1

Introduction To Computer Networks

1.1 Data Communications

Communication is the process of transferring messages from one point to another. When we communicate we are sharing information. The sharing can be local or remote. Local communication is between the two individuals and it usually occurs face to face while remote communication takes place over distance. The term telecommunication means communication at a distance and it is usually carried out with the help of telephones, television etc.

The term data refers to raw facts, letters or symbols that are processed into meaningful information. In the strictest sense, data consists of the raw numbers that computers organize to produce information. Data can be in the form of sequence of bits or sequence of voltage shifts or a signal suitable for transmission. The field of data communications links the computer and the telecommunications industries. Computers are digital in nature and transfer information via parallel connections.

Definition

> *Data communication is basically the transmission of signals in a reliable and efficient manner.*

Evolution of Data Communication Systems

Data communication system came into existence shortly after computer was widely used in organizations. In order to take the services of the computer, user simply walked to the room where the computer was located and submitted a request for the computer to perform a service. The computer accepts the user's job, performed it operation and returned the results on hard-copy printouts. This process was called a batch run.

As the use of computer grew, it became inefficient for all users to walk to the computer room, submit their job and return to get the results. Consequently, computer based terminals were built and placed in user workspaces within a building. These systems required that the terminal be connected to the computer through some type of communication media in order for the user to transmit and receive signal to and from the computer.

Typically, private communication lines were wired between the computer and the workstation to meet this requirement. This approach also allowed many users to share the computational power. This concept is known as time-sharing, i.e., multiple users can share the facilities of the machine.

As organization grew and the need for the computer grew, it becomes necessary to share the computer with other users in different buildings. The simple private line was not sufficient and received data through telephone system. This approach is known as remote time-sharing.

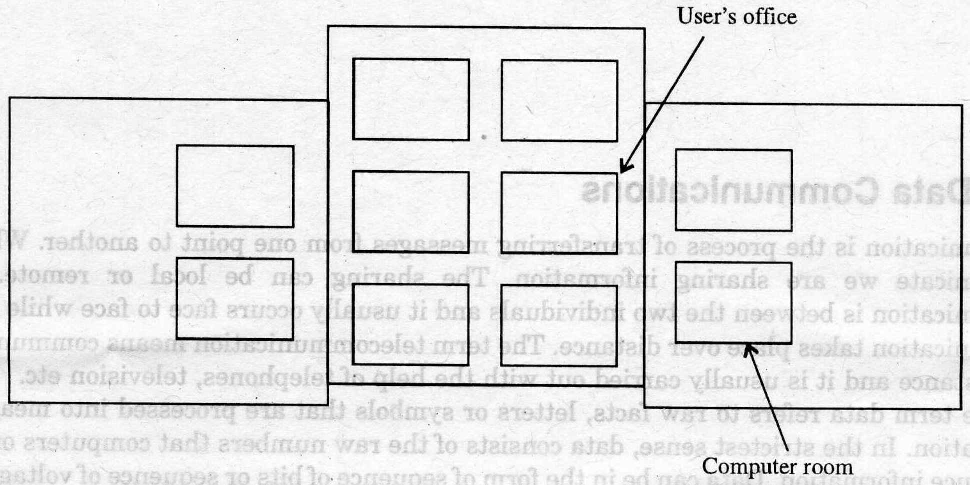

Fig. 1.1 (a)

a) User took jobs to the computer room and picked up the results (Batch runs).

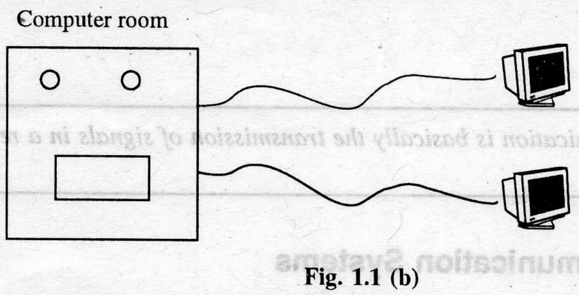

Fig. 1.1 (b)

b) The computer was then accessed by users with terminals (time sharing).

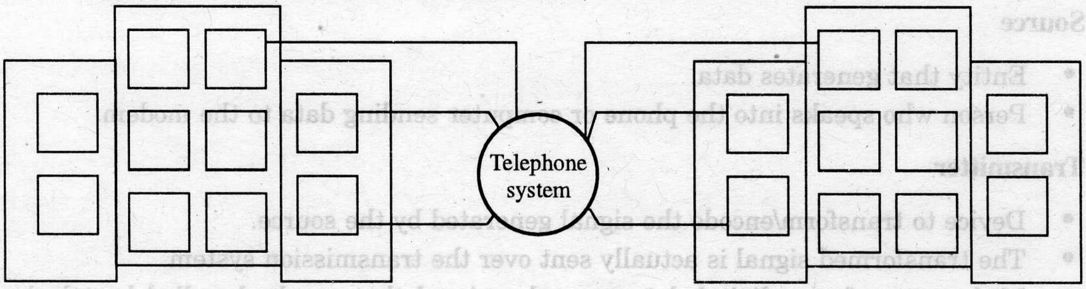

Fig. 1.1 (c)

c) The "Remote Users" eventually access the computer (remote time sharing).

1.2 A Communications Model

The purpose of a communication system is the exchange of data between two entities. The key elements of the model are as follows:

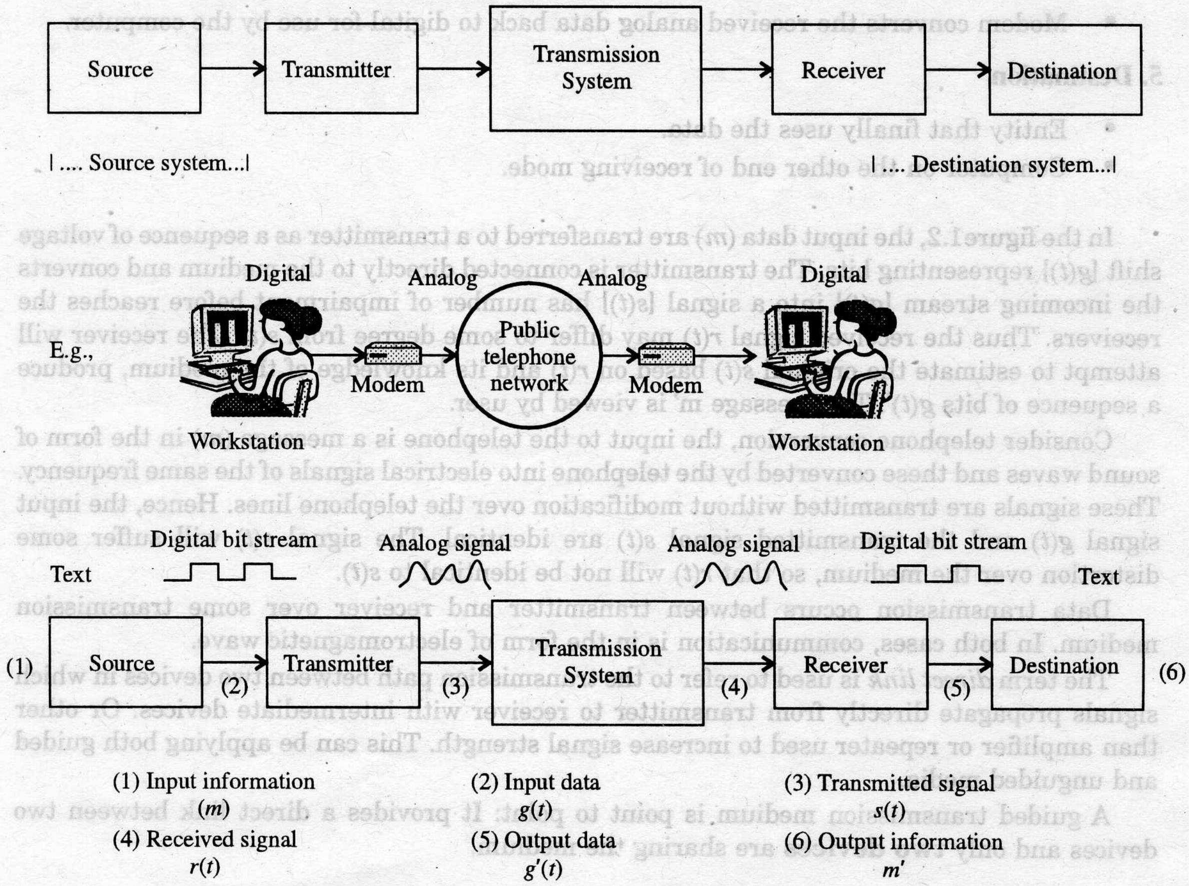

Fig. 1.2. Communication Model

1. **Source**

    - Entity that generates data.
    - Person who speaks into the phone or computer sending data to the modem.

2. **Transmitter**

    - Device to transform/encode the signal generated by the source.
    - The transformed signal is actually sent over the transmission system.
    - Modem transforms digital data to analog signal that can be handled by telephone network.

3. **Transmission System**

    - Medium that will allow transport of signal from one point to another.
    - Telephone network for our computer/modem example.

4. **Receiver**

    - Device to decode the received signal for handling by destination device.
    - Modem converts the received analog data back to digital for use by the computer.

5. **Destination**

    - Entity that finally uses the data.
    - Computer on the other end of receiving mode.

In the figure1.2, the input data (*m*) are transferred to a transmitter as a sequence of voltage shift [*g*(*t*)] representing bits. The transmitter is connected directly to the medium and converts the incoming stream [*g*(*t*)] into a signal [*s*(*t*)] has number of impairment before reaches the receivers. Thus the received signal *r*(*t*) may differ to some degree from *s*(*t*). The receiver will attempt to estimate the original *s*(*t*) based on *r*(*t*) and its knowledge of the medium, produce a sequence of bits *g*(*t*)'. The message m' is viewed by user.

Consider telephone conversion, the input to the telephone is a message (*m*) in the form of sound waves and these converted by the telephone into electrical signals of the same frequency. These signals are transmitted without modification over the telephone lines. Hence, the input signal *g*(*t*) and the transmitted signal *s*(*t*) are identical. The signal *s*(*t*) will suffer some distortion over the medium, so that *r*(*t*) will not be identical to *s*(*t*).

Data transmission occurs between transmitter and receiver over some transmission medium. In both cases, communication is in the form of electromagnetic wave.

The term *direct link* is used to refer to the transmission path between two devices in which signals propagate directly from transmitter to receiver with intermediate devices. Or other than amplifier or repeater used to increase signal strength. This can be applying both guided and unguided media.

A guided transmission medium is point to point: It provides a direct link between two devices and only **two devices** are sharing the medium.

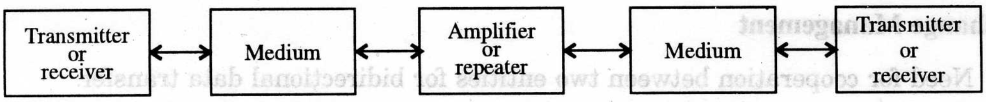

Fig. 1.3 (a) Point to Point

In a Multipoint guided configuration, more than two devices share the same medium.

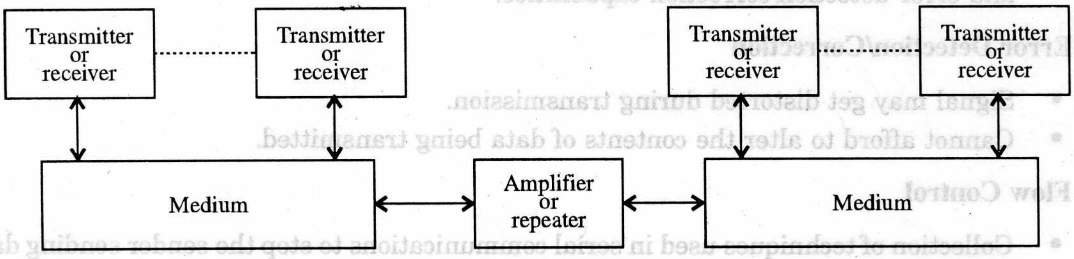

Fig. 1.3 (b) Multipoint

1.2.1 Tasks to be Accomplished in the Model

The purpose of a communication system is to transmit an information-bearing signal, from a source, located at one point, to a user or destination, located at another points some distance away.

1. **Transmission System Utilization**
   - Efficient use of transmission network typically shared among a number of communicating devices.
   - Multiplexing is used to share the total capacity of network among a number of consumers.
   - Congestion control to ensure that the system does not get overwhelmed by excessive transmission network demand.
2. **Interface**
   - Point of interaction or communication between two entities, such as a device and the transmission system.
   - Communication is achieved through signal generation.
   - Properties of signal
     - □ Possible to propagate through the transmission system.
     - □ Possible to interpret as data by the receiver.
3. **Synchronization**
   - Operation of transmitter and receiver in unison.
   - Receiver must be able to determine when a signal begins to arrive and when it ends.
   - Receiver must also know the duration of each signal element.

4. Exchange Management

- Need for cooperation between two entities for bidirectional data transfer.
- Conventions or protocols to decide whether data is transferred simultaneously by more than one entity in a network connection or whether they take turns.
- Other things to worry about are the amount of data to be transferred, data format, and error detection/correction capabilities.

5. Error Detection/Correction

- Signal may get distorted during transmission.
- Cannot afford to alter the contents of data being transmitted.

6. Flow Control

- Collection of techniques used in serial communications to stop the sender sending data until the receiver can accept it.
- Receiver typically has a fixed size buffer into which received data is written as soon as it is received; when the amount of buffered data exceeds a "high water mark", the receiver will signal to the transmitter to stop transmitting until the process reading the data has read sufficient data from the buffer that it has reached its "low water mark", at which point the receiver signals to the transmitter to resume transmission.

7. Addressing/Routing

- Source must identify the identity of intended destination in a shared network.
- Transmission system must ensure that only the intended destination receives the data.
- The transmission system may choose any of the various available routes to deliver the data; it may even send data in parts with each part taking a different route.

8. Recovery

- In the event of transmission interruption, should the transmitter resend entire data, or send the remaining data only from the point of interruption.

9. Message Formatting

- Preestablished patterns of signals between transmitter and receiver.

10. Security

- Safe delivery of data to intended recipient only.
- Data should not get modified during transmission.
- Data must be authenticated to be from the sender only.

11. Network Management

- Configure the system.

- Monitor system status.
- React to failure and overload .
- Plan for future growth.

1.2.2 Classification of Communication

Communication is broadly divided into two categories:

1. Line Communication

The medium of transmission is a pair of conductors called transmission line. This is also called as line channel. This means that in line communication, the transmitter and the receiver are connected through a wire or line.

2. Wireless or Radio Communication

In wireless communication message is transmitted through open space by electromagnetic waves called as radio waves. Radio waves are radiated from the transmitter in open space through a device called antenna. A receiving antenna intercepts the radio waves at the receiver. All the radio, T.V. and satellite broadcasting are wireless or radio communication.

1.2.3 Example of Data Communications : E-Mail

Consider the figure 1.2 to study this example

1. Keyboard receives data and puts it in computer memory as a sequence of bits *m*.
2. Data goes from memory to modem over local communications bus of the computer, and is denoted by $g(t)$ during this transition phase.
3. It is picked up by modem (transmitter) and converted to sequence of voltage shifts (digital-to-analog conversion) which are sent over the network (communications medium); data are now denoted by $s(t)$.
4. Finally, the signal reaches the destination (receiver) as $r(t)$ because it may get modified during the transmission by addition of noise.
5. Receiver attempts to recover the signal $g(t)$ from $r(t)$ and produces a sequence of bits $g'(t)$.
6. The final message *m'* should generally be as close to *m* as possible, ideally an exact copy of *m*.

1.3 What Is A Network?

A network means an interconnected system of things or people. To understand the meanings of a network consider the following cases:

1. He owned a network of shops.
2. Retirement meant dropping out of a whole network of people who had been part of my life.

3. A communication system consisting of a group of broadcasting stations that all transmit the same programs.
4. A system of intersecting lines or channels like a railroad network or a network of canals.
5. An electronic network that means a system of interconnected components or circuits.

1.4 Computer Network

It is a set of computers that are connected and able to exchange data. It can be defined as a communications system that links two or more computers and peripheral devices and enables transfer of data between the components. It is a hardware mechanism that computers use to communicate. The computers in a network share information, software, peripheral devices and processing power.

Definition

> *A **computer network** is a connected set of autonomous computers. Normally each computer has its own operating system that is basically a network operating system. Then the user is aware of the network and the different computers in a network operating system. A user must explicitly connect to other computers in order to communicate with them.*

A **distributed system** is also a connected set of computers, but the system hides the existence of the network and the user is not aware of the different computers. A single system (operating system) runs on all computers and distributes work etc. without the user's knowledge or assistance.

1.4.1 How do Networks Fit into Computer Systems?

There are three primary ways in which networks are used by computers.

Distributed Operating Systems. User sees a single large virtual computer system. The system hides the details of the network and the existence of multiple machines from the user, providing the abstraction of a single virtual computer system. The presence of the network is integrated into the system, and the services can be accessed transparently, that is, without the user knowing that the service does not reside on the local machine. There are few true distributed operating systems in existence, and none are commercial products.

Autonomous System. Standalone machines run fine even disconnected from network. Users invoke special commands to use the network. That is, explicit commands are needed to access files on remote machines.

Network File System. Mostly autonomous machines share file systems located on remote file servers. The network is not totally integrated into the system (all processes run on the local machine, for instance), but remote files are accessed transparently. These are the most common systems today. Client-server paradigm means that clients receive services from server(s) on the network by sending requests of service to the server(s), the server(s) perform the requested work and send results back to the clients.

1.5 Goals Of Computer Networking

The main purpose of computer networking is to allow distributed programs to communicate. This is a sweeping definition, covering local and wide-area networks (LANs and WANs) and modems, the world-wide web and Internet telephony. It excludes older communications technologies such as traditional telephony and the broadcast media, which were never designed for computer-to-computer communication.

What separates computer communication from the other technologies is the need to exchange bytes and collections of bytes among programs. This imposes a number of requirements:

1. It must be possible for a program to indicate where the bytes must go, by specifying a destination address, which uniquely identifies the receiver.
2. It must be possible for a computer to send the bytes to at least another computer, which must be "closer" (by some definition of "closer") to the destination. Communicating with a directly connected computer is done at the data link layer. Forwarding the packet towards the destination is the job of the network layer.
3. In some applications, if bytes are not correctly received at the destination, the sender should send them, until the destination acknowledges their receipt. This is a job for the transport layer, which can also slow down the sender if the network or the receiver is overwhelmed. The transport layer may also decide which of many programs on a given destination machine needs to receive the bytes.

Some examples of what can happen when these requirements are not met:

- A user telnets to an address, but the address identified two different computers, so the user inadvertently types the password on a competitor's machine.
- If it is not possible to send bytes, the network is down. No web, email, chat, file transfers, stock quotes.
- If the bytes are not sent closer to the intended destination, they might wander around the net forever, taking up valuable resources.
- If the bytes are sent incorrectly, the web page might look funny, the file could be corrupted, the wrong command could be issued on the remote machine, or the email could be delivered to the wrong person.
- If the network or the receiver are given more data than they can handle, everything gets very, very slow.

Some of the uses of computer networks are listed below:

- Computer communications and networks have become essential part of modern computing.
- As a designer, developer, programmer or user, it is absolutely necessary to have a good

understanding of the concepts and techniques involved in these modern networking technologies.

- It is an exciting field and combines many technologies.
- There is explosive growth in this field and its demand continues to grow.
- It provides employment opportunities both in industrial and service sector.

1.5.1 Primary Functions of Computer Networks

The primary function of computer networks is to provide access to hardware and software resources that will allow users to perform one or more of the following activities:

- **File serving** : A large storage disk drive acts as a central storage repository.
- **Print serving :** Providing the authorization to access a particular printer, accept and queue print jobs, and providing a user access to the print queue to perform administrative duties.
- **Video transfers :** High speed LANs are capable of supporting video image and live video transfers.
- **Manufacturing support :** LANs can support manufacturing and industrial environments.
- **Academic support :** In classrooms, labs, and wireless.
- **E-mail support.**
- **Interconnection between multiple systems.**

1.5.2 Advantages of Computer Networks

Computer networks make a more cost-effective use of hardware and software. The various advantages of computer networks are listed below:

Resource Sharing. One printer (or other hardware) can be shared by many machines instead of requiring each machine to have its own printer. Other expensive resources include plotters, color laser printers, terminals, storage devices, special machine architectures, etc.

Information Sharing : Electronic mail, news groups, WWW.

Improved Reliability : Eliminate single points of failure through replication.

Reduced Cost : More processing power and storage capacity by buying many PCs and workstations than a single main frame machine.

Effect on Society : Networks are changing not only computer science but all of society. Typical uses of networks include:

- **E-mail :** Very quick turn-around, one can have an email conversation with someone else across the world in a matter of seconds, almost real-time.
- **Bulletin board :** Instead of having private message exchange, everyone can post to

bulletin board, making it a public forum. There are a few thousands specialized newsgroups.

- World Wide Web
- Storing files on a file server, giving users access to their files regardless of what machine they actually use.
- Anonymous FTP service : Users place files on a special account where anyone with network access can copy the files using FTP to their own machines.

1.5.3 Disadvantages of Computer Networks

- Equipment and support can be costly.
- Level of maintenance continues to grow.
- Private ownership possible.
- Some types of hardware may not interoperate.
- Just because a LAN can support two different kinds of packages does not mean their data can interchange easily.
- A LAN is only as strong as its weakest link, and there are many links.

1.6 Network Hardware And Transmission Technology

The medium through which a host computer transfers data to and from other computers is called the subnet. Usually, it is some kind of cable, but there are other kinds as well, e.g., radio (perhaps over a satellite), infrared light, etc.

There are two main types of subnets:

1. Point-to-Point Subnets

Data is sent on a path directly to the destination host. No other hosts are involved. This is common in cable-based WANs.

Key points about point-to-point networks

- Each communication line connects a pair of nodes.
- A packet (or message) is transmitted from one node to another.
- Intermediate nodes, in general, receive and store entire packet and then forward to the next node.
- Also called "store-and-forward" or "pack-switched" networks.
- Some topologies to represent such networks are: star, ring, tree.
- Routing algorithms are important for deciding a route in these networks.
- Typically used for large networks.

2. Shared Media subnets

These are also known as **Broadcasting subnets**. Each data packet is sent to all hosts, but is addressed in such a way that only the destination host listens. This is common in satellite-based WANs and in LANs.

Key points about broadcast networks

- Have a single communication media shared by all computers on the network.
- Some topologies to represent such networks: bus, satellite, radio.
- Short messages, or packets, are sent from one machine and received by all machines.
- Address held within the packet specifies intended destination.
- Packet not intended for a machine is ignored by that machine.
- Multicasting
  - □ Transmission is sent only to a subset of machines
  - □ Possible by reserving one bit in the address field to indicate the presence of multicasting, with remaining bit holding a group number
  - □ A machine can subscribe to one or more groups
  - □ Packet sent to a group is delivered to all machines in that group
- Typically used for smaller localized networks.

1.6.1 Data Communication Networking

It is impractical to connect every pair of communicating devices directly as point-to-point connection because:

- Any pair of devices may be very far apart, making it expensive to have multiple dedicated links.
- A set of devices may require a link to many other devices at different times, for example telephones in an organization.

The above problem can be solved by attaching each device to a communication network. Most networks can be categorized into one of the following classes: wide area networks, metropolitan area networks, local area networks and internetwork. Internetwork is a connection of two or more networks.

1.7 Network Classifications

The two most important characteristics of a network are size and shape. Both of these factors influence the transmission technologies and communication protocols that the network uses.

- Networks are classified according to the area over which they extend.
- The smallest networks consist of two nodes connected by a cable in the same room.
- The largest networks include millions of nodes around the world.
- The size and extension of a network depend on the number of nodes that need to communicate, and where these nodes are in relation to each other.

Types of Networks

I. **Server-based Networks :** Server-based networks are defined by the presence of servers on a network that provide security and administration of the network. Other computers are the clients of the network.

II. **Peer Networks :** Peer networks are defined by a lack of central control over the network. There are no servers in peer networks. Users simply share disk space and resources, such as printers and faxes.

III. **Hybrid Networks :** Hybrid networks have all three types of computers on them. This means that while most shared resources are located on servers, network users still have access to any resource being shared by peers in your workgroup.

Advantages of Server-Based Networks

- Strong central security.
- Central file storage, which allows all users to work from the same set of data and provides easy backup of critical data.
- Ability of servers to pool available hardware and software, lowering overall costs.
- Ability to share expensive equipment, such as laser printers.
- Optimized dedicated servers, which are faster than peers at sharing network resources.
- Less intrusive security.
- Freeing users from the task of managing the sharing of resources.
- Easy manageability of a large numbers of users.
- Central organization, which keeps data from getting lost among computers.

Disadvantages of Server-Based Networks

- Expensive dedicated hardware.
- Expensive network operating system software and client licenses.
- A dedicated network administrator is usually required.
- When server goes down, operations will cease across the network.

Advantages of Peer Networks

- No extra investment in server hardware or software is required.
- Easy setup.
- No network administrator required.
- Ability of users to control resources sharing.
- No reliance on other computers for their operation.
- Lower cost for small networks.

Disadvantages of Peer Networks

- Additional load on computers because of resource sharing.

- Inability of peers to handle as many network connections as servers.
- Lack of central organization.
- No central point of storage for file archiving.
- Requirement that users administer their own computers.
- Weak and intrusive security.
- Lack of central management, which makes large peer networks hard to work with.

Advantages and Disadvantages of Hybrid Networks

Share many advantages and disadvantages of server-based and peer computers.

How do you decide which type of network to use?

■ **Use Peer-to-peer if**

- There are fewer than 10 people in your organization.
- The people in your organization are sophisticated computer users.
- Security is not an issue or if users can be trusted to maintain good security.
- The cost of an additional computer just to serve files exceeds available funds.
- Users can be relied upon to back up their own data.
- Users are physically close together and there are no plans for expansion of the network.

■ **Use A Server-based Network if**

- There are more than 10 people in your organization.
- Many of the people are not sophisticated computer users.
- Your organization maintains information that must be centrally controlled.
- You have enough users that central file servers and applications are cost-effective.
- A central administrator will administer the network and set network policies.

1.8 Types Of Networks, By Size

Networks can be classified depending on how large area they cover.

1.8.1 Local Area Network (LAN)

Computers networked together in a self-contained group form a Local Area Network, or LAN. A LAN typically is contained within a single building or a group of neighbouring buildings. It is a communication network that interconnects a variety of data communicating devices within a small geographic area and broadcasts data at high data transfer rates with very low error rates. Two computers linked together at home are the simplest form of a LAN. Several hundred computers cabled together across several buildings at school form a more complex LAN. LANs are usually connected with coaxial or CAT5 cable.

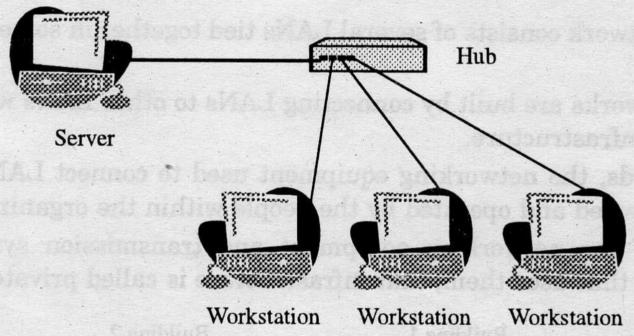

Fig. 1.4 Local Area Network

In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards in each computer.

Characteristics of LANs

1. Smaller scope compared to WANs, typically a single building or campus. (10 m–1 km)
2. Usually owned by same organization as attached devices.
3. Distinguished from other networks by size, transmission technology, and topology.
4. Small size restriction binds the worst-case transmission time and simplifies network management.
5. Internal data rates on LANs are much greater than those of WANs.
6. Make use of a broadcast network approach rather than a switching approach :
   a. No intermediate switching nodes.
   b. Transmitter/receiver at each node communicates over a medium shared by other nodes.
   c. Transmission from any station is received by every other station.
   d. Data are transmitted in packets, allowing only one station to transmit at any given time.
7. Generally use a single cable for transmission to which all machines are attached.
8. Traditional speed is 10-100 Mbps, with low delay and with fewer errors.
9. LAN topologies are bus and ring. (Topologies to be discussed in next chapter)

1.8.2 Campus Networks

When computers are connected across multiple buildings, the entire collection of computers is often referred to as a campus network.

Characteristics of campus networks are:

- A campus network consists of several LANs tied together in some way to form a larger network.
- Campus networks are built by connecting LANs to other LANs with an organization's networking infrastructure.
- In other words, the networking equipment used to connect LANs to form a campus network is owned and operated by the people within the organization.
- When all of the networking equipment and transmission systems belong to the organization that uses them, that infrastructure is called private facilities.

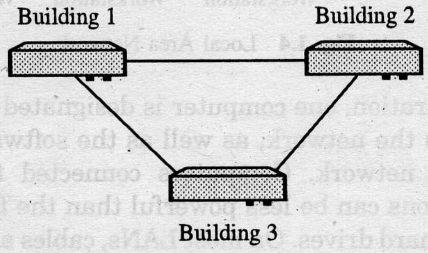

Fig. 1.5 Campus Networks

1.8.3 Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

A workstation in a wireless LAN can be anywhere as long as it is within transmitting distance to an access point.

Characteristics of wireless LANs are:

- Newer IEEE 802.11 and 802.11b standard defines various forms of wireless LAN connections.
- Speeds up to 11 Mbps with 802.11b standard.
- Workstations reside within a basic service set, while multiple basic service sets create an extended service set.
- Two basic components necessary : the client radio, usually a PC card with an integrated antenna, and the access point (AP), which is an Ethernet port plus a transceiver.
- The AP acts as a bridge between the wired and wireless networks and can perform basic routing functions.
- Workstations with client radio cards reside within a basic service set, while multiple basic service sets create an extended service set.

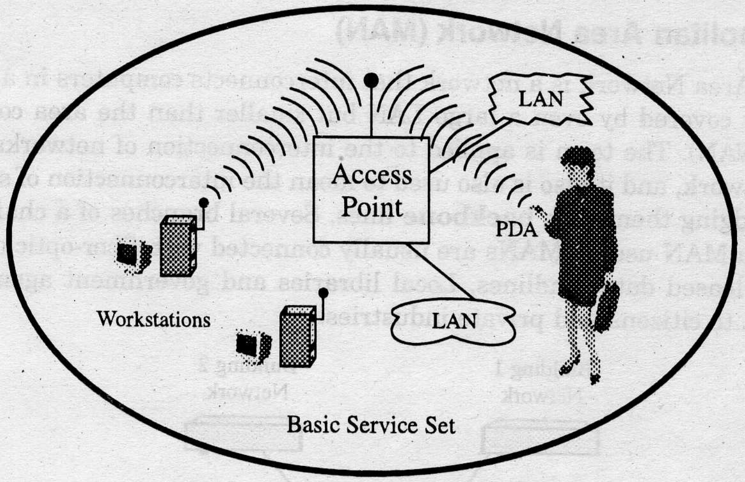

Fig. 1.6 A Wireless LAN Configuration

- With directional antennae designed for point-to-point transmission (rare), 802.11b can work for more than 10 miles.
- With an omni-directional antenna on a typical AP, range may drop to as little as 100 feet.
- Distance is inversely proportional to transmission speed — as speed goes up, distance goes down.
- In actual tests, 11 Mbps 802.11b devices managed 5.5 Mbps .
- To provide security, most systems use Wired Equivalent Privacy (WEP), which provides either 40- or 128-bit key protection.

Some Wireless Standards

- IEEE 802.11 (older 2 Mbps)
- IEEE 802.11b (11 Mbps, 2.4 GHz)
- IEEE 802.11a (54 Mbps, 5 GHz, in 2002)
- IEEE 802.11g (54 Mbps, 2.4 GHz, in 2002)
- HiperLAN/2 (European standard, 54 Mbps in 5 GHz band)

Peer-to-Peer LANs

Characteristics of peer-to-peer LANs :

- Not as common as server-based LANs.
- Less, if any, reliance on servers.
- Most peer-to-peer LANs still use one or more servers.
- Interesting collaborative-type applications.

1.8.4 Metropolitan Area Network (MAN)

A Metropolitan Area Network is a network that interconnects computers in a geographic area larger than that covered by even a large LAN but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network, and it also is also used to mean the interconnection of several local area networks by bridging them with **backbone** lines. Several branches of a chain store within a city might find a MAN useful. MANs are usually connected with fiber-optic cable, microwave transceivers or leased data landlines. Local libraries and government agencies often use a MAN to connect to citizens and private industries.

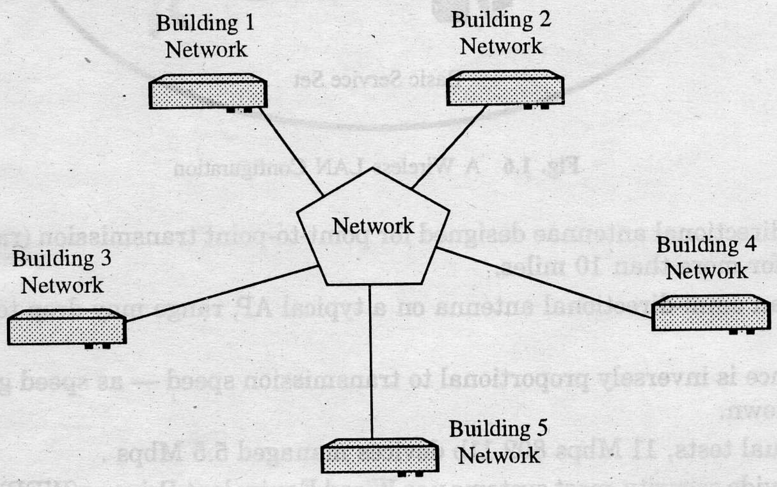

Fig. 1.7 A Metropolitan Area Network

Characteristics of MANs

1. A metropolitan area network (MAN) interconnects two or more LANs across a city-wide area and it can extend up to 50 km.
2. Fiber optics is a popular technology for MANs.
3. It may be private or public.
4. It may involve a number of organizations, e.g., cable TV networks (CATV), ATM networks, a business might interconnect several branch offices.
5. One of the primary differences between a MAN and campus network is that a campus network uses private facilities for interconnecting individual LANs, and a MAN uses public or shared facilities leased from a local telephone company.
6. These leased services include point-to-point lines such as T-carriers (fractional T1, T1, or T3), or switched services such as Integrated Services Digital Network (ISDN), frame relay, or Asynchronous Transfer Mode (ATM).

1.8.5 Wide Area Network (WAN)

A WAN is geographically large. It is often formed by joining together of LANs in distant places.

A national banking organization, for example, may use a WAN to connect all of its branches across the country. The difference between LANs and WANs is getting blurry as fiber optic cables have allowed LAN technologies to connect devices many kilometers apart. WANs are usually connected using the Internet, ISDN landlines or satellite. It might cover a large city a country, or the whole world. It is often a point-to-point system.

Within each city, we may have LAN, campus, and MAN connectivity. The WAN portions of the network are the connections that provide communication between cities. Information travels across the WAN portion of the network only when it is destined for another computer in another city.

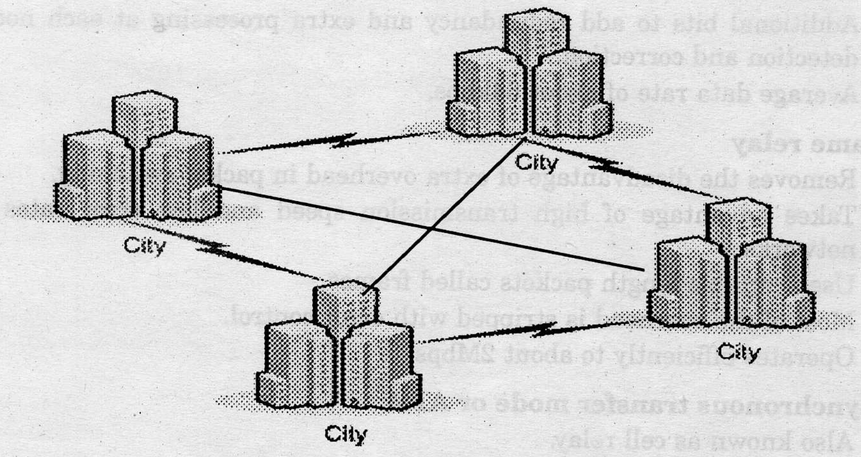

Fig. 1.8 A Wide Area Network

Characteristics of WANs

1. They generally spread over a large geographic area, from across the city to across the continent (100-1000 km).
2. Require crossing public area and may rely on circuits provided by a common carrier.
3. Typically is made up of a number of interconnected switching nodes.
4. Transmission from one device goes through internal nodes of the network to a specified destination device.
5. Nodes are not concerned with the contents of the message but just bounce the message to the next node towards the destination.
6. Implemented using circuit switching, packet switching, frame relay, or ATM.

(a) Circuit switching

□ A dedicated communication path is established between source and destination through the network nodes.

□ Path is a connected sequence of physical links between nodes.

□ On each link, a logical channel is dedicated to the connection.

□ Data from the source is transmitted through the dedicated link as fast as possible.

□ No delay between reception and retransmission of data at each node.

□ Best example is the telephone network.

(b) Packet switching

□ No dedicated transmission capacity along a path.

□ Data are sent in terms of packets.

□ Packets travel through the network from node to node.

□ At each node, packet is received and stored briefly before being transmitted to the next node.

□ Commonly used for computer-to-computer communications.

□ Considerable amount of overhead to compensate for errors.

□ Additional bits to add redundancy and extra processing at each node for error detection and correction.

□ Average data rate of about 64kbps.

(c) Frame relay

□ Removes the disadvantage of extra overhead in packet switching.

□ Takes advantage of high transmission speed and low error rates in modern networks.

□ Uses variable length packets called frames.

□ Most of the overhead is stripped with error control.

□ Operates efficiently to about 2Mbps.

(d) Asynchronous transfer mode or ATM

□ Also known as cell relay.

□ Commercial state-of-the-art networks.

□ Uses fixed length packets called cells to reduce the processing overhead.

□ Provides little overhead for error control, depending on inherent reliability of transmission network and higher order logic at stations for error detection and recovery.

□ Works in the order of 10–100 Mbps range and may even achieve Gbps range.

□ Data rate on each channel in the system can be dynamically set on demand.

ATM vs. Circuit Switching

□ Circuit switching allows only fixed-data-rate circuits for the end systems.

□ ATM allows multiple virtual channels with data rates that are dynamically defined at the time of creation of virtual channel.

□ ATM is efficient due to the use of small fixed-size cells allowing it to offer a constant data rate channel while using packet switching.

7. ISDN and Broadband ISDN

□ Integrated services digital network.

□ Designed to replace existing public telecom network while delivering a wide range of services.

□ Multiple networks within national boundaries with a single, unified view dictated by user interface standards.

□ First generation or narrowband ISDN

- Uses 64kbps channel with circuit switching and frame relay.

□ Second generation or broadband ISDN

- Supports high data rates at 100s of Mbps with packet switching and ATM.

1.8.6 Network Cloud

When an organization must connect more than a few sites over a metropolitan or wide area, a cloud network is usually more economical and flexible than a mesh of point-to-point links. The network cloud represents a public mesh network of switching devices, often owned by a telephone company.

Common types of cloud networks include the public telephone system, the Internet, or switched transmission services such as frame relay or ATM.

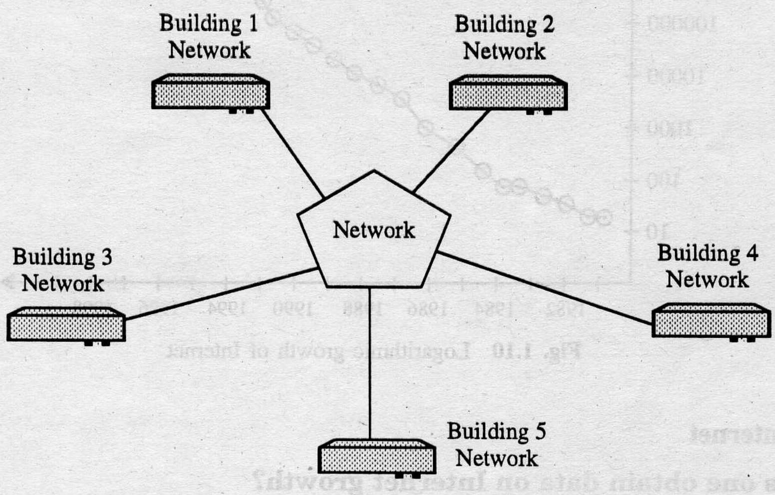

Fig. 1.9 A Network Cloud

To use the services of a cloud network, a company subscribes to the service, and then sets up a point-to-point connection between each location and a device at the edge of the cloud. The network provider is responsible for moving each message across the cloud to its destination.

1.8.7 The Internet

The Internet is a global network that came into being when the first WANs were interconnected. It allows any user on a LAN to communicate with any other user on any other LAN. The Internet is not regulated by any single body or government, and is defined at any particular moment by the users currently using it. The Internet is a form of mesh topology, because there are many possible routes data can travel between one user and another user. When you dial up your Internet Service Provider (ISP) at home, you are becoming part of a global network that has hundreds of millions of other users connected at the same time. The Internet relies on the global acceptance of protocol standards such as TCP/IP, HTTP, POP, IMAP and FTP.

Internet Growth

- The *Internet* has grown from a research prototype to a global communication system.
- During 1998, one computer per second was added to the Internet.
- The *Internet* has been doubling in size every nine to twelve months.
- The graph in Fig 1.10 shows the Logarithmic Growth of Internet:

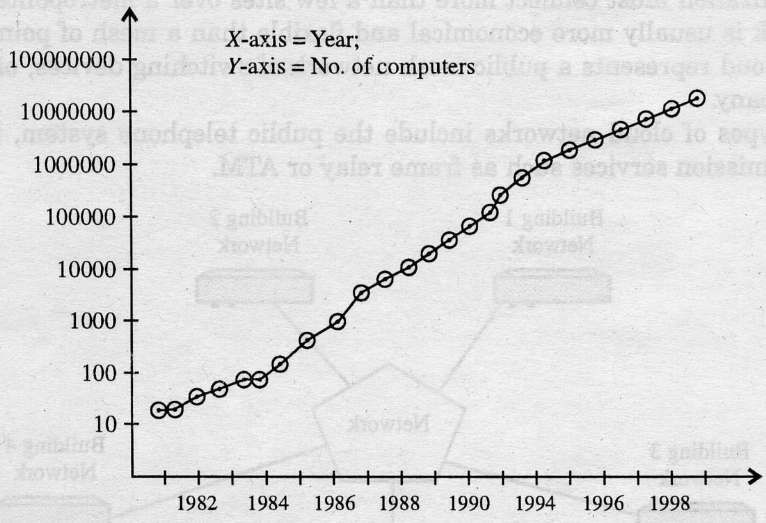

Fig. 1.10 Logarithmic growth of Internet

Probing the Internet

How does one obtain data on Internet growth?

- *Ping* : simple probing tool to determine if a specific computer is available and attached to a network.
  - □ Sends a message to a specified computer
  - □ Waits a short time for a response
  - □ If a reply arrives, ping reports the computer is alive, otherwise the computer does not respond.
- *Traceroute* : simple tool to determine the path from one computer to another computer on a network.
  - □ Uses a program like ping to determine if the computers en-route is available.
  - □ Keeps a list of all computers along the path.

1.9 Communication Between Processes

Computers and processes generally cooperate using three methods of communication:

- Master/slave
- Peer-to-peer
- Client/server

In a LAN, peer-to-peer and client/server communication are the most common.

1.9.1 Master/Slave Communication

Master/slave communication occurs when one node has much greater computing capacity than another. For example, a typical master/slave relationship occurs in mainframe environments where a powerful central computer runs all the applications, stores all the data, and does all the processing.

Key points of master/slave communication

- Simple "dumb" terminals function as slaves to this master, because they have no real processing or data storage capability.
- Individual terminals may not initiate an interaction, but must wait for the master mainframe to command it to send information.
- The slave merely displays text received from the master and sends information to the master in the form of the operator's keystrokes.

1.9.2 Peer-to-peer Communication

A 'peer' is a person who is on the same level of authority and power as you. In a Peer-to-Peer network, there is no computer with more control or authority than any other. There is no file server, little protection of one workstation against another, no hierarchy of "super users" and "standard users". Any computer can begin a network transaction with any other computer on the network.

Peer-to-Peer networks usually are used in the home or very small organizations with trusted users who want to share files, an Internet connection, or a printer. Without a server, costs are low and installation is simple, but users are vulnerable to each other.

Peer-to-Peer Computing (P2P) is an alternative to the traditional centralized (or client-server) computing model. A centralized model uses server-based sharing and requires an intermediary such as a Web, e-mail, or corporate server. P2P has two or more computers linked for the purpose of sharing information files (locally or remotely) with each taking an equal role in the data-transfer process without a central server. No server is needed to share information among systems; instead, each user's computer handles the serving. There are, however, flavours of P2P: some models do not use a central server, while others use central servers to hold directories and to direct traffic (but not to store data).

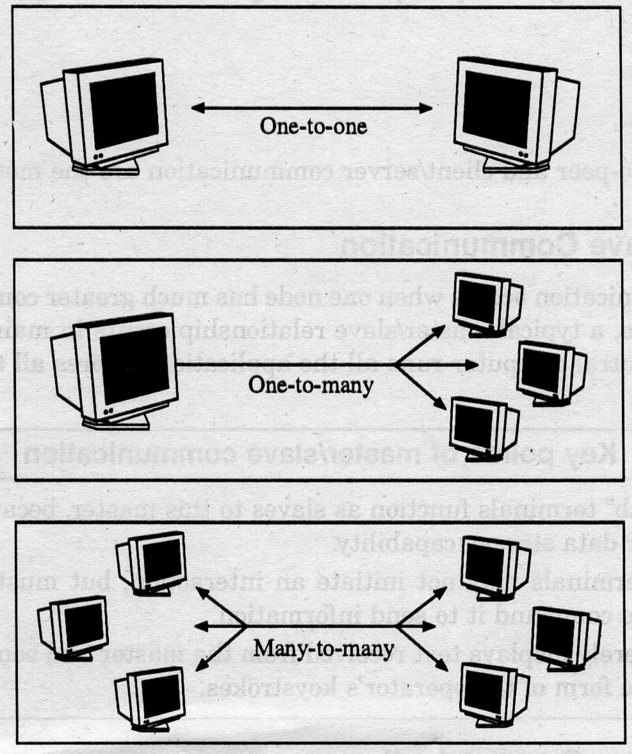

Fig. 1.11 Peer-to-Peer Networking

Key points of peer-to-peer communication

- When two processes have roughly the same power and can perform approximately the same services for each other, we call them "peer" processes.
- When processes use peer-to-peer communication, neither one controls the other.
- A peer-to-peer computer network allows various combinations of workers to share files, folders, applications, and printers.
- No single computer sets the rules for these interactions.
- However, each computer's user can decide what resources to make available to other peer users.
- Most popular desktop OSs, such as Windows 2000 or the Mac OS, has built-in software for creating peer-to-peer networks.

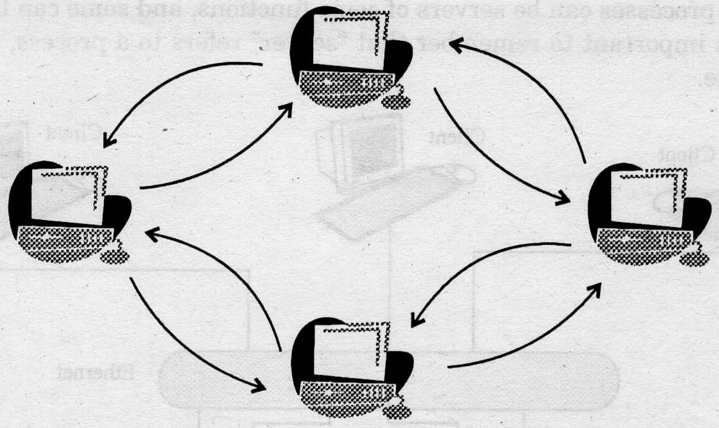

Fig. 1.12 Peer-to-Peer Communication

1.9.3 Client/Server Communication

In client-server networking one computer program (the 'client') asks another computer program (the 'server') to provide a service, such as looking up and providing data. It is similar to you (the client) asking your mum (the server) where your clean socks are. The main difference is that a real server does not respond, "Wherever you dropped them, you messy child."

In a network, the client/server model provides a convenient way to interconnect programs distributed across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to your computer, which displays the information for you. The client/server model has become one of the central ideas of network computing.

When using the Internet, your web browser is a client program that requests services (such as the sending of Web pages or files) from a web server in another computer somewhere on the Internet.

Typically, a client process is found on a lower capability, end-user node, such as a workstation or personal computer (PC). The server process runs on a node with larger capacity or greater power, such as a network file server. A client/server network is implemented with a specialized network operating system (NOS) such as Novell NetWare, Windows NT Server, or Windows 2000 Server. Unix and Linux also provide client/server features.

Both client and server processes are dedicated to their respective tasks, and those roles never reverse. However, the same computing machine can run multiple processes.

Some of those processes can be servers of some functions, and some can be clients of other servers. Thus it is important to remember that "server" refers to a process, not necessarily a particular machine.

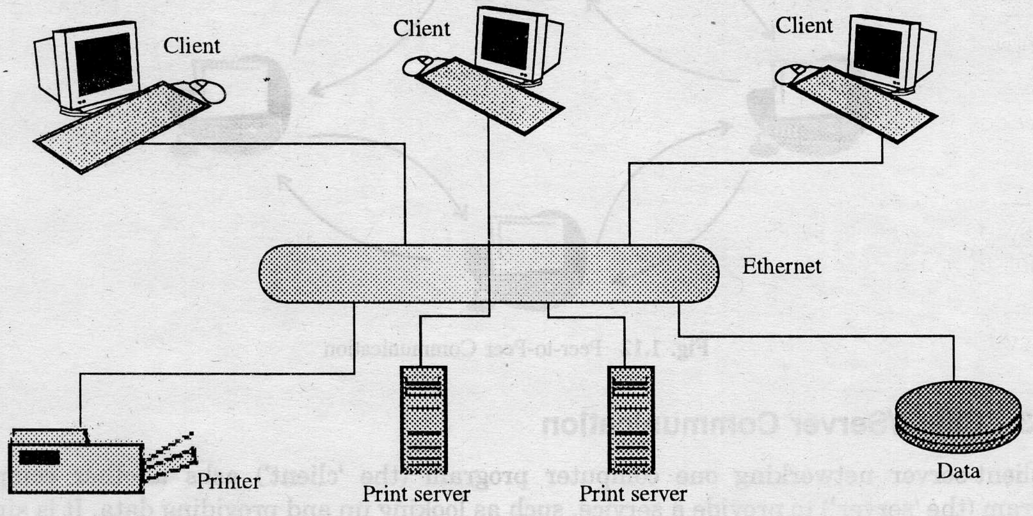

Fig. 1.13 Client/Server Communication

Client and server processes interact with each other by transmitting request/reply pairs. The client process initiates an interaction by issuing a request to the server. The server process responds with a reply satisfying the request. This request/reply communication essentially divides a task into two parts and executes each part on a different system on the network.

Also, peer-to-peer communication can still occur on a client/server network. If servers have been established for shared functions such as file sharing or printing, two computers may still exchange data as peers.

Client and server processes share a common protocol. However, the protocol defines entirely different conventions for communications originating from the client and those originating from the server. This is in contrast with peer-to-peer communication, in which the protocol is more or less the same in both directions.

Key points of client/server communication

- Another way that processes can communicate is for one process to assume the role of client and the other that of server.
- The client process makes requests for the server process to perform some task.
- Client/server communication is typically used to allow sharing of centralized resources, such as data, applications, peripheral devices, or storage space.

1.9.4 Comparing Communication Methods

Peer-to-Peer Advantages	Peer-to-Peer Disadvantages	Client/Server Advantages	Client/Server Disadvantages
Simplicity	Not practical in large networks	Access to common resources	Complexity
Low cost	Most OSs limit number of nodes connected	Scalable to very large environments	High cost for small networks
Easy to manage in small networks	No single point for backup and administration	Dedicated shared resources and administration points	Often requires trained personnel
Easy to trouble shoot			Harder to troubleshoot

1.10 Types Of Servers

A server is a heavy-duty computer designed to be the core of a network. It does not have any special or exotic hardware in it, but it is designed to work continuously for long periods under heavy workloads to control the network and run the network operating system. The different types of servers are discussed below:

1.10.1 File Servers

When a network is based on a central file server, it allows networked computers to share resources such as printers, and users can store their files in a secure centralized location. The file server offers services to all users, but each workstation on the network does its own processing. For example, if a user wanted to use a spreadsheet she would run the spreadsheet on her own PC, but would be able to save her work in her home directory on the server, and use a shared network printer.

File servers typically have very large hard disks, lots of memory, and are stored under high security. In large networks, there is often more than one file server, to distribute the workload or to handle specialist tasks. (such as a proxy server, web server, email server, login server, print server, CD-ROM server etc.)

Since the file server is the heart of the network, if it fails it can severely affect network users, so it is usually treated like royalty. They are usually kept firmly under lock and key in air-conditioned rooms with uninterruptible power supplies (UPS) to protect against power blackouts, brownouts and voltage spikes.

1.10.2 Application Servers

While a file server (as its name suggests) serves out files to users, an application server actually runs programs on behalf of users. Similar to the earliest mainframe computers that ran programs for users and send the results of the calculations to the users, an application server actually runs application programs like Word, Excel, databases itself.

It allows **Thin Client Computing** (e.g. Citrix Metaframe and Windows Terminal Server): users' workstations need only be very cheap and low powered (really just a keyboard, screen, mouse) and enough IQ to send the user's typing and clicking to the application server. The application server is the real brain of the outfit. It runs the programs for the user and sends back screen images that appear on the user's screen.

The benefit for an organization is that they can use any old nasty, horrible, low powered computer as a workstation and it will *behave* as if it were a fire breathing, supercharged state-of-the-art PC. This is handy, for example, if the organization needs lots of workstations but does not have much cash; or if they need to put workstations in high-risk areas such as factories or on construction sites. If the PC is wrecked by dust or is stolen, it does not matter a lot because it was cheap and there is no valuable data stored on it: all data is stored securely and centrally on the application server.

Another benefit is that network managers do not have to configure hundreds of workstations: any change to software or operating system settings is done once, on the application server. It is far easier to install a new program once, on the application server, than it is to go around and install it on 200 workstations! Application servers typically have twin CPUs, a gigabyte of RAM, massive hard disks... **very expensive!**

1.10.3 Server Blades

A **server blade** is an entire server (processor, system memory, network connection, and associated electronics) on a single motherboard, which slides into an enclosure that can contain dozens of other blades. The enclosure supplies all of the blades with power, fans and cabling.

Unlike traditional servers in individual boxes, the use of server blades takes little physical room and allows thousands of blades to be deployed relatively cheaply. It is also quite easy to service the hardware, increase its power and manage the hardware resources. Installing, servicing, and removing blades is much easier than working with chassis-mounted servers. Shared power supply, cabling, fans and storage reduce the number of duplicated and failure-prone components in the environment. IT managers can easily monitor, configure, and troubleshoot systems. Organizations can also add to their systems in much smaller, more precise increments. Perhaps most important, blades offer the highest computing densities: they can't be beaten when measuring how much processing grunt you can get into a square meter of floor space.

1.10.4 Information Appliances

Information appliances are specialized servers dedicated to one task. They are extremely easy to install and add to infrastructure. Using specialized and proprietary components with embedded operating systems, they require little or no administration. Their abilities are preinstalled and preconfigured, and web browsers are used for configuration and administration. They are the classic "black box" devices where the user does not need to know *how* they work, just that they *do* work.

Information Appliances (also called network appliances) are a growing new class of dedicated devices that include: Internet (web) servers, Proxy/caching servers, Database servers, Email servers, and File servers.

Their Benefits Include

- Easy and quick installation
- Big cost saving for management and administration
- Easy remote configuration through a Web browser
- Operators do not have to be computer experts
- They need minimal user intervention
- They provide support for multiple versions of every leading operating system and are not tied to a specific OS
- Many are upgradeable via FTP or downloading code from the Internet
- They should not require any client software (programs on other computers in the organization)

A common information appliance is the multipurpose server appliance that provides, in one little box, some features as:

- Internet connectivity
- Website hosting
- A proxy server, to cache (store) downloads to avoid having to download them again soon afterwards
- Firewall servers
- Web access
- E-mail
- FTP
- Virtual Private Networking (VPN) facilities to connect employees, customers and e-business networks
- Print server functions (controlling printers on the network)
- File server operations
- Enterprise database management
- Transaction acceleration software
- Cluster administration (managing groups of servers)
- E-commerce hosting (e.g., website "shopping trolleys")

The product usually consists of an embedded OS with features like e-mail and Internet access managed through a browser, network-connected hardware, a hard disk, a processor, routing software, and a modem. Most appliances use a version of Linux running on an Intel processor.

Who uses information appliances rather than traditional servers? Those who want a job done, but don't want to be forever fiddling with settings and software installation. Dedicated information appliances often lack the sheer power of traditional servers, but score points for ease of use, flexible management, and reliability. Small organizations with little IT expertise would find such appliances attractive.

The drawback to such appliances is a result of their "sealed unit" nature : they are not usually designed to be expanded or seriously reconfigured. Like laptop computers, what you buy will be all you will have for the life of the product.

1.11 How Servers Are Different To Desktop Computers?

Servers tend to differ from the average computer in terms of:

Memory : Servers require large amounts of RAM to work efficiently. Application servers require huge amounts of RAM to run programs for remote users.

Storage : Servers need very large and fast hard disks. Many large servers use RAID (Redundant Array of Independent [or Inexpensive] Disks) arrays for maximum reliability and speed. RAID uses a group of hard disks that work as a unit and usually offer built-in backup of data. RAID disks are usually "Hot Swap" drives that can be removed and inserted without turning off the server or disrupting the network's operation.

Processing power : While processing power is not so important in a file server, application servers benefit greatly from having multiple CPUs.

Backup : Most servers have inbuilt high-capacity tape backup drives to protect against data loss. Tape drives usually use QIC (Quarter Inch Cartridge) tapes.

Connectivity : Servers often have two or more fast network cards to multiply the rate at which they can send and receive data to the rest of the network.

Robustness : Since servers run all day for years on end, the components used in them need to be of higher quality than those in the average desktop computer. As you may suspect a server will cost far more than a desktop PC - perhaps up to ten times as much.

Scalability : Servers are designed to be expandable as network demand grows. Scalability is the ability to increase the size and power of equipment and networks as required. Many servers let you add up to 8 hard disks, two power supplies, two NICs (Network Interface Cards), two CPUs etc. The design and engineering of this expandability is expensive.

The larger the network, the more work a server must perform. Bigger networks often use multiple servers to share the workload. Special load balancing software is used to distribute the workload efficiently between the servers.

Sometimes, networks use specialist servers that are dedicated to jobs such as:

- Login servers — which authenticate users
- Proxy servers — which cache recent downloads in case they're requested again
- DHCP servers — which allocate IP addresses to users as they log in
- Print servers — which manage the queues of print jobs
- CD towers and Virtual CD servers - which imitate large CD towers

- Web servers and FTP servers - which handle requests for web pages or files from the Internet
- Email servers - which receive, store and distribute e-mail.

On smaller networks, most of these services are performed by software in a single server. Overworked servers can be helped by using server blades. These slim units plug easily into a network and act as file servers. Network storage can be enhanced by plugging in NAS (Network Access Storage) units. With up to 960G of hard disk in a slim package, NAS devices greatly expand a network's storage capacity.

1.12 What Is Networking Hardware?

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data processing and communications within the network.

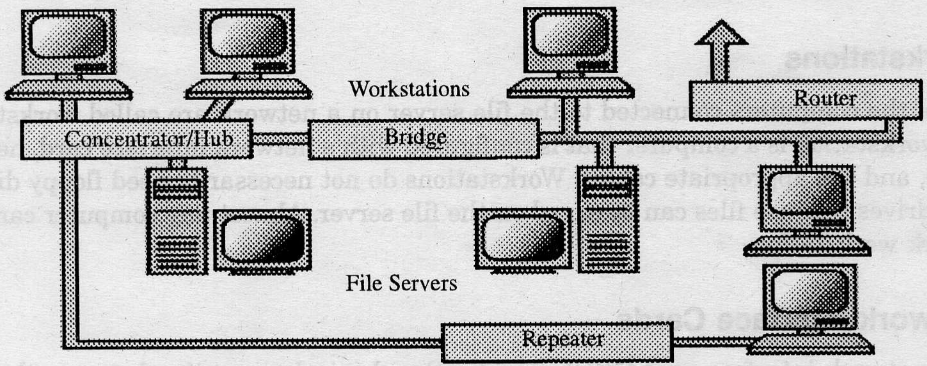

Fig. 1.14 Components of networking hardware.

It includes the following components:

1. File Servers
2. Workstations
3. Network Interface Cards
4. Concentrators/Hubs
5. Repeaters
6. Bridges
7. Routers

1. File Servers

A file server stands at the heart of most networks. It is a very fast computer with a large amount of RAM and storage space, along with a fast network interface card. The network operating system software resides on this computer, along with any software applications and data files that need to be shared.

The file server controls the communication of information between the nodes on a network. For example, it may be asked to send a word processor program to one workstation, receive a database file from another workstation, and store an e-mail message during the same time period. This requires a computer that can store a lot of information and share it very quickly. File servers should have at least the following characteristics:

- 166 megahertz or faster microprocessor (Pentium, PowerPC)
- A fast hard drive with at least nine gigabytes of storage
- A RAID (Redundant Array of Inexpensive Disks) to preserve data after a disk casualty
- A tape back-up unit (i.e. DAT, JAZ, Zip, or CD-RW drive)
- Numerous expansion slots
- Fast network interface card
- At least of 32 MB of RAM

2. Workstations

All of the computers connected to the file server on a network are called workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need floppy disk drives or hard drives because files can be saved on the file server. Almost any computer can serve as a network workstation.

3. Network Interface Cards

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer. Some computers, such as Mac Classics, use external boxes, which are attached to a serial port or a SCSI port. Laptop computers can now be purchased with a network interface card built-in or with network cards that slip into a PCMCIA slot.

Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards. According to an International Data Corporation study, Ethernet is the most popular, followed by Token Ring and LocalTalk.

Ethernet Cards

Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.

Local Talk Connectors

LocalTalk is Apple's built-in solution for networking Macintosh computers. It utilizes a special adapter box and a cable that plugs into the printer port of a Macintosh. A major disadvantage of LocalTalk is that it is slow in comparison to Ethernet. Most Ethernet connections operate at 10 Mbps (Megabits per second). In contrast, LocalTalk operates at only 230 Kbps (or .23 Mbps).

Ethernet Cards vs. LocalTalk Connections	
Ethernet	**LocalTalk**
Fast data transfer (10 to 100 Mbps)	Slow data transfer (.23 Mbps)
Expensive - purchased separately	Built into Macintosh computers
Requires computer slot	No computer slot necessary
Available for most computers	Works only on Macintosh computers

Token Ring Cards

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

4. Concentrators/Hubs

A concentrator is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central concentrator. Hubs are multislot concentrators into which can be plugged a number of multi-port cards to provide additional access as the network grows in size. Some concentrators are passive that is they allow the signal to pass from one computer to another without any change. Most concentrators are active that is they electrically amplify the signal as it moves from one device to another. Active concentrators are used like repeaters to extend the length of a network. Concentrators are:

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management
- Also called hubs
- Usually installed in a standardized metal rack that also may store net modems, bridges, or routers

5. Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

6. Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical topologies. They must, however, be used between networks with the same protocol.

7. Routers

A router translates information from one network to another; it is similar to a super intelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts. While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest—they can then redirect data around those sections until they clear up.

If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet. Routers can:

- Direct signal traffic efficiently

- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies
- Route messages across fiber optic, coaxial, and twisted-pair cabling

1.13 What Is A Network Operating System?

Unlike operating systems, such as DOS and Windows95 that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

Peer-to-Peer

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1.15). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. AppleShare and Windows for Workgroups are examples of programs that can function as peer-to-peer network operating systems.

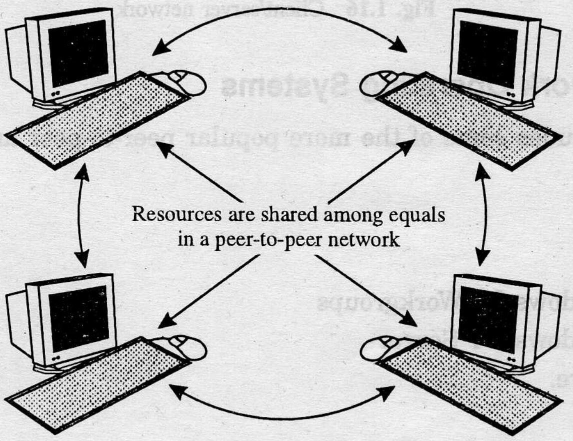

Fig. 1.15 Peer-to-Peer Network

Client/Server

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 1.16). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows NT Server are examples of client/server network operating systems.

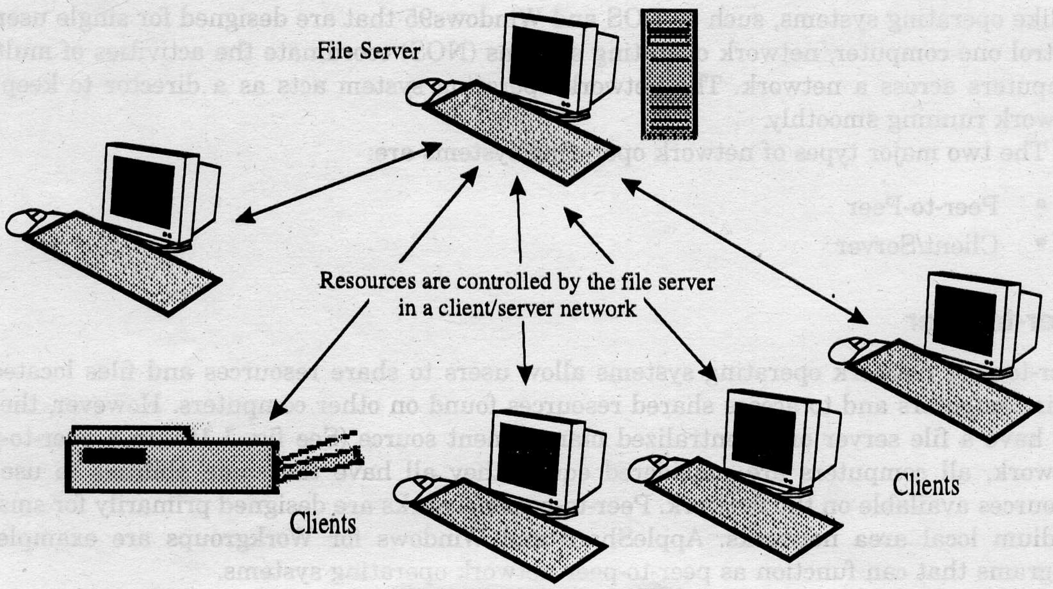
File Server
Resources are controlled by the file server in a client/server network
Clients
Clients

Fig. 1.16 Client/server network

Examples of Network Operating Systems

The following list includes some of the more popular peer-to-peer and client/server network operating systems.

- AppleShare
- LANtastic
- Microsoft Windows for Workgroups
- Microsoft Windows NT Server
- Novell Netware.

● ● ●

2

Network Topologies

2.1 What Is A Topology?

A topology is a generalized geometric configuration of some class of objects that join together. Topologies are the architectural "drawings" that show the overall physical configuration for a given communications system.

In networking, the term topology refers to the layout of connected devices on a network. It can be considered as the logical "shape" of the network wiring. This logical shape does not necessarily correspond to the actual *physical* layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle, but it would be highly unlikely to find an actual ring topology there.

'Logical' means how it looks as a pure design concept, rather than how it actually looks physically, e.g., the topology pictures you will see have nice straight lines between bits of the network, they don't try to show all the corners that need to be turned and holes that have to be drilled in a real cable installation.

A topology will indicate the access methods and will govern the rules that are used to design and implement the communication system. They represent the drawing of your network cable plant. It is important to make a distinction between a topology and architecture. A topology is concerned with the physical arrangement of the network components. In contrast, architecture addresses the components themselves and how a system is structured (cable access methods, lower level protocols, topology, etc.). An example of architecture is 10 base T Ethernet that typically uses the star topology.

Each topology has its advantages and disadvantages: usually related to cost, complexity, reliability and traffic "bottlenecks".

2.2 Basic Architectures

Prior to today's complicated computer network topologies, computer networks often consisted of either point-to-point or multipoint links.

(A) Point-to-Point

A point-to-point link is a direct connection between two devices (nodes). One example of this is a PC connected to a printer. A more common example is a mainframe terminal connected to a mainframe front-end processor.

(B) Multi Point

A multipoint link is a connection between three or more points on a link. Year's 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.

Addressing and Bandwidth

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.

2.3 Types Of Topologies

The different types of topologies are discussed below:

2.3.1 Star Topology

In a Star Network, all the nodes (PCs, printers and other shared peripherals) are connected to the central server.

It has a central connection point - like a hub or switch. A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator (See fig. 2.1).

All traffic emanates from the hub of the star. Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable. The hub offers a common connection for all stations on the network. Each station has its own direct cable connection to the hub.

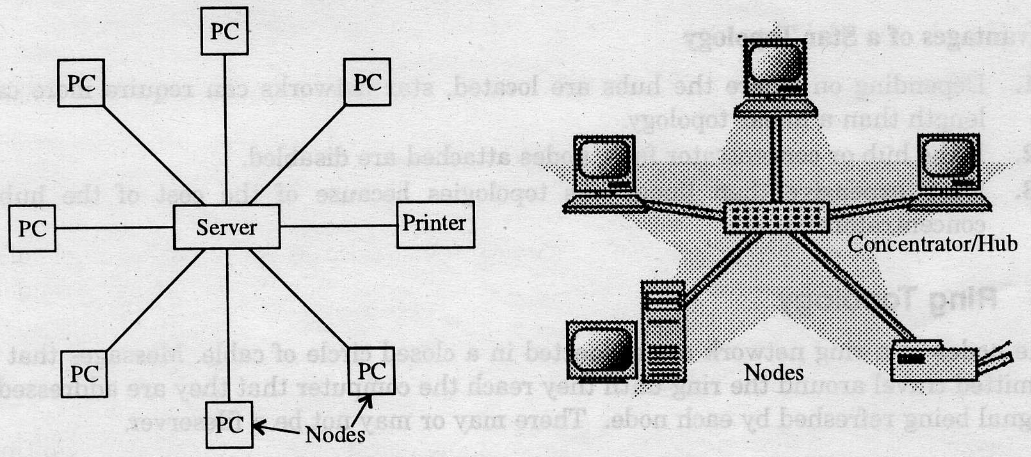

Fig. 2.1 Star Topology

Features of Star Network

- In a star network each node is connected by a point-to-point link to a central point.
- These central points are called hubs, concentrators or multipoint repeaters.
- These central points can be passive or active.
- If passive these hubs simply connect the points of the star.
- If active, these hubs regenerate (repeat) the electrical signals they receive.
- A hub-centered star topology is a broadcast network, because the hub copies each signal to all other computers attached to it.
- The hub may have extra features like LEDs that indicate activity and errors on each port, making it even easier to isolate problems.
- With the introduction of switches, you can dramatically increase network performance by replacing the hub with a switch.

Advantages of a Star Topology

1. Easy to install and wire.
2. Easy to add new stations as each station has its own direct cable connection to the hub. If a cable is cut, it only affects the computer that was attached to it.
3. It can accommodate different wiring. It can be installed using twisted pair, coaxial cable or fiber optic cable.
4. Since all information in a star topology goes through a central point star, topologies are easy to troubleshoot. A star can simplify troubleshooting because stations can be disconnected from the hub one at a time until the problem is isolated.
5. The main advantage is that one malfunctioning node does not affect the rest of the network.

Disadvantages of a Star Topology

1. Depending on where the hubs are located, star networks can require more cable length than a linear topology.
2. If the hub or concentrator fails, nodes attached are disabled.
3. More expensive than linear bus topologies because of the cost of the hub or concentrators.

2.3.2 Ring Topology

All the nodes in a ring network are connected in a closed circle of cable. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. There may or may not be a fileserver.

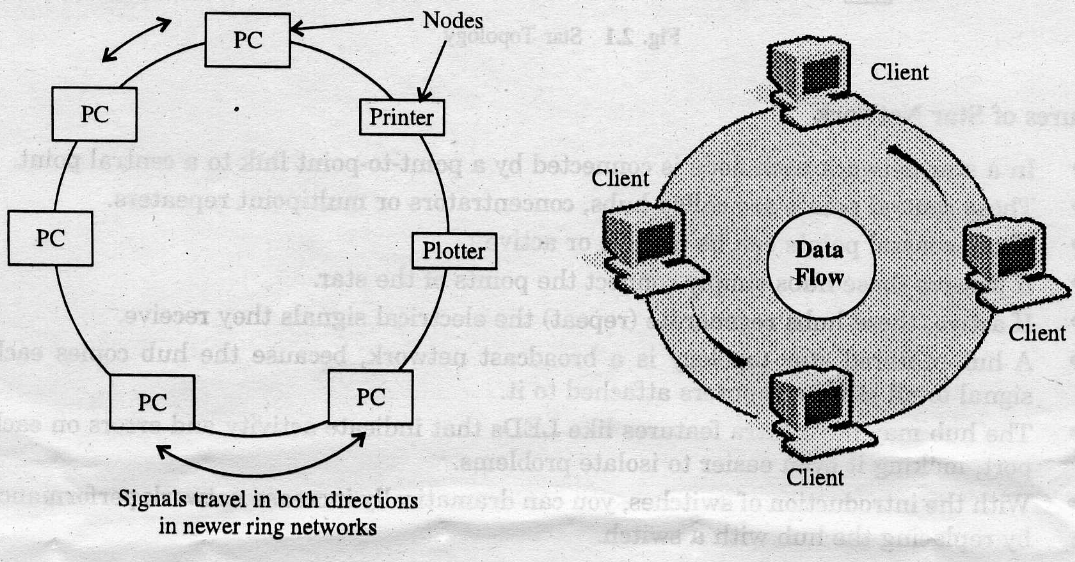

Fig. 2.2 Ring Topology

In a ring network, every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction. There are no terminated ends to the cable; the signal travels around the circle in a clockwise direction.

Under the ring concept, a signal is transferred sequentially via a "token" from one station to the next. When a station wants to transmit, it "grabs" the token, attaches data and an address to it, and then sends it around the ring. The token travels along the ring until it reaches the destination address. The receiving computer acknowledges receipt with a return message to the sender. The sender then releases the token for use by another computer.

Each station on the ring has equal access but only one station can talk at a time. In contrast to the 'passive' topology of the bus, the ring employs an 'active' topology. Each station repeats or 'boosts' the signal before passing it on to the next station.

Rings are normally implemented using twisted pair or fiber-optic cable.

Features of Ring Network

- A "pure" ring topology is a collection of separate point-to-point links, arranged to make a ring.
- Each node's network interface card (NIC) has one input and one output connection, so each node is connected to two links.
- When a node receives a signal on its input connection, its repeater circuitry retransmits that signal, immediately and without buffering, to its output connection.
- Thus, in many rings, data flows only in one direction.
- To send a message, a node transmits new bits onto the ring.
- If a message is addressed to a node, that node copies bits off the ring as they go by.
- If a node receives a message that is not addressed to it, it repeats the message without copying it.

Advantages of Ring Topology

1. Growth of system has minimal impact on performance. The ring networks can be larger than bus or star because each node regenerates the signal.
2. Degrade nicely under high utilization. Everybody gets to talk...
3. Fault tolerance builds into the design (can bypass damaged nodes).
4. All stations have equal access.
5. Data packets travel at a greater speed.

Disadvantages of Ring Topology

1. Expensive topology.
2. Failure of one computer may impact others. A failure in any cable or device breaks the loop and will take down the entire segment.
3. It is complex to implement and to extend the network; you must break the ring (which brings the network down). If any device is added to or removed from the ring, the ring is broken and the segment fails.
4. Data clashes can also occur if two machines send messages at the same time. Tokens or electronic signals that travel around the ring were invented to solve this problem. In a Token Ring Network, a computer can only send a message when the token is with it at the time.

2.3.3 Mesh Topology

In the topologies shown above, there is only one possible path from one node to another node. If any cable in that path is broken, the nodes cannot communicate. In a mesh topology, every device has a dedicated point-to point link to every other device. Such a network is called *complete* because between any two devices there is a special link; one could not add any non-redundant additional links.

Mesh topology uses *lots* of cables to connect every node with every other node. It is very expensive to wire up, but if any cable fails, there are many other ways for two nodes to communicate. Some WANs, like the Internet, employ mesh routing. In fact the Internet was deliberately designed like this to allow sites to communicate even during a nuclear war.

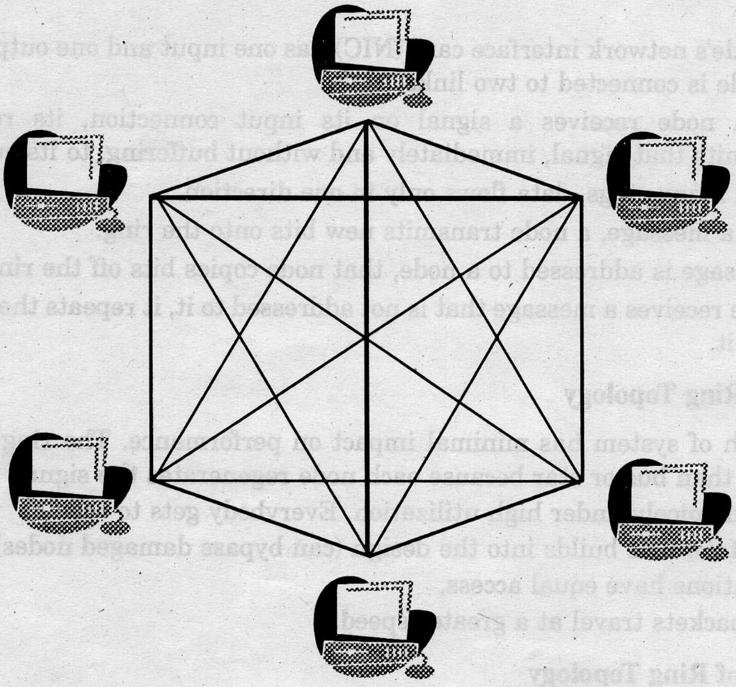

Fig. 2.3 Mesh Topology

Features of Mesh Network

- In a mesh topology, point-to-point links directly connect every site to every other site.

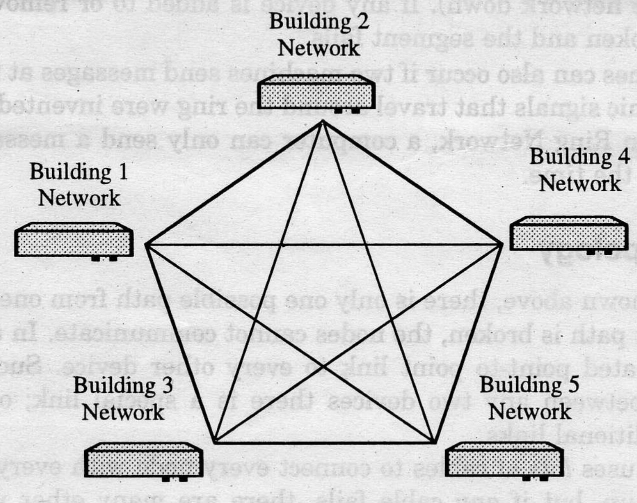

Fig. 2.4 Mesh Network

- Mesh networks are usually built over time as new sites are added to the overall network.
- A mesh topology is often used for MAN or WAN networks.
- The number of point-to-point links increases sharply with the number of locations. Thus, if a network must connect more than a few sites, a mesh topology is usually too expensive.

Advantages of Mesh Topology

1. Redundant links between devices.
2. *Good security*: If the line is not tapped only the intended recipient can see the data.
3. *Reliability*: Increasing network traffic does not affect the speed of other connections.
4. Easy fault identification and -isolation, an unusable link does not incapacitate the entire system

Disadvantages of Mesh Topology

1. Each node must have an interface for every other device.
2. Large amounts of cable for many devices to be connected in a mesh environment. A mesh topology for n devices needs $n \times \frac{(n-1)}{2}$ connections. It is therefore hard to install and expensive because of the extensive cabling.
3. Unless each station sends to every other station frequently, bandwidth is wasted. (Links that are not being used).
4. Another disadvantage is that there is only a limited amount of I/O-ports in a computer, but every connection uses one up.

2.3.4 Bus Topology

In a bus topology, all stations are attached to the same cable. In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code with the message. Most Local Area Networks (LANs) are Bus Networks because the network will continue to function even if one computer is down.

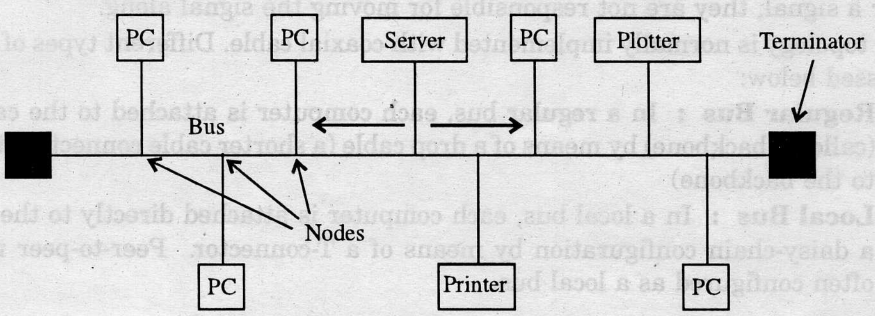

Fig. 2.5 Bus Topology

The purpose of the terminators (resistors) at either end of the network is to stop the signal being reflected back. If a bus network is not terminated, or if the terminator has the wrong level of resistance, each signal may travel across the bus several times instead of just once. This problem increases the number of signal collisions, degrading network performance.

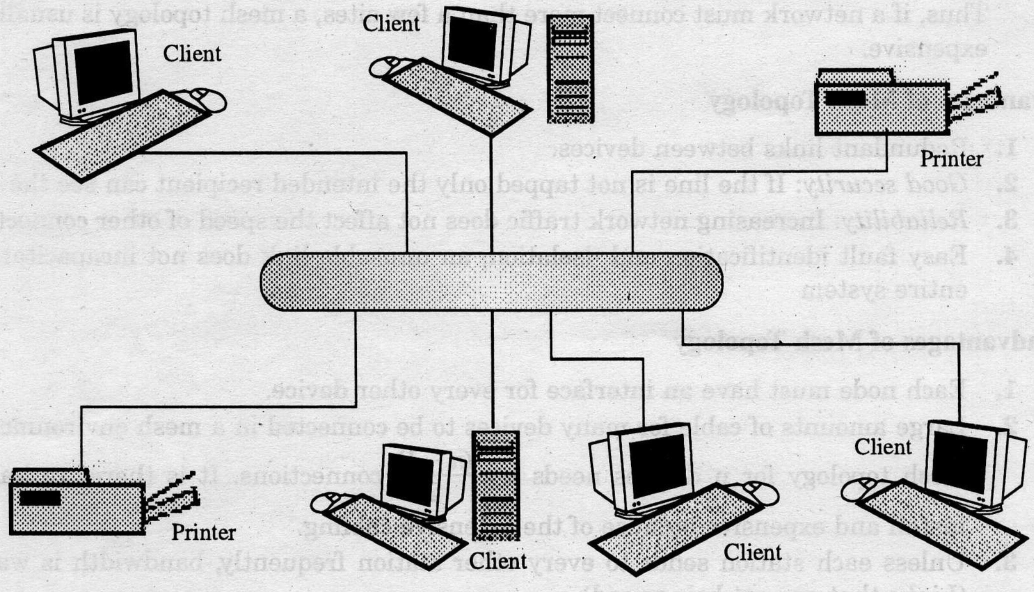

Fig. 2.6 Bus Topology

In a bus topology, signals are broadcast to all stations. Each computer checks the address on the signal (data frame) as it passes along the bus. If the signal's address matches that of the computer, the computer processes the signal. If the address doesn't match, the computer takes no action and the signal travels on down the bus.

Only one computer can 'talk' on a network at a time. A media access method called CSMA/CD is used to handle the collisions that occur when two signals are placed on the wire at the same time. The bus topology is passive. In other words, the computers on the bus simply 'listen' for a signal; they are not responsible for moving the signal along.

A bus topology is normally implemented with coaxial cable. Different types of bus topology are discussed below:

(a) **Regular Bus** : In a regular bus, each computer is attached to the cable segment (called a backbone) by means of a drop cable (a shorter cable connecting the computer to the backbone)

(b) **Local Bus** : In a local bus, each computer is attached directly to the backbone in a daisy-chain configuration by means of a T-connector. Peer-to-peer networks are often configured as a local bus.

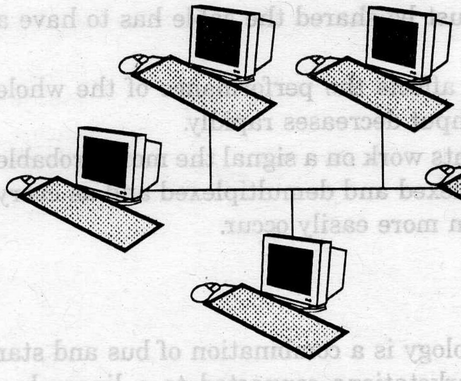

Fig. 2.7 Regular Bus

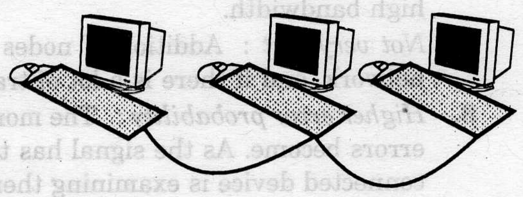

Fig. 2.8 Local Bus

Features of Bus Network

- A bus is a single electrical circuit to which all devices in the network are connected (although the bus might be made up of many individual pieces of wire).
- A bus topology is a broadcast network.
- When a node transmits data, the signal travels down the bus in both directions.
- Each node connected to the bus receives the signal as it passes that connection point.
- However, a node ignores any signal that is not specifically addressed to it.
- The cable is terminated at each end.
- The wiring is normally done point to point.
- A faulty cable will take the entire LAN down.

Advantages of Bus Topology

1. Bus topologies are relatively easy to install and don't require much cabling compared to other topologies.
2. Easy to connect a computer or peripheral to a linear bus.
3. Requires less cable length than a star topology, as you only need to chain the stations together.
4. There is no central point of failure on a bus because there is no hub.
5. Simple and easy to implement and extend.
6. Well suited for temporary networks that must be set up in hurry.
7. Failure of one station does not affect others.

Disadvantages of a Linear Bus Topology

1. Entire network shuts down if there is a break in the main cable.
2. Terminators are required at both ends of the backbone cable.
3. Difficult to identify the problem if the entire network shuts down.
4. Not meant to be used as a stand-alone solution in a large building.
5. Maintenance costs may be higher in the long run.

6. *More expensive cabling* : Because the line must be shared the cable has to have a high bandwidth.
7. *Not very fast* : Addition of nodes negatively affects the performance of the whole network, and if there is a lot of traffic throughput decreases rapidly.
8. *Higher error probability* : The more components work on a signal the more probable errors become. As the signal has to be multiplexed and demultiplexed and as every connected device is examining them errors can more easily occur.

2.3.5 Tree Topology

Also known as the 'Hierarchical topology', the tree topology is a combination of bus and star topologies. It consists of groups of star-configured 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. They are very common in larger networks.

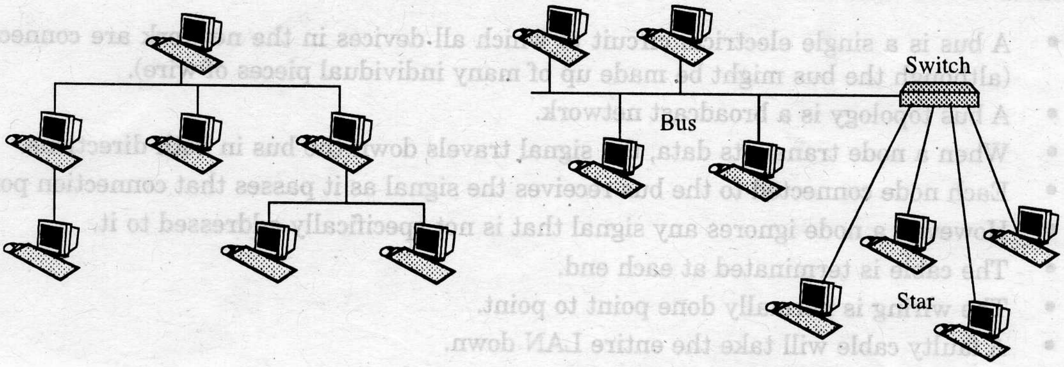

Fig. 2.9 Tree Topology

A typical scenario is : A file server is connected to a 24-port switch. A cable goes from the switch to a computer room where it connects to another switch. Many cables pass from this switch to the computers in the computer room. The node at the highest point in the hierarchy-usually a file server-controls the network.

Advantages of a Tree Topology

1. Point-to-point wiring for individual segments.
2. Supported by several hardware and software vendors.

Disadvantages of a Tree Topology

1. Overall length of each segment is limited by the type of cabling used.
2. If the backbone line breaks, the entire segment goes down.
3. More difficult to configure and wire than other topologies.

2.3.6 Hybrid Topology

Hybrid networks are simply networks that use multiple topologies. WANs usually use point-to-point links to connect remote rings or stars. The hybrid topology is popular in designing building, campus and enterprise networks.

There are many different ways the basic topologies can be combined. The World Wide Web itself is a giant hybrid topology.

- A hybrid star bus topology is a bus topology where at least one of the stations is replaced with the hub star topology network.
- A hybrid star ring topology looks like a star network except that the hub is wired as a logical ring. Such a hub is much easier to implement than a physical ring topology.
- A hybrid mesh topology is any hybrid topology where some of the key computers are connected in a mesh fashion. The WWW has its domain name servers as part of a hybrid mesh network.

A simple hybrid topology is shown in figure 2.10.

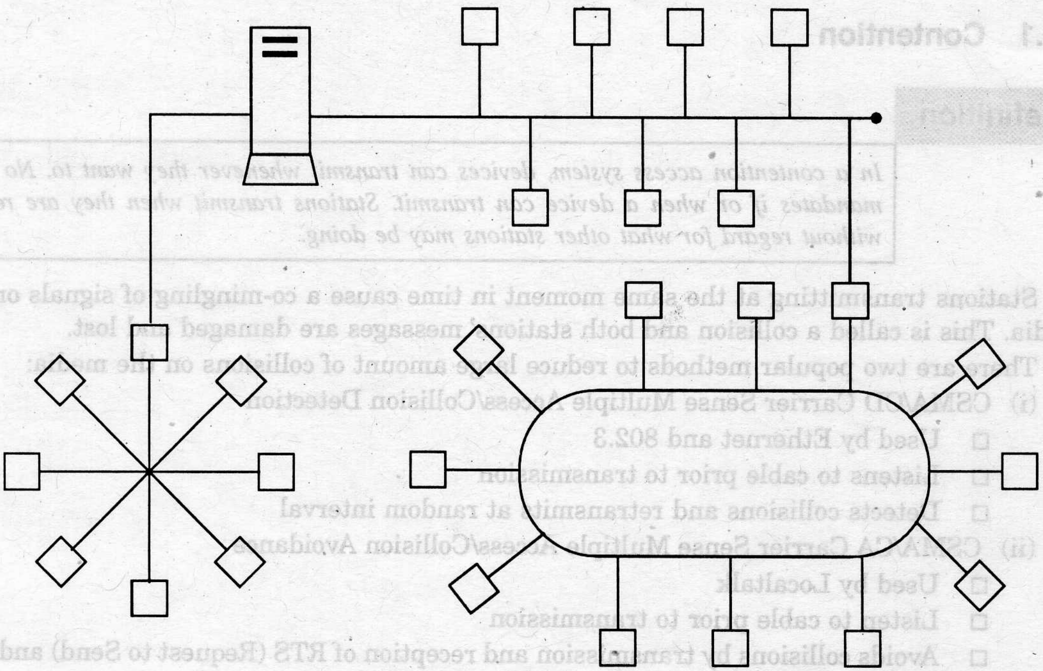

Fig. 2.10 Hybrid topology

2.3.7 Considerations When Choosing A Topology

- **Money :** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.

- **Length of cable needed :** The linear bus network uses shorter lengths of cable.
- **Future growth :** With a star topology, expanding a network is easily done by adding another concentrator.
- **Cable type :** The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

As a general rule, a bus topology is the cheapest to install, but may be more expensive to maintain because it does not provide for redundancy.

2.4 Access Methods

When several devices are connected to a single channel forming a multipoint connection, rules of communication need to be followed so that devices transmit and receive data without having their transmissions garbled. Access methods are the rules devices follow to access, transmit and release the communications channel.

2.4.1 Contention

Definition

In a contention access system, devices can transmit whenever they want to. No one mandates if or when a device can transmit. Stations transmit when they are ready without regard for what other stations may be doing.

Stations transmitting at the same moment in time cause a co-mingling of signals on the media. This is called a collision and both stations' messages are damaged and lost.

There are two popular methods to reduce large amount of collisions on the media:

(i) CSMA/CD Carrier Sense Multiple Access/Collision Detection
- □ Used by Ethernet and 802.3
- □ Listens to cable prior to transmission
- □ Detects collisions and retransmits at random interval

(ii) CSMA/CA Carrier Sense Multiple Access/Collision Avoidance
- □ Used by Localtalk
- □ Listen to cable prior to transmission
- □ Avoids collisions by transmission and reception of RTS (Request to Send) and CTS (Clear to Send) packets.

Advantages

- Simple
- Little overhead
- Throughput is high at light loads

Disadvantages

- As load increases throughput drops sometimes to unacceptable levels.
- There is no guarantee that a station will be able to transmit (in theory)

2.4.2 Polling

Definition

> *Polling designates one device as a Master Controller who is in charge of who can transmit. The master queries each other device called secondaries or slaves to see if they have information to transmit.*

One of the most common polling topologies is a star where the points of the star are secondary or slave machines and the master is the hub. This is a popular method to connect terminals to a terminal or communications controller.

Advantages

- Central control of channel access
- Priorities can be set
- Deterministic access to the media

Disadvantages

- Polling uses up a lot of bandwidth sending requests, acknowledgements and listening for messages
- Practical Implementation
- Assembly line or Robotic operation.

2.4.3 Token Passing

Definition

> *A special frame called a token is passed in an orderly manner from node to node. When a device has the token it ıemporarily had control of the media and can transmit. Passing the token distributes access control to each of the nodes attached to the media.*

Each device knows whom it receives the token from and who to pass the token to when finished. Each device on the network gets the opportunity to receive the token. Devices can only hold the token for a short amount of time before relinquishing it.

Several popular token passing topologies are in use. IEEE 802.5 Token Ring and IEEE 802.4 Token Bus. FDDI (Fiber Distributed Data Interface) also uses a token like access scheme.

Advantages

- Token passing is deterministic and is suitable for controlling automated equipment.
- Token passing schemes allow for setting priority.
- When the channel load is increased, throughput increases as well. High loads do not decrease data throughput.
- Token passing may offer the highest data throughput under high load conditions.

Disadvantages

- Token passing requires complicated software in all devices. This makes the hardware and software used to operate a token passing access scheme more expensive than a Collision based scheme.