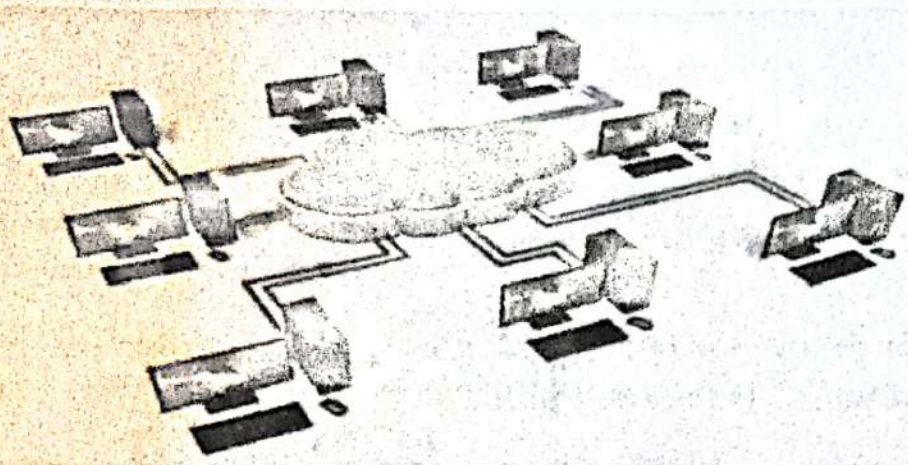


1

NETWORKS : AN INTRODUCTION

INTRODUCTION

- An arrangement of two or more inter connected computers is called a computer network.
- It is a logical extension of a data communications system.
- Two or more computers or processors are linked together with data communication devices and transmission media in a computer network.
- The basic purpose of making such a network is communication between two or more machines.
- Each computer in a network can have its own processing capabilities and can share data files, programs and even hardware peripherals of other computers in the network.

1.1 DEFINITION

Two or more computers connected logically with the help of data communication devices and transmission media reffered to as computer Network.

1.2 NETWORK COMPONENTS

The important components used in the computer network are:

1. Media It is the medium through which the data travels. The various alternatives for transmission media are

Twisted pair cable, Coaxial cable, Fibre optics, Microwave satellite, Cellular Radio, Transreceiver.

2. Processor Processor is the hardware Which helps to transfer the data from source to destination. Different processor used in the data communication are :

Modems, Multiplexer, Concentrator, Routers, Bridges, Gateway, Front end processor, Client and Server computers.

3. Software To transfer the data from source to destination we require software. Various software are :

Communication Software, Network Operating system software, SLIP, PPP, SMTP, MSN internet explorer, Netscope Navigator; Middle ware.

4. Channels Various channels used in data communication are

Analog/digital, switched/non switched, Circuit/Message/Packet switching, Simplex/Duplex/Full Duplex, Synchronous/Asynchronous.

5. Topology It is way through which the data travels. The various topologies available for the communication are :

Point to Point, Multidrop, Star, Ring, Mesh, Bus, Tree, etc.

6. Architecture. The various Architecture available for computer networks are

OSI, IEEE, ISDN, PSTN

1.3 ADVANTAGES OF COMPUTER NETWORK

Network is the sharing of 1. Files 2. Resources 3. Programs

Advantages of computer network is :

1. Sharing.

- Networks lets you share the information with other computer on the network.
- Depending on how you set your network. Network can be set in two ways :

1. To send the files directly.
2. To send the files to an intermediate.

- From where the different computer can pick up.
- One way or the other the data travels from one computer to another computer through network cable.

2. Sharing Resource.

- This means that you can set-up certain computer resources like a disk drive or network points that all of the computer on the network can access them.
- For example the laser printer attached to Server Computer in shared resource.
- Any node which is attached with the server can use it by giving the command from this node.
- You can share the resources too, such as CD ROM or Modem etc.

3. Backups.

- As all data is stored on the server, backing up the critical data is a simple process.

4. Communication.

- With the help of computer network we can communicate the electronic mail and group ware applications.

5. Reduction in the cost.

- As we can share the resources, files etc. It will automatically reduce the cost of executing the data.

Disadvantages of Computer Network

1. Crash If the server crashes. Then whole of the system will be disturbed.

2. Data Insecurity As all the data is shared it is possible unauthorised person can access the data if the network security is poor or weakly implemented.

3. No Privacy. Network may also means loss of privacy. Specially your boss, with the right network privileges may be in the position to read your private e-mail.

1.4 NEED OF A COMPUTER NETWORK

- Now the question arises what is the need of a computer network. The need arose out of the common economic problems. These problems are
  * Limited Resources
  * A desire to share the Resources.
  * A desire to have fast and Reliable Communication.
- The most important resource is information and in order to share information there should be some system through which it can be communicated from one place to another.
- It is possible with any communication network like PSTN of Postal network, but the cheapest and fastest media with capability of sharing large information's is the computer network.
- This communication or exchange of information is achieved by resource sharing. In resource sharing the software's/programs, data files or even computer peripherals can be shared by various computers connected in a network.
- Even some time a remote computer can use memory space of a larger computer or compiler programs which are used on smaller peripheral machines.
- The resource sharing automatically results in cost reduction. Expensive machines can be used in offices, shops, restaurants and at homes and they can use facilities of widespread networks by accessing information's software of other computers and their peripherals according to need. This improves accessibility and accuracy.

1.5 GOALS OF COMPUTER NETWORK

- There are many organizations which use computer for management of various jobs.
- They may have a number of computers performing different jobs in different departments of same organization.
- They can have many branches of that organization in different cities. Now some times it becomes necessary to load same program files, software's and some times to load the same data file on all the computers with same information.

- This wastes time as well as memory space. If any how these files stored on a single computer can be shared by all computers of the organization then it reduces time consumption, labour as well as saves money too.
- So basically there is a need of resource sharing. Starting from the basic needs these computers were connected to each other resulting into a computer network.
- Various transmission media/transmission channels were used to make a network.
- The main goals of these networks are as follows.

1. Resource Sharing :

- It means to make all programs, peripherals and data available to any one computer on the network to all other computers in the network without regard to the physical locations of them.
- Thus a user at a large distance can share the resources or can see data of a computer in the same way that a local user uses them.

2. Cost Reduction :

- Computer networking is an important financial aspect for organisations because it saves money.
- Organisations can use separate personal computers one per user instead of using mainframe computer which are expensive.
- The organization can use the workgroup model (peer to peer) in which all the PCs are networked together and each one can have the access to the other for communicating or sharing purpose.
- The organisation, if it wants security for its operations it can go in for the domain model in which there is server and clients . All the clients can communicate and access data.through the server.
- The whole arrangement is called client server model and it is shown as.

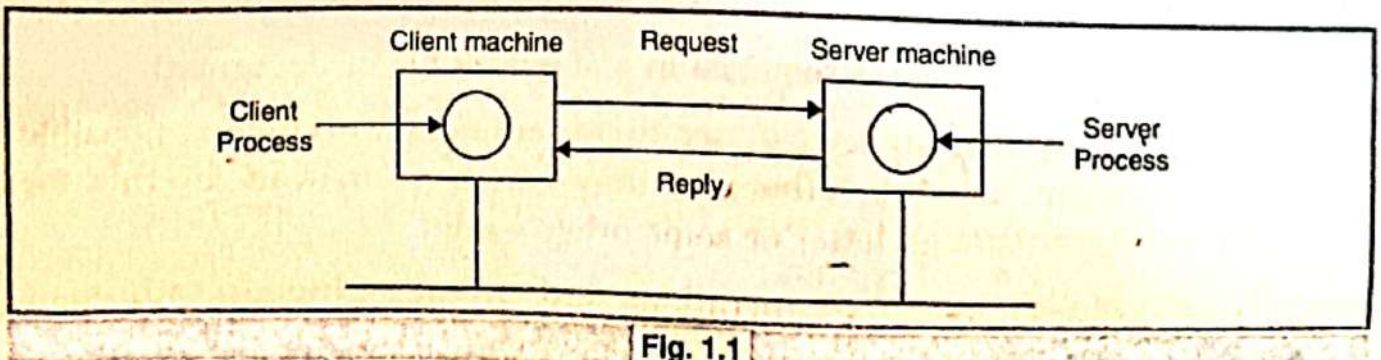


Fig. 1.1

- Hence the job of network is to do the same job in minimum cost is possible. It will save the huge amount of money.
- Resource sharing automatically reduces cost and hence money can be saved.
- One more aspect is that the price of small computers is very less as compared to main frames.
- Though main frames are roughly ten times faster as compared to micro computers but even then the price to performance ratio is much better for small/micro computers as compared to large/mainframe computers.
- The large computers cost thousand times more than small computers. Because of this imbalance more powerful personal computers are developed and are able to share data and other resources kept on one or more shared file server machines.
- Thus one goal of network is to do same job in minimum cost in terms of money which is possible on large computers only which are very expensive.

3. Improve Performance :

- The performance of a computer can be improved by adding one or more processors to it as the work load on it grows.
- For example if the system is full, instead of replacing it by a larger one at large expense it is better to add more processors to it on less cost and less disruption to the user.
- This improves both accessibility as well as performance of a system.

4. Provide Communication Medium :

- It is easy for two or more people living for apart to work on same project by portioning it using a network. They can make programs can discuss or can even write a report using a network while they are far off.
- Some times a change is required in some data file or document.
- It is done on line, others can see them immediately which is possible only through network, otherwise they can have to wait for this for several days through letter or some other media.
- Thus it makes speedy co-operations and enhances human to human communication.

1.6 FACTORS FOR NETWORK'S EFFECTIVENESS AND EFFICIENCY

To measure the effectiveness and efficiency of the computer network the various factors are its **Performances, Reliability and Security.**

1. Performance :

- Performance can be measured in many ways, including transit time and response time.
- Transit time is the amount of time required for a message to travel from one device to another.
- Response time is the elapsed time between an enquiry and response.
- The performance of a network depends on a number of factors including no. of users, the type of transmission medium, the capabilities of the connected hardware and the efficiency of the software.

(i) **Number of users:** Number of user using the network. Larger the number of user the slower will be the response time in a network. A network responds to loading is measure of its performance.

(ii) **Types of transmission medium:** Performance depends on the type of transmission medium which is used in computer network. It is directly link with speed of the transmission. Higher its speed the better will be its Performance.

(iii) **Hardware:** The type of hardware affect the speed at which data can be sent through a connected computer. Greater storage capacity gives better performance.

(iv) **Software :** The software used to process data at various nodes also affects network performance. A good software can speed process and make transmission more effective and efficient.

2. Reliability :

- Network reliability is ability to deliver the Correct data.
- It also includes recovery from error or lost data in the network in case of some failure.

(*i*) **Frequency of failure :**

- All network fails occasionally. A networks that fails often, is of little value to a user. Frequent failure will lead to little reliability.

(ii) **Recovery time of a network after failure:**

- A network that recovers quickly is more useful than one that does not.

(iii) **Catastrophe :**

- Networks must be protected from catastrophic events such as fire, earth quake or the theft . One protection against unforeseen damages is to be taken into account by taking the back up of network software.

3. Security :

- Network security means protecting data from unauthorized access and viruses.

(i) **Unauthorized access :**

- Sensitive data has to be protected from unauthorized access.
- To Protect the data from unauthorised user numbers of levels are used Like codes and passwords.
- At higher level encryption techniques is used.

(ii) **Viruses:**

- A network is accessible from many points and so is susceptible to computer viruses.
- A good network is protected from virus by hardware and software designed specially for such protection.

1.7 APPLICATIONS OF NETWORK

Data communication network have become an integral part of business, industry, and entertainment. Some of the network applications in different fields are given below :

1. Sales and Marketing. Computer networks are used by marketing professionals to collect, exchange and analyse the data relating to customers needs and product development cycles sales application includes teleshoping and online reservation services for airline, railway, hotel etc.

2. Manufacturing. Computer networks are used in many aspects of manufacturing including CAD, CAM etc.

3. Directory Services. It allows list of files to be stored in a central location to speed up world wide operation.

4. Electronic Data Interchange. EDI helps in exchange the business information which includes purchase order and invoice processing without using pen and paper.

5. Cellular Telephone. Cellular Network make it possible to maintain wireless phone connection even while travelling.

6. Electronic Message. E-mail is one of the most wide used application of networking business, the cost of sending message is very low and speed is very high.

7. Information Services. Network information services include bulletin boards and date bank. With the help of which one can get the up to date information.

8. Tele Conferencing. This service allows conferences to occur without the participants being in the same place yet they can see and talk face to face on the computer screens.

9. Financial Services. Financial services are now more and more dependent on computer networks. Application includes foreign exchange and investment services and Electronic Fund Transfer (EFT).

10. Email programs. They allow users to type messages at their local nodes and then send to someone on the network. It is a fast and easy way of transferring mail from one computer to another. Examples of electronic mail programs (Clients) are:-

- Outlook express
- Eudora Windows mail
- Fox mail
- Opera
- Mozilla Thunderbird
- Windows mail.

11. File transfer protocol (FTP). This application facilities transfer of files from one computer to another e.g. from a client to a server. There are 2 common processes involved in FTP

Downloading: - This is the process of obtaining files from a server to a workstation or a client (for example when you download programs and music from a server).

Uploading:- This is obtaining of files from a workstation to a server (for instance when you attach documents and upload them to a server, a good example being when you upload photos to Facebook).

Examples of FTP programs are:-

- FTP in Unix
- FTP in Linux or
- FTP in Windows

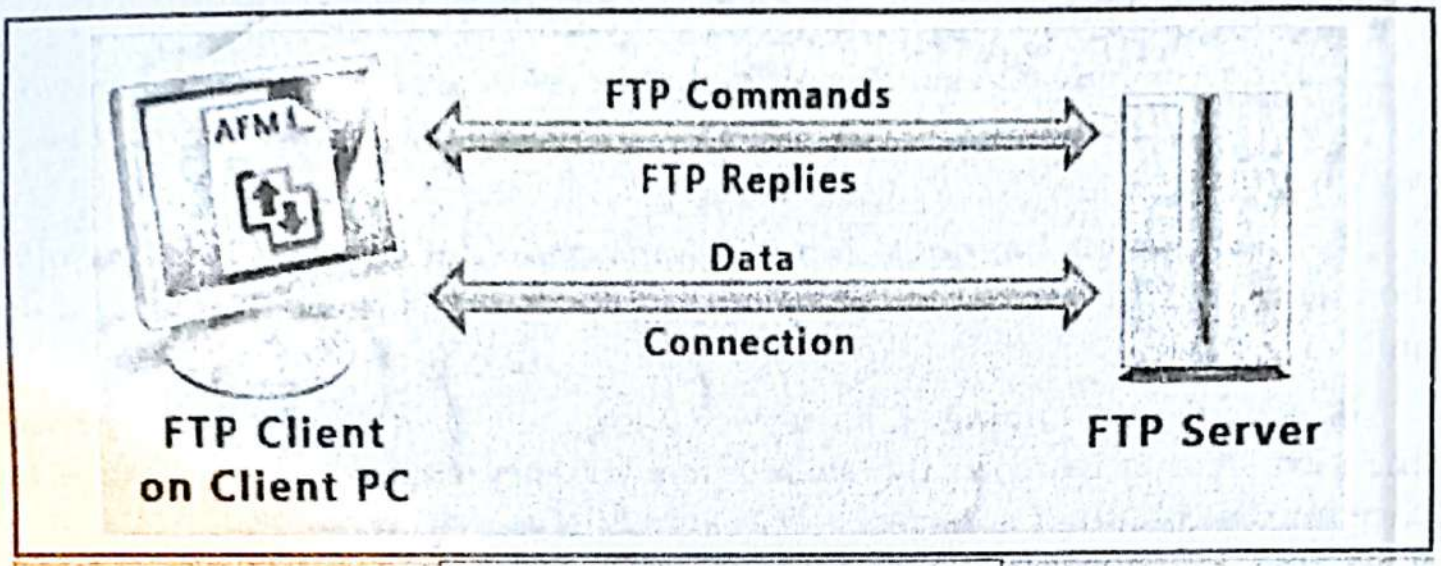


Fig. 1.2 File transfer protocol process

12. Terminal emulation (TELNET). It allows a workstation to access the server for an application program. This enables you to control the server and communicate with other servers on the network. The workstation appears as a down terminal that is directly attached to the server. The user feels like he/she is using the server directly. **TELNET** enables PCs and workstations to function as dumb terminals in sessions with hosts on inter-networks.

13. Groupware. These applications are used to automate the administration functions of a modern office for instance **video conferencing** and **chatting**. They facilitate the work of groups and improve on their productivity; they can be used to communicate, co-operate, coordinate, solve problems, compete, and negotiate among others.

(i) Video Conferencing. This is the process of conducting a ***conference*** between two or more participants at different sites by using computer networks to transmit audio and video data. For example, a *point-to-point* (two-person) video conferencing system works much like a video telephone.

Each participant has a video camera, microphone, and speakers mounted on his or her computer. As the two participants speak to one another, their voices are carried over the network and delivered to the others speakers, and whatever images appear in front of the video camera appear in a window on the other participant's monitor.

(ii) Chatting. It is a real-time communication between two users via computer. Once a chat has been initiated, either user can enter text by

typing on the keyboard and the entered text will appear on the other user's monitor. The two must be online for a chat to be initiated. Most networks, cyber and online services offer a chat feature which enables computer users to chat as they go on with their work.

1.8 NETWORK HARDWARE

- Network hardware is the physical equipments needed to perform the data processing and communication within the network.
- It connects the different computer peripherals among a group of users, network hardware, NICs (Network Interface Cards), hubs, switches, cables, routers, modem, ISDN adaptors etc.
- Some of the common Network devices are :

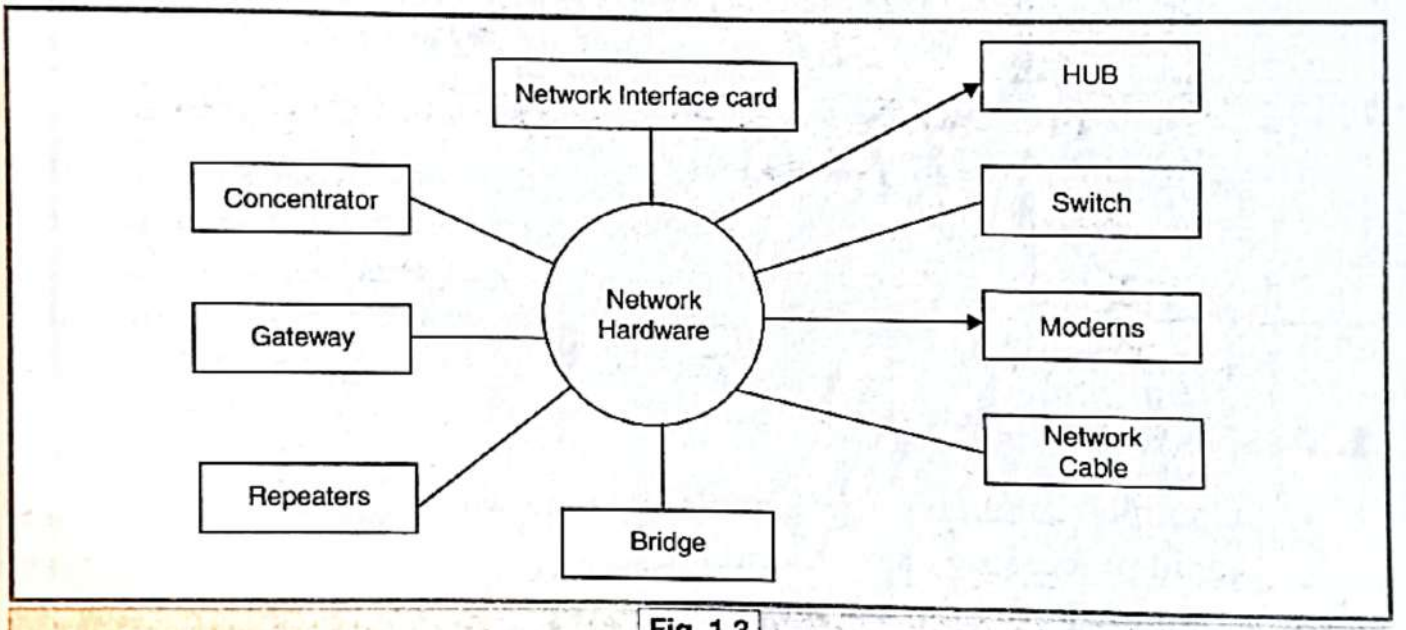


Fig. 1.3

1. Hub

- It connects the multiple ethernet segment together making them to act as a single segment.
- A hub is used to join number of Input lines. Data coming from any of Input line is transmitted to all other line. When using a hub, every attached devices share the common broadcast domain. Hence only one computer connected to hub is able to transmit at a time.
- Depending on the network topology, the hub provides the basic level I OSI model connection among the network objects.
- Hub are multiple port repeaters, and as such they obey the same rule as repeaters.

- They operate at OSI model physical layer.
- Hub organizes the cables and relays signal to the other media segment.

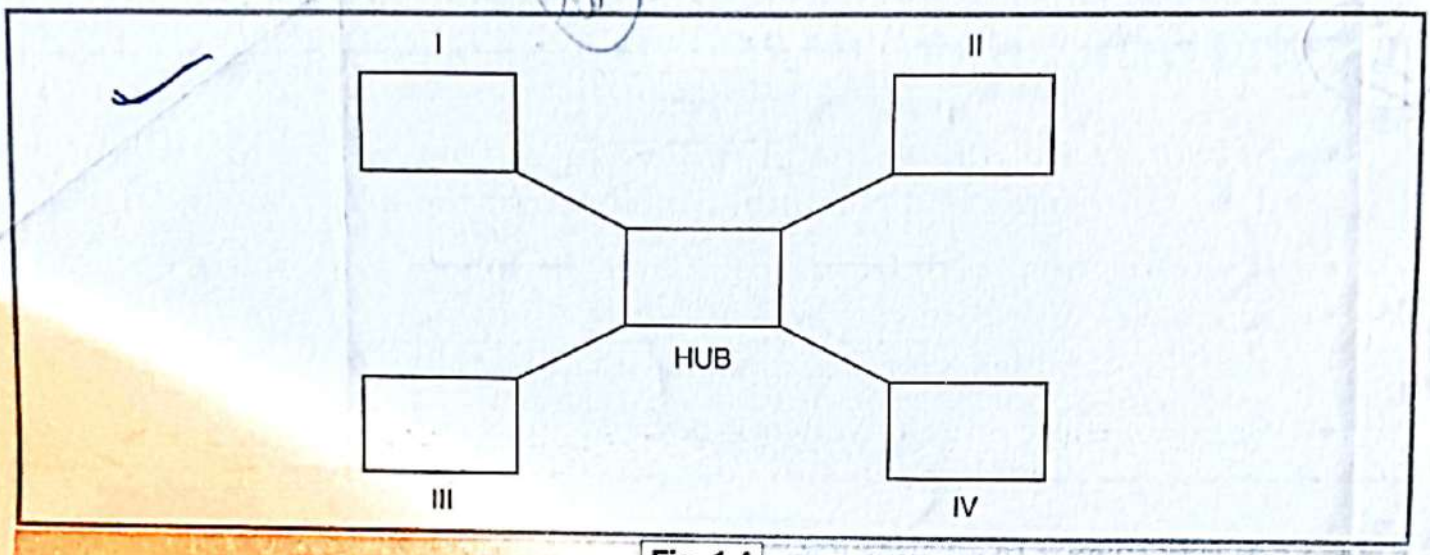


Fig. 1.4

There are three main types of hubs :

1. Passive Hub
2. Active Hub
3. Intelligent Hub

2. Passive Hub

- It simply combines the signals of a network segment. There is no signal processing or regeneration.
- It reduces the cable distance by half because it does not boost the signals.
- With a passive hub, each computer receives the signals sent from all other computers connected to the hub.

3. Active Hub

- They are like passive hub but have electronic components which regenerate and amplify the signals.
- By using active hub the distance between the devices can be increased.
- The major problem with the hub is that it amplifies the noise along with signal.

4. Intelligent Hub

- In addition to signal regeneration, intelligent hub performs some network management and intelligent path selection.
- Hubs can also be used to create multiple levels of hierarchy.

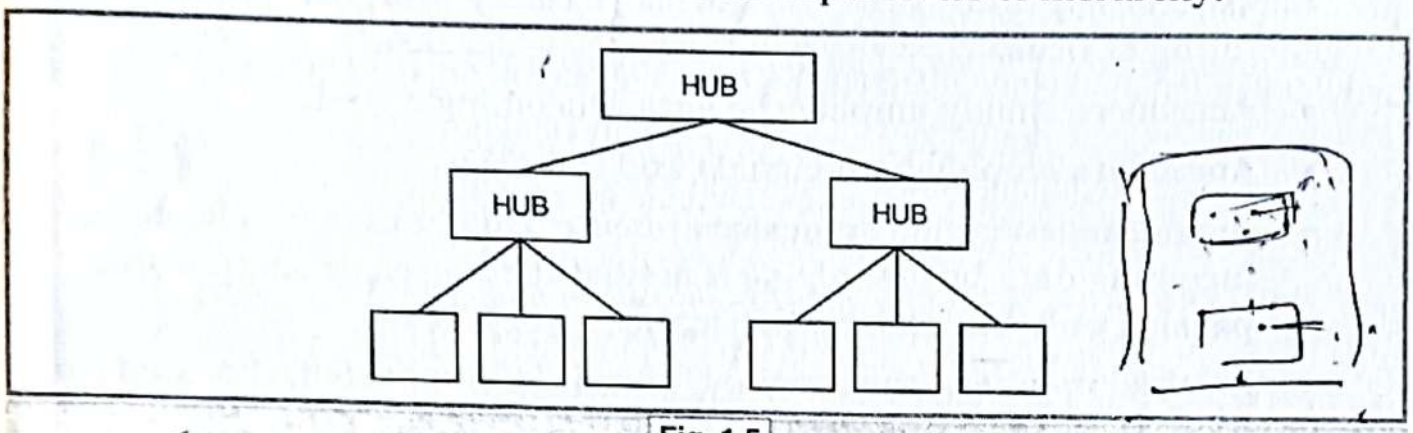


Fig. 1.5

5. Switch

- It is a device that allocate the traffic from one network segment to certain lines which connects the segment to another network segment. So unlike a hub a switch splits the network traffic and sends it to the different destination rather than to all system on the network. It works an the layer 2 of OSI reference model. It is a data link layer network device. There are four forwarding methods of a switch.

1. Store and forward : It buffers and perform checksum on each frame before forwarding it on.

2. Cut through : the switch only reads upto the frame hardware address before starting to forward it. There is no error checking with this method.

3. Fragment free : It retains the benefits of both "Store and forward" and "cut through". Fragment free checks the first 64 bytes of the frame, where addressing information is stored.

4. Adaptive switching : A method of automatically switching between the other three modes.

6. Repeaters

- All transmission media attenuate the electro magnetic waves that travel through them.
- Attenuation therefore limits the distance any medium can carry data. Adding device that amplifies the signal can allow it to travel farther, increasing the size of the network.

- For example, if one is connecting computers that are more than 100 meters apart using Ethernet cable, one will need a device that amplifies signals to ensure data transmission.
- Devices that amplify signals in this way are called repeaters.

Repeaters fall into two **categories namely amplifiers and signal-**regenerating devices.

- Amplifiers simply amplify the entire incoming signal.
- Amplifiers amplify both signals and the noise.
- Signal regenerating repeaters create an exact duplicate of the incoming data by identifying it amidst the noise, reconstructing it and passing only the desired information.
- In this manner, the original signal is duplicated, boosted to its original strength and then sent.
- A repeater is a hardware device used to extend a LAN.
- The repeater, which connects two cable segment, amplifies and sends all the signals that occur on one segment to other segment.
- Any pair of computers on the extended LAN can communicate. The computer do not know whether repeater separates them.
- Repeaters extend the distance of a signal of a single network. When a repeater is installed, it creates a physical break in the cable.
- The signal is received on the side of the repeater, regenerated and passed on to the next section of cable.

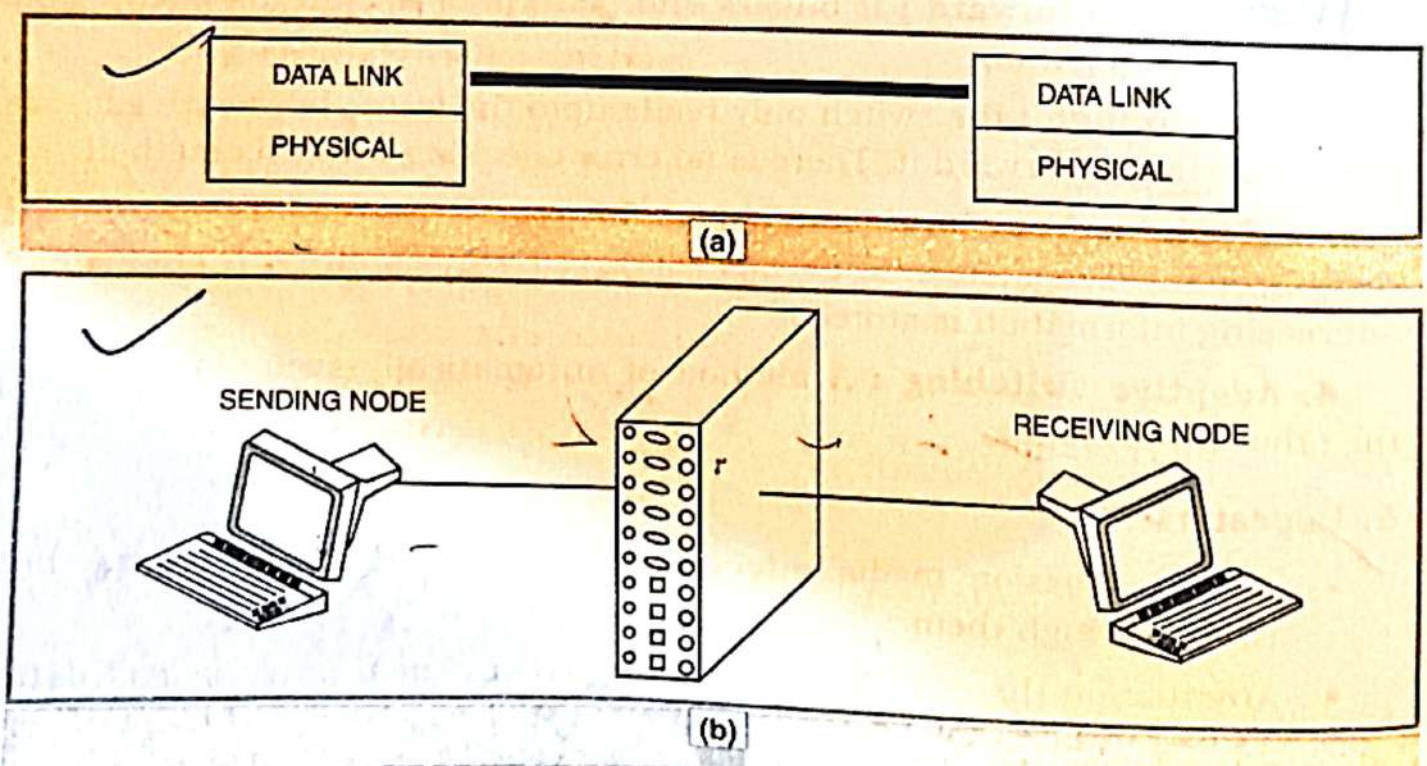


Fig. 1.6 (*a*) Repeater (*b*) The Application layer

- A repeater does not split a network, but takes everything from each side and pass it out the other side.
- The sole purpose is to compensate for any degradation in signal quality that may have occurred prior to the repeater being used.
- Repeater Simply deal with the actual, physical signal on a network, they operate at physical layer of OSI model.

7. Bridge

- The next level of connection between two networks is called bridge.
- A bridge connects two fundamentally identical networks that have some different physical element at the bottom.
- For example, a bridge connect at Layer 3 two networks with different bottom layer; everything from layer 3 up must be same.
- The best example of a bridge in current use is between a broadband token and a base band token network.
- Everything on them is identical except the hardware system.
  - Bridges can regenerate signals in order to extend network lengths. Because bridges actually read the packet address, they are considered to operate at the Data Link layer of the OSI model.
- The use of the bridge increase the maximum possible size of network. unlike a repeater, which simply passes on all the signals it receives, a bridge selectively determines the address of all the signal it receives.
- The bridge reads the physical location of the source and the destination computers from this address. A bridge operates in the following manner.
  (a) A bridge receives all the signals from both segment A and B.
  (b) The bridge reads the addresses and discards all signals from segment A, That signals from segment A addressed to a computer on segment B are retransmitted to segment B.
  (c) The signals from segment B are treated in the same way.

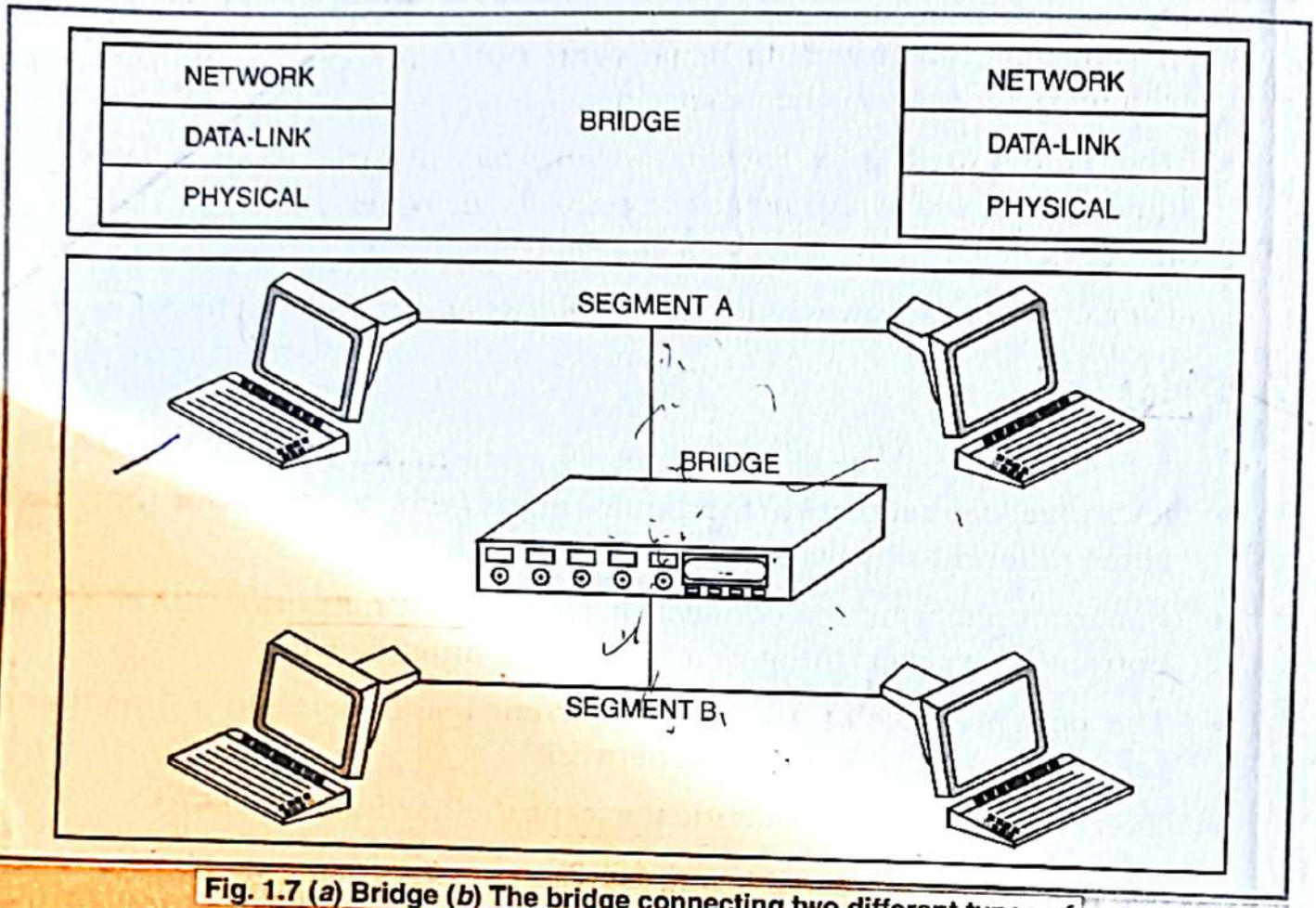


Fig. 1.7 (*a*) Bridge (*b*) The bridge connecting two different types of networks illustrates how signal pass through a bridge.

- Bridges are regenerate signals in order to extend network lengths.
- Because bridges actually read the packet address, they are considered to operate at the Data link layer of the OSI Model.

8. Router

- Routers are devices that connect two or more networks. It consists of a combination of hardware and software. the hardware can be network server, a separate computer.
- The hardware includes the physical interfaces to the various networks in the inter network.
- The two main pieces of software in a router are the operating systems and the routing protocol.
- Routers use logical and physical addressing to connect two or more logically separate networks.
- They accomplish the connection by organizing the large networks into logical network segments.
- Each of these sub networks if given a logical address.

- This allows the network to be separate but still access each other and exchange data when necessary.
- Data is grouped into packets, or blocks of data. Each packet, in addition to having a physical devices address has a logical network address.
- A router between two LANs receives messages from both networks, checks their destination and transmits the message to the required LAN.
- Since messages are stored in the routers system before re-transmission, routers are said to implement a store and forward technique.

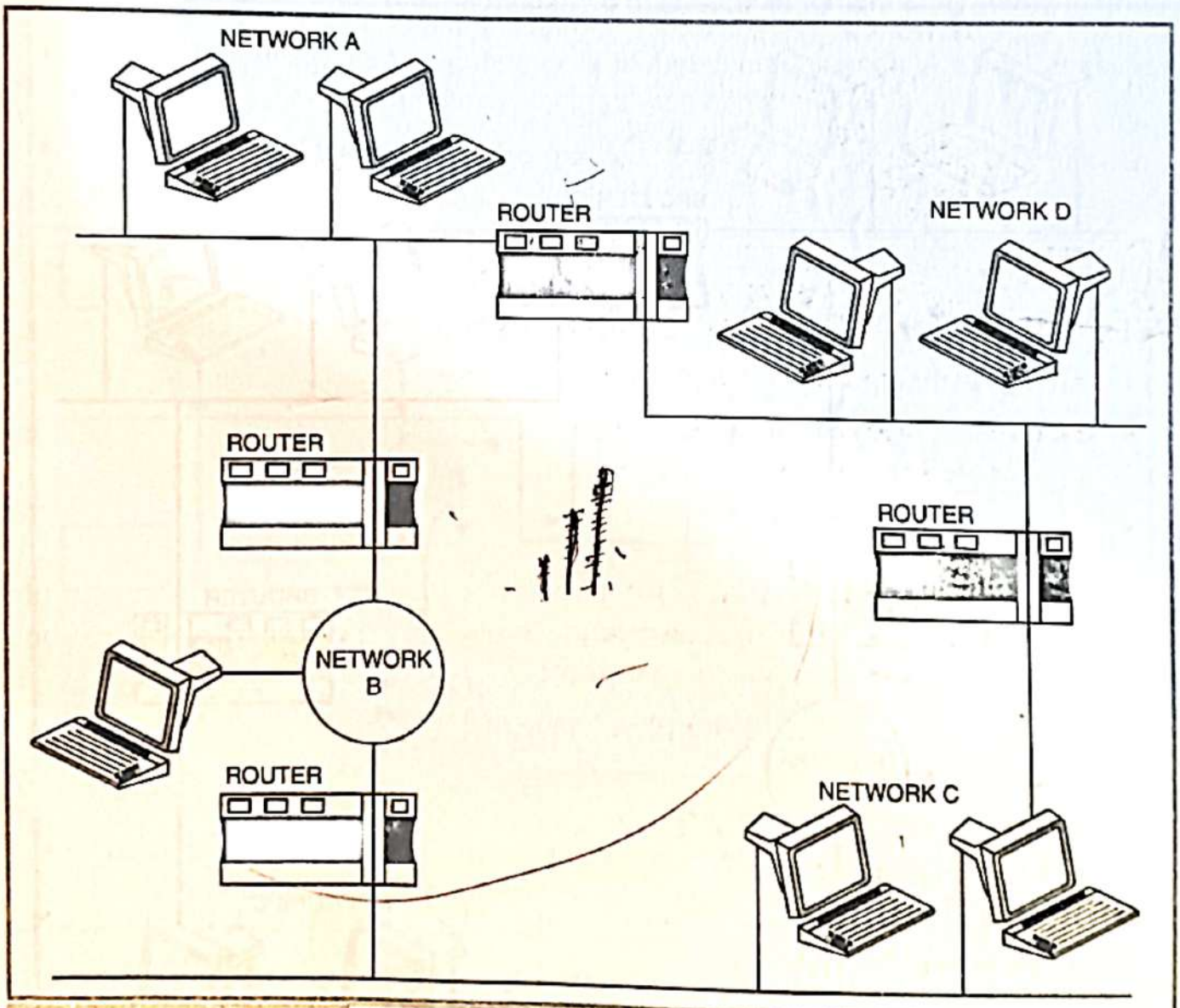


Fig. 1.8 Networks connected by routers

- Router work at the network layer of the OSI Reference model. Routers slow down network communication to a small extent, so do not use them unnecessarily.

9. Brouter :-

- It is the Combination of Bridge and router.
- A brouter first ties to deliver the packet based on the network protocol information.
- If the brouter does not support the protocol the packet is using or cannot deliver the packet based on protocol information, it bridges the packet by using the physical address.
- The router simply discards a packet if it does not have a correct logical address.
- A brouter can be a more affordable option to having both a router and a bridge.

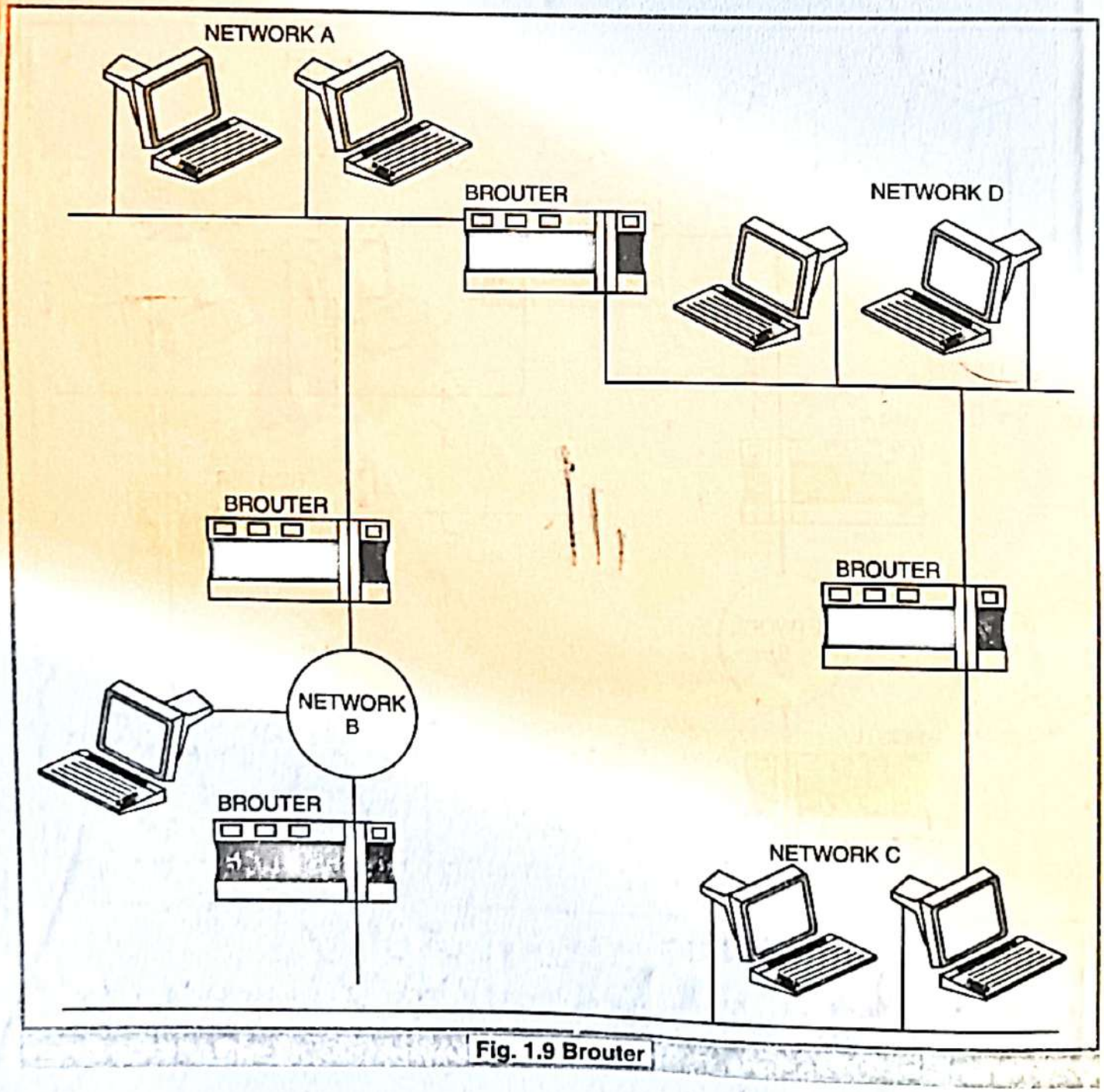


Fig. 1.9 Brouter

10. Gateways

- As we know that Router cannot interconnect two different networks that use different protocols.
- To do this job, special device, called gateway are used.
- The network using different protocols use different addressing formats.
- These types of addresses are different for different type of network.
- For example, the SNA network of IBM use different addressing and protocols from Ethernet.
- If SNA and Ethernet are to be connected, a gateway will have to be used.
- In the below figure the gateway is in between Network A and Network B.
- The gateway translates the packet from one type of network to another type.

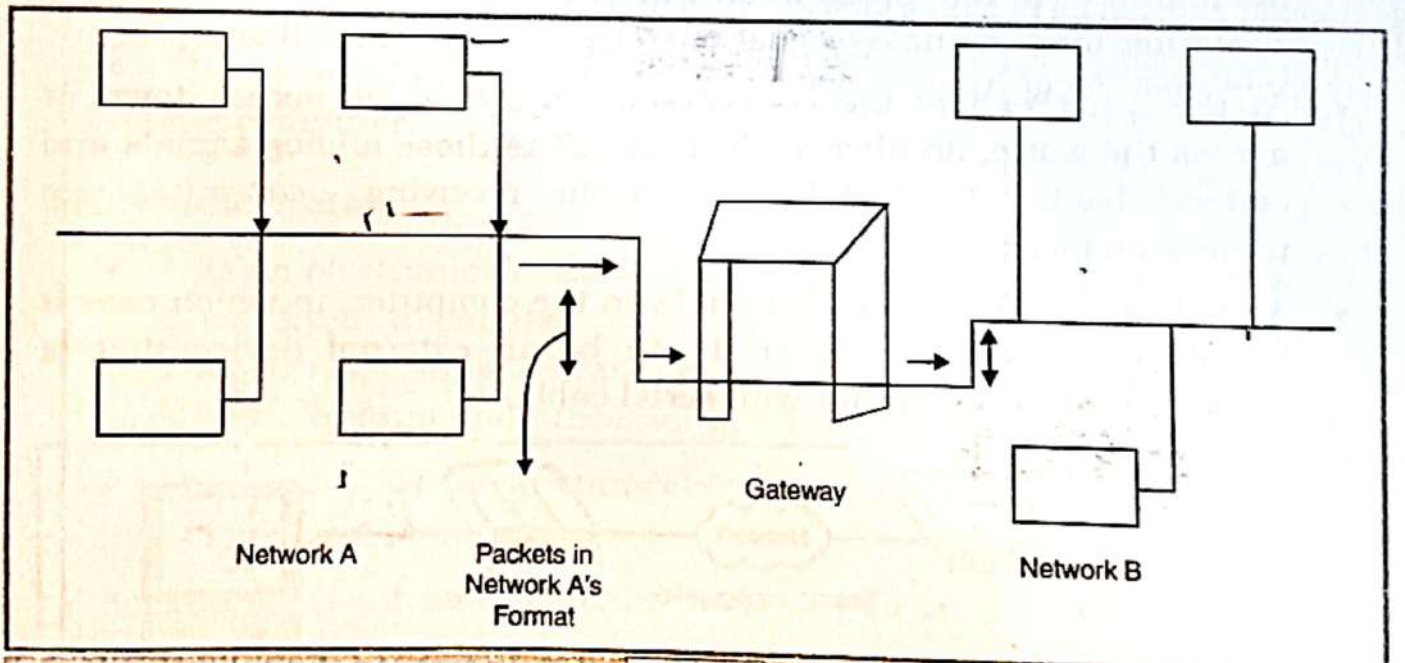


Fig. 1.10

- Gateway has the potential to work at all seven layers of OSI Reference model. It is protocol converter.

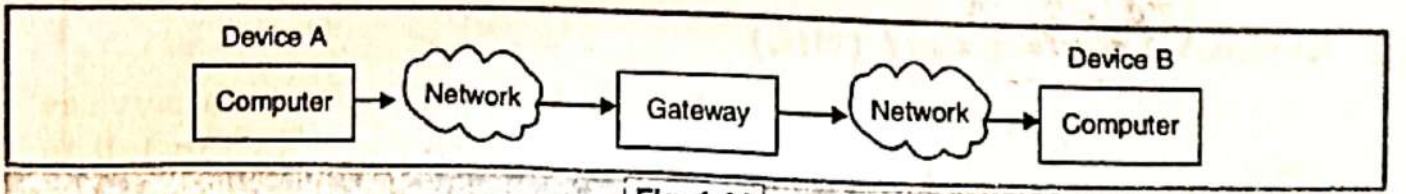


Fig. 1.11

- A gateway is generally software installed within a router.

- The gateway understands the protocols used by each network linked into the router and is thereforeable to translate frame one to another.
- In some cases, the only modification necessary are the header and trailer of packet.
- In other cases, the gateway may adjust the data rate, size and format as well.

11. Modems

- Modem is the device used to convert digital signals to be communicated over an analog channel such as a telephone line to sine wave at sending station end and back to digital signals at the receiving end.
- They are used to connect two distant located PCs so that PCs can communicate with each other using telephone lines.
- Modem convert communication signals from a the computer can understand to a form the phone system can convey and vice-versa. Modulation is the process of converting a digital signal from a computer into an analog signal the telephone system will accept.
- At the other end of the connection, whether it be across town or across the world, another modem interprets those analog signals and convert back into digital form so the receiving computer can understand them.
- A modem can be installed internally in the computer, in which case it is called internal modem or it can be an external device that is connected to the computer with serial cable.

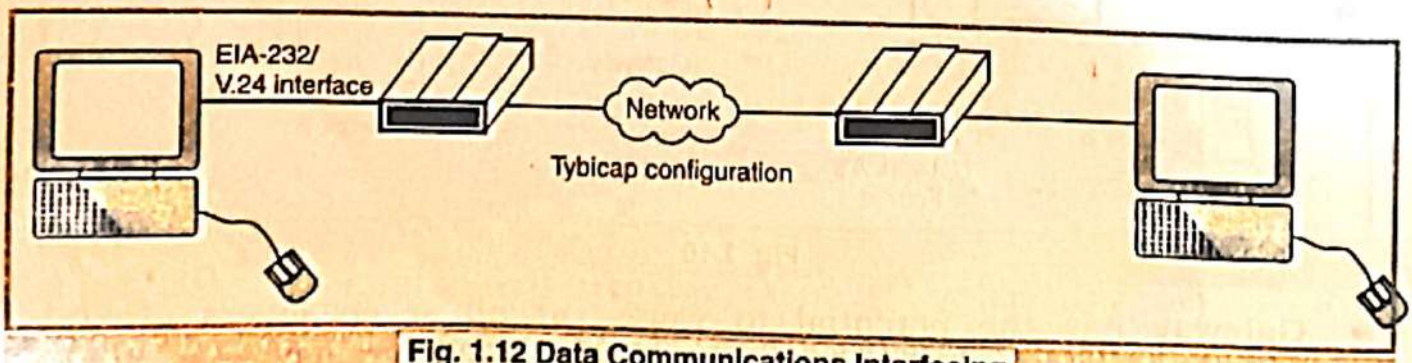


Fig. 1.12 Data Communications Interfacing

12. Network Interface Card (NIC)

- All LANS that use wire as the physical Transmission media services the client machine to have a network interface card (NIC) install to provide the circuitry and connection to this wires.

- These NIC must be compatible with both computer's own internal bus and type of Network architecture that is used.

13. Network Cable

The network cable can be twisted pair, coaxial or fiber optic cable.

— Twisted pair cable is cheap but is the slowest.

— Co-axial cable are of two type baseband and broadband. Baseband cable can carry only one signal at a time, but it is fast. Broadband co-axial cable can carry more than one signal at a time.

— Fiber-optic cable are made from tiny strands of glasslike material. These strands transmit light pulses with very high frequency. Each pulse represents one bit of data.

14. Cable Interface Unit

- The cable interface unit, sometime called a hub, sends and receives signals on the network cable.
- This units is a box outside the computer.
- The network interface card is inserted into an expansion slot inside the computer.

15. Concentrator

- It is an electronic device which can merge the various communication lines from a number of hosts and provides a link to another concentrator in a hierarchical or tree shape arrangement or link directly to front end processor of a host computer.
- It provides a central connection point for cables from workstations, servers and peripherals.
- Most concentrators contain the ability to amplify the electrical signal they receive.
- To avail the facility of network you have to maintain the co-ordination between network hardware and software.

1.9 NETWORK SOFTWARE

For the smooth working of network software the following are the important elements.

1. Network Operating System (NOS)

2. Network Protocol (NP)
3. Device Driver or Network Driver System

1. Network Operating System

Definition :

Network Operating System (NOS) is program or set of programs that instruct the computer to schedule and supervise work, managed shared computer resources operate and control peripheral devices such as modems and printers.

Commonly used NOS are

1. Windows NT
2. Linux

1. It controls a network and its messages (e.g. packets) traffic and queues,
2. It control in access by multiple users to network resources such a files.
3. It control network administrative functions.
4. It provides the security.
5. It provides file, print, web services back up and replication services.
6. Support internetworking such as routing and WAN ports.
7. User management and support for logon and logoff, remote access; system management, auditing tools with graphics.

2. Network Protocol (NP)

- It is set of rules and conventions for communication between network devices.
- Protocols for computer networking all generally uses packet switching technique to send and receive messages in the form of packets.
- It provides the techniques to identify and make connection with each other, as well as formatting rules that specify how data is packaged into messages sent and received.
- Modem operating system like microsoft windows contain built-in service that implement support for some network protocols.
- Application like web browser contain software libraries that support high level protocol necessary for that application to functions.

3. Device Driver

- It is a small computer program that acts as an interface, between hardware component and computer system typically for communicating with the devices.
- In computing, software driver is a compute program allowing higher level computer programs to interact with a hardware device.
- Drivers are hardware dependent and operating system specific.
- They usually provide in interrupt handling required for any necessary asychronous time dependent hardware interface.
- Device deriver program control overall working of some hardware like printer, scanner etc.
- Every different model of same hardware may have different model of same hardware may have different deice driver *e.g.* all in different models printer of HP have different device driver.
- In computer networks, communication occurs between entities in different system.
- An entity is anything capable of receiving or sending the information.
- Two entities cannot simply send bit stream to each other and expect to be understood.
- For communication to occur, the entity must agree on a protocol.
- A protocol is set of rules that governs the communication.
- Hence for the communication between the two entities set of rules are required.
- Software by definition is the set of rules in a sequence.
- Software defines what is communicated, how it is communicated, and when it is to be communicated.

The key elements of the software are

1. Syntax
2. Semantics
3. Timing

1. Syntax.

- The term syntax refers to the structure or format of the data, meaning the order in which they are present.

- For example a simple protocol might expect the first 8 bit of data to be the address of sender, the second 8 bit to be the address of the receiver, and the rest of the stream to be the message itself.

2. Semantics. It refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation. For example, does an address identify the route to be taken or final decision of the message ?

3. Timings. The term timing refers to two characteristics

1. When the data to be sent.
2. What is the speed of sending the data

For Example, If a sender produces data 100 Mbps but the receiver can produce the data at only 1 mbps, the transmission will overload the receiver and some data will be lost.

1.10 PROTOCOL HIERARCHY

- In layered architecture a computer network is partitioned into interconnected end systems using a subnetwork.
- The communication process is decomposed into hirarachical functional layer and hence a computer network has layered architecture. There can be N functional layer in computer network end system.
- The lowest layer is the inter connection media which is completely a physical layer.
- In general each layer has an active element which can be a piece of hardware or software to carry out various functions of each layer.
- It is known as **layer entity.** In layered architecture two types of communications takes place.
  * Hierarchical communication
  * Peer to Peer communication
- **Hierarchical communication** is the communication between layers of an end system for requesting and receiving services from lower layer.
- **Peer to peer** communication works between peer layers of two end systems for carrying out an assigned set of functions.

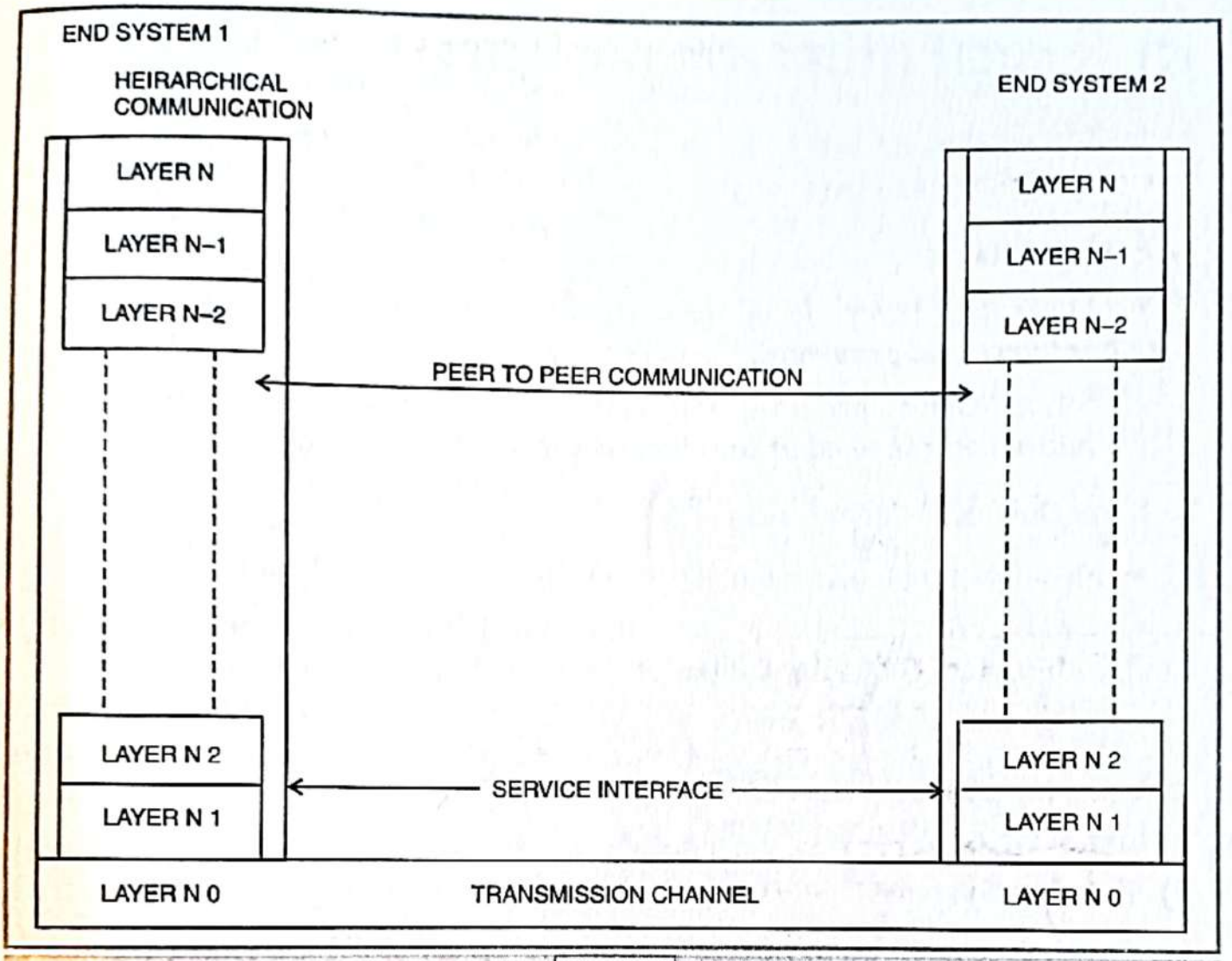


Fig. 1.13

- The procedures and rules for hierarchical communication are specified by the service interface definition while for peer to peer communication they are called **protocol.**
- The message exchange between adjacent layers during hierarchical communication are called interface control information while the message exchanged between the peer layers are called **protocol control information.**
- The layered architecture of a computer network in shown is fig. 1.13 along with hierarchical & peer to peer communication.
- For heirarchical communication the direct paths are available between two layers of a subsystem.
- But for peer to peer communications the direct paths are not available between peer layers.
- Hence protocol control information is exchanged using the services provided by the lower layers.

1.11 DESIGN ISSUES FOR THE LAYERS

In this section we are going to discuss some of the key design issues that occur in computer networking.

1. Addressing

- For every layer, it is necessary to have a mechanism to identify senders and receivers.
- Since there are multiple possible destinations, some form of addressing is needed in other to specify a specific destination.

2. Direction of Transmission

- Another point in design issues is the direction of data transfer.
- Based on whether the system communicates only in one direction or otherwise, the communication systems are classified as :
  - (i) Simplex systems
  - (ii) Half duplex systems
  - (iii) Full duplex systems

(i) Simplex Systems

- In these systems the information is communicated in only one direction. For example the radio or TV broadcasting systems can only transmit. They cannot receive.
- In data communication system the simplex communication takes place as shown in Fig. 1.14.
- The communication from CPU to monitor or keyboard to CPU is unidirectional.
- Keyboard and traditional monitors are examples of simplex devices.

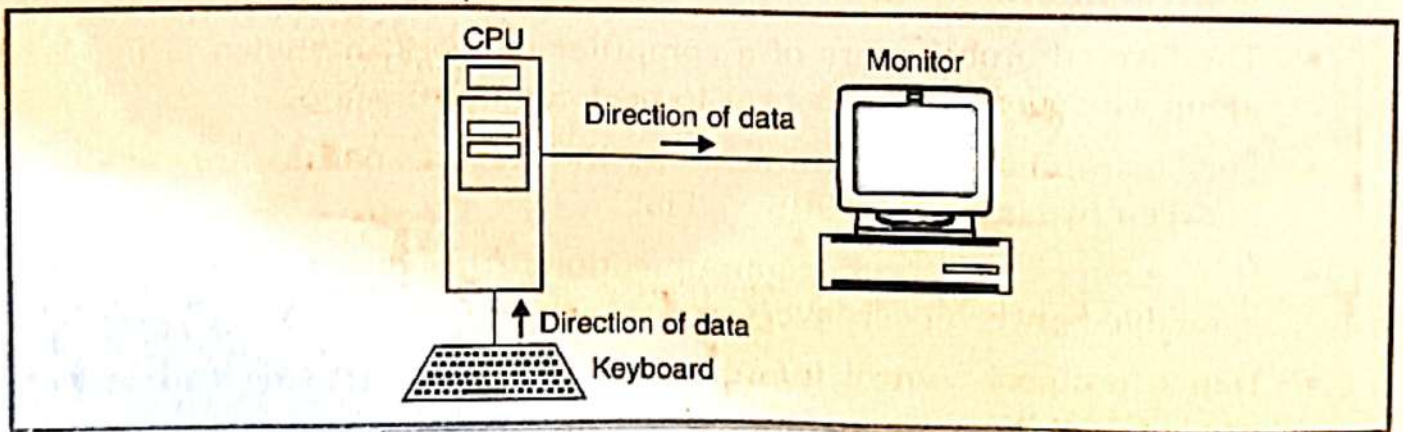


Fig. 1.14 Simplex mode of data transmission

(ii) Half duplex systems

- These systems are bi-directional, i.e. they can transmit as well as receive but not simultaneously.
- At a time these systems can either transmit or receive, for example a transreceiver or walky talky set.
- A data communication system working in the half duplex mode is shown in Fig. 1.15.
- Each station can transmit and receive, but not at the same time. When one device is ending the other one is receiving and vice versa.

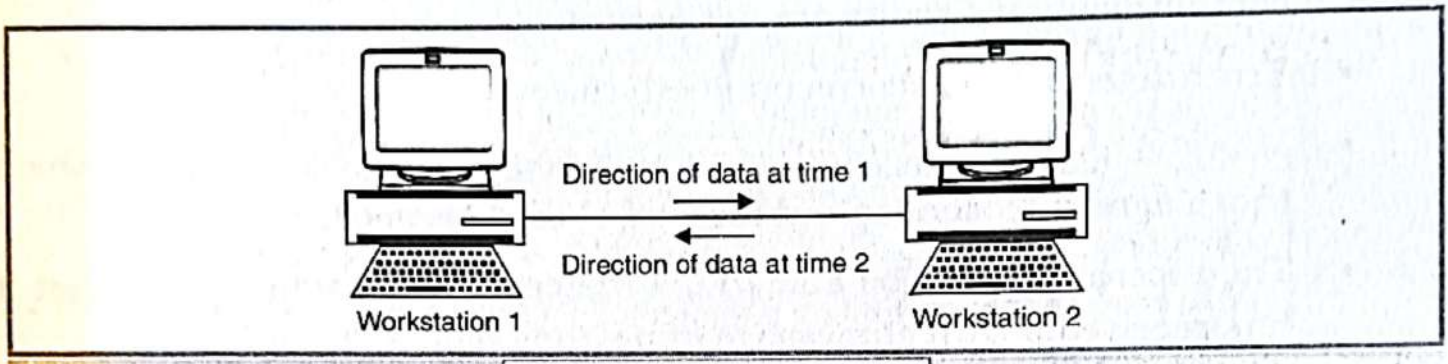


Fig. 1.15 Half duplex system

- In half duplex transmission, the entire capacity of the channel is taken over by the transmitting (sending).

(iii) Full duplex systems

- These are truly bi-directional systems as they allow the communication to take place in both the directions simultaneously.
- These systems can transmit as well as receive simultaneously, for example the telephone systems.
- A full duplex data communication system is shown in Fig. 1.16. Each station can transmit and receive simultaneously.

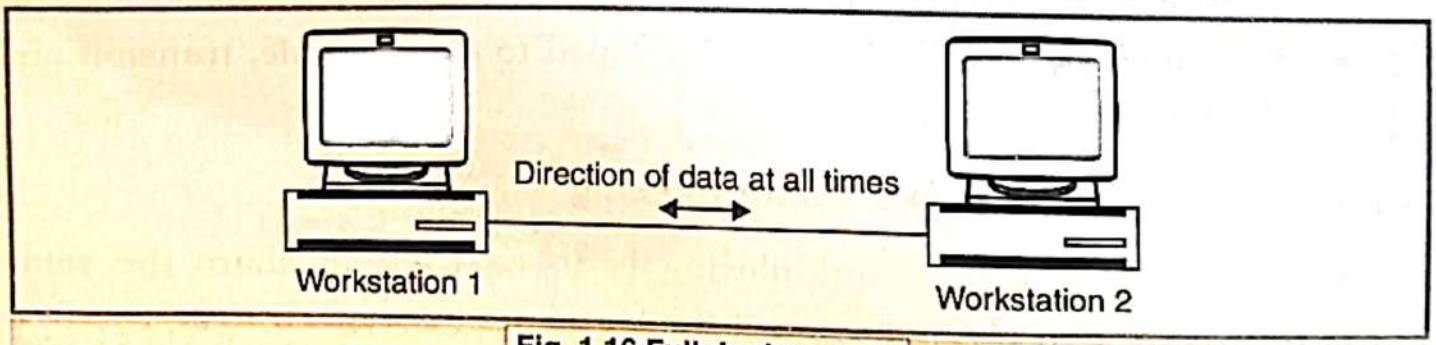


Fig. 1.16 Full duplex mode

- In full duplex mode, signals going in either direction share the full capacity of link.

- The link may contain two physically separate transmission paths one for sending and another for receiving.
- Otherwise the capacity of channel is divided between signals travelling in both directions.
- Many networks provide atleast two logical channels per connection, one for the normal data and the other for urgent data.

3. Error Control

- Another important issue is the error control because physical communication circuits are not perfect.
- Error detection and correction both the essential.
- Many error detecting and correcting codes are known out of which those agreed by sender and receiver should be used.
- The receiver should be able to tell the sender by some means, that it has received a correct message or a wrong message.

4. Avoid loss of sequencing

- All the communication channels cannot preserve the order in which messages are sent on it.
- So there is a possibility of loss of sequencing.
- To avoid this, all the pieces should be numbered so that they can be put back together at the receiver in the appropriate sequence.

5. Ability of receiving long messages

- At several levels, another problem should be solved, which is inability of all processes to accept arbitrarily long messages.
- So a mechanism needs to be developed to disassemble, transmit and then reassemble messages.

6. To use multiplexing and demultiplexing

- Multiplexing and demultiplexing is to be used to share the same channel by many sources simultaneously.
- It can be used for any layer. Multiplexing is needed in the physical layer.

1.12 INTERFACES AND SERVICES

- The basic function of each layer in the layered structure is to provide service to the layer above it.
- Now we will discuss exactly what service does it provide. But before that, let us define some important terms.

1. Entities and Peer Entities

- An entity is defined as the active element in each layer. An entity can be either a software entity or a hardware entity.
- The example of software entity is a process and that of a hardware entity is an intelligent I/O chip.
- Entities in the same layer but on different machines are called as peer entities.

2. Service Provider and Service User

- The entities at layer n implement services for the layer $(n+1)$ which is above the nth layer.
- So layer n which provides service is called as service provider and layer $(n+1)$ which takes this service is called as service user.

3. Service Access Points (SAPs)

- Refer Fig. 1.17 to understand the definition of SAPs.
- The long form of SAP is service access point. They are available at the interface of n and $n+1$ layer as shown in Fig. 1.17.

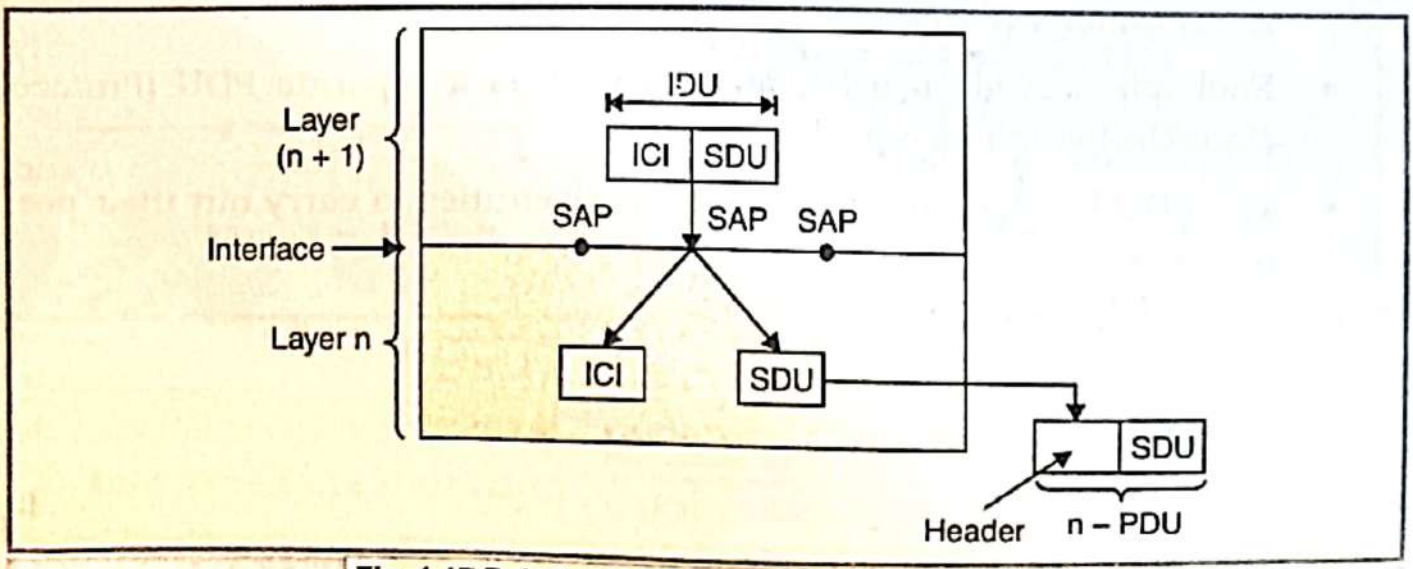


Fig. 1.17 Relations between layers at an Interface

- Services are available at SAPs. That means the layer *n* SAPs are those places at the interface where layer (*n* +1) can access the services being offered.
- Each SAP has a unique address for its identification.

4. Interface Data Unit (IDU)

- For successful exchange of information between two layers, a set of rules about the interface should be present.

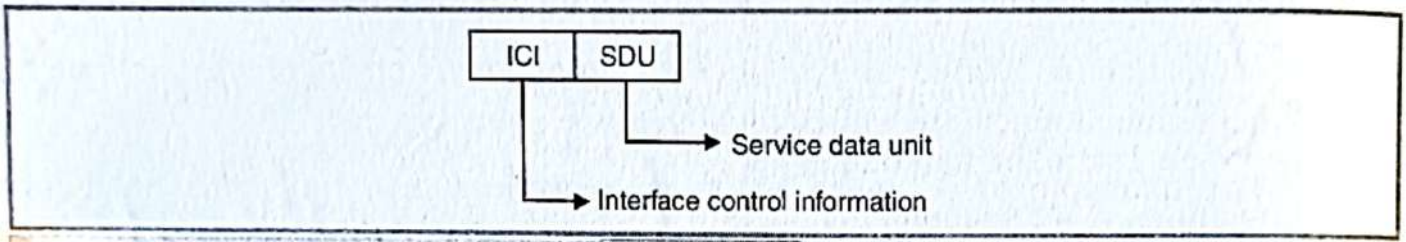


Fig. 1.18 IDU

- As shown in Fig. 1.18 the layer (*n*+1) entity passes in IDU (interface data unit) to the layer *n* entity through the SAP.
- An IDU consists of two parts namely SDU (service data unit) and ICI (interface control information).

5. Service Data Unit (SDU)

- SDU is a part of IDU. The SDU is the information passed across the network to the peer entity and then upto layer (*n*+1).
- ICI contains the control information which is necessary to help the lower layer (n) to do the necessary job.

6. Protocol Data Unit (PDU)

- In order to transfer the SDU, the layer n entity has to divide it into many smaller pieces.
- Each piece is given a header and sent as a separate PDU (Protocol Data Unit) such as a packet.
- The PDU headers are used by the peer entities to carry out their peer protocol.

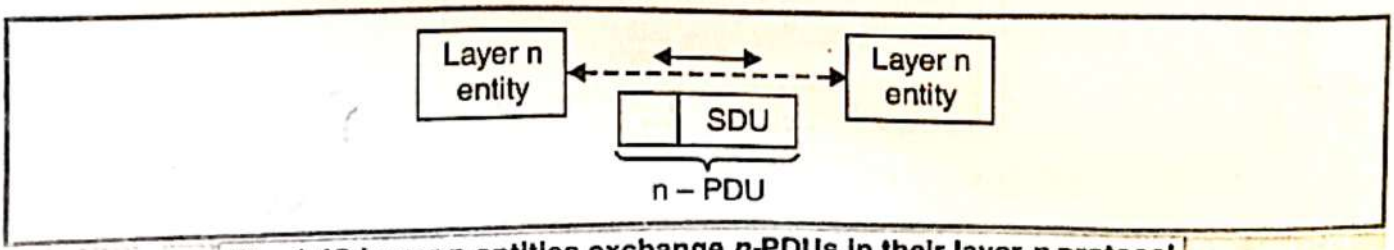


Fig. 1.19 Layer n entities exchange *n*-PDUs in their layer *n* protocol

- Some PDUs contain data while other PDUs contain the control information. The PDU header will identify or differentiate between different types of PDUs.
- They also provide sequence numbers and counts.

1.13 DATA UNITS

- There are five types of data units which are exchanged between adjacent and peer layers during their communication. The data unit and their functions are as follows.

1. Service Data Unit (SDU) :

- This is the user data which is transferred between ends of (N) **connections**.
- It is transferred transparently by layer (N + 1) to layer N, then to (N-1) and so on.
- The identity of data is preserved during the transfer. It is a part of interface data unit.

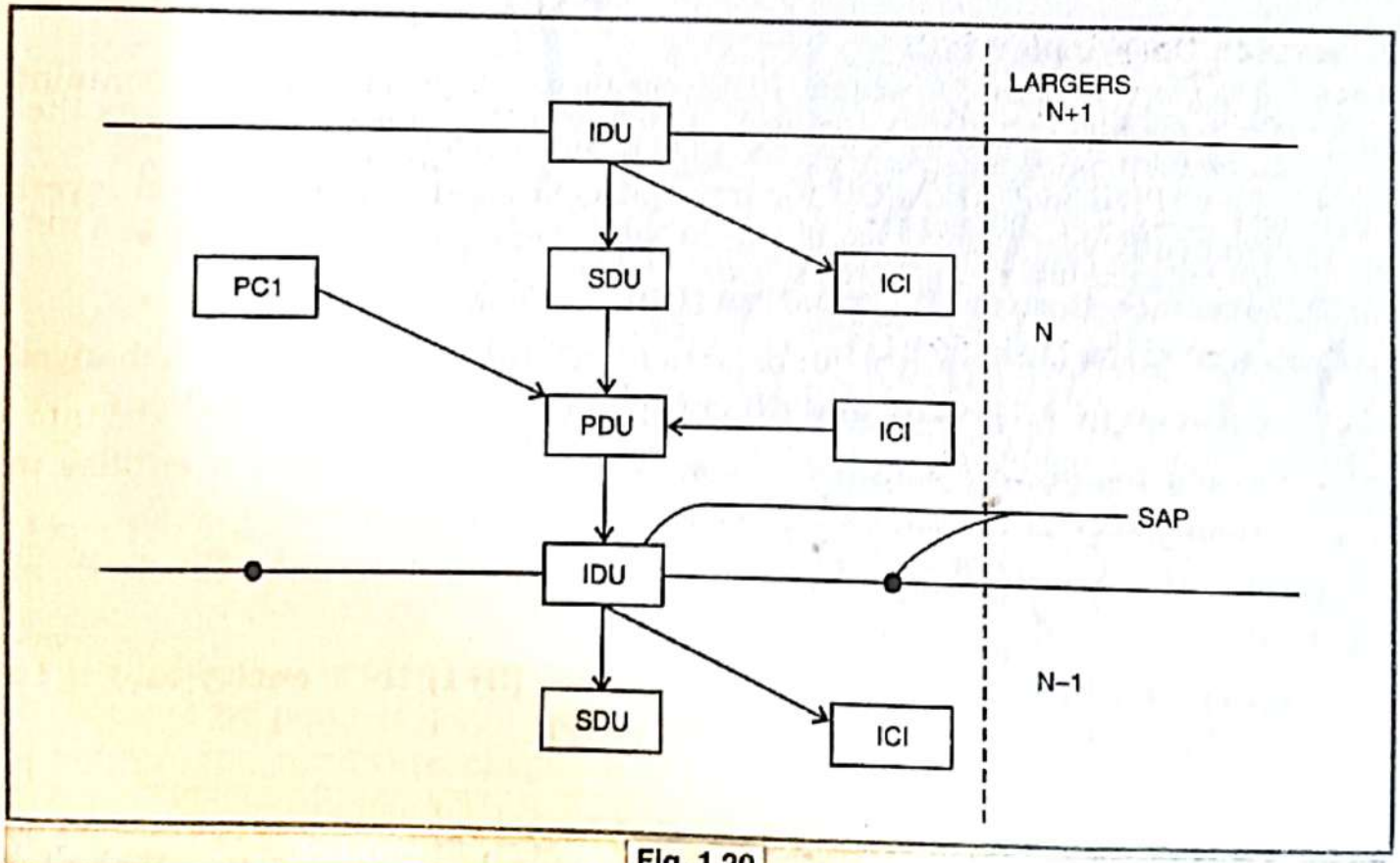


Fig. 1.20

2. Interface Data Unit (IDU) :

- The interface data unit is the total data unit transferred across the service access point between (N + 1) entity and N (entity).

- It includes the service data unit and some control information's known as interface control information.
- The interface data unit is transferred across layer boundaries.

3. Protocol Control Information (PCI) :

- It is the information exchanges by peer entities at different sites of the network.
- It instructs and entity to perform a service function. PCI is a fancy name for header.

4. Protocol Data Unit (PDU) :

- It is a combination of service data unit and protocol control information.
- When SDU is to be transferred the layer N entity fragments it into several pieces.
- Each of this piece is given a header and sent as a separate protocol data unit.
- The PDU headers are used by peer entities to carry out their peer protocol.
- They can identify which PDU contains data and which contains control information.
- The TPDU, SPDU, APDU for transport, session and application layers respectively.

5. Interface Control Information (ICI) :

- The interface control information is the information exchanged between (N + 1) entity and (N) entity to coordinate their functions.
- It is a temporary parameter passed between (N + 1) and N entities to invoke service functions like a procedure call argument.

The communication between layers with various data units is shown in fig. 1.20.

The point where IDU's are crossing from (N+1) to N entity and N to (N-1) entity is the service access point (SAP).

1.14 CONNECTION ORIENTED SERVICE

- The ***connection-oriented service*** establishes a logical connection between source and destination machines before any data are transferred that provides error control and flow control.

- Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received.
- Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.
- With connectionless service, in contrast, it is conceivable that a lost acknowledgement causes a packet to be sent several times and thus received several times. Connection-oriented service, in contrast, provides the network layer processes with the equivalent of a reliable bit stream.

When connection-oriented service is used, transfers go through three distinct phases.

1. In the first phase, the connection is established by having both sides initialize variables and counters needed to keep track of which frames have been received and which ones have not.
2. In the second phase, one or more frames are actually transmitted.
3. In the third and final phase, the connection is released, freeing up the variables, buffers and other resources used to maintain the connection.

- The used error control mechanism is the **ARQ (Automatic Repeat Request),** ARQ treats with two different errors : Lost PDU and Damaged PDU. The general performance of ARQ is :
  - The transmitter sends the frame.
  - When the frame is in the receiver, the station checks whether there are any errors in the frame using a Cyclic Redundancy Check (CRC).
  - The receiver send one acknowledge or a negative acknowledge depend whether the result of CRC.
  - The transmitter will retransmit the frame if receive a negative ACK or doesn't receive any ACK.

Consider a typical example : A WAN subnet consisting of routers connected by point-to-point leased telephone lines. When a frame arrives at a router, the hardware checks it for errors, then passes the frame to the data link layer software (which might be embedded in a chip on the network interface board). The data link layer software checks to see if this is the frame expected, and if so, gives the packet contained in the payload field to routing software. The routing software then chooses the appropriate outgoing line and passes the packet back down to the data link layer

software, which then transmits it. The flow over two routers is shown in Fig. 1.21.

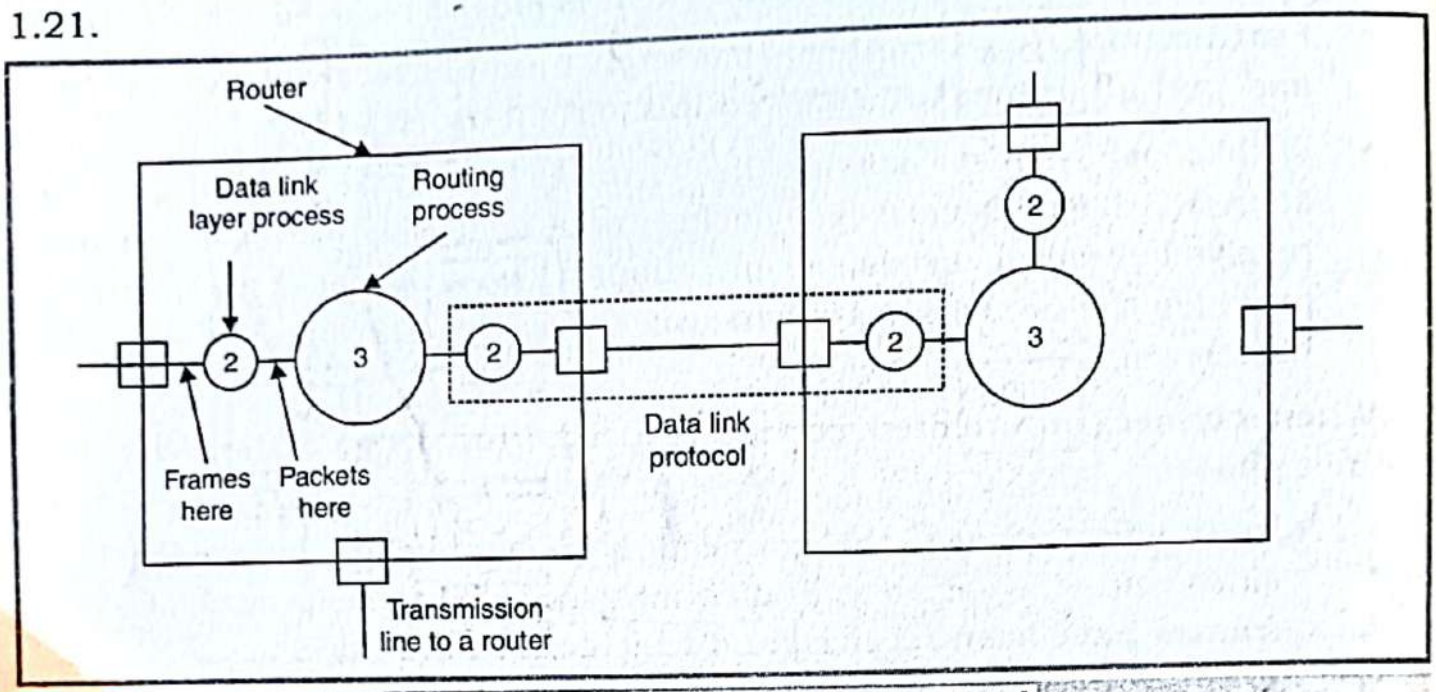


Fig. 1.21 Placement of the data link protocol

- The routing code frequently wants the job done right, that is, with reliable, sequenced connections on each of the point-to-point lines.
- It does not want to be bothered too often with packets that got lost on the way.
- It is up to the data link protocol, shown in the dotted rectangle, to make unreliable communication lines look perfect or, at least, fairly good.
- As an aside, although we have shown multiple copies of the data link layer software in each router, in fact, one copy handles all the lines, with different tables and data structures for each one.
- Connection-oriented network also support two types of connections :

1. Point-to-Point *(private) connections refer to a pathway from one location to another* (Node A to Node B).

- An example is a mainframe terminal connected to a mainframe front-end-processor. **Point-to-Point Networks** have many connections between individual pairs of machines.

2. Point-to-Multipoint (conference) *connections refer to a pathway from one location to many locations* (Node A to Node B, C, and D).

- Years age, multipoint links were used to connect multiple terminals to a mainframe front-end processor.
- In today's LAN environment, multipoint links are used to connect multiple devices in bus, tree or star topologies.

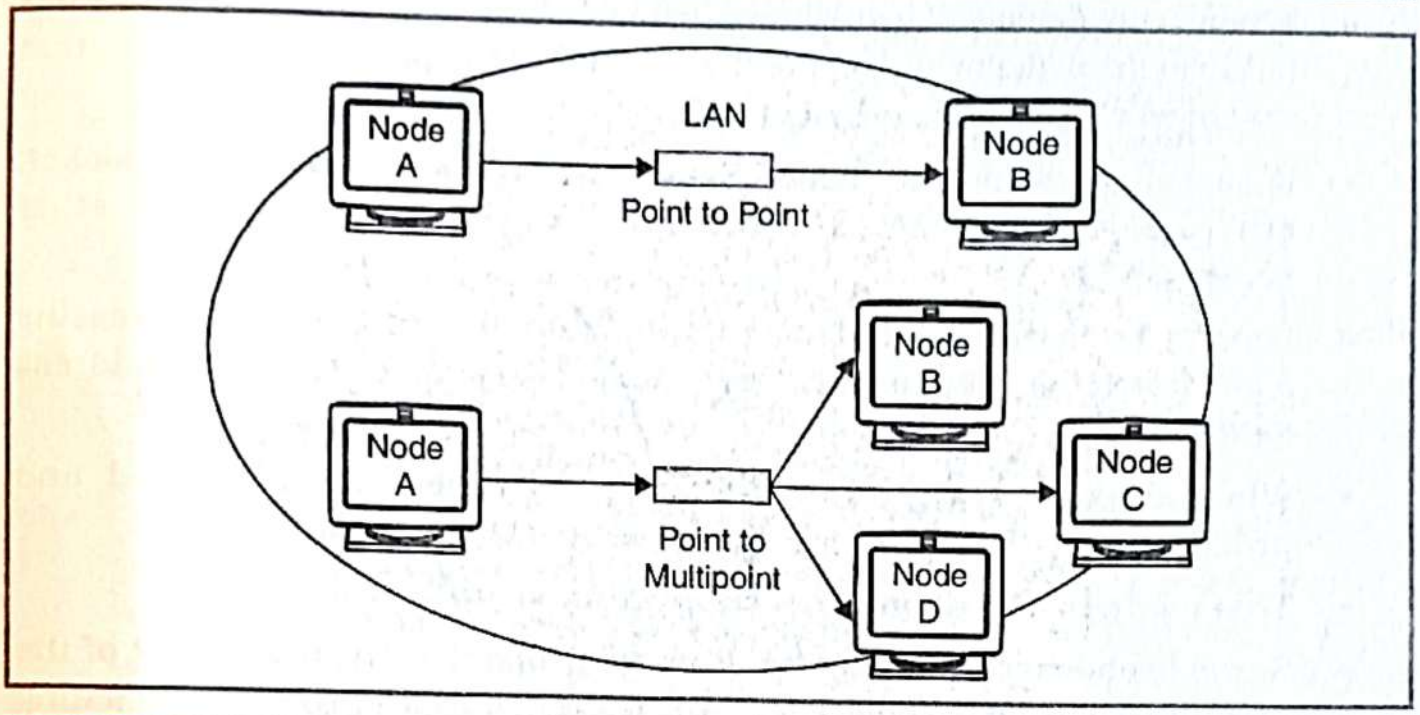


Fig. 1.22 Connection oriented service

- **Point to Point links** are ***different*** than Multipoint because it implies dedicated bandwidth.
- Because the bandwidth is dedicated in a point to point environment, no addressing (of nodes) is needed.

In a multipoint link the channel (the communication path) is shared which complicates communication and the efficiency of using the channel.

1.15 Connectionless/Broadcast Network

- **Broadcast-based communication** is connectionless in that it does not require the transmitting party to contact the receiving party before sending information.
- With a radio station, the news is **broadcast** whether you are listening or not.
- If you were listening, but you missed something, you cannot ask the announcer to go back and repeat what they just said.
- In the same way, a **connectionless networks** simply broadcasts information to all who may or may not be listening.
- ***Broadcast Networks*** have a single communication channel.
- This single communication channel is shared by all the machines on the network. Information can be transfer from source to destination in short messages called ***packets.***

- Where the packet is to be transmitted, it is specified by an address field within the packet. While receiving a packet, a destination machine checks the address field.
- If the address is matched, then the machine processes the packet; otherwise it just ignored because the packet is intended for other some other machine.
- Broadcast Networks generally also allow the possibility of addressing a packet to all destinations by using a special code in the address field.
- 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.***
- Some broadcast systems also support transmission to a subset of the machines, it is known as ***multicasting.*** In the multicasting technique, one bit is reserve in the address field.
- The remaining (n – 1) address bits can hold a group number.
- Each machine can subscribe to any or all of the groups. When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.
- ***Unreliable Unacknowledge connectionless service*** does not require a session connection between sender and receiver.
- The sender simply starts sending **packets (Called datagrams)** to the destination.
- This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers.
- Neither system must maintain state information for the systems that they send transmission to or receive transmission from.
- A connectionless network provides minimal services.
- If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer.
- Most LANs use unackowledged connectionless service in the data link layer. The advantages are :
  - When is not necessary to have information of the successful delivery of the data, such as applications involving the periodic sampling of data sources, for example monitoring sensors. It is also appropriate for real-time traffic, such as voice, in which late

data are worse than bad data. With this service we are free of overhead of connection establishment and maintenance.

- When a higher layer protocol provides the necessary error control, flow control and reliability, it would be inefficient to duplicate them in the LCC.

- In ***Acknowledged connectionless service*** the source machine send the frames independently to the destination machine without logical connection used, but with acknowledgement to each and every frame from the destination machine, and the error and flow control is handed through ARQ method, stop and wait.
- The advantages are in process control and automated factory environments and time-critical alarm or emergency control signals are the scenarios where acknowledged connectionless service distinguishes because the delivery is assured and is not necessary to wait for a connection to be established.
- The network layer can always send a packet and wait for it to be acknowledged.
- If the acknowledgement is not forthcoming before the timer expires, the sender can just send the entire message again.
- The trouble with this strategy is that frames usually have a strict maximum length imposed by the hardware and network layer packets do not.
- If the average packet is broken up into, say, 10 frames and 20 percent of all frames are lost, it may take a very long time for the packet to get through.
- If individual frames are acknowledged and retransmitted, entire packets get through much faster.
- On reliable channels, such as fiber, the overhead of a heavyweight data link protocol may be unnecessary, but on wireless channels, with their inherent unreliability, it is well worth the cost.

1.15.1 Connection oriented and Connection Less Services

Layers can offer two different types of services :

(1) Connection oriented services.

(2) Connectionless services

1. Connection Oriented Service.

- The connection oriented service requires the user to first establish a connection, use the connection and then release the connection.

- It is modeled after the telephone system.
- To talk to some one, you pick up the phone, dial the number, talk and then hang up.
- Hence establishes connection means dial up the phone to make a connection, use the connection means talk and disconnect the connection means hang up.
- In context with the transferring of the data it is reliable in terms of packet arriving in the same order as it in desired.
- Packet does not carry the destination address since the connection is explicitly made with the destination before sending the data.
- Example of connection oriented service are TCP, X.25 connection oriented service can be of three types :
  (1) Reliable Message Stream
  (2) Reliable Byte Stream
  (3) Unreliable Connection

2. Connectionless Services.

- It does not require a session require a session connection between sender and receiver.
- This is modelled after the postal system.
- This service is not reliable, since the packet may arrive in any order.
- In this scheme, the datagram is used in which the address of destination is given.
- Each datagram routed independent of the other.
- There is no sequence of arrival because it is possible if two messages are sent at the same may reach at the same time on the same destination as the message is routed independently.

Example of connectionless services in UDP. It can be of following type :
(1) Unreliable datagram
(2) Acknowledge datagram
(3) Request Reply

- To summarizes the type of services provided by connection oriented and connectionless services are :

	Service	Example
Connection oriented	Reliable Message Stream Reliable byte Stream Unreliable Connection	Sequence of Pages Remote login Digitized Voice

Connection less	Unreliable datagram Acknowledge datagram Request reply	Electronic junk mail Registered Mail Data base query

- The concept of using unreliable communication may be confusing because why we people prefer unreliable communication to reliable communication.
- The reliable communication is not available.
- For example, Ethernet does not provide reliable communication.
- Packet can be damaged in transit.
- It is upto the higher level protocol to deal with this problem.
- Both reliable and unreliable communication is used frequently as per the requirement and its use.

1.15.2 Difference between Connection Oriented and Connectionless Network

Connection Oriented Network	Connection Less Connection less Network
1. The connection oriented service requires the user to first establish a connection, use the connection and then release the connection.	1. This type of system call service does not require a session connection between sender and receiver.
2. This is modelled after the telephone system.	2. This is modelled after the postal system.
3. This is often called reliable in terms of packets arriving in same order.	3. This service is not reliable, since the packets may arrive in any order.
4. In this the packet does not carry and destination address, since the connection is explicitly made with the destination before sending data.	4. In this scheme, the datagrams contain full destination address and each datagram is routed independent of the others.
5. Example of connection oriented service: TCP, X.25	5. Example of connection less service : UDP
6. Connection Oriented service can be of following 3 types : • Reliable Message Stream • Reliable Byte Stream • Unreliable Connection	6. Connectionless services can be of following types : • Unreliable datagram • Acknowledged Datagram • Request-Reply

1.16 NETWORK STRUCTURE AND ARCHITECTURE

(1) Network Structure

1. Broadcast Network

- The communication channel that is shared by all the machines on the network.
- The message which consists of packets sent by any machine are received by all others.
- The address field within the packet specifies the intended packet means where the packet is to be received.
- After receiving a packet, a machine checks the address field.
- If the packet is meant for that machine, that machine process the packet; if the packet is intended for some other machine, it is just ignored.
- It allow the possibility of addressing a packet to all destination by using a special code in the address field.
- When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of the operation is called Broadcasting.

Example : WAN

2. Multicast

- Basically concept of multicast evolves from the concept of Broadcast.
- Some broadcast system supports transmission to a subset of machines which in known as **Multicasting.**
- In the addressing one bit is reserved for multicasting.
- The remaining (n–1) address bit can hold a group number.
- Each machine can "subscribe" to any or all of the groups.
- When a packet is sent to a certain group, it is delivered to all machines subscribing to that group.

3. Point to Point Network

- It consist of many connections between individual pair of machines.
- To go from the source to destination, a packet on this type of network may have to first visit one or more intermediate machines.

- Point to point transmission with one sender and one receiver is sometime called unicast.
- As a general rule smaller, geographical localized network tends to use broadcasting where as larger network with the short distance point to point network is preferred. Distance is very important factor for selecting the type of network.

Processor Distance	Location	Example
1 m	Square meter	Personal Area Network
10 m, 100m, 1 km	Room, Building Campus	LAN Local Area Network
10 km	City	MAN (Metropolitan Area Network)
100 km	Country	WAN
1000 km	Continent	Wide Area Network
10,000 km	Planet	Internet

(ii) Network Architecture :

- A set of layers and protocols is called as network architecture.
- Protocol stack is defined as a list of protocols used for a certain system, one protocol per layer.

(1) Virtual Communication between Layers

- Let us now go into technical details of the communication between say layer 3 of two machines.
- Refer Fig. 1.23 and go through the steps given below to understand the communication.

Step 1 : A messages M is produced by layer 5 of machine 1 and given to layer 4 for transmission.

Step 2 : Layer 4 adds a **header** in front of the header so as to identify the message and passes the (header + message) to layer 3.

A header includes the control information and it allows a layer 4 in machine 2 to deliver the messages in right order.

Step 3 : Layer 3 breaks up the incoming messages into small units, packets and appends a layer 3 adder to each packet M_1 and M_2 as shown in Fig. 1.23 and passes these packets to layer 2.

Step 4 : Layer 2 adds header as well as trailer to each packet obtained from layer 3 and hands over the resultant unit to layer 1 for physical transmission.

- This sequence of operation taking place at machine 1 is shown in Fig. 1.23

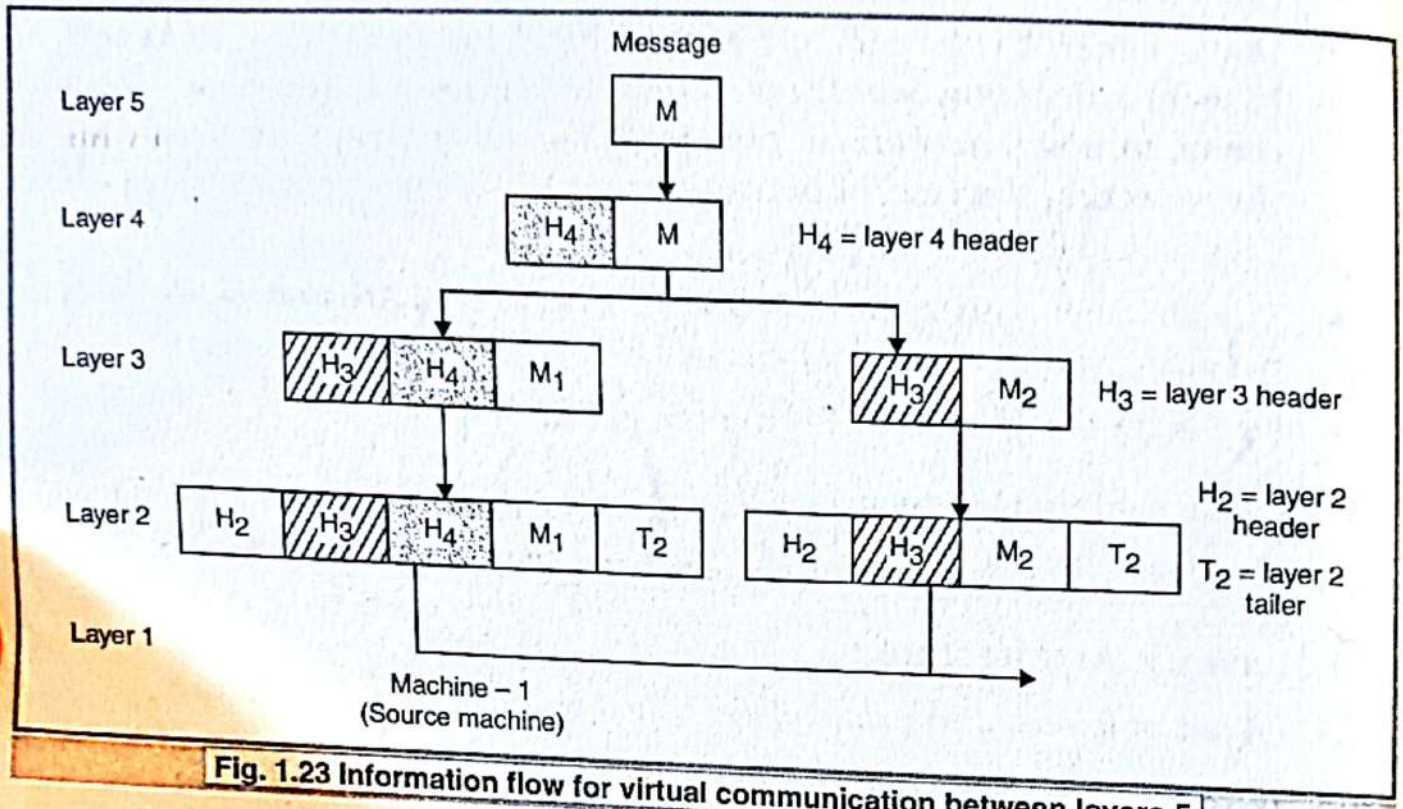


Fig. 1.23 Information flow for virtual communication between layers 5

- The control information placed in headers is used at the destination machine (machine 2) to convey the message to layer 5 as shown in Fig. 1.24.

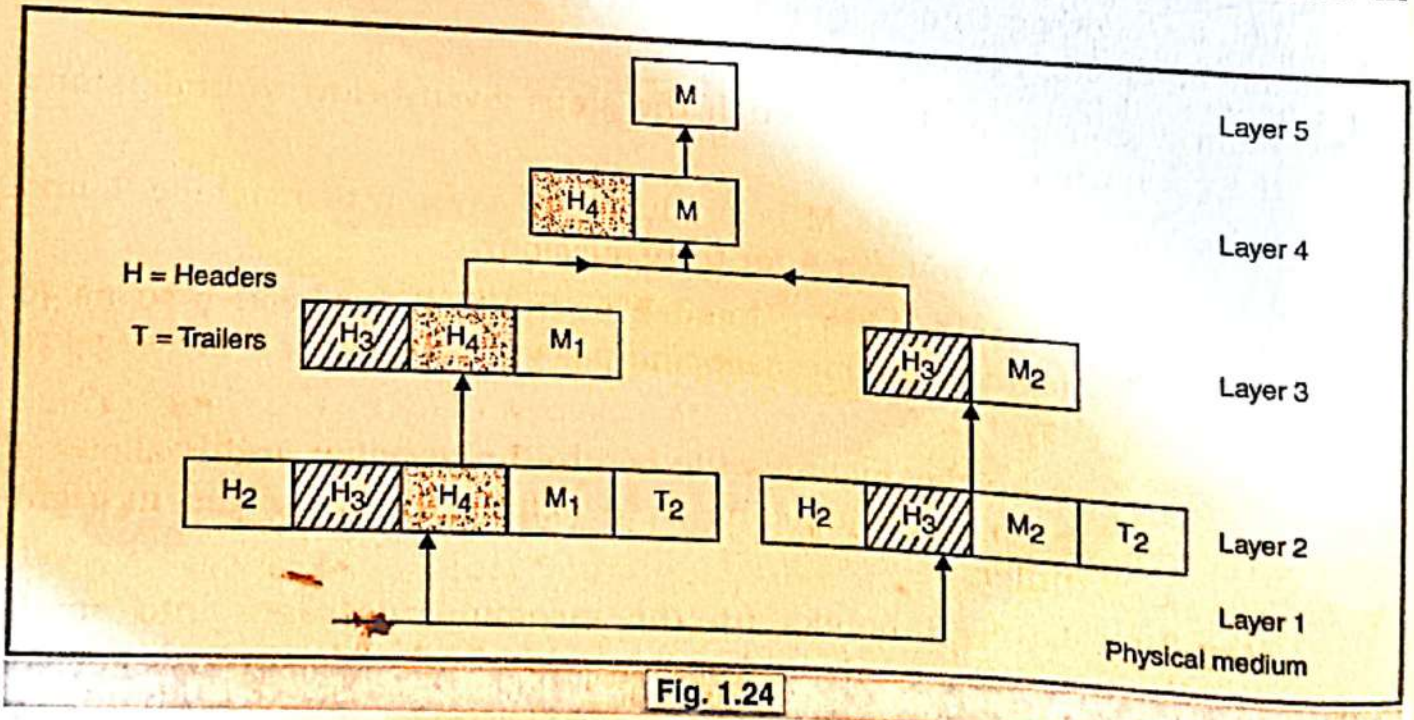


Fig. 1.24

1.17 CLASSIFICATION OF COMPUTER NETWORKS

There are three types of a network. They are

* Local Area Network (LAN)
* Wide area Network (WAN)
* Metropolitan area Network (MAN)

- A local area network enables you to connect a group of personal computers within a single building or small geographical area while a wide area network is a network of computers dispersed geographically.
- The metropolitan area network lies between LAN and WAN. It is a network which covers entire city.
- Let us discuss these three in more detail.

1.17.1 Local Area Network (LAN)

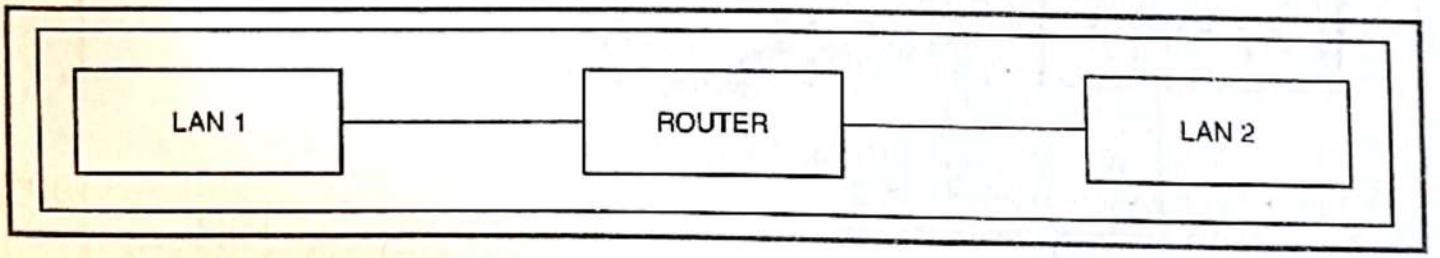
- When two or more computers are connected in a small area i.e. within a diameter of not more than a few kilometers then such a network is known as local area network.
- It is made for an organization and most of the times it is within a single building.
- The data rate in LAN is of the order of Mbps i.e. Mega bits per second. A LAN consists of
  * Computers
  * Graphic stations
  * User terminal stations or workstations
  * Cables of transmission media
  * Peripherals like printer, scanner etc.
  * Network interface unit.
- All the LAN components are connected through cables or some transmission media.
- A LAN may use one of the various topologies like star topology, ring topology, bus topology (Dual bus or bus in the repeater) etc.
- It uses physical transmission medium. The overall purpose of LAN is to provide inter connection in order to find resource sharing and cost reduction.
- A LAN has following characteristics.
  * It covers an area of less then 5 kilometer.
  * It provides high speed data communication.
  * The physical interconnecting medium is privately owned.

  - * The physical inter connecting medium is usually shared by all the stations or nodes connected to LAN.
  - * They have low error rates.
  - * They use simple data communication protocols.
  - * Usually the implementation is homogeneous i.e. the computers are of same brand or compatibles in the network.
- In local area networks the transmission medium is in twisted pair cable, coaxial cable or fiber optical cable.
- Choice of transmission medium depends on its bandwidth, connectivity, noise immunity, security and cost.
- The hardware required for LAN. includes NIU i.e. network interface unit.
- The NIU connects each device in the LAN network to shared transmission device.
- It contains rules and logics to access the LAN. It is used to implement LAN protocol and for device attachment. Its function depends on type of topology used in LAN.
- LAN hardware includes servers too. A server is a dedicated computer which controls one or more resources in the LAN.
- It contain both hardware and software interface for LAN.
- File server, Printer server and modem server are three major categories of servers used in LAN.
- To operate LAN system LAN operating system is required. It has two aspects
  - * server software
  - * workstation software
- A LAN operating system provides resource sharing, data security and connection to other network.
- Various LAN operating systems are ARC net, Ethernet, Corves, Omni net, Penet Novel Network. etherlic plus etc.

1.17.2 Wide Area Network

- A wide area network is connection of two or more computers which are geographically dispersed.
- It has longer distance communications than LAN.

- It uses public networks like telephone network or microwave relays for communication facilities.
- A cost is involved with such networks so highs mostly it is used by government agencies.
- WANs in contrast to LAN needs involvement of another authority like telecom department.
- They use radio waves, microwaves or communication satellites for data transmission.
- The hardware components required for WAN include Bridges, Routers, Gateways and X. 25 standard interface.
- Bridge is a hardware device which connects two or more local area networks to form a wide area network.
- Generally the LAN's connected by it use same network protocol but they can be used with two LAN's having different wiring or network protocols.
- The bridge operates at data link layer of OSI reference model.
- It manages the flow of traffic between two LAN's by reading the address of every data packet received by it.
- The amount of processing required at the bridge is minimal because all the devices use the same protocol.
- If the distance between two LAN's to be connected is large than two identical bridges at either ends of communication links are employed as shown below in the diagram



- Router is a special type of hardware device which connects two or more dissimilar LAN's to form a WAN.
- It is an intelligent connecting device which can send packets to the correct LAN segment for their delivery to the destination.
- They operate at Network layer of OSI reference model.
- The LAN's connected can use similar or different network protocols.
- They compute best routes for data message packets on the basis of information provided by the devices participating in routing protocol.

- Various types of routers are central router, local router, remote router, peripheral router, internal router, external router etc.
- Gateways are used to connect two dissimilar LAN's.
- It is a shared connection between a LAN and a larger system such as main frame computer or a large packet switching network.
- The communication protocols of all of them are different.
- They are slower than a bridge or router.
- It has its own processor in it and it is a combination of hardware and software both.
- It contains memory which is used to perform protocol conversions.
- It converts data packets from one protocol format to another before forwarding it because it connects two dissimilar networks.
- The gate way operates on Application layer of OSI model.
- Router is another networking device which combines the features of a bridge and a router.
- It can route one or more specific protocols i.e. it can be used to connect two or more similar or dissimilar LAN's to form a wide area network.

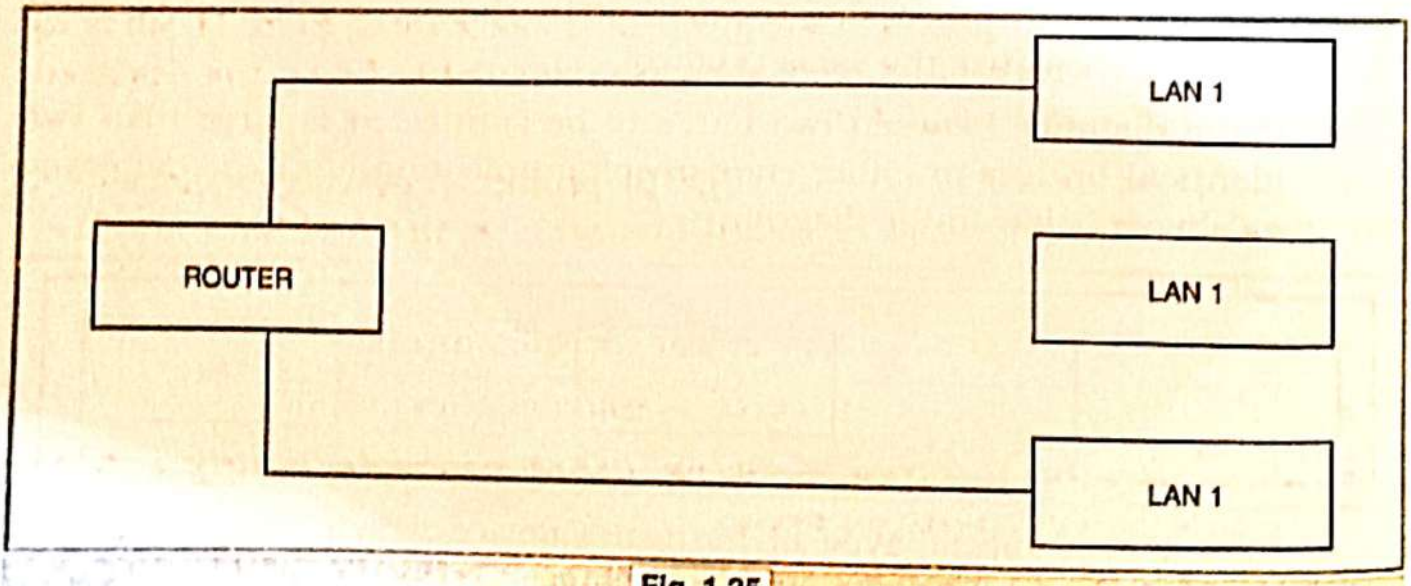


Fig. 1.25

- X.25 is a protocol which is used for interfacing to a Public Packet switched network.
- It does not implements a network rather simply interfaces a network.
- Two types of WAN's are Public networks and Private networks. Mostly the topologies used are multi drop topology.
- It is a complex network with several layers of protocols.

- The characteristics of WAN are
  * It inter connects computers at different sites.
  * It can connect two or more LAN's too.
  * It operates nationwide or world wide.
  * The transmission media is leased lines or public systems such as telephone lines, micro wave or satellites.
  * There may or may not be a direct physical connection between various computers.
  * Links are slow as compared to LAN's i.e. 1200 kbps to 1.544 mbps.
  * Distance of computers is from several miles to several hundred miles.
  * Links are error-prone relative to LAN's.

1.17.3 Metropolitan area Network (MAN)

- It resides between LAN and WAN.
- It interconnects computer within a city.
- It uses dual queue dual bus protocol.
- The implementation for MAN provides transfer rates from 34 Mbps to 150 mbps which is not very slow as compared to LAN. It is designed with two unidirectional bus.
- The Dual Queue Dual Bus (DQDB) protocol has two topologies as open bus architecture or closed bus architecture and both are used with MAN.
- They use broad band cables as transmission media.
- They also use fiber optical cable as transmission media.
- ***A Metropolitian Area Network (MAN) connects multiple LANs within a metropolitian area.***
- This connection provides even more resources for the users on the included LANs.
- 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. Fig. 1.26 illustrates campus networks connected through a metropolitian network.

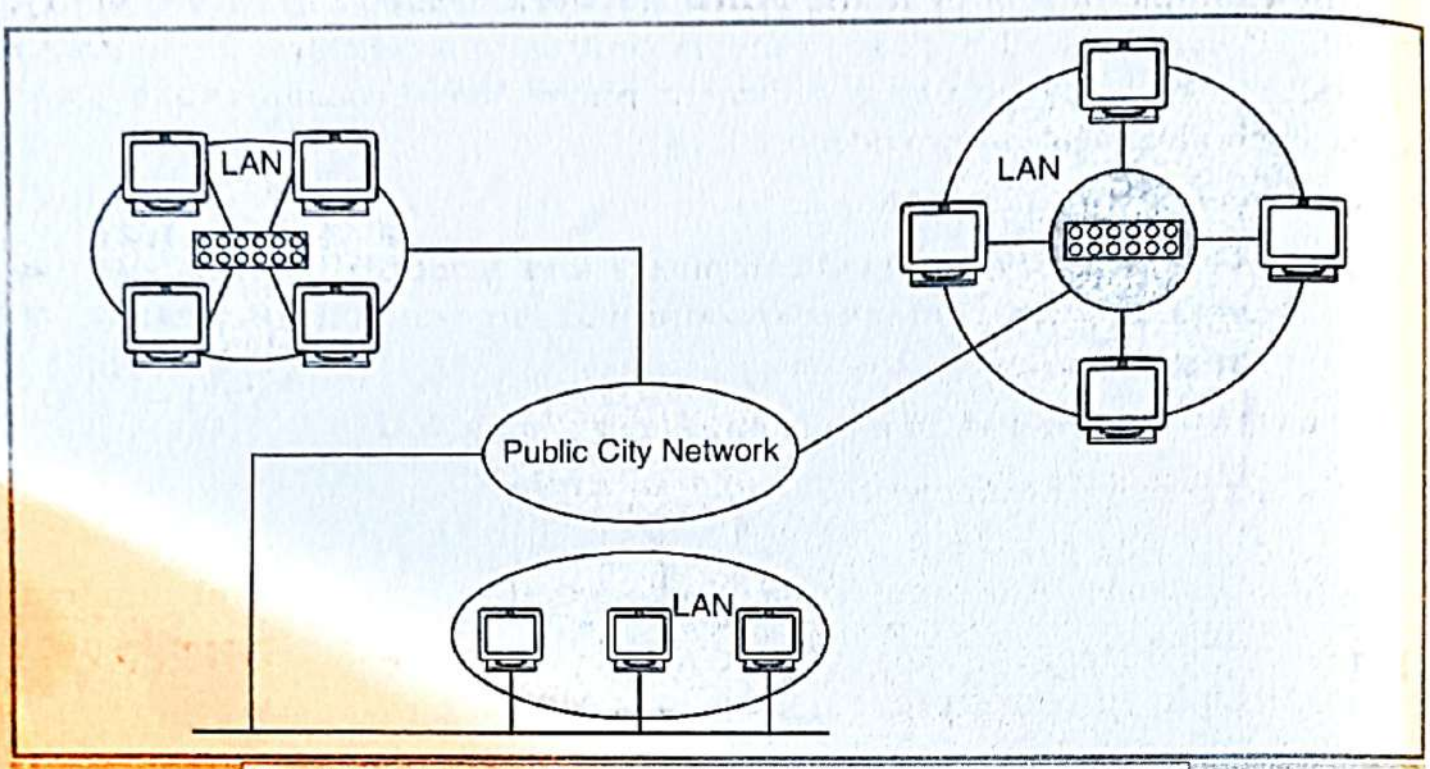


Fig. 1.26 A Metropolitian Area Network (MAN) connects multiple LANs within a metropolitian area

The Metropolitan Area Network (MAN) is the often ignored sibling to LANs and WANs.

- A MAN is often seen as an extension of a LAN.
- MANs are meant to bridge the geographical differences between LANs and WANs.
- LANs and WANs are less than adequate to their needs.
- LANs are too small or specialised for some applications while telnet, timnet or other WANs are overkilled for a modest community of users within a 50Km diameter.
- This gave rise to MAN.
- MANs were originally oriented towards data, but now often carry voice and video-traffic as well.
- They support two-way communication over a shared medium such as an optical fiber cable and may offer point-to-point high speed circuits or packet switched communication.
- They do not however have the capability of a switched exchange network such as the present telephone system or the future broadband integrated semies digital network which will offer world wide service.
- Example of A MAN

One example of a MAN is the **MIND Network** located in Pasco Country, Florida. It connects all of Pasco's media centres to a centralized mainframe at the district office by using dedicated phone lines, coaxial cabling, and wireless communication providers.

Characteristics of a MAN

- In a group of connected computers and associated peripherals that can share files and other resources in large campus or organization spread over a city size area.
- MAN is slower than a LAN but faster than a WAN
- Expensive Equipment
- Moderate Error Rates

1.18 COMPARISON BETWEEN THE DIFFERENT CATEGORIES OF NETWORKS

(1) Comparison between LAN and WAN

LAN	WAN
1. It works in a small geographic area such as office, building or campus.	1. It works in a large geographic area such as country, continents or even whole of world.
2. It is privately owned.	2. It can be private, public or leased type.
3. It is easy to design and maintain.	3. It is very difficult to design.
4. It operates on the principle of Broadcasting.	4. It is based on the principle of switching.
5. LAN offers high speed data rate of communication.	5. It offers low data rate communication.

(2) Comparison between LAN and MAN

LAN	MAN
1. LAN stands Local Area Network.	1. Man stands for metropolitan area network.
2. It operates in a small Geographic area such as office, building or campus.	2. It can operate with large geographic area such as a city or Metropolitan.
3. LAN is easy and cheap to design.	3. MAN is difficult and expensive to design.
4. It is used to connect the computer with other network devices.	4. It is used to connect various LAN.

5. The various equipment used in LAN are repeaters, hubs, Network interface card (N.I.C.).	5. The various devices used in MAN are routers, telephone.

(3) Difference between LAN, WAN and MAN

ITEM	LAN	WAN	MAN
1. Full Form	Local Area Network	Wide Area Network	Metropolitan Area Network
2. Location	Computers are located within the same building	Computers are distributed all over the country or the continents	Computers are Located within a city
3. Transmission Medium	The Data is Transferred through wires.	The data is transferred through sattelite	Data is transferred through wires or telephone line.
4. Cost	Very Cheap	Costly	Moderate
5. Speed	High	Less	Moderate
6. Ownership	Privately owned	Public owned	Private owned
7. Example	In an office various departments are attached	Internetworking	Cable network in a city

(4) Point to Point Network and Broadcast Network

POINT TO POINT	BROADCAST NETWORK
1. This network uses the dedicated link between the two devices.	1. Broadcast Network, all devices are attached to a single communication line.
2. Different network routes are available from one device to another.	2. No alternate routes are possible in broadcast network.
3. The entire capacity of link between two devices is used for transmission between those two devices.	3. The entire capacity of the single communication link is shared by all the devices in a network.

SUMMARY

- Two or more inter connected computers make a network. A network is basically made for sharing information and peripherals. Its basic

need came up due to limited resources and fast and reliable communication resource sharing results in cost reduction. Goals of a network are resource sharing, cost reduction, improve performance and providing communication medium.

- The description of physical connection of computers in a network is called network topology. Various network topologies are star, ring, bus, tree, mesh and multi drop network topology. Star needs one server in centre and work stations connected to it. In ring topology the DTE's form a ring structure. A token passing method is generally used for communication. A common bus between work stations is used in bus topology. A hierarchical structure of work stations is formed in tree topology. All the systems are connected to each other in fully connected mesh topology. A single cable around all modes is used in multidrop network making it highly reliable.
- The specifications of various hardware components used in a network along with their inter relationship is known as network architecture. A network computer has two components : physical and logical. Partitioning is used for designing complex system. This concept given birth to layered Architecture. Two types of communications are used in layered architecture called hierarchical and Peer to Peer communication.
- The set of rules and procedures for controlling communication is known as communication protocol. Functions of communication protocol are connection establishment, Frame formatting, Data routing, Data security, Flow control and error control, Precedence and order of transmission, addressing and multiplexing.
- Various types of computer networks are LAN, MAN and WAN. LAN is established in a single building with in a few kilometers. MAN is a network with in a metropolitan city. WAN is a network connecting system at geographical distances. Various LAN operating systems are Omni net, Corves, Ether net etc. A special device used to connect two LAN's to make a WAN is Router. Some other such devices are Bridges and Gateways.

EXERCISE

I. FILL UP THE BLANKS

1. Two types of communications in a layered architecture of network are ..... and .....

2. Frame formatting is a function of .....
3. OSI stands for .....
4. SAP stands for .....

II. VERY SHORT ANSWER TYPE QUESTIONS

1. What do you understand by a network ?
2. What are 2 basic needs of computer network ?
3. What are the various components of computer network?
4. What was the need of network architectural models?
5. Define point to point configuration.
6. What are the network hardware used in Networking?
7. What are the various user of Network?
8. What are the different application of network ?
9. What is SDU ?
10. What is PDU ?
11. Define IDU ?
12. Define Entity.
13. Define Protocol ?

III. SHORT ANSWER TYPE QUESTION

1. What is a computer network ? Discuss the needs of a computer network in brief.
2. Explain the term network architecture in brief. What is layered architecture and what are its advantages ?
3. Define communication protocol ? What are the basic needs of a protocol?
4. Discuss the functions of a communication Protocol.
5. What is network architecture model ? Why it is required? Name any four architecture models along with their developers.
6. What are the different issues for layer ?
7. What are the different data units of data exchange ?
8. Explain connection oriented and connectionless oriented services.
9. Explain Network Structure Architecture.

10. Classify the computer network with example.

11. Differentiate between

(1) LAN and MAN

(2) LAN, WAN and MAN

(3) Connection oriented and connectionless network.

(4) Point to Point and Broadcast Network

12. What are service access points ? Explain the concept of SAP address in brief.

ANSWERS

I. FILL UP THE BLANKS

1. peer to peer Horizontal 2. communication protocols 3. Open system Interconnection 4. Service access Points.

□□□□□