model. What are the advantages?
14. Explain different types of LAN? How do they differ in functionality?
15. Explain the classification of services. Also explain them.
16. Explain the relationship between services and protocol.
17. What are the types of topologies?

Q.III Define the following terms:

1. LAN
2. Communication Modes
3. Network Components
4. Peers
5. Interfaces
6. Network software
7. Wireless Network

Previous Exams Questions

Summer 2018

1. Define network topology. List different types of topologies. Explain any one in detail. [5 M]

Ans. Please refer to section 1.2.

2. What are different modes of communication? Explain any one in detail. [5 M]

Ans. Please refer to section 1.4.

3. Write a note on protocols and standards. [5 M]

Ans. Please refer to section 1.6.

Winter 2018

1. Define Network Topology. List different types of Topologies. Explain any one in detail. [5 M]

Ans. Please refer to section 1.2.

2. Explain different components of LAN. [5 M]

Ans. Please refer to section 1.3.1.1.

3. Define Computer Network. Explain goals of Computer Network. [5 M]

Ans. Please refer to section 1.1.

4. Explain server based and peer to peer LAN's. [5 M]

Ans. Please refer to section 1.5.

5. What are different modes of communication? Explain any one. [5 M]

Ans. Please refer to section 1.4.

6. Write a note on protocols and standards. [5 M]

Ans. Please refer to section 1.6.

7. Write note on: SAP. [5 M]

Ans. Please refer to section 1.7.2.

Summer 2019

1. Compare connection oriented and connectionless Network Models. [5 M]

Ans. Refer to section 1.7.3.

2. Explain Server Based and Peer-To-Peer LANs. [5 M]

Ans. Refer to section 1.5.3.

3. Define Computer Networks. Explain goals of Computer Networks. [5 M]

Ans. Refer to section 1.1.

4. Write short notes on:

(a) Modes of communication [5 M]

Ans. Refer to section 1.4.

(b) Intranet and Extranet [5 M]

Ans. Refer to section 1.3.4.

❖ ❖ ❖