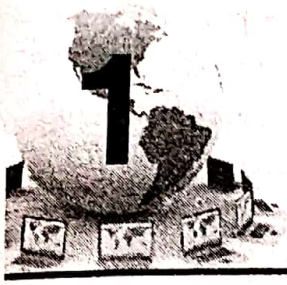


1 Network Basics

1.1. Introduction

In today's age networks are everywhere and our lives are influenced by them directly or indirectly. The advent of communication technology and computer technology have created wonders for common man. The merging of computers and communications has had a deep influence on the way computer systems are organized. The old model of a single computer serving all of the organization needs, is rapidly being replaced by one in which a larger number of separate but interconnected computers do the job. These systems are called computer networks. Let us take some examples to clear this concept. Do you know that you use a network when you take out some cash from local ATM? Even when you want to book your railway-tickets or airline tickets or hotel-room, you are using a network. whenever you send an email or make online shopping, again you are using network. The cable TV that comes to your room is just because of a network. There are so many other numerous examples of network usage in our daily lives. In most of these cases, you will find out that it is the computer network that is making it realize.

1.2. What is Network?

A network is a group of computers connected in some fashion in order to share resources. A group of computers in network would provide greater storage capacity and processing power than that by stand-alone independent machines. In addition to computers, a network also consists of peripheral devices with carriers and data communication devices used for the purpose of exchanging data and information.

By using computer networks, the cost of data transfer can be made economical because computers can send data at a very fast speed. Thus, computers enable us to reduce both cost and time in transferring data or information. In a network, computer of different make can be connected together and users can work together in a group. Software packages have been developed for group working in Data Base Management (DBMS) as well as in graphical artworks. Also, data from different departments located at distant places can be transferred to and stored on a central computer. This data can then be accessed by the computers located in different departments. The data at the central computer is updated and accessed by all users. This method would prevent any bottlenecks in the smooth functioning of the organization because all the users will get the latest information (for example, inventory) stored in the central computer.

Following figure shows you a typical network.

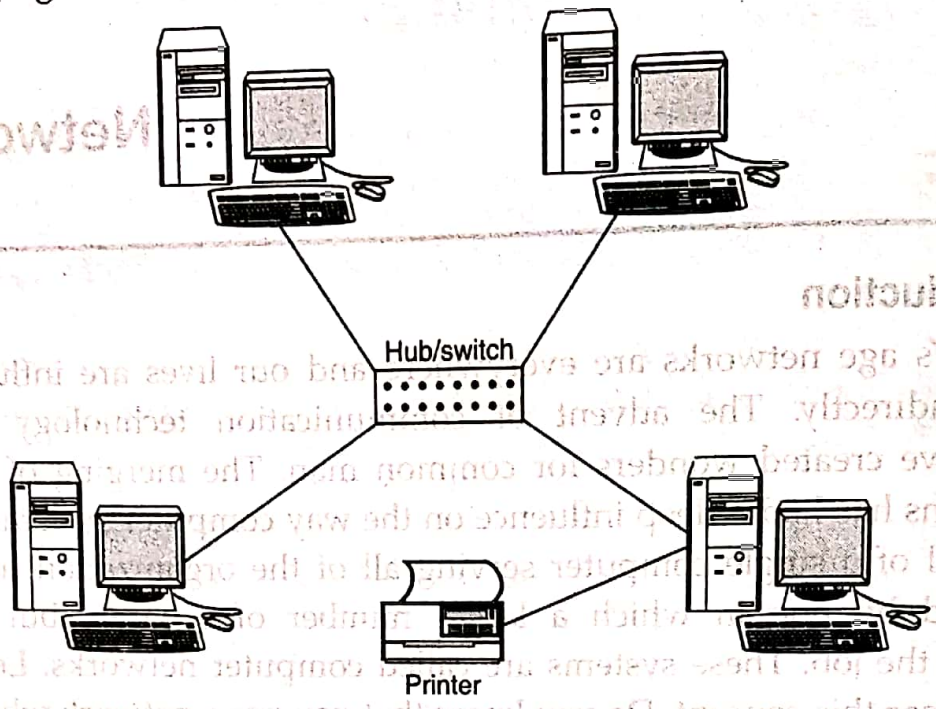


Fig. 1.1. A typical computer network

Every network includes :

- At least two computer's Server or Client workstation.
- Networking Interface Card's (NIC).
- A connection medium, usually a wire or cable, although wireless communication between networked computers and peripherals is also possible.
- Network Operating system software, such as Microsoft windows NT or 2000, Novell Netware, Unix and Linux.

So, by now it must be clear to you that a computer network consists of two or more computers that are linked together. This facilitates resource-sharing, file-exchange electronic-communication etc. As it will become clear to you in the coming section.

1.3. Need for Networking

Before getting into the technical details of computer networks, we must find out why people are interested in it and what makes it necessary for the survival of any organization in this competitive era.

1.3.1. Network Goals

Many organizations already have a substantial number of computers, often located far apart. For example, a company with many offices may have computers at each location to keep track of customer orders, monitor sales, and do the local payroll. Previously, each of these computers may have worked in isolation from others but at some point, management decided to connect them to gather information about entire company. In general we can refer to it as :

(i) **Resource Sharing** : The aim is to make all programs, data and peripherals available to anyone on the network irrespective of the physical location of the resources and the user.

(ii) **Reliability :** A file can have copies on two or three different machines, so if one of them is unavailable (hardware crash), the other copies could be used. For military, banking, air reservation and many other applications, it is of great importance.

(iii) **Cost Factor :** Personal computers have better price/performance ratio than micro computers. So it is better to have PC's, one per user, with data stored on one shared file server machine.

(iv) **Communication Medium :** Using a network, it is possible for managers, working far apart, to prepare financial report of the company. The changes at one end can be immediately noticed at another and hence it speeds up co-operation among them.

1.3.2. Application of Networks

Computer networks have made a major impact on the society as a whole but we will discuss only the important ones.

1. Sharing : The potential advantage of network is to provide an easy and flexible means of sharing. There are three distinct types of sharing :

(a) **Peripherals :** These are often expensive. It is impractical for each computer on the network to have both its laser printer (for quality printing) and dotmatrix printer (for all general printouts). A mainframe may have one of each connected to it allowing all users controlled access in a cost effective manner.

(b) Users of a multiuser system can share and exchange information in a number of ways. Examples are; sending electronic mail or having controlled access to the some files or database.

(c) In a traditional time sharing system, all control is performed centrally ; if the processor fails then enitre system fails. In a network system, this need not be the case. The failure of one node should not have a 'domain' effect on the rest. This is called distributed control and is a very lively area of research at present.

2. Access to Remote Database : Another major area of network use is access to remote database. It is easy for the averge person sitting at his PC to make reservation for airplanes, trains, hotels and so on anywhere in the world with instant confirmation.

3. Communication Facilities : A third category of potential widespread network use is as a communication medium. It is possible for everyone, not just people in the computer business, to send and receive electronic mail. This mail is also able to contain digitized voice, still pictures and even moving television and video images.

Using computer network as a sophisticated communication system may reduce the amount of travelling done, thus saving energy. The information revolution is expected to change society as much as the Industrial Revolution did.

Advantages of Networks

- **Share resources :** Such as printers and scanners. This is cheaper than buying equipment for each computer.
- **Share storage :** Being able to access files from any machines on the network can share data.
- **Can share software :** Software can be installed centrally rather than on each machine. Metering software can then be used to limit the number of copies being run at any one time. This is much cheaper than buying licenses for every machine.
- **Improve communications :** Messages can be sent—*e.g.* internal email.

Disadvantages of Networks

- The systems are more sophisticated and complex to run. This can add to costs and you may need specialist staff to run the network.
- If networks are badly managed services can become unusable and productivity falls.
- If software and files are held centrally, it may be impossible to carry out any work if the central server fails. People become reliant on the communications, if these fail it can cause havoc.
- File security is more important especially if connected to WANs e.g. protection from viruses.

1.4. Key Issues for Computer Network

The following are the major key issues to be trashed out very carefully before we go for a computer network.

1. **Nature of Nodes :** Whether participating nodes are homogeneous or heterogeneous in nature ?
2. **Topology :** Which of the computer topology has to be followed? Computer topology accounts for the physical arrangement of participating computers in the network.
3. **Interconnection Type :** Whether interconnection type is point-to-point, multipoint, or broadcast type.
4. **Reliability :** How reliable our network is ? Reliability aspect includes error rate, redundancy and recovery procedures.

5. **Channel Capacity Allocation :** Whether allocation of channel capacity is time-division or frequency division ?
6. **Routing Techniques :** Whether messages between nodes are to be routed through : Deterministic, Stochastic and distributed routing techniques?
7. **Models :** Which of the models *i.e.* analytical models, queuing models, simulation models, measurement and validation models are applicable?
8. **Channel Capacity :** What are the channel capacities of the communication lines connecting nodes?
9. **Access :** Whether computer access in the network is direct-access or through a sub-network?
10. **Protocols :** What levels, standards and formats are to be followed while establishing communication between participating nodes?
11. **Performance :** How is higher performance of computer network achieved ? Response time, time to connect, resource utilization, etc. contribute towards performance of computer network.
12. **Control :** Whether centralized control, distributed control or hierarchical control or participating nodes of computer network is suitable?

1.5. Elementary Terminology of Networks

It is now time to learn about the components/terms mostly used in networking. Whenever we talk about a network, it includes the hardware and the software that make up the network. Now let us have a look at some typical hardware components of network.

Nodes (Workstations)

The term nodes to the computers that are attached to a network and are seeking to share the resources of the network. Of course, if there were no nodes (also called workstations), there would be no network at all.

Server

On small networks, sometimes, all the shareble stuff (like files, data, software etc.) is stored on the server. A network can have more than one server also. Each server has unique name on the network and all users of network identify the server by its unique name.

Servers can be of two types : (i) non-dedicated and (ii) dedicated servers.

Non-dedicated Servers : On small networks, a workstation that can double up as a server, is known as non-dedicated server since it is not completely dedicated to the cause of serving. Such servers can facilitate the resource-sharing among workstations on a

proportionately smaller scale. Since one computer works as a workstation as well as a server, it is slower and requires more memory. The (small) networks using such a server are known as PEER-TO-PEER networks.

Dedicated Servers : On bigger network installations, there is a computer reserved for server's job and its only job is to help workstations access data, software and hardware resources. It does not double-up as a workstation and such a server is known as dedicated server. The networks using such a server are known as MASTER-SLAVE networks.

On a network, there may be several servers that allow workstations to share specific resources. For example, there may be a server exclusively for serving files-related requests like storing file, deciding about their access privileges and regulating the amount of space allowed for each user. This server is known as **file server**. Similarly, there may be **printer server** and **modem server.** The printer server takes care of the printing requirements of a number of workstations and the modem server helps a group of network users use a modem to transmit long distance messages.

1.6. Criteria for Classification of Computer Network

The following are the characteristics used to classify different types of computer's networks :

Topology : Topology is nothing but the geometric management of positioning computer systems to involve them in the form of a network. For example, Star topology Bus topology, etc.

Protocol : The protocols are nothing but the set of rules and signals that are used for communication in the network. For example, 'Ethernet' is one of the most popular protocols for LANs.

Architecture : Networks can usually be classified in the following two types :

1. Peer-to-peer architecture
2. Client-server architecture

1.7. Networking Models

A network model represents the architecture of computer network. The most popular network models are described below.

Peer-to-Peer Model

A network architecture in which all computers on the network have equal status and no one has control over ohters in called peer-to-peer model.

In peer-to-peer network there is no central computer to control other computers on the network. Each computer can share data and devices (or resources) of other computers in the network. For example, a printer attached with any computer can be used by all computers connected in the network. Each computer stores its own data and program files.

Advantages

The main advantages of peer-to-peer model are as follows :

- It is useful in small offices.
- It is easy to design and to maintain.
- It does not require any powerful computer.

Disadvantages

- The main disadvantages of peer-to-peer model are :
- It becomes slow under heavy use.
- There is no central place for storing data and software.
- It does not provide the security to protect the data stored on computers connected in the network.

Client-Server Model

A network architecture in which many clients request and receive services from a server is called client-server model.

The server is a dedicated powerful computer. It controls the whole network and provides a centralized storage area for data and software. It also processes the requests received from clients and manages other resources in the network. The resources may include printers and scanners.

All computers (other than computer server) connected in the network are called clients. A client provides interface the user. The user sends request to the server. Server receives the request from client computer and takes proper action on it. The result of request is sent to the client.

Client server network may consist of two or more servers. Some servers on a network perform only one specific task. These servers are called dedicated servers. For example, a file server stores and manages files. A database server stores and manages databases. It also provides access to databases. Similarly, a print server manages printers and print jobs.

Advantages

The client/server network has the following advantages :

- It reduces the volume of data traffic on the network.

- It provides faster responses to the client.
- It allows using less expensive computers as clients because most of the work is done by server.

Disadvantages

- The main disadvantages of this network are as follows :
- The servers are costly.
- The entire network is affected if there is any problem in the server computer.

Hybrid Nework Model

The hybrid network has combined features of both client/server and peer-to-peer network models. It also has one or more servers. The users can share the data and software. Similarly, each node can store its own data files and programs.

1.8. Categories of Network

A computer network means a group of 'networked' computers *i.e.*, computers that are linked by means of a communication system. A network can mean a small group of linked computers to a chain of a few hundred computers of different types spread around the world. Therefore networks vary in size, complexity and geographical spread. Mostly, computers are classified on this basis of geographical spread and on this basis, there can be four types of networks :

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Personal Area Network (PAN)

Local Area Network (LAN)

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include voice, sound, and video peripherals. Currently, LAN size is limited to a few kilometres.

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware e.g., a printer, software e.g., an application program, or data. A common example of a LAN, found in many business environments, links a work group of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large-capacity disk drive and become a server to the other clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of

software, or by restrictions on the number of users licensed to access the operating system. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Traditionally, LANs have data rates in the 4 to 16 Mbps range. Today, however speeds are increasing and can reach 100 Mbps with gigabit systems in development.

Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device. For example, a company can use a MAN to connect the LANs in all of its offices throughout a city.

A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company, such as a local telephone company. Many telephone companies provide a popular MAN service called Switched Multi-megabit Data Services (SMDS).

Wide Area Network (WAN)

A wide area network (WAN) provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, a continent, or even the whole world. In contrast to LANs (which depend on their own hardware for transmission), WANs may utilize public, leased, or private communication devices, usually in combinations, and can therefore span an unlimited number of miles. A WAN that is wholly owned and used by a single company is often referred to as an enterprise network.

Personal Area Network (PAN)

A personal area network (PAN) refers to a small network of communication capable IT enabled devices within a range of reachability of an individual person. This range is typically upto 10 metres. For instance, when we connect two cell phones through bluetooth, it forms PAN or connect our laptop with a cell phone, this also forms a PAN.

Note that, it can be wired or wireless. Wired PAN is established through some types of cable such as USB cables. The wireless PAN uses wireless technologies such as Bluetooth, IrDA, Z-wave etc.

Comparing these Networks

When the term computer network was first used, it described any interconnections between computers. Since that time, three subclasses have emerged that are distinguished primarily by their geographical scope.

The first of these is the wide area network (WAN). This network spans a large area-possibly several continents. The second major type is the local area network (LAN) and, as the name suggests, it is confined to relatively small areas such as a building or a group of buildings, for example a university campus. A third type, is the metropolitan area network (MAN). The scope of this class of network lies between LANs and WANs *i.e.*, spanning a small city or a town. MAN basically uses LAN technology. Cable Television networks are examples of analog MANs for television distribution. The MANs we are interested in are digital and are intended to connect computers. Most of the discussion on LAN also holds for MANs, so we will not mention the latter explicitly.

In naming these types of networks, the main distinguishing factor would appear to be the size of the area covered.

Difference between a LAN and a WAN

The next task is to distinguish between LANs and WANs. LANs are different in the following important respects :

- The distance between the nodes is limited. There is an upper limit of approx. 10 km, and a lower limit of 1 m.
- While WANs usually operate at speeds of less than 1 mbps (one mega bits per second), LANs normally operate at between 1 and 10 mbps. Using optical fiber technology, it is possible to achieve speeds of the order of hundreds of mbps.
- Because of the short distances involved, the error rates in LANs are much lower than in WANs. LANs error rate is 1000 times lower than in WANs so are normal.
- The distance limitations involved in LANs normally mean that the entire network is under the ownership and control of a single organization. This is in sharp contrast to WANs, where the network is normally operated by the countries post and telecommunications authorities rather than by its users.

It can be seen from the above, the LANs, differ from other types of network in that the area they cover is limited. This means they can operate at high speeds and with very low error rates. These two properties are the main distinguishing features of LANs.

1.9. Network Services

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Examples are the Domain Name System (DNS) which translates domain names to internet protocol (IP) addresses and the Dynamic Host Configuration Protocol (DHCP) to assign networking configuration information of network hosts. Authentication servers identify and authenticate users, provide user account profiles, and may log usage statistics.

E-mail, printing and network file system services are common services on local area networks. They require users to have permissions to access the shared resources.

Other network services include :

- Directory services
- e-mail
- File sharing
- Instant messaging
- Online game
- Printing
- File server
- Voice over IP
- Video on demand
- Video telephony
- World Wide Web
- Simple Network Management Protocol
- Time service
- Wireless sensor network
- Network file system

1.9.1. Directory Services

A directory service is the software system that stores, organizes and provides access to information in a computer operating system's directory. In software engineering, a directory is a map between names and values. It allows the lookup of named values, similar to a dictionary. As a word in a dictionary may have multiple definitions, a directory service can associate a name with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Directories may be very narrow in scope, supporting only a small set of node types and data types, or they may be very broad, supporting and arbitrary or extensible set of types. In a telephone directory, the nodes are names and the data items are telephone numbers. In the DNS the nodes are domain names and the data items are IP addresses (and alias, mail server names, etc.) In a directory used by a network operating system,

the nodes represent resources that are managed by the OS, including users, computers, printers and other shared resources. Many different directory services have been used since the advent of the internet.

A directory service called a naming service, maps the names of network resources to their respective network addresses. With the name service type of directory, a user does not have to remember the physical address of a network resource; providing a name locates the resource. Each resource on the network is considered an object on the directory server. Information adout a particular resource is stored as attributes of that object. Information within objects can be made secure so that only users with the available permissions are able to access it. More sophisticated directories are designed with namespaces as Subscribers, Services, Devices, Entitlements, Preferences, Content and so on. This design process is highly related to identity management.

A directory service defines the namespace for the network. A namespace in this context is the term that is used to hold one or more objects as named entries. The directory design process normally has a set of rules that determine how network resources are named and identified. The rules specify that the names be unique and unambiguous. In X 500 (the directory service standards) and LDAP the name is called the Distinguished name (DN) and refers to a collection of attributes (relative distinguished names) that make up the name of a directory entry.

A directory service is a shared information infrastructure for locating, managing, administering, and organizing common items and network resources, which can include volumes, folders, files, printers, users, groups, devices, telephone numbers and other objects. A directory service is an important component of a NOS (Network Operating System). In the more complex cases a directory service is the central information repository for a service delivery platform. For example. looking up "computers" using a directory service might yield a list of available computers and information for accessing them.

Replication and Distribution have very distinct meanings in the design and management of a directory service. The term replication is used to indicate that the same directory namespace (the same objects) are copied to another directory server for redundancy and throughput reasons. The replicated namespace is governed by the same authority. The term distribution is used to indicate that multiple directory servers, that hold different namespaces, are interconnected to form a distributed directory service. Each distinct namespace can be governed by different authorities.

1.9.2. e-mail

Electronic mail, most commonly referred to as email or e-mail is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model.

Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to a mail server, for as long as it takes to send or receive messages. Historically, the term electronic mail was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to describe fax document transmission. As a result, it is difficult to find the first citation for the use of the term with the more specific meaning it has today.

An Internet email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

Electronic mail predates the inception of the internet and was in fact a crucial tool in creating it, but the history of modern, global internet email services reaches back to the early ARPANET. Standards for encoding email messages were proposed as early as 1973 (RFC 561). Conversion from ARPANET to the internet in the early 1980 s produced the core of the current services. An email sent in the early 1970s looks quite similar to a basic text message sent on the internet today.

Email is an information and communications technology. It uses technology to communicate a digital message over the internet. Users use email differently, based on how they think about it. There are many software platforms available to send and receive. Popular email platforms include Gmail, Hotmail, Yahoo! Mail, Outlook, and many others.

Network-based email was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is now carried by the Simple Mail Transfer Protocol (SMTP), first published as internet standard 10 (RFC 821) in 1982. In the process of transporting email messages between systems, SMTP communicates delivery parameters using a message envelope separate from the message (header and body) itself.

1.9.3. File Sharing

File sharing is the practice of distributing or providing access to digital media, such as computer programs, multimedia (audio, images and video), documents or electronic books. File sharing may be achieved in a number of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers of computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking.

Types of File Sharing

Peer-to-peer File Sharing : Users can use software that connects into a peer-to-peer network to search for shared files on the computers of other users connected to the network. Files of interest can then be downloaded directly from other

users on the network. Typically, large files are broken down into smaller chunks, which may be obtained from multiple peers and then reassembled by the downloader. This is done while the peer is simultaneously uploading the chunks it already has to other peers.

File Sync and Sharing Services : Cloud-based file syncing and sharing services allow users to create special folders on each of their computers or mobile devices, which the service then synchronizes so that it appears to be the same folder regardless of which computer is used to view it. Files placed in this folder also are typically accessible through a website and mobile app, and can be easily shared with other users for viewing or collaboration. Such services have become popular via consumer products such as Dropbox and Google Drive.

Rsync is a more traditional program released in 1996 which synchronizes files on a direct machine-to-machine basis.

Data synchronization in general can use other approaches to share files, such as distributed file systems, version control, or mirrors.

1.9.4. Instant Messaging

Instant messaging (IM) is a type of online chat offers real-time text transmission over the internet. A LAN messenger operates in a similar way over a local area network. Short messages are typically transmitted bi-directionally between two parties, when each user chooses to complete a thought and select "send". Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, or video chat.

Non-IM types of chat include multicast transmission, usually referred as "chat rooms" where participants might be anonymous or might be previously known to each other (for example collaborators on a project that is using chat to facilitate communication). Instant messaging systems tend to facilitate connections between specified known users (often using a contact list also known as a "buddy list" or "friend list"). Depending on the IM protocol, the technical architecture can be peer-to-peer (direct point-to-point transmission) or client-server (a central server retransmits messages from the sender to the receiver).

1.9.5. Online Game

An online game is a video game played over some form of computer network. This network is usually the internet or equivalent technology, but games have always used whatever technology was current. modems before the internet, and hard wired terminals before modems. The expansion of online gaming has reflected the overall expansion of computer networks from small local networks to the internet and the growth of internet access itself. Online games can range from simple text based environments to games incorporating complex graphics and virtual worlds populated by many players simultaneously. Many online games have associated online communities, making online games a form of social activity beyond single player games.

1.9.6. Print Server

A print server, or printer server, is a device that connects printers to client computers over a network. It accepts print jobs from the computers and sends the jobs to the appropriate printers, queuing the job locally to accommodate the fact that work may arrive more quickly than the printer can actually handle it. Ancillary functions include the ability to inspect the queue of jobs to be processed, the ability to reorder or delete waiting print jobs, or the ability to do various kinds of accounting (such as counting pages printer, which may involve reading data generated by the printer (s). Some softwares, like Printer Logic's web application, is designed to manage printing and provide the ancillary functions listed above without using print servers.

Print servers may support a variety of industry-standard or proprietary printing protocols including internet printing protocol, Line printer daemon protocol, Netware, Net BIOS/Net BEUI, or Jet Direct.

A print server may be a networked computer with one or more shared printers. Alternatively a print server may be a dedicated device on the network, with connections to the LAN and one or more printers. Dedicated server appliances tend to be fairly simple in both configuration and features. Print server functionality may be integrated with other devices such as a wireless router, a firewall, or both. A printer may have a built-in print server.

All printers with the right type of connector are compatible wiht all print server; manufactures of servers make available lists of compatible printers because a server may not implement all the communications functionality of a printer (e.g. low ink signal).

1.9.7. File Server

In computing, a file server is a computer attached to a network that has the primary purpose of providing a location for shared disk access, *i.e.* shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. The term server highlights the role of the machine in the client-server scheme, where the clients are the workstations using the storage. A file server is not intended to perform computational tasks, and does not run programs on behalf of its clients. It is designed primarily to enable the storage and retrieval of data while the computation is carried out by the workstations.

File servers are commonly found in schools and offices, where users use a LAN to connect their client computers.

1.9.8. VoIP

Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol (IP) networks, such as the internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, broadband telephony, and broadband phone service.

The term internet telephony specifically refers to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public internet, rather than via the public switched telephone network (PSTN). The steps and principles involved in originating VoIP telephone calls are similar to traditional digital telephony and involve signaling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, however, the digital information is packetized, and transmission occurs as IP packets over a packet-switched network. Such transmission entails careful considerations about resource management different from time-division multiplexing (TDM) networks.

Early providers of voice-over-IP services offered business models and technical solutions that mirrored the architecture of the legacy telephone network. Second-generation providers. such as skype, have built closed network for private user bases, offering the benefit of free calls and convenience while potentially charging for access to other communication networks, such as the PSTN. This has limited the freedom of users to mix-and-match third-party hardware and software. Third-generation providers, such as Google Talk, have abopted the concept of federated VoIP—which is a departure from the architecture of the legacy networks. These solutions typically allow dynamic interconnection between users on any two domains on the internet when a user wishes to place a call.

VoIP systems employ session control and signaling protocols to control the signaling, set-up and tear-down of calls. They transport audio streams over IP networks using special media delivery protocols that encode voice, audio, video with audio codecs, and video codecs as digital audio by streaming media. Various codecs exist that optimize the media stream based on application requirements and network bandwidth; some implementation rely on narrowband and compressed speech, while others support high fidelity stereo codecs. Some popular codecs include μ-law and a-law versions of G. 711, G. 722 which is a high-fidelity codec marketed as HD voice by polycom, a popular open source voice codec known as iLBC, a codec that only uses 8 kbit/s each way called G. 729, and many others.

VoIP is available on many smartphones, personal computers, and on Internet access devices. Calls and SMS text messages may be sent over 3G or Wi-Fi

1.9.9. Video on Demand

Video on demand (VoD) or audio and video on demand (AVoD) are systems which allow users to select and watch/listen to video or audio content when they choose to rather than having to watch at a specific broadcast time. IPTV technology is often used to bring video on demand to televisions and personal computers.

Television VoD systems can either stream content through a set-top box, a computer or other device allowing viewing in real time, or download it to a device such as a computer, digital video recorder (also called a personal video recorder) or portable media player for viewing at any time. The majority of cable-and telco-based television

providers offer both VOD streaming, including pay-per-view and free content, whereby a user buys or selects a movie or television program and it begins to play on the television set almost instantaneously, or downloading to a DVR rented from the provider, or downloaded onto a PC, for viewing in the future. Internet television, using the Internet, is an increasingly popular form of video on demand.

Some airlines offer AVOD as in-flight entertainment to passengers through individually controlled video screens embedded in seatbacks or armrests or offered via portable media players. Airline AVOD systems offer passengers the opportunity to select specific stored video or audio content and play it on demand including pause, fast forward and rewind.

Other forms of video on demand also include "subscription video on demand" (SVOD), which includes services such as Netflix that require users to pay a monthly fee to access a bundled set of content. Another subset of video on demand is "advertising video on demand" (another kind of AVOD), which includes services such as Hulu or Sony's Crackle. This AVOD is often free for users, and the platforms rely on selling advertisements as a main revenue stream.

1.9.10. Video Telephony

Video telephony comprises the technologies for the reception and transmission of audio-video signals by users at different locations, for communication between people in real-time.

At the dawn of the technology, videotelephony also included image phones which would exchange still images between units every few seconds over conventional POTS-type telephone lines, essentially the same as slow scan TV systems.

Currently videotelephony usage has made significant inroads in government, healthcare, education and the news media. It is particularly useful to the deaf and speech-impaired who can use the technology with sign language and also with a video relay service, and well as to those with mobility issues or those who are located in distant places and are in need of telemedical or tele-educational services. It is also used in commercial and corporate settings to facilitate meetings and conferences, typically between parties that already have established relationships. Like all long distance communications technologies (such as phone and internet), by reducing the need to travel to bring people together the technology also contributes to reductions in carbon emissions, thereby helping to reduce global warming.

1.9.11. World Wide Web

The World Wide Web (abbreviated as **WWW**, commonly known as the Web) is a system of interlinked hypertext documents that are accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia and navigate between them via hyperlinks.

Tim Berners-Lee, a British computer scientist and former CERN employee and Belgian computer scientist Robert Cailliau are considered the inventors of the Web. On March 12, 1989, Berners-Lee wrote a proposal for what would eventually become the World Wide Web. The 1989 proposal was meant for a more effective CERN communication system but Berners-Lee eventually realised the concept could be implemented throughout the world. Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "to link and access information of various kinds as a web of nodes in which the user can browse at will", and Berners-Lee finished the first website in December of that year. The first test was completed around 20 December 1990 and Berners-Lee reported about the project on the newsgroup alt hypertext on 7 August 1991.

1.9.12. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

1.9.13. Time Server

A time server is a server computer that reads the actual time from a reference clock and distributes this information to its clients using a computer network. The time server may be a local network time server or an internet time server.

The most important and widely used protocol for distributing and synchronising time over the Internet is the Network Time Protocol (NTP), though other less-popular of outdated time protocols continue in use. A variety of protocols are in common use for sending time signals over radio links and serial connections.

The time reference used by a time server could be another time server on the network of the Internet, a connected radio clock or an atomic clock. The most common true time source is a GPS or GPS master clock. Time servers are sometimes multi-purpose network servers, dedicated network servers, or dedicated devices. All a dedicated time server dose is provide accurate time.

An existing network server (*e.g.* a file server) can become a time server with additional software. The NTP homepage provides a free and widely used reference

implementation of the NTP server and client for many popular operating systems. The other choice is a dedicated time server device.

The term "stratum "is used to label the closeness to a central or high quality time server. The stratum indicates the place of a particular time server in a hierarchy of servers. The scale is 0 to 14 where 0 is the most accurate and likely a highly specialized physical hardware device. Sometimes clients will reject a time update from a server whose stratum is too high and most will prefer low strata time sources to higher ones. This can be a pitfall for administrators setting up an in-house time server with no true time source.

1.9.14. Wireless Sensor Network

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or enviromental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes"—from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts; a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arraged each year, for example IPSN, SenSys and EWSN.

1.9.15. Network File System

Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

The Network File System is an open standard defined in RFCs, allowing anyone to implement the protocol.

1.10. Network Topologies

In order to form a network, computers need to be interconnected in some layouts, known as topologies.

1. Cost : For a network to be cost effective, one would try to minimize installation cost. This may be achieved by using well understood media and also, to a lesser extent, by minimizing the distances involved.

2. Flexibility : Because the arrangement of furniture, internal walls etc. in offices is often subject to change, the topology should allow for easy reconfiguration of the network. This involves moving existing nodes and adding new ones.

3. Reliability : Failure in a network can take two farms. Firstly, and individual node can malfunction. This is not nearly as serious as the second type of fault where the network itself fails to operate. The topology chosen for the network can help by allowing the location of the fault to be detected and to provide some means of isolating it.

1.10.1. Point-to-Point Link

Before we talk about topologies in details, let us learn about point-to-point link. Point-to-Point link basically relies upon two functions—transmit and receive. The main characteristic of P-P network is that each station receives exactly from one transmitter, and each transmitter transmits to exactly one receiver. The transmit and receive operations can occur over separate wires (for better performance) or they can take turns over the same wire using a variety of techniques.

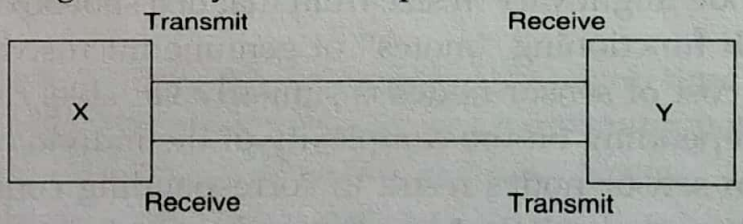


Fig. 1.2. Point-to-Point Network

Point-to-point networks can grow in several ways. One method is simply to install a P-P link between each pair of computers in the network. This approach is called a Mesh.

Many topologies have been developed, but major ones are :

- star topology;
- bus;
- ring or circular;
- tree;
- graph;
- mesh.

1.10.2. Star Topology

This topology consists of a central node to which all other nodes are connected by a single path. It is the topology used in most existing information network involving data processing or voice communications. The most common example of this is IBM 370 installations. In this case multiple 3270 terminals are connected to either a host system or a terminal controller.

Advantages of the Star Topology

1. Ease of Service : The star topology has a number of concentration points (where connections are joined). These provide easy access for service or reconfiguration of the network.

2. One Device per Connection : Connection points in any network are inherently prone to failure. In the star topology, failure of a single connection typically involves disconnecting one node from an otherwise fully functional network.

3. Centralized Control/Problem Diagnosis : The fact that the central node is connected directly to every other node in the network means that faults are easily detected and isolated. It is a simple matter to disconnect failing nodes from the system.

4. Simple Access Protocols : Any given connection in a star network involves only the central node. In this situation, contention for who has control of the medium for the transmission purposes is easily solved. Thus in a star network, access protocols are very simple.

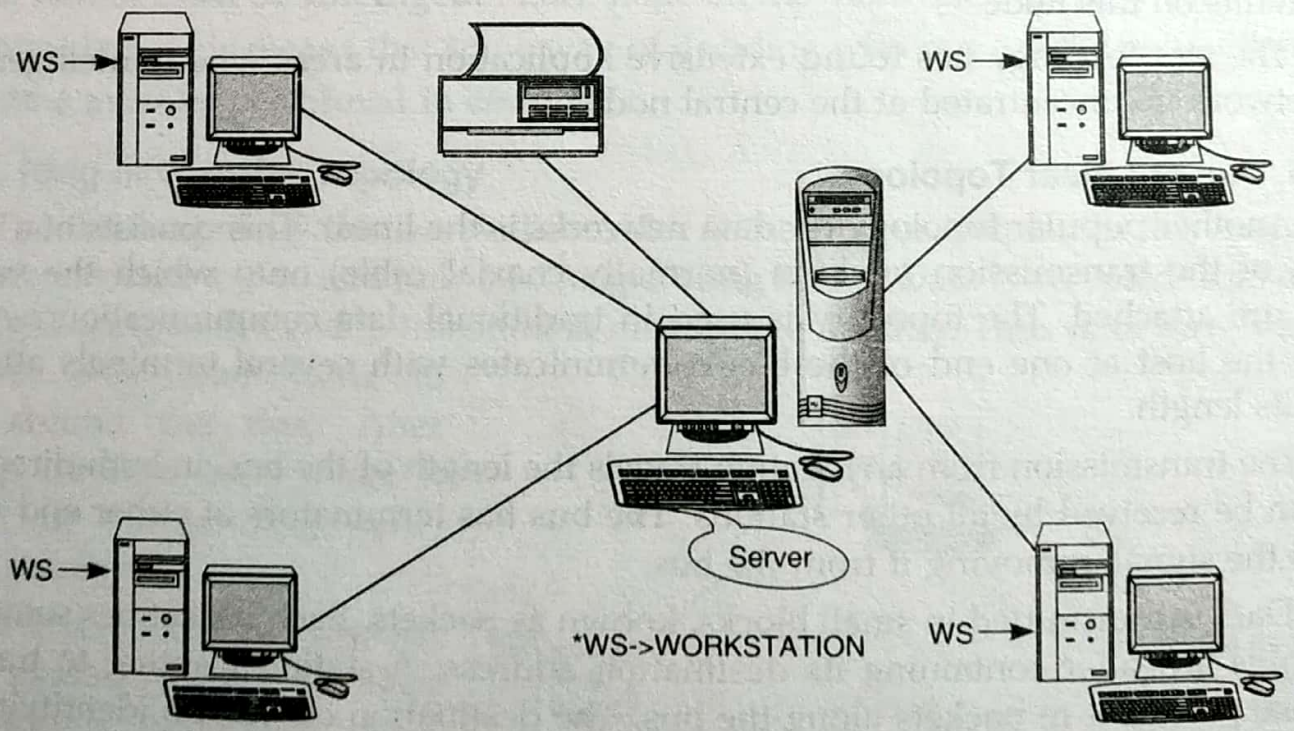


Fig. 1.3. Star Topology

Disadvantages of the Star Topology

1. Long Cable Length : Because each node is directly connected to the center, the star topology necessitates a large quantity of cable. Whilst the cost of cable is often small

congestion in cable ducts and maintenance and installation problems can increase cost considerably.

2. Difficult to Expand : The addition of a new node to a star network involves a connection all the way to the central node.

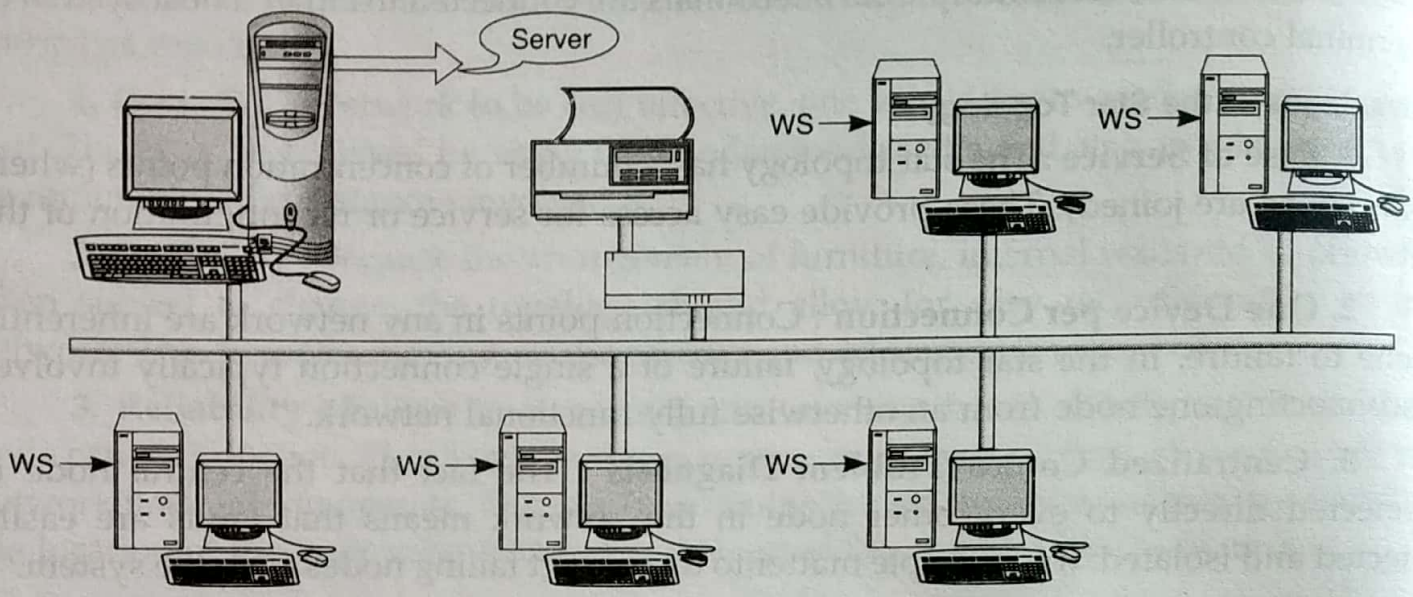


Fig. 1.4. Bus Topology

3. Central Node Dependency : If the central node in a star network fails, the entire network is rendered inoperable. This introduces heavy reliability and redundancy constraints on this node.

The star topology has found extensive application in areas where intelligence in the network is concentrated at the central node.

1.10.3. Bus or Linear Topology

Another popular topology for data networks is the linear. This consists of a single length of the transmission medium (normally coaxial cable) onto which the various nodes are attached. The topology is used in traditional data communication network where the host at one end of the bus communicates with several terminals attached along its length.

The transmission from any station travels the length of the bus, in both directions, and can be received by all other stations. The bus has terminators at either end which absorb the signal, removing it from the bus.

Data is transmitted in small blocks, known as packets. Each packet has some data bits, plus a header containing its destination address. A station wanting to transmit some data sends it in packets along the bus. The destination device, on identifying the address on the packets, copies the data onto its disk.

Advantages of the Linear Topology

1. Short Cable Length and Simple Wiring Layout : Because there is a single common data path connecting all nodes, the linear topology allows a very short cable

length to be used. This decreases the installation cost, and also leads to a simple, easy to maintain wiring layout.

2. Resilient Architecture : The LINEAR architecture has an inherent simplicity that makes it very reliable from a hardware point of view. There is a single cable through which all the data propagates and to which all nodes are connected.

3. Easy to Extend : Additional nodes can be connected to an existing bus network at any point along its length. More extensive additions can be achieved by adding extra segments connected by a type of signal amplifier known as *repeater.*

Disadvantages of the Linear Topology

1. Fault Diagnosis is Difficult : Although simplicity of the bus topology means that there is very little to go wrong, fault detection is not a simple matter. Control of the network is not centralized in any particular node. This means that detection of a fault may have to be performed from many points in the network.

2. Fault Isolation is Difficult : In the star topology, a defective node can easily be isolated from the network by removing its connection at the center. If a node is faulty on the bus, it must be rectified at the point where the node is connected to the network.

3. Repeater Configuration : When BUS type network has its backbone extended using repeaters, reconfiguration may be necessary.

4. Nodes must be Intelligent : Each node on the network is directly connected to the central bus. This means that some way of deciding who can use the network at any given time must be performed in each node.

1.10.4. Ring or Circular Topology

The third topology that we will consider is the ring or circular. In this case, each node is connected to two and only two neighboring nodes. Data is accepted from one of the neighboring nodes and is transmitted onwards to another. Thus data travels in one direction only, from node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

It is important to note that data 'passed through' rather than 'travels past' each node. This means that the signal may be amplified before being 'repeated' on the outward channel.

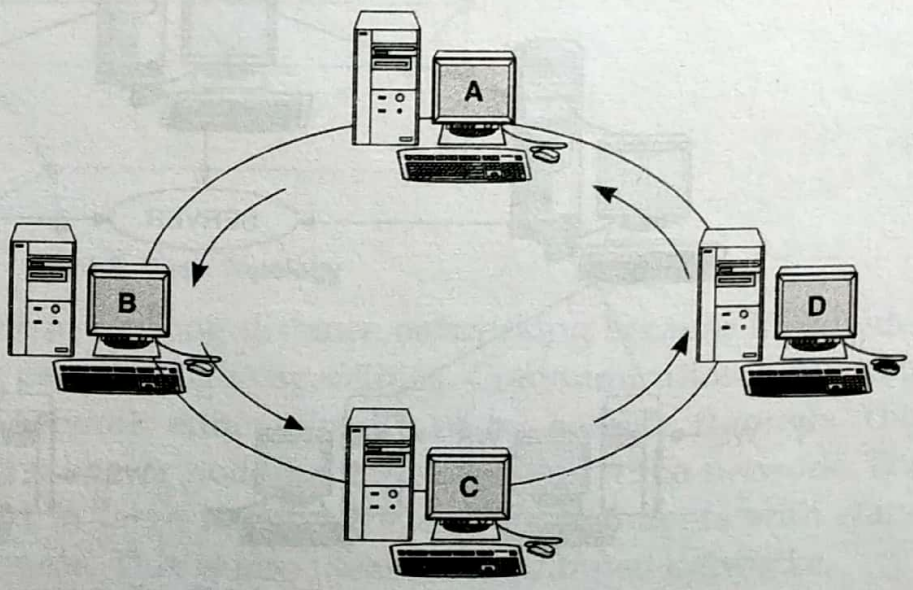


Fig. 1.5. Ring Topology

Advantages of the Ring Topology

1. Short Cable Length : The amount of cabling involved in a ring topology is comparable to that of a bus and is small relative to that of a star. This means that less connections will be needed, which will in turn increase network reliability.

2. No Wiring Closet Space Required : Since there is only one cable connecting each node to its immediate neighbours, it is not necessary to allocate space in the building for wiring closets.

3. Suitable for Optical Fibres : Using optical fibres offers the possibility of very high speed transmission. Because traffic on a ring travels in one direction, it is easy to use optical fibres as a medium of transmission.

Disadvantages of the Ring Topology

1. Node Failure Causes Network Failure : The transmission of data on a ring goes through every connected node on the ring before returning to the sender. If one node fails to pass data through itself, the entire network has failed and no traffic can flow until the defective node has been removed from the ring.

2. Difficult to Diagnose Faults : The fact that failure of one node will affect all others has serious implications for fault diagnosis. It may be necessary to examine a series of adjacent nodes to determine the faulty one. This operation may also require diagnostic facilities to be built into each node.

3. Network Reconfiguration is Difficult : It is not possible to shut down a small section of the ring while keeping the majority of it working normally.

1.10.5. Tree Topology

A variation of bus topology is the *tree topology*. The shape of the network is that of an inverted tree with the central root branching and sub branching to the extremities of the network.

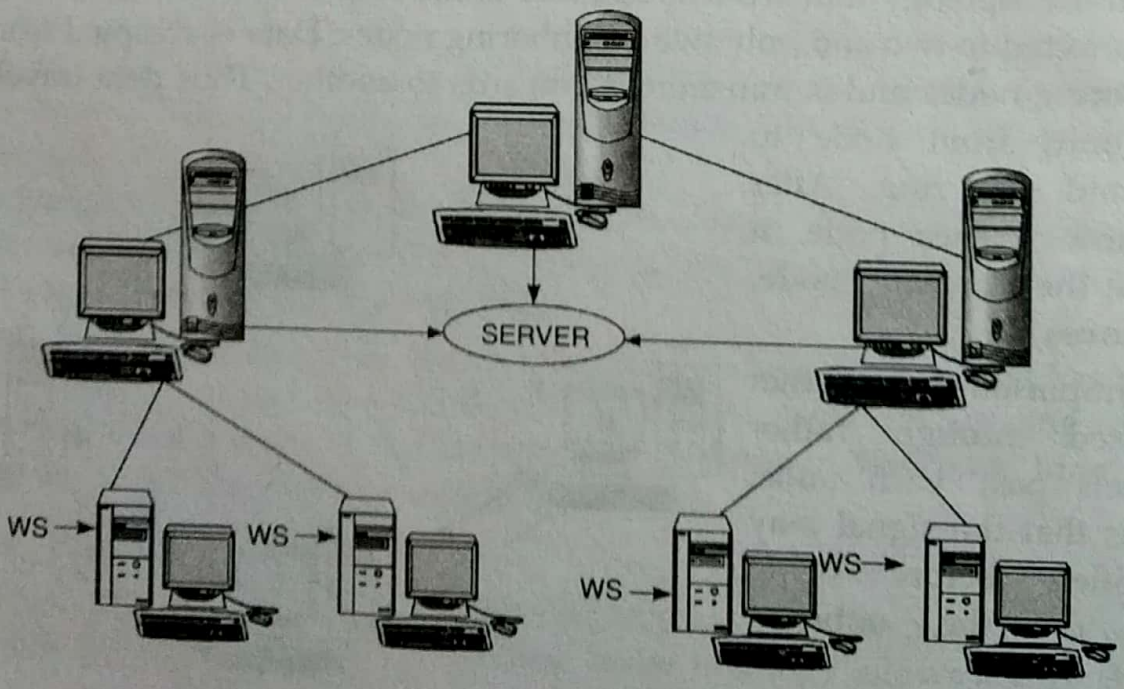


Fig. 1.6. Tree Topology

Transmission in this topology takes place in the same way as in the Bus topology. In both cases, there is no need to remove packets from the medium because when a signal reaches the end of the medium, it is absorbed by the terminators. Tree topology is best suited for applications which have a hierarchical flow of data and control. Since the tree topology is a modification of a 'pure' network topology, Bus topology, it is a *hybrid* topology.

1.10.6. Graph Topology

In this topology, nodes are connected together in an arbitrary fashion. A link may or may not connect two or more nodes. There may be multiple links also. It is not necessary that all the nodes are connected. But if a path can be established in two-nodes via one or more links, it is called a connected graph.

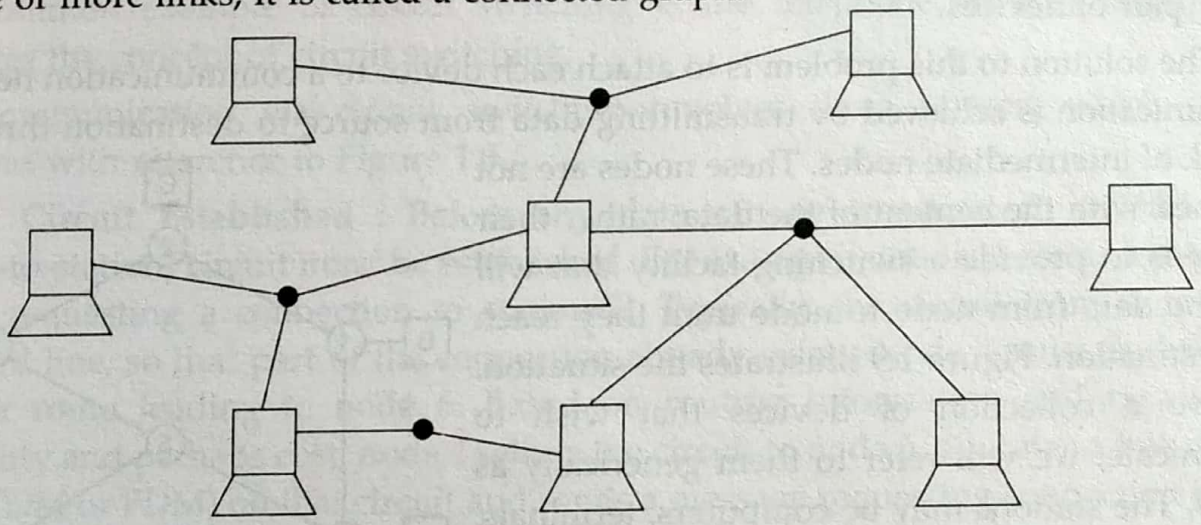


Fig. 1.7. Graph Topology

1.10.7. Mesh Topology

In this topology, each node is connected to more than one node to provide an alternative route in the case the host is either down or too busy. It is an extension to P-P network.

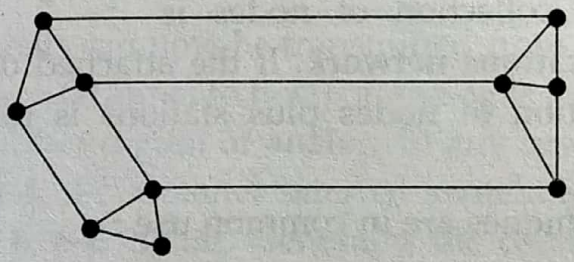


Fig. 1.8. Mesh Topology

The mesh topology is excellent for long distance networking because it provides extensive back-up, rerouting and pass-through capabilities. Communication is possible between any two nodes on the network either directly or by passing through. This function is needed in the event of a line or node failure elsewhere in the network. The mesh topology is commonly used in large internetworking environments with stars, rings and buses attached to each node. This is also ideal for distributed networks.

1.11. Switching Techniques

Data communication takes place between two devices that are directly connected by some form of transmission medium. Often however, it is impractical for two devices to be directly connected. This is so for one (or both) of the following contingencies :

- The devices are very far apart. It would be inordinately expensive, for example, to string a dedicated link between two devices thousands of miles apart.
- There is a set of devices, each of which may require a link to many of the others at various times. Examples are all of the telephones in the world and all of the terminals and computers owned by a single organisation. Except for the case of a very few devices, it is impractical to provide a dedicated wire between each pair of devices.

The solution to this problem is to attach each device to a communication network. Communication is achieved by transmitting data from source to destination through a network of intermediate nodes. These nodes are not concerned with the content of the data; rather their purpose is to provide a switching facility that will move the data from node to node until they reach their destination. Figure 1.9 illustrates the situation. We have a collection of devices that wish to communicate; we will refer to them generically as **stations.** The stations may be computers, terminals, telephones or other communicating devices. We also have a collection of devices whose purpose is to provide communications, which we will refer to as **nodes.** The nodes are connected to each other in some fashion by transmission links. Each station attaches to a node. The collection of nodes is referred to as **a communications network.** If the attached devices are computers and terminals, then the collection of nodes plus stations is referred to as **a commuter network.**

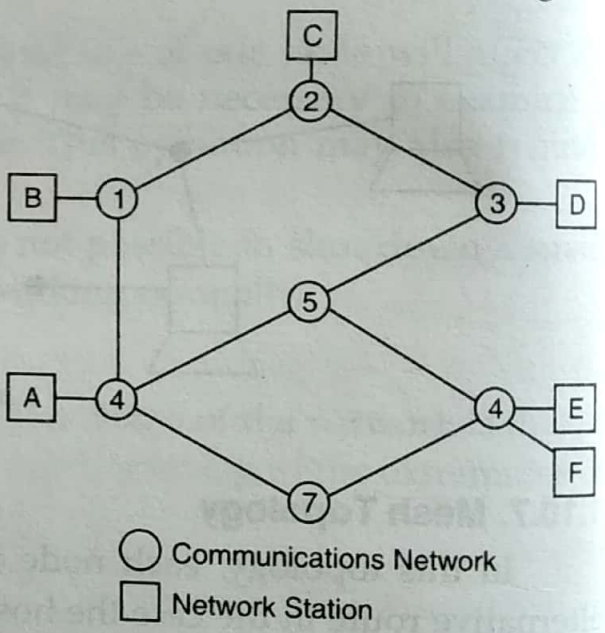


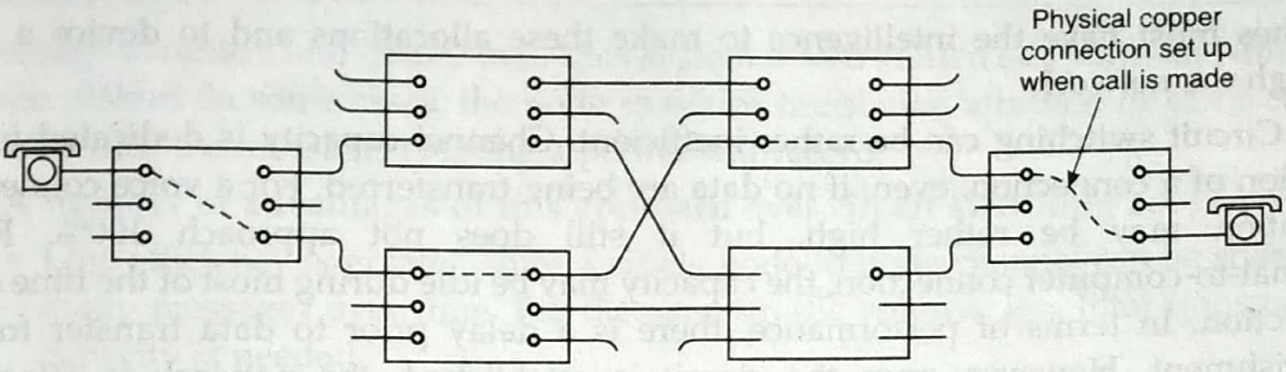
Fig 1.9. Generic Switching Network

Three switching techniques are in common use :

- Circuit switching
- Message switching
- Packet switching

Circuit Switching

Communication via circuit switching implies that there is a dedicated communications path between two stations. That path is connected sequence of links



(a)

Fig 1.10 Circuit Switching.

between nodes. On each physical link, a channel is dedicated to the connection. The most common example of circuit switching is the telephone network. Figure 1.10 illustrates the concept of circuit switching.

Communication via circuit switching involves three phases, which can be explained with reference to Figure 1.9.

1. Circuit Established : Before any data can be transmitted, an end-to-end (station-to-station) circuit must be established. For example, station A sends a request to node 4 requesting a connection to station E. Typically, the circuit from A to 4 is a dedicated line, so that part of the connection already exists. Node 4 must find the next leg in a route leading to node 6. Based on routing information and measures of availability and perhaps cost, node 4 selects the circuit to node 5, allocates a free channel (using TDM or FDM) on that circuit and sends a message requesting connection to E. So far, a dedicated path has been established from A through 4 to 5. Since a number of stations may attach to 4, it must be able to establish internal paths multiple stations to multiple nodes. The remainder of the process proceeds similarly. Node 5 dedicates a channel to node 6 and internally ties that channel to the channel from node 4. Node 6 completes the connection to E. In completing the connection, a test is made to determine if E is busy or is prepared to accept the connection.

2. Data Transfer : Signals can now be transmitted from A through the network to E. The data may be digital (*e.g.* terminal to host) or analog (*e.g.*, voice). The signaling and transmission may each be either digital or analog. In any case, the path is : A-4 circuit, internal switching through 4, 4-5 channel internal switching through 5, 5-6 channel, internal switching through 6, 6-E circuit. Generally, the connection is full duplex, and data may be transmitted in both directions.

3. Circuit Disconnect : After some period of data transfer, the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to 4, 5 and 6 to deallocate the dedicated resources.

Note that the connection path is established before data transmission begins. Thus channel capacity must be available are reserved between each pair of nodes in the path, and each node must have internal switching capacity to handle the connection. The

switches must have the intelligence to make these allocations and to device a route through the network.

Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even, if no data are being transferred. For a voice connection, utilisation may be rather high, but it still does not approach 100%. For a terminal-to-computer connection, the capacity may be idle during most of the time of the connection. In terms of performance, there is a delay prior to data transfer for call establishment. However, once the circuit is established, the network is effectively transparent to the users. Data are transmitted at a fixed data rate with no delay other than the propagation deley through the transmission links. The delay at each node is negligible.

Message Switching

Circuit switching is an appropriate and easily used technique in the case of data exchanges that involve a relatively continuous flow, such as voice (telephone) and some forms of sensor and telemetry input. However, circuit switching does have two drawbacks :

- Both stations must be available at the same time for the data exchange.
- Resources must be available and dedicated through the network between the two stations, with the inefficiency mentioned above.

An alternative approach, which is generally appropriate to digital data exchange, is to exchange logical units of data, called **messages.** Examples, messages are telegrams, electronic mail, computer files, and transaction queries and responses. If one thinks of data exchange as a sequence of messages being transmitted in both direction between stations, then a very different approach, known as message switching, can be used.

With message switching, it is not necessary to establish a dedicated path between two stations. Rather, if a station wishes to send a message (a logical unit of information), it appends a destination address to the message. The message is then passed through the network from node to node. At each node, the entire message is received, stored briefly, and then transmitted to the next node.

In a circuit-switching network, each node is an electronic or perhaps electro-mechanical switching device which transmits bits as fast as if receives them. A message-switching node is typically a general-purpose minicomputer, with sufficient storage to buffer messages as they come. A message is delayed at each node for the time required to receive all bits of the message plus a queuing delay waiting for an opportunity to retransmit to the next node.

Again using Figure 1.9, consider a message from A to E. A appends E's address to the message and sends it to node 4. Node 4 stores the message and determines the next leg of the route (say to 5). Then node 4 queues the message for transmission over the 4-5 link. When the link is available, the message is transmitted to node 5, which will forward

the message to node 6 and finally to E. This system is also known as a **store-and-forward** message system. In some cases, the node to which the station attaches, or some central node, also files the message, creating a permanent record.

A number of advantages of this approach over circuit switching are :

- Line efficiency is greater, since a single node-to-node channel can be shared by many messages over time. For the same traffic volume, less total transmission capacity is needed.
- Simultaneous availability of sender and receiver is not required. The network can store the message pending the availability of the receiver.
- When traffic becomes heavy on a circuit-switched network, some calls are blocked. On a message-switched network, messages are still accepted, but delivery delay increases.
- A message-switching system can send one message to many destinations. This facility is not easily provided by a circuit-switched network.
- Message priorities can be established.
- Error control and recovery procedure on a message basis can be built into the network.
- A message-switching network can carry out speed and code conversion. Two stations of different data rates can be connected since each connects to its node at its proper data rate. The message-switching network can also easily convert format (*e.g.* from ASCII to EBCDIC). These features are less often found in a circuit-switched system.
- Messages sent to inoperative terminals may be intercepted and either stored or rerouted to other terminals.

The primary disadvantage of message switching is that it is not suited to real-time or interactive traffic. The delay through the network is relatively long and has relatively high variance. Thus it cannot be used for voice connections. Nor is it suited to interactive terminal-host connections.

Packet Switching

Packet switching represents an attempt to combine the advantages of message and circuit switching while minimizing objection is met. Figure 1.10(b) illustrates the concept of packet switching.

Packet switching is very much like message switching. The principle external difference is that the length of the units of data that may be transmitted is limited in a packet-switched network. A typical maximum length is 1000 to a few thousand bits. Message switching systems accommodate far larger messages. From a station's point of view, then, messages above the maximum length must be divided into smaller units and send out one at a time. To distinguish the two techniques, the data units in the latter system are referred to as packets.

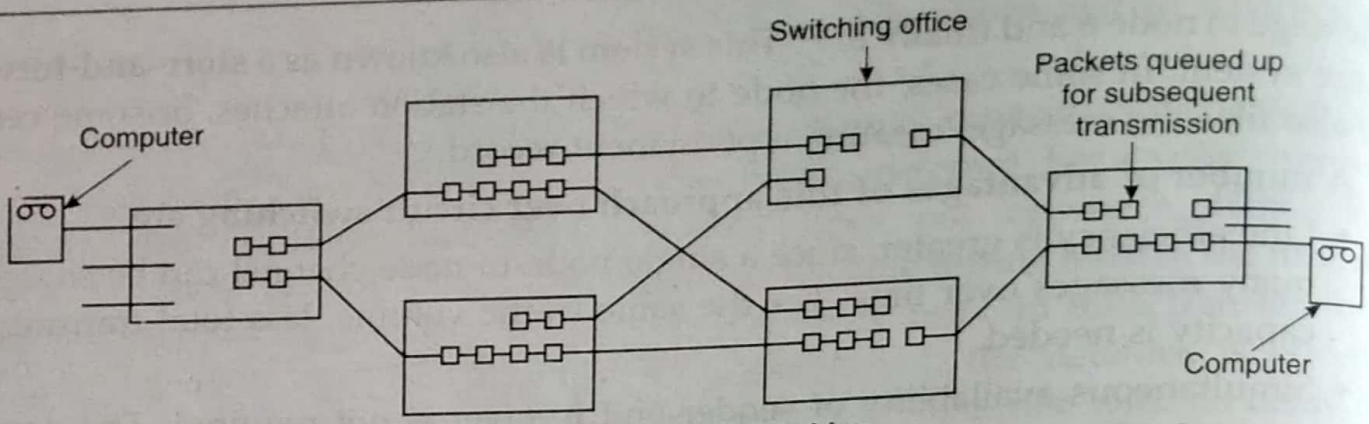


Fig 1.10 (b) Packet switching

Again using Figure 1.9 for an example, consider the transfer of a single packet. The packet contains data plus a destination address. Station A transmits the packet to 4, which stores it briefly and then passes it to 5, which passes it to 6, and on to E. One difference from message switching is that packets are typically not filed. A copy may be temporarily stored for error recovery purposes, but that is all.

On its face, packet switching may seem a strange procedure to adopt, with no particular advantage over message switching. Remarkably, the simple expedient of limiting the maximum size of a data unit to a rather small length has a dramatic effect on performance. Before demonstrating this, we define two common procedures for handling entire messages over a packet-switched network.

The problem is this. A station has a message to send that is of length greater than the maximum packet size. It breaks the massage into packet and sends these packets to its node. Questions : How will the network handle this stream of packets ? There are two approaches; datagram and virtual circuit.

In the **datagram** approach, each packet is treated independently, just as each message is treated independently in a message-switched network. Let us consider the implications of this approach. Suppose that station A has a 3-packet message to send to E. It pops the packets out, 1-2-3, to node 4. On each packet, node 4 must make a routing decision. Packet 1 comes in and node 4 determines that its queue of packets for node 5 is shorted then for node 7, so it queues the packet for node 5. Ditto for packet 2. But for packet 3, node 4 finds that its queue for node 7 is shortest and so queues packet for node 3 for that node. So the packets, each with the same destination address, do not all follow the same flute. Furthermore, it is just possible that packet 3 will beat packet 2 to node 6. Thus it is possible that the packets will be delivered to E in a different sequence from the one in which they were sent. It is up to E to figure out how to recorded them. In this technique each packet, treated independently, is referred to as a "datagram".

In the **virtual circuit** approach, a logical connection is established before any packets are sent. For example, suppose that A has one or more messages to send to E. It first sends a Call Request packet to 4, requesting a connecting to E. Node 4 decides to route the request and all subsequent data to 5, which decides to route the request and all subsequent data to 6, which finally delivers the Call Request packet to E. If E. is prepared

to accept the connection, it sends out a Call Accept Packet to 6. This packet is passed back through nodes 5 and 4 to A. Stations A and E may now exchange data over the logical connection or virtual circuit that has been established. Each packet now contains a virtual circuit identifier as well data. Each node on the preestablished route knows where to direct such packets; no routing decisions are required. Thus every data packet from A traverses nodes 4, 5 and 6; every data packet from E traverses nodes 6, 5 and 4. Eventually, one of the stations terminates the connection with a Clear Request packet. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

So the main characteristics of the virtual circuit technique is that a route between stations is set up prior to data transfer. Note that this does not mean that there is a dedicated path, as in circuit switching. A packet is still buffered at each node, and queued for output over a line. The difference from the datagram approach is that the node need not make a routing decision for each packet. It is made only once for each connection.

If two stations wish to exchange data over an extended period of time, there are certain advantages to virtual circuits. They all have to do with relieving the stations of unnecessary communications processing functions. A virtual circuit facility may provide a number of services, including sequencing, error control and flow control. We emphasise the word "may" because not all virtual circuit facilities will provide all these services completely reliably. With that proviso, we define terms. Sequencing refers to the fact that, since all packets follow the same route, they arrive in the original order. Error control is a service that assures not only that packets arrive in proper sequence, but all packets arrive correctly. For example, if a packet in a sequence fails to arrive at node 6 or arrives with an error, it can request a retransmission of that packet from node 4. Finally, flow control is a technique for assuring that a sender does not overwhelm a receiver with data. For example, if station E is buffering data from A and perceives that it is about to run out of buffer space, it can request, via the virtual circuit facility, that A suspend transmission until further notice.

One advantage of the datagram approach is that call setup phase is avoided. Thus if a station wishes to send only one or a few packets, datagram delivery will be quicker. Another advantage of the datagram service is that, because it is more primitive, it is more flexible. A good example of this is the use of the datagram approach of internetworking. A third advantage is that datagram delivery is inherently more reliable. If a node fails, all virtual circuits that pass through that node are lost. With datagram delivery, if a node is lost, packets may find alternate routes.

We now return to the questions or performance, illustrating the techniques discussed in Figure 1.11. This figure intends to suggest the relative performance of the techniques; however, actual performance depends on a host of factors, including :

- Number of stations
- Number and arrangement of nodes

- Total load on system
- Length (in time and data) of typical exchange between two stations

And more. Given the difficulty of comparing these methods, we hazard a few observations.

- For interactive traffic, message switching is not appropriate.
- For light and or intermittent loads, circuit switching is the most cost effective, since the public telephone system can be used, via dial-up lines.
- For very heavy and sustained loads between two stations, a leased circuit-switched line is the most cost effective.
- Packet switching is to be preferred when there is a collection of devices that must exchange a moderate to heavy amount of data; line utilization is most efficient with this technique.
- Datagram packet switching is good short messages and for flexibility.
- Virtual circuit packet switching is good for long exchanges and for relieving stations of processing border.

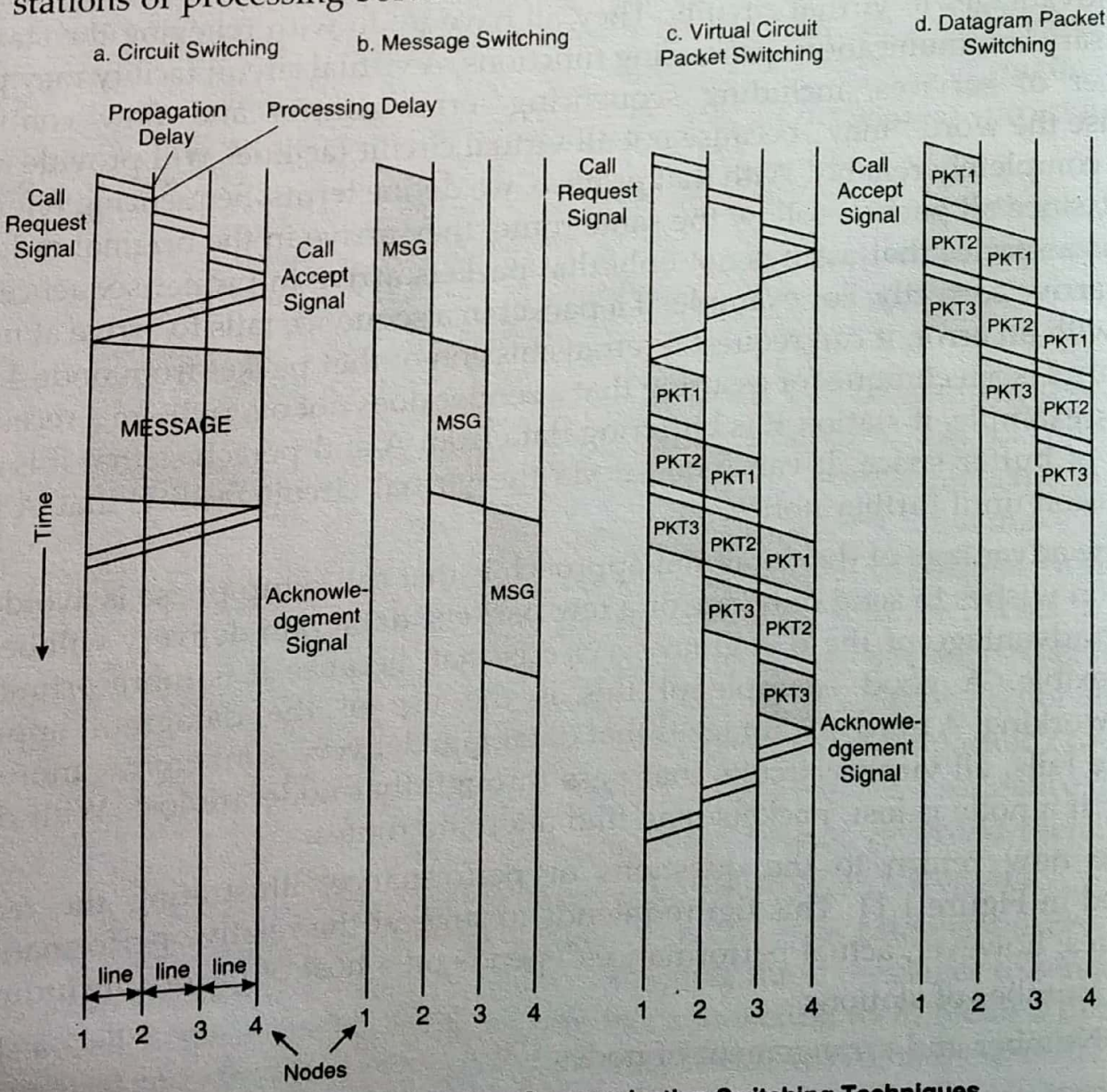


Fig 1.11 Event Timing for various Communication Switching Techniques

Table : Comparison of Switching Techniques

Circuit Switching	Message Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of messages	Transmission of packets	Transmission of packets
Fast enough for interactive	Too slow for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Messages are filed for later retrieval	Packets may be stored until delivered	Packets stored
Path is established for entire conversation	Route established for each message	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Message transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	No busy signal	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases message delay	Overload increase packet delay	Overload may block call setup; increases packet delay
Electro-mechanical or computerized switching nodes	Message switch center with filling facility	Small switching nodes	Small switching nodes
User responsible for message-loss protection	Network responsible for messages	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each message	Overhead bits in each packet	Overload bits in each packet

As a final point, we mention one common means of making packet-switched networks cost effective and that is to provide a public connection service. Examples of such networks in the United States are TELENET and TYMNET. The network consists of nodes owned by the network service provider and linked together by leased channels from common carriers such as AT&T. Subscribers pay fees for attaching to the network and for transmitting packets through it. Whereas individual subscribers may not have sufficient traffic to make a packet-switched network economically feasible, the total demand of all subscribers justifies the network. These networks are referred to as value-added networks (VANs) because they take a basic long-hand transmission service (*e.g.*, AT&T) and add value (the packet-switching logic). In some other countries, there is a single national-monopoly network, called a public data network (PDN). Circuit switching is a widely used switching technique for local network. The types of networks that use this technique are the digital switch and the digital private branch exchange (PBX).

Packet switching is also commonly used for local networking. In many cases, however, there is only a single, direct path from source to destination. Thus, often there is no routing or switching function in a local network. Packet rather than message switching is used, to facilitate techniques for preventing any source from monopolizing the medium.

EXERCISE

1. Define network.
2. What are the networking goals?
3. Why do we need to have networking?
4. Mention some advantages and disadvantages of having networks.
5. What are the key issues for computer network?
6. Define the following terms : Node, Server.
7. What are the characteristics used to classify different types of computer networks?
8. What are the two types of networking models? Explain.
9. List and explain different types of computer networks.
10. Differentiate between LAN and WAN.
11. What do you mean by network service? Explain any five.
12. Define topology. Mention some computer topologies.
13. Explain in brief star topology.
14. List and explain different types of switching techniques.
15. Compare different types of switching techniques.