UNIT 10

COMPUTER NETWORKS

Objectives

This unit will help you to understand :

* The hardware and software components of networks and the manner in which they function
* various kinds of network topologies
* standards established for multi- vendor networking
* applications of networks.

Structure

10.1 INTRODUCTION

The word 'computer' quite a few years back, conjured up images of very large grey metal boxes housed in air-conditioned glass rooms accessible only to those who had security clearances. These were once the exclusive domains of very large companies, universities and government offices. The advances in electronic technology have led to changes in the size as well as the cost of these machines. These changes have made it possible for even individual users to avail of this sophisticated technology. With the increase in the use of small computers distributed over a large network of individual users, the demand for interconnection in order to exchange information has dramatically increased. This is the basis behind the concept of 'net work'

What is Network ?

Throughout this unit we use term computer network to mean interconnection of autonomous (stand - alone) computers for information exchange. The connecting media could be a copper wire, optical fibre, micro - wave or satellite.

The physical location of a network could be a single or multi-storeyed building or a building complex covering an area as wide as the world itself.

The term, a 'local area network' (LAN) is used to describe a network covering an area ranging from a room to a small complex such as a university campus. The physical distance covered varies from 1 m. to 1 km. The term 'wide area network' (WAN) is used when the physical distance covered is more than 10 kms. WAN could be spread over a city, a district, or a country. It may also include the whole globe. Sometimes the term long haul network is also used to mean a wide area network.

Most of the time a network conjures up a picture of computer systems linked together to provide access to information. However, a network consists of much more than just computer systems. It includes transmission media such as cables, fibres, radio frequency equipment etc. It also includes devices which facilitate, maintain and control the flow of transmission of data between two or more computer systems. Example of such devices are modems, multiplexers and switching devices.

In particular LANs used in engineering environment consist of mainframes as well as engineering workstations. In a manufacturing environment they support a broad variety of applications including manufacturing, resource planning, real time process control, inventory control, maintenance management etc. Devices in this type of network include powerful mini-computers with monitoring and logic controllers. In this real time environment, errors as well as down time can cause unacceptable delays and cost overruns. Network performance and reliability are very critical.

The wide area networks consist of medium/large mainframes with a variety of peripheral devices. WAN also includes a variety of switching equipment and commuication software to facilitate easy access by users. In this environment user accesses the network through a variety of computer interfaces. The applications that can be performed on a network are unlimited.

10.2 DEFINITION OF A LOCAL AREA NETWORK

Local Area Network is a transmission system that allows a large number and variety of computing equipment to exchange information at high speeds, over limited distances. The computing equipment may range from large mainframe system to personal computers and peripherals.

Resource Sharing is perhaps the greatest advantage of local area networks. LAN allows a large number of intelligent devices to share resources, such as storage devices, program files and even data files. Whereas on a traditional network each machine will be directly wired into a switching device, on a LAN a single physical medium is usually shared.

Area Covered by the LANs are normally restricted to moderate size, such as an office building, a factory, or a campus. the limiting factors are usually the overall length of the cable used and any interdevice restrictions imposed. In practice, the distances involved range from a few meters to a few kilometers.

Low Cost per Connection is also an important characteristic of LANs. Many applications for LANs involve low-cost microprocessor systems, so that the connection of these systems to a LAN should also be inexpensive.

Loacal Area Networks are becoming more cost - effective as technology expands and new items, like fan-out units and networks interface units, become prevalent.

High Channel Speed is another quality of LANs. Most LANs transfer data at rates between 1-10 million bits per second. This is equivalent to 200 pages of the book you are presently reading. This is especially beneficial for applications with high resolution, movable colour graphics and for bulk data transfer between mainframe computers.

Furthermore, flexibility in growth, low error rates, reliability of operation and simple maintenance are all distinguishing features of LANs. When we discuss networking, we generally consider two situations : one, where the systems interconnected are in the same building or campus and the other where the systems are spread all over the country. In addition to these, there are two other interconnections that are already in vogue. One of them is the "bus" that connects the subsystems within a computer system and the other where the existing telephone network is used for networking. All the four methods have their own "niche" in the world of networking. Let us look at Figure 10.1 We find that "Computer Bus Networks" are very fast but covers very small distances only. The "telephone exchange based networks" have very slow speed operation but cover distances of the order of 10-1000 meters. But when we come to wide area networking, the speed of operation is marginally higher compared to the telephone exchange network but distances covered are extremely large of the order of one thousand kilometers. Local Area Networks, deftly combine the high speed of operation and provide a geographic spread of 1-10 kilometers, which is in time with the requirements of today.

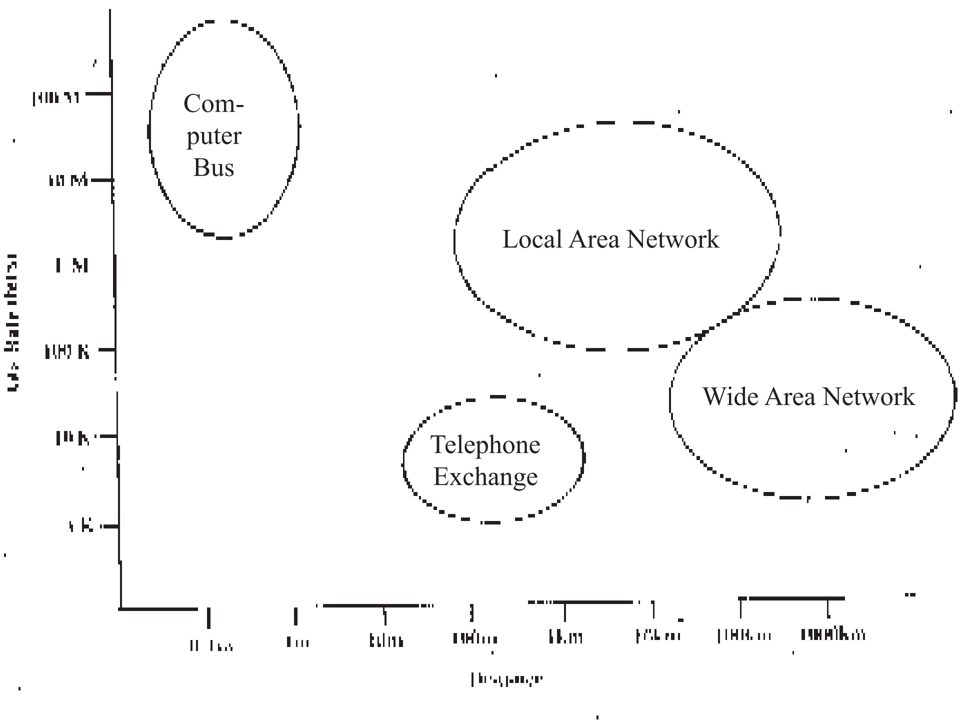


Fig. 10.1. LANs Relative controller network

The block schematic of a typical local area network is shown in Figure 10-2 . It consists of several workstations and servers. The workstations and servers. The workstations can be a personal computer or a workstation with multi-user and multi-tasking capability. A server on the network, as the name implies, provides a specific service for all workstations. The example shown in the figure are the File Server, Print Server, and Communication Server. They provide file storage and access facility, printing facility and external communication facility respectively to all the workstations connected to the local area network.

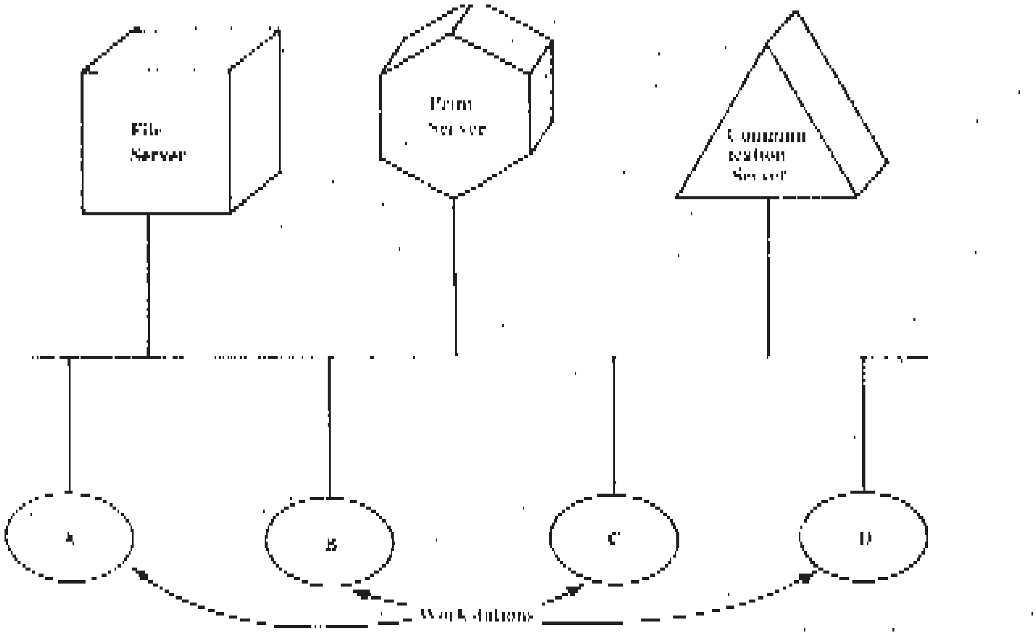


Fig. 10.2. A Typical Local Area Network.

10.3 CHARACTERISTICS OF LOCAL AREA NETWORKS

A LAN is best described by the following characteristics.

* LAN is wholly contained within a limited geographical area.
* LAN provides a high degree of interconnection between devices which are otherwise independent.
* LAN uses inexpensive transmission media and interface to devices.
* Every device has the potential to communicate with any other device on the LAN.
* LANs facilitate sharing of information and Hardware.

The contemporary LANs differ in the ways in which the above mentioned characteristics are actually implemented in practice. The LANs can be compared by considering the following factors:

* The type of cabling used.
* The Topology.
* Method used to control access to the shared medium.
* The nature of the interface unit which connects a device to the network.
* The rate at which digital data can be transmitted across the common shared line.
* The application services that are provided on the LAN.
* The facilities that are available to configure and manage the LAN.

Some examples of LAN are Ethernet, IEEE 802.3, Token Ring and Token Bus.

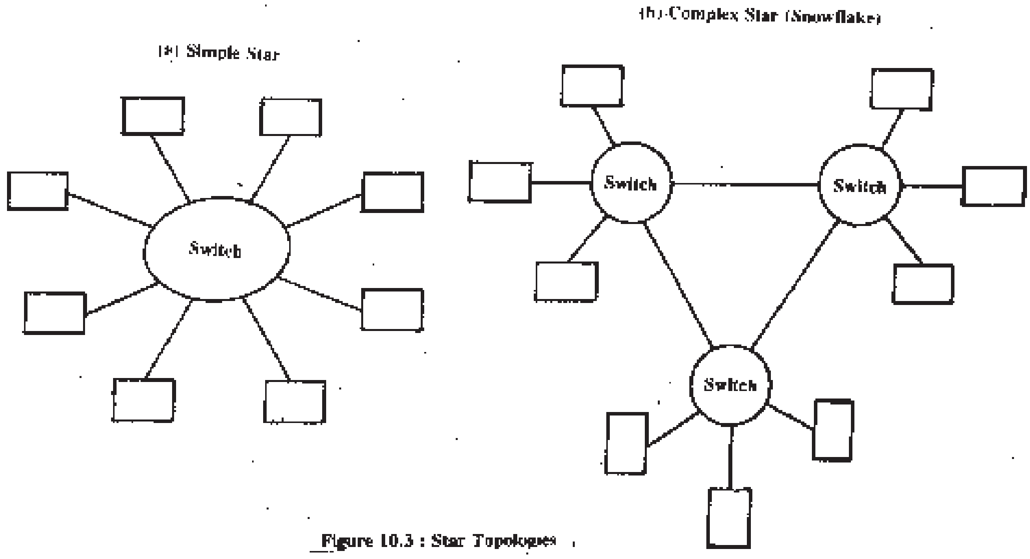


Figure 10.3 : Star Topologies

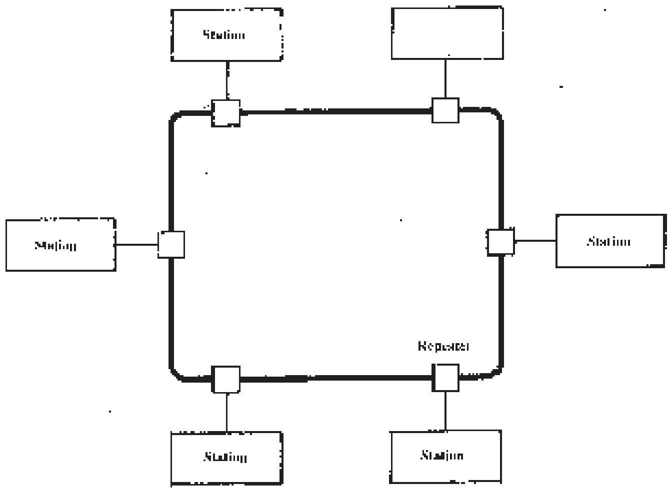


Figure 10.4 : Ring Topology

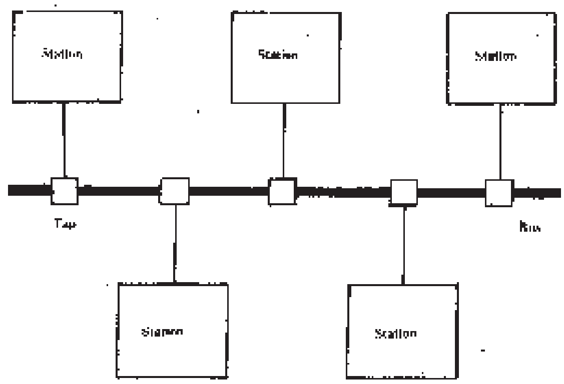


Figure 10.5 : Bus Topology

10.4 NETWORK TOPOLOGIES

Network topology is the basic outlay or design of a computer network. Think of topology as the architectural drawing of the network components, which is much like the architectural drawing of a home or building (some are simple, some are very complex). This design can be varied in accordance with the company's needs, but certain base elements to configure the topology of a network still apply. Any system on a network is called a node. Nodes are connected to each other by links. Links can be phone lines, private lines, satellite channels, etc. When you draw a road map of the communication links between nodes, you then have a network topolgy.

When we talk about links, we always refer to two basic types of links: physical and virtual. To give a very simple explanation.

If you can see and touch it, it is PHYSICAL

If you can see it but not touch it, it is VIRTUAL

Networks use virtual links to allow the sharing (multiplexing) of the physical line by multiple network programs or data transters. If a new physical line is to be installed for every new network program that was started up, it would be VERY expensive to provide communications capability to many locations. Therefore, virtual communications over physical lines are extremely valuable in providing cost-effective communication capabilities.

Depending on the processing needs of an organisation, different types of networks may be needed, sometimes even in the same organisation. There are several network models that describe most networks in existence today. Figure 10.6 describes these topologies.

Point-to-Point Topology

In pont-to-point topology nodes can communicate only with an adjacent node-one that is “next” to the system. It should be observed that just because two systems are not in the same room, that does not mean that they cannot be adjacent. In its basic form, a point-to-point network is two nodes directly connected. In its advanced forms, it could be 200 nodes connected to adjacent nodes and those nodes connected to other adjacent nodes, ad infinitum.

Multipoint or Multidrop Topology

A multipoint or multidrop network is one where nodes share lone line by sharing time on the line. Multipoint networks are very useful where high speed data transmission capabilities are NOT necessary and where cost of implementation is an important factor. Many manufacturing companies that use systems to automate their production, run their own wires throughout the production area. If the company had to run a separate set of wires to every machine, the cost could be prohibitively high. By using multipoint communications, however, the company can implement a functional network of prodution systems quickly and without major cost considerations Remember that multipoint does not lend itself well to high-speed data communications, nor where there is a great volume of communications. Also, the more the number of nodes on the trunk, the higher are the chances that some other node is communicating when the need to communicate arises. Thus, it will take longer to get the data to other systems.

Mesh Topology

Mesh networks are most commonly employed for long-distance transmission of data between nodes which act as message switches, circuit switches or packet switches. A fully connected mesh linking n nodes requires n(n-1)/2 links but it is unusual for all the possible connections to be provided. Throughout depends upon the media and the capacity of the switching nodes. Distance may be extended indefinitely and the number of stations may increase up to the limits imposed by the maximum throughput and the size of the address field in the message header. The multiple message paths’ reduce vulnerability to link or node failure if stable re-routing facilities are built into the nodes. Messages delay may be high because long-distance transmission media have relatively low data rates and the throughput limitations of the nodes may result in queuing for retransmission in store-and-forward nodes. The cost of a mesh network may be optimised by eliminating redundant link capacity.

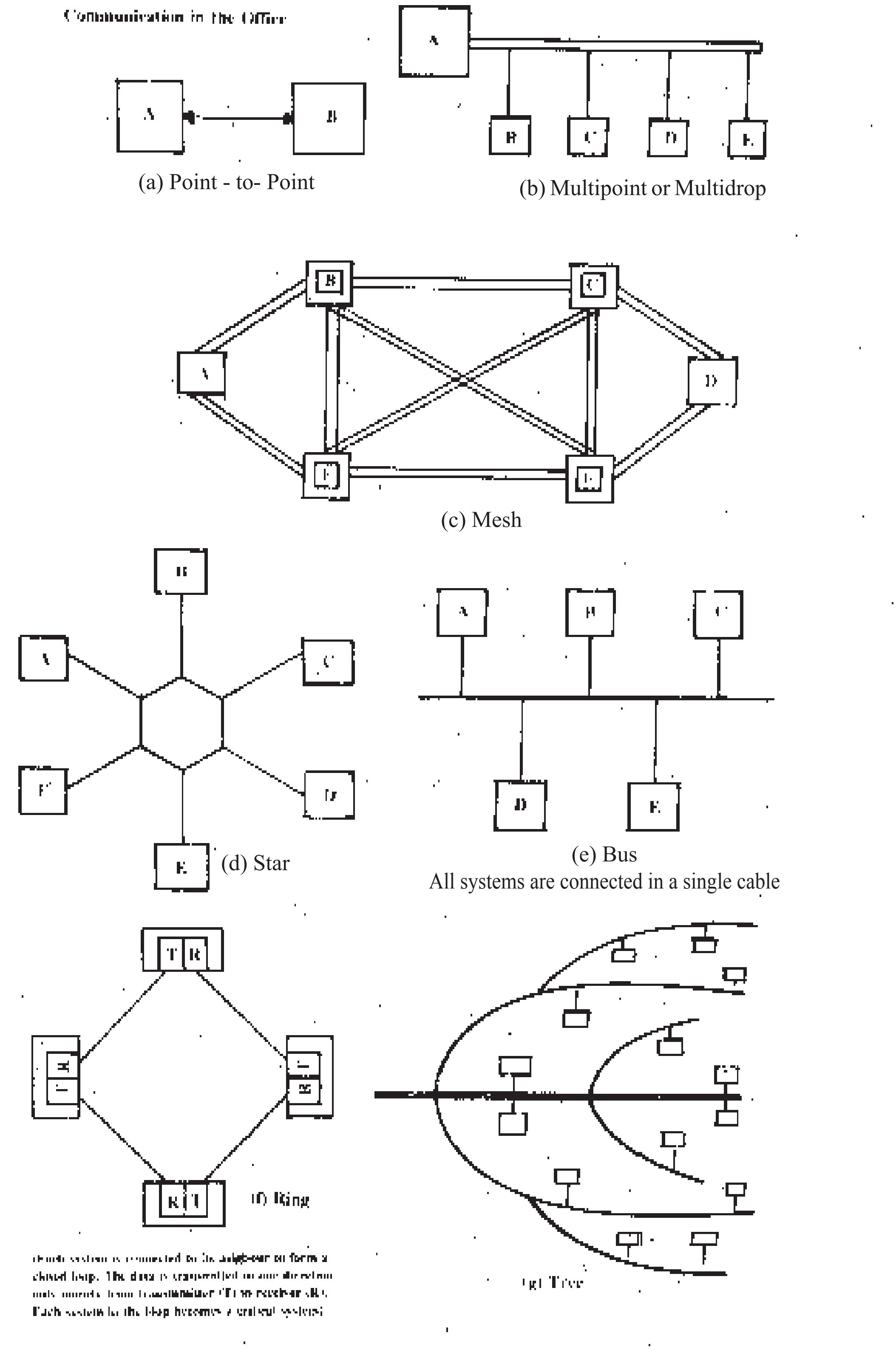


Fig. 10.6. Network Topologies

Star Topology

The star topology consists of a central node to which all other nodes are connected by individual dedicated parts. This topology is normally used in networks that use the electronic PABX. A familiar example of star topology is the distribution of terminals from a computer where a dedicated cable is laid for each terminal from the computer system.

In some cases, the building is wired in such a way that from a central node cables are drawn to wiring closets in each floor, From the wiring closets (the connection points), individual wires are taken to individual nodes. The star topology generally implies that there is central intelligence availble for controlling the operation of all the nodes.

Star networks are most commonly employed to connect remote and local terminals to mainframe computers and in private branch exchanges (PABXs). The throughput of computer-based star networks is constrained by the rate at which the central hub can accept messages and retransmit them if necessary. The distance covered by a star network is determined by the communication link. Each link must have the full length required to connect the hub to the station. The number of stations may be expanded only up to the limits of expansion permitted by the central hub. The central hub is a single point of failure which may cause the entire network to fail; single cable failures affect only single stations.Message delay may be high because of throughput limitations at the central hub which causes queuing. The initial cost of a star network is high because the central hub must be installed with a margin for expansion. Incremental cost for additional stations is low up to the expansion limits of the hub.

Bus Topology

Bus is the next popular topology for LANs. This consists of a single segment of a transmission medium (normally a coaxial cable of thick or thin variety) on to which various devices can be attached. This is analogous to the traditional CPU to the terminal connection in multidropped mode. The main advantage of this approach is the simple wiring and the ease with which the network can be extended to cover large distances. Also, the interface to the Bus is uniform. simple and can be repeated for any number or type of devices.

Bus networks are used extensively for baseband local area networks. multipoint terminal clusters and military data highways. The maximum length of the cable is often low because a high bandwidth is required to support many virtual channels. New stations may be added without reconfiguring the network until the throughput and message delay limits are reached. Message delay in token passing buses increases with the number of stations and in contention buses, delay increases with traffic volumes. Polled systems have a delay determined by the polling sequence. Cost per station is generally lower than star networks but higher than ring networks and buses do not involve a high initial investment.

Ring Topology

Another topology that is quite useful in the case of LANs is the Ring Topology. In this case, each node is connected only to the two neighbouring nodes. The medium is connected to the node by a repeater. Data is accepted from one of the neighbouring nodes and is transmitted to the immediate next node. The data travels in one direction only from node to node around the ring. Thus the opportunity to transmit data around the ring is passed on from node to node in a fixed order. It may so happen that some stations on the ring do not have anything to transmit and may transmit the opporturnity to use the ring to the neighbouring node in a transparent fashtion. The data in fact, circulates around the ring and comes back to the centre all the time.

The ring topology is almost exclusively used by local area networks which use token passing or slotted ring access control. Throughput is determined by the media and the capability of the repeater. The total length of the ring and the distance between nodes is limited but the total span is generally greater than that of a linear bus. The maximum number of nodes is limited by the system design. Each additional node involves system disruption and reduces performance. A ring is vulnerable to a single break in any link of node repeater. Message delay increases as more nodes are added to the ring and is greater compared to a lightly loaded bus with contention access control. The cost per node is generally lower than other topologies offering similar performance and the amount of cable required is generally less than for a star topology.

Tree Topology

Tree topology is another form of bus topology. Unlike the bus topology, the segments in a tree extend similar to the branches of a tree with the trunk as the root. Tree topology is normally implemented using a coaxial cable. The main difference between the bus and tree topology is that while the former uses baseband transmission techniques the latter uses the broadband techniques. The data transmitted by a node always goes through the trunk on headend before reaching the destination.

Tree network may be formed from a number of linked linear buses but are most commonly employed by broadband local area networks which have as branching tree topology converging at a headend. Throughput of broadband tree systems is high and limited only by the bandwidth of the cable. The maximum distance covered is greater than linear buses because many branches may be linked using repeaters. Broadband systems may span several kilometers and have extremely large number of stations added without reconfiguring the network. The single point of vulnerability in a broadband tree is the headend equipment which is commonly duplicated. Cable or repeater failure elsewhere in the tree removes all station in the branches beyond the point of failure. Message delay in a broadband system is low when independent channels are provided by frequency division multiplexing. Cost is generally similar to that of linear bus systems.

Activity A

List the various topology alternatives available for designing a computer network.

....

....

....

....

....

10.5 NETWORK STRUCTURES

Networks can be classified into switching and non-switching.

A switching network has three components. These are the computer systems' (Host), transmission media and the switching nodes (Figure 10.7).

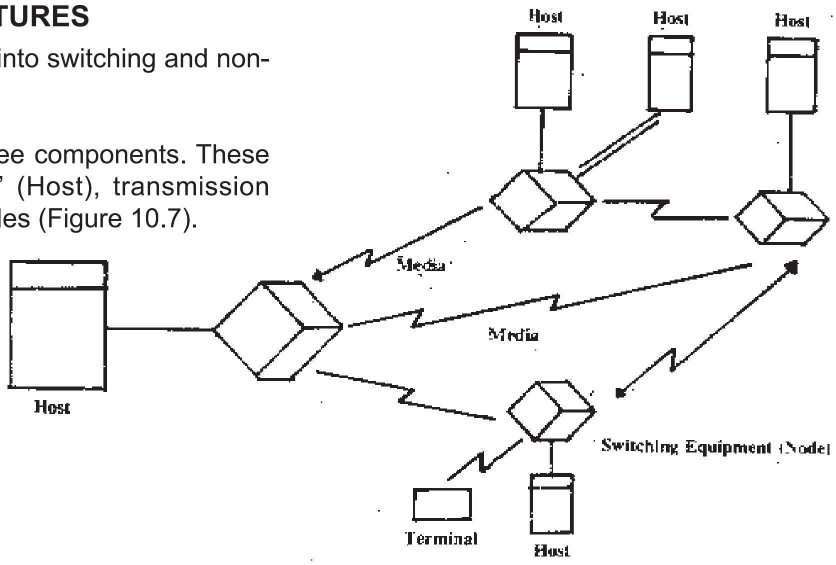


Figure 10.7 : A Switching Network

The computer systems are mainly used for processing and storing information. The transmission media are used to transport information beetween these computer systems. The switching nodes are specialised computers which are connected via the transmission media to hosts.

In the early stages of networks, Host computers were directly connected to each other via the transmission lines and were responsible for performing both the switching and processing functions. But with the growth of network usage valuable host resources were used for the switching functions. To improve response times, specialised computers have been evolved to perform the switching functions. These functions mainly involve setting up a link between two hosts, and monitoring it, and disconnecting it when no longer needed.

Before proceeding further consider the following analogy.

Let us take the telephone network at Delhi . It has several exchanges. Each telephone is connected to its local exchange. Any individual who wishes to make a call has to connect via one or more of the exchange till the local telephone of the called party is reached.

In our analogy there are three important components namely telephone sets, exchanges, and lines connecting exchanges. Here the telephone sets relate to the computer systems, the roads related to the transmission media and the exchanges play the role of switching nodes. The computer network handles calls from computers to transter data to each other, just as the telephone network allows people to send voice signals to each other systems.

10. 6 CONNECTIVITY THROUGH SWITCHED NETWORKS

Switching systems are connected to each other through point-to-point media. The media could be leased telephone lines. radio or satellite circuits.

In our analogy, if there are six localities and if each of these localities are to be connected directly with each other then we would require 15 roads (Figure 10.8). However if the traveller does not have any distance limitation or time limitation then the number of roads could be reduced considerably to as low as five roads. We can also have the scenario where each locality is connected through one or more interactions (Figure 10.8).

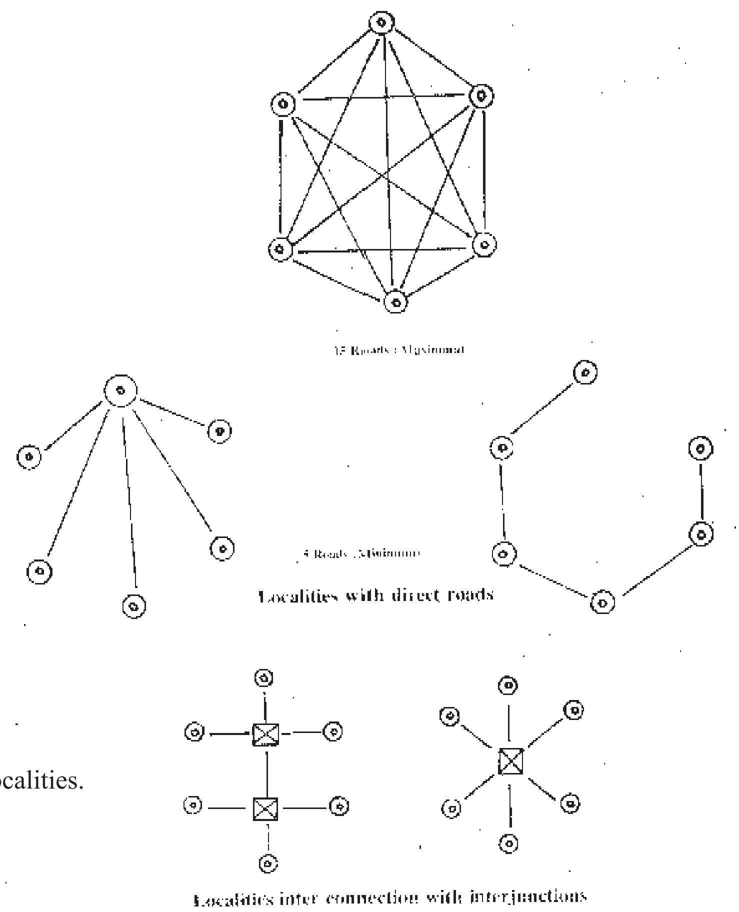


Fig. 10.8. Interconnection of localities.

If we assume in our network, N hosts then the maximum number of lines that would be required to have complete connectivity would be N (N-1)/2. The minimum number would be (N-1). Depending upon the applications and the requirements the number of point-to-point lines varies. There are a number of possible topologies which depict these. Some of these are shown in figure 10.9

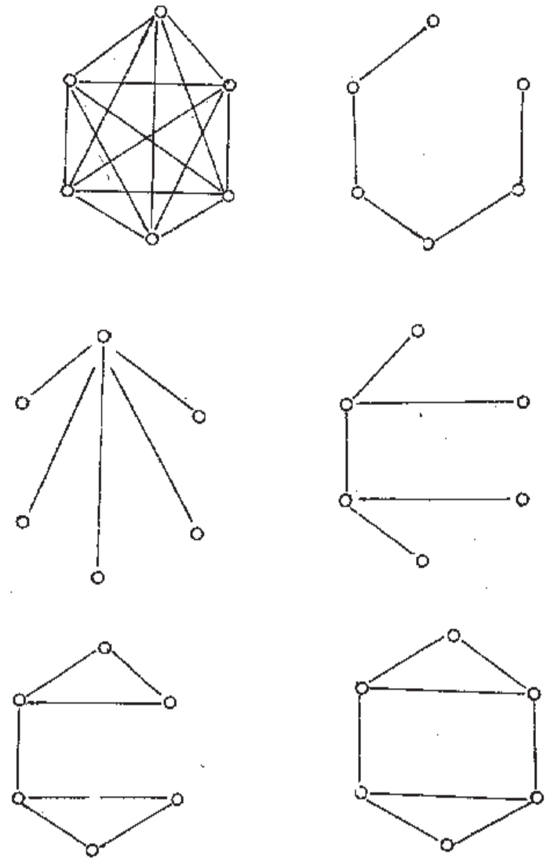


Fig. 10.9. Some Possible 6-Node Topologies

The switching mainly provides economical and flexible type of interconnection arrangements that would allow temporary connection between any two hosts . This methodology eliminates the need for direct connections between all hosts in a network.

The basic functions of switching systems are: the identification of a communication path between two hosts; the establishment and release of various connections; and monitoring the performance of the network equipment.

10.7 TYPES OF SWITCHING

There are two types of switching networks, Circuit (line) switching networks and store forward switching networks.

10.7.1 Circuit Switching

Circuit switching works in real time. The connection is established between two hosts and messages can be directly sent to each other. In circuit switching the physical path established remains connected till the end of the session. No other host can use the circuit. It may take a few seconds to establish the circuit but only a few milliseconds for the data to reach the destination. At any one time only the two communicating hosts can transmit information to each other. Result--slow speed. A simple analogy is the pre-setting of a route of railway tracks for a particular train. When the train has to change from mainline to sideline or any other line, the railwaymen change the track by physically (mechanically) operating a lever. It takes time to switch the track and is usually done in advance.

Circuit switch networks provide a connection pipe through which data pours without being stored any where within the network. The store and forward technique is fundamentally diifferent when it comes to providing a connection between two hosts. The public switched telephone network and telex networks are examples of circuit switching.

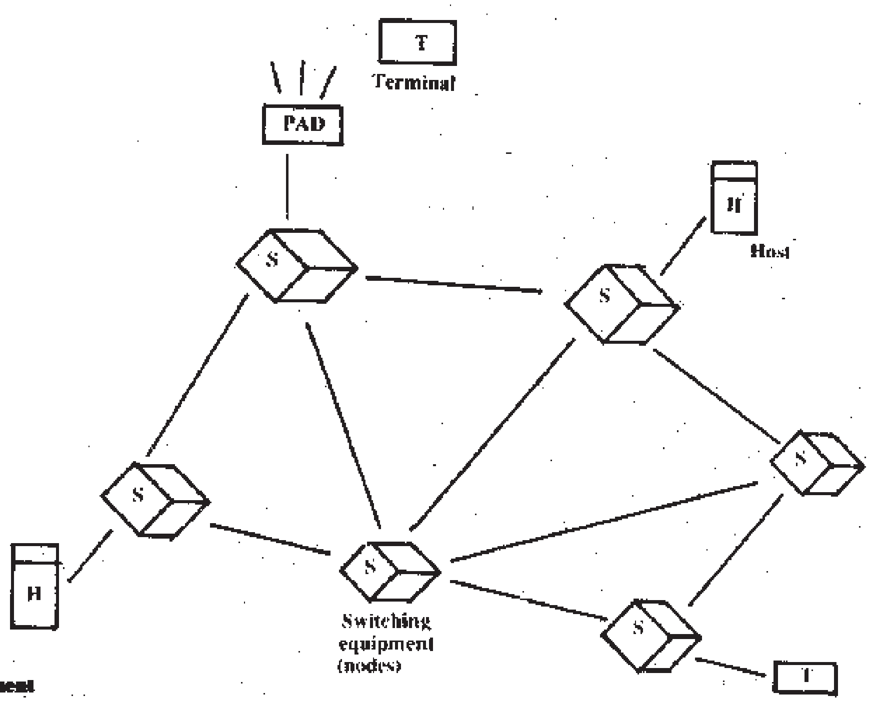
10.7.2 Store and Forward Communication Switching

In store and forward communication switching, the switching nodes store the incoming messages and route the message to the next switch as per the address on the message. The user would not usually know what physical path the message took to reach its destination. Store and forward switching can give better line utilization compared to circuit switching. As the data transmission is bursty in nature with long periods of silence between bursts. Storing the message of many different hosts allows them to be forwarded at a steady rate without the bursts and the idle periods associated with a single host-to-host transfer. Even though the cost of a store forward network may be higher than a circuit switched one, greater sharing of cost may be achieved.

There are two types of store and forward switching - message switching and packet switching.

Packet Switching

Packet switching is special case of message switching. In these switchings, circuits remain permanently connected and the data are received at the switching nodes and are routed onward to the requisite destination. The data (message) contain the address of the destination and the network takes care of delivering it. It gives better line utilisation. These switching methods are better suited to the handing of a large volume of data traffic on complex networks. The interesting feature of this type of switching is the ability to make use of the same



KEY

H Host

T Terminal

S Switching equipment (Node)

PAD Packet Assembly deassembly equipment

(Remark : Each switching equipment is a node with multiple paths)

Figure 10.10 : A Packet Switching Network with a PAD

circuit by several hosts via the switching equipnent. The packets are routed dynamically. It is possible that two packets of a message may take different paths to reach the same destination.

Most of the todays major networks use packet switching techniques. In the packet switching networks, the data is broken into small packets. These packets are routed independently through the network to its destination. The packets contain the address and other information. Because of this the terminals conneted to the network should have the intelligence to identify the packet. It should also have the capability to re-assemble the individual packets into their original messages. Less capable computers are attached to the packet switching network through an intermediary device that implements a packet assembly and de-assembly (PAD) function. High speed communication links are normally used to interconnect the packet switching equipment. The network is usally designed so that if one of the lines fails, there is always an alternative path to the destination. **The packet switching equipment form the nodes of a multipath network (Figrue 10.10). The packet switching equipment determines the route for each packet which is quickly passed from one node to another. The packets are stored long enough to get acknowledgement of correct delivery from the next node on the route.**

Message Switching

Store-and-forward techniques are used at switching exchanges to receive and acknowledge messages from the originator, then to store these messages until appropriate circuits are available to forward the message to its destinations. Private and military teleprinter networks commonly employ message switching.

Classical and forward switching relays the entire message through the network while storing the message in full at each relay point. This concept permits code, speed, or format conversions to take place during the in-switch processing, and appears essentially non-blocking to the subscribers. Powerful processing, with large storage capacities are required at each node of the data network. There is a very large variance in delivery delay, especially for messages which find themselevs in queue behind a very long one, leading to poor responsiveness for interactive traffic.

10.8 COMPARISON OF THE SWITCHING TECHNIQUES

Figure 10.11 presents a comparison of the switching techniques. The message delay varies according to the switching technique employed. Circuit switching imposes the minimum dealy on the transmission once the call has been set up but the setting up time may be lengthy and it is possible that an inadequate number of circuit stages are available when required. When channels are not fully utilised, circuit switching is less efficient than the other techniques in utilising trunk capacity. No addressing data is required in messages sent by circuit switched networks which simplifies the protocol.

Message switching may introduce a long delay because the message is stored at the exchange until suitable circuits are available to transmit the message to the next stage in the transmission path. Each store and forward stage must wait until it has received the complete message which is then relayed to the next stage.

Packet switched systems reduce the long delays inherent in message switching exchanges. Message delays are lower in packet switched systems and the trunk capacity utilisation is greater than that of circuit switched systems but the interface equipment is more complex.

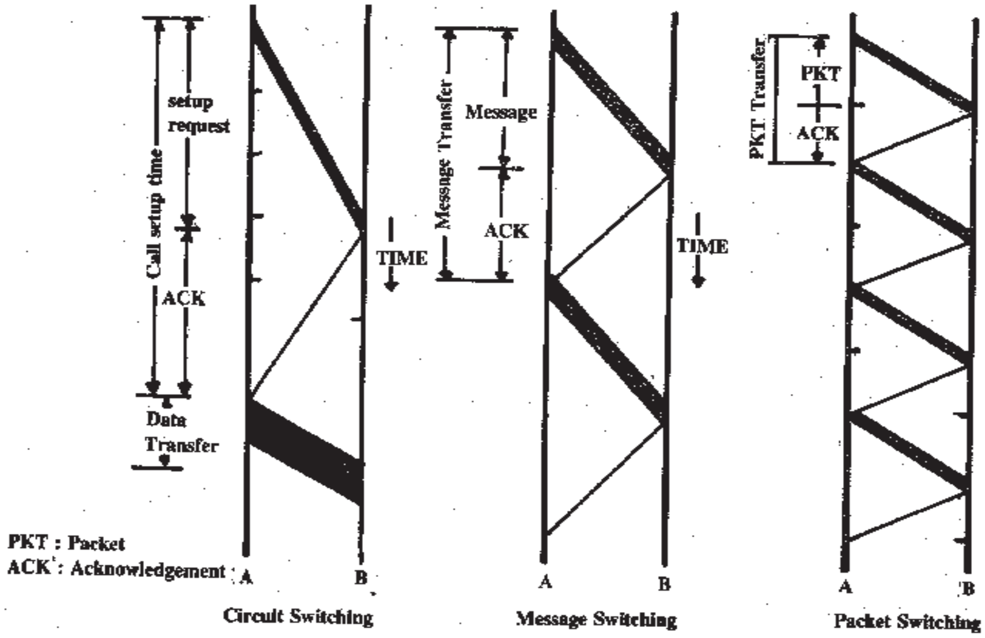


Figure 10.11 : Comparison of Switching Techniques.

Activity B

List the three impotant Switching Techniques for networks.

....

....

....

....

....

....

Non-Switched Networks

These networks do not use switches to connect host computers to each other. All hosts are physically connected to each other, although they may have to share a common physical media. Non-Switched Networks use two kinds of connections as building blocks: point-to-point and multipoint (multidrop). By multipoint we mean a connection with several drop points. On multipoint connections, only one host can transmit at any one time. Each receiver must have an address and must have the ability to recognise that a message is being sent to his address. Multipoint configuration also has the capability to make use of multicast (group) or broadcast addresses, in which more than one can receive the data. In multicast (group) the data is transmitted containing the address of a preselected subgroup of receivers and hence only this sub-group receives the data. In broadcast transmission the data is transmitted with a universal address, which is recognised by all.

When hosts share a common communication path it becomes essential to control the right to start data transmission over the path line. It is important to devise procedures and control that will allow allocation of the limited (line) capacity to many hosts. There are two basic approaches -contention and central control and contention

In the central control system, central computer controls all messages transmission to and for from all terminals (computers.)

In the central system, individual hosts are restrained from transmission without the clearance from the central system. Variety of procedures are followed to exercise this control. One such procedure is “polling”in which the central computer sends a ‘go-ahead’ to the code of each of the other computers in turn. The “polling” methods are used for efficient use of the communication. Another scheme is to allocate fixed time slots media so that all the users have an opportunity to transmit data.

In the contention schemes any terminal is free to transmit at any time. Whoever first seizes the communication media, gets the chance to transmit to others again after a randomised interval.

Sometimes “contention” leads to nobody at all being able to use the line, especially when several stations have heavy transmission demands. Certain arbitration techniques are used to reduce the occurrence of these deadlocks. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is one such arbitration technique or “protocal”.

10.9 MULTI-VENDOR NETWORK

The problem of interlinking different vendor machines is more complex than interlinking the machines of the same vendors. Interlinking a multi-vendor computer systems was initiated way back in late’60s. The first approach of this was, ARPANET, developed by the Department of Defence Advance Research Project agency (DARP) to meet its large number of users requirement. This network allowed its users to transfer files, emulate terminals and perform certain important network functions on the equipment that complies with the protocol. A similar effort was also made by the University of California to design certain software to facilitate multi-vendor network. The protocols were similar to the ARPANET.

These two protocols were widely used for interlinking multi-vendor systems for quite sometimes. In fact, they became de facto standards in the early phase of multi-vendor networking.

In the early’ 70s the American National Standard Institute (ANSI) developed a distributed systems reference model. Based on the model, International Standards Organisation (ISO)had come up with Open Systems Interconnection (OSI) reference model in the late’ 70s.

10.10 OSI REFERENCE MODEL

International Standards Organisation had published the OSI reference model in 1983. It is a seven layer model that provides a structure for data transfer among different vendor machines through the network (Figure 10.12). It defines the functions that had to be performed by each layer of this reference model. The layers have been organised to reduce complexity and bring clarity. Attempt has also been made so that internationally standardised protocols can be defined.

The layers 1 to 4 of the model define how to establish connection between computers, enabling data in any format to move from its source to its destination. The standardised function of these layers ensures that the transmitted data are received as send. If errors occur, that error is reported and diagnosed. The layers 5 to 7 address the interconnection of computer applications. This standardization of functions of these layers makes it possible for the application to translate data into meaningful information (Figure 10.13)

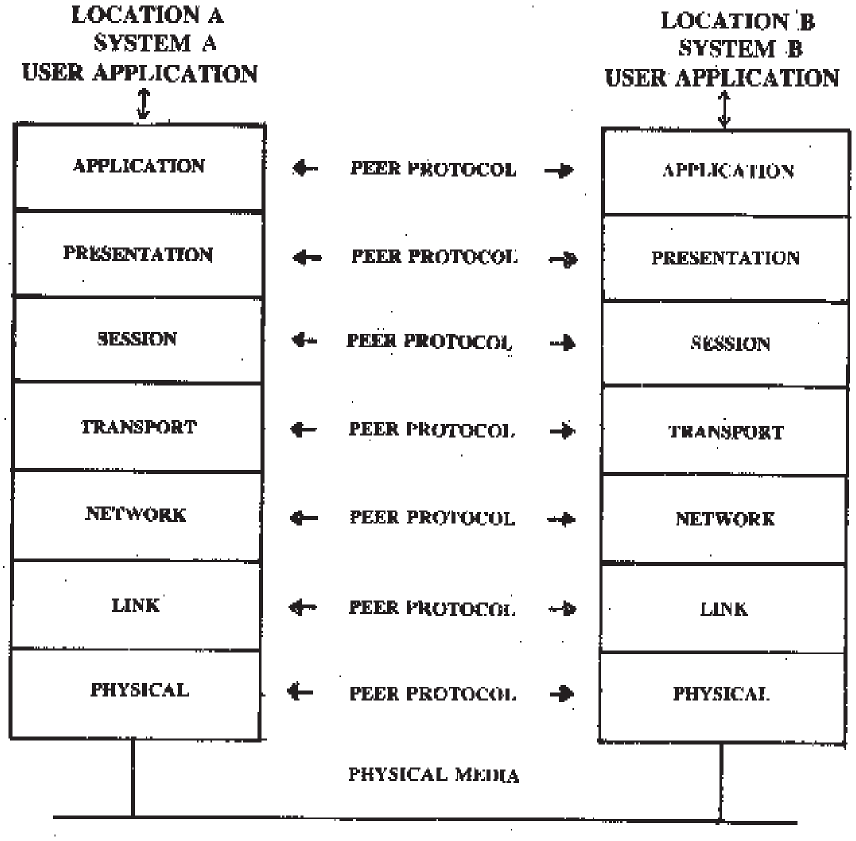


Fig. 10.12. ISO Layers

PHYSICAL LAYER: This layer is responsible for transmitting digital signals from the transmitting node to other nodes. The specifications of the physical laytер is concerned with the signal layers, polarities, duration, mechanical attachments, cable lengths etc.

DATA LINK: This layer is responsible for managing access to the physical layer and for transforming data from the medium into a form usable by the network layer. It is responsible also for the integrity of the data. In addition to this it does the error recovery, flow control and multiplexing.

NETWORK LAYER: This layer determines the route to be taken by a packet travelling from the source to the destination. In very large networks where there exist multiple choice of paths it becomes extremely, important to decide the path to be taken based on the speed, reliability, cost, time etc.

TRANSPORT LAYER: This layer ensures reliable end to end transmission of data. The layers above the transport layers deal with data in larger units then do those below it. It is the responsibility of the transport layer to break up the outgoing data into smaller packets and then re-assemble packets in the correct order at the receiving end. It is the transport layer which makes request for retransmission .

SESSION LAYER: This layer provides services related to the entire task which may consist of smaller tasks and is responsible for complete transmission and restart if errors occur.

PRESENTATION: This layer provides services to the application layer particularly those dealing with the presentation of the data. In addition to encoding data this layer presentation may also be responsible for data encryption and compression.

APPLICATION: This layer is custom made to the user's requirements. It includes file transfer, electronic mail, directory services, messaging protocol, network managenent, virtual terminals etc.

The OSI reference model and standards are important steps in promoting multi-vendor networking.

The model consists of a framework telling what the layers are but does not itself specify the protocol to be used in each layer. The OSI has standardised certain protocol but other non-standard protocols also exist. However, in some layers multiple, incompatible standard protocols also exist. If two computers at each side use different protocols in any layer then they will not be able to communicate.

10.11 LAN STANDARDS

The lower layer of OSI have correspondence with LAN standards. The bottom two layers of the OSI model are specified as a three layer standard by Institution of Electrical and Electronics Engineers. The subcommittee of IEEE has made a series of recommendations called 802 series of recommendations. The 802.3 describes the medium access control technique to be adopted in the case of a Bus or Tree LAN. This is the CSMA\CD protocol. The 802.5 recommendation describes the operation of a token passing ring LAN. The 802.4 series of recommendation describes the-medium access control for a token between two stations of a LAN will be controlled. This is common to 802.3, 802.4 and 802.5 networks.

Figure 10.14 shows the correspondence between the ISO-OSI model for computer networks and the IEEE model for LANs. The OSI model is applicable to any

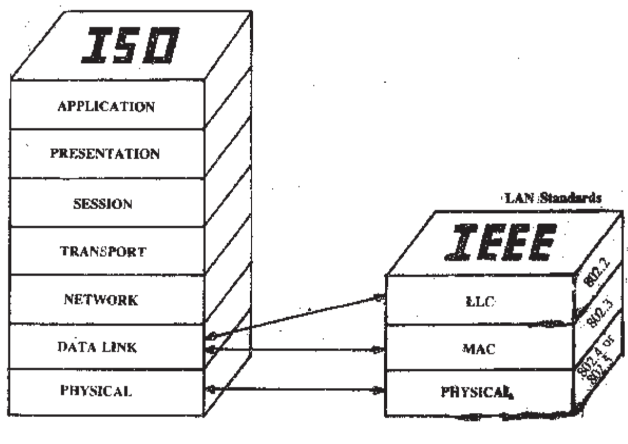


Figure 10.14 : ISO and IEEE Protocol Architecture

computer network, while the IEEE model is specially meant for LAN. Both the models specify the corresponding Protocol Architecture. The seven layers are Physical Layer, Data Link Layer, the Network Layer, Transport Layer, Session Layer, Presentation Layer and the Application Layer. In the case of IEEE Protocol Architecture, the layers are the Physical Layer, the Medium Access Control Layer and the Logical Link Control Layer.

10.12 IEEE 802.3 LAN AND CSMA/CD PROTOCOL

Similar efforts are also made to have certain standards for the LANs. The IEEE 802.3 committee specified the way that a local area network using the bus topology should construct its frames or packets of information and send them over the network to avoid collisions. The protocol is known as Carrier-Sense Multiple Access with Collision Detection (CSMA/CD). The CSMA portion of this protocol can be visualised by imagining a LAN node or station that wishes to send a message. The node listens to the bus to detect carrier signal from another node that is already sending a message. If no other signal is detected, the user sends its message.

There are problems with this seemingly tidy solution to control traffic on a LAN. What happens if two LAN nodes are located fairly far apart? It is possible for them to issue a carrier-sense signal, listen and hear nothing, and then send their messages only to have the data collide. To avoid this type of accident, the committee added Collision Detection (CD) to the CSMA approach. A node continues to listen as it transmits a message. If it detects a collision, then it transmits the message again.

There is still another problen with this approach. Let us look at an analogy. Imagine two drivers who arrive simultaneously at an intersection having four-way stop signs. Both drivers come to a complete stop, wait for a reasonable time, and then begin to move again only to have to slam on their brakes to avoid a collision. Embarrassed by the near collision, the two drivers pause before starting again. Unfortunately, they start again at the same time and once again narrowly avoid a collision.

To avoid this possibility, LAN designers have designed their CSMA/CD approach so that each workstation waits for a (different) random amount of time immediately after a data collision before transmitting the message again. Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) is a protocol for defining the way in which LAN will avoid data collisions. After a collision, a special signal called a **jam** signal is sent through the network. This signal ensures that all network stations, no matter how far apart, are aware that there has been a collision.

After repeated collisions, the network will double its random delays before permitting stations to transmit again. This approach doesn't totally eliminate collisions since it is still theoretically possible for two well separated workstations to wait different amounts of time and still transmit messages that collide. These accidents, however, are infrequent and thus manageable.

Despite the ingenuity of this approach to avoid collision, there is one additional consideration. A heavily used bus based LAN utilising CSMA/CD can begin to look like a highway during rush hour. Even though data is supposed to move at 10 million bits per second, the doubling and redoubling of the delay duration after a few collisions can reduce the LAN's throughput to as little as 1-3 million bits per second.

10.13 ACCESS METHODS AND TOPOLOGIES

The access methods associated with LANs depend on the topology used. For example, in the access method used in the ring networks, a token is constantly circulating from node to node. For any node, the reception of a token signifies the opportunity, to transmit data using the ring. Whenever a station receives a token, and if the station already has data to be sent, then the station makes use of the token and sends the data around the ring. The data is sent in the form of a collection of bytes called a 'packet'. The 'packet' carries information about the station from which the packet has originated and the station to which it is destined. The receiving station or the destination picks up the 'information' and sends an acknowledgement back to the sender. The data after travelling around the ring reaches back to the sender and the sender removes the data from the ring. The token is now handed over to the neighbouring node. What is described here is one particular (popular) approach to control the access to the ring. There are several variations of this scheme available for accessing a ring.

In the case of a Bus or Tree, the access to the medium is independently available to all the stations connected to the LAN. That means a station of LAN which uses Bus or Tree Topology can freely transmit and/or receive data simultaneously. This is true for all the stations that are connected on to the LAN. Therefore, very often 'Collision' will occur in such LAN. As the medium is shared by all the nodes, detection of collision and controlling the time of transmission are seen as the responsibility of the individual stations connected to the LAN. Here again, there are many variations available which control the transmission time or those which differ in the way in which collision is detected and a corrective action is taken.

In the case of Star topology, either a token passing scheme or a circuit switching sceme, can be used. When the token passing scheme is used, the centralised switch in the star is seen as a shared resource and the availability to a token has the same significance as that of a ring. When circuit switching is used, the situation is analogous to the exchange in a telephone network. A dedicated path is established between the source and the destination for the duration of transmission.

We have seen so far in this unit, the concepts relating to LANs, technologies and topologies relevant to LANs and so various access methods associated with the LANs. In the next section we will discuss the architectural issues relating to LANs. By LAN architecture we refer to the functional division of tasks from technology at one end to the user applications at the other end.

10.14 LAN ARCHITECTURE

In a LAN, both the hardware and the software have different components. In the hardware, there are stations specific and network specific subsystems which have to coexist. Supporting local requirements of the user and conforming to the network specifications are the tasks to be performed in order to coexist with other workstations on the LAN. This necessitates an unambiguous definition of the functional division of tasks from the technology to the application. The software has three specific components namely the **Application Software, Network System Software and Network Management Software.** The appliction software makes the facilities of the network available to the user in a friendly way. The network system software ensures that the stations have error free communication with each other. The network management software helps the network supervisor in maintaining, administering and operating the network.

The interaction between hardware and sofware can occur at different levels. Obviously, the work performed by hardware will be faster as compared to the same work carried out by an equivalent software. Many functions can be done directly in hardware if they are very well understood and standardised to a level that VLSI implementation of these functions are available.

10.15 NETWORK MANAGEMENT

Another important aspect that needs to be considered in the multi-vendor network involves the management aspect of this network. OSI made efforts to deveolop standards that satisfy services and protocol for the communication of network management information in a multi-vendor network. These standards enable users to manage entire multi-vendor network, including monitoring the network for traffic, performance and communication problems and controlling the network to correct faults and optimize performance. In 1988 a Network Management Forum under OSI was formed to evolve guidelines (Frame work) towords this. The OSI Management Framework addressed five areas of functional requirements for multi-vendor network management called specific management functional areas of SMFAs. These functional requirement must be met by the network management to be effective. Specific standards in the network management functions have been developed individually. However, these can be combined in different ways to achieve this specific result. The Framework also defined common functions required by two or more of these functional areas, called Common Management Information Services and Protocol. (CMIS and CMIP).

The specific management functional areas fault management, configuration management, performance management, accounting management and security management.

The multi-vendor network management gives the organisation maximum flexibility to choose among projects of different vendors to meet their particular computing and network requirements. Multi-vendor network systems will be delivering the best information services by maximizing the performance and availability of complex multi-vendor computing and data communication networks.

10.16 APPLICATIONS OF NETWORKS

Popular network application are file transfer, electornic mail, bulletin board, remote **login,** remote program execution, remote database access and resource sharing. The three applications namely file transfer, electronic mail and bulletin board result in transfer of data from one station to another. The applications like remote login, remote program execution and remote database access imply that a conversational link be established between two systems. The resource sharing application implies that all the stations share a particular resource available in anyone or a few stations on the network. A resource can be either hardware like a powerful CPU, laser printer, plotter etc. or software like a language compiler or an application program. All these applications have their own requirements and they have to be mapped on to the network in an appropriate manner. While the layers of software as described by the standards ensure error free communication between two stations, the applications have thier own requirements of protocols. For example, even though data is physically transferred from one station to another in the case of file transfer and electronic mail the protocol requirements for these two applications are quite different. For example, the file transfer tries to identify receiver station and establishes a logical link over which the entire file is transmitted. At every step, messages are exchanged between the sender and the receiver so that both of them know that the file has been transmitted fully and correctly. On the other hand, the electronic mail system functionally is very similar to the postal system in our country. The sender gives the message to an 'Agent' who then transfers it to another agent in whose domain the recipient of the message resides. This is similar to one person writing a letter to another using the postal system. The sender may be in Madras and the receiver may be in Delhi. The sender prepares the letter, writes the address and gives it to the agent through Mail Box. The agent (in this case is the Post Office in whose domain the sender lives) sorts the letter and sends it to his counterpart in Delhi. The exchange of letters between the post offices is similar to the exchange between Mail Transfer Agents. The post office in Delhi through a delivery mechanism delivers the letter to the receiver. Thus the application requirements of an electronic mail is quite different from that of file transfer.

In the case of an electronic bulletin boards, a given message is transmitted in a broadcast mode a group of users called recipients. The group is a subset of the total number of users available on the network and is selectively chosen depending on the message. For example, in an academic department, a notice about a particular conference will be of interest only to those people who are actively working in the area covered by the conference and who are likely to contribute to the conference. On the contrary, a general, information like a faculty meeting will be of interest to everybody. Such things can be transacted using the bulletin board. The situation is similar to the physical bulletin board in which a number of notices are struck on the board and the reader only picks up the notices that are of relevance to him/her.

The networks can be used in a variety of environments. For each environment, the major activities in the environment will decide the applicability of Netwoks to that environment. Some examples of environments are administrative offices, finance and insurance, transport, hotels, manufacturers and hospitals.

An adminitrative office has got both clerical service supporting the main business of the organisation and the supervisory service supporting the decision-making process of the organisation. Traditionally, a single mainframe computer with terminals in each department was the model of an automated office. But today, each department can own one or more PCs of varying capacity. Word processing has fast become a national substitute for the typewriter.

With the full availability of PCs, an internal electronic mail can effectively replace the movement of paper within the office. The traditional services like client-account servicing, client-record accessing, documentation control and distribution, financial administration and purchasing and sales can all be integrated into a Network which is nothing but an effective interconnection of PCs.

10.17. SUMMARY

This unit described certain hardware and software components of networks and how they operate. Definition and characteristics of Local Area Networks were given. Network topologies of various kinds of switching involved in networks was also discussed. Multi - vendor compatibility standards establishment in networks

was discussed in the context of network management. In conclusion, various applications to which networks can be put was discussed.

10.18. KEY WORDS

Application Layer : Layer 7 of the OSI model. This layer determines the interface of the system with the user.

Bandwidth : Refers to the relative range of frequencies, that is, the difference between the highest and lowest frequencies transmitted. For example, the bandwidth of a TV channel is 6 MHz.

Baseband : Transmission of signals without modulation. In the baseband local network, digital signals. (1s and 0s) are inserted directly on to the cable as voltage pulses. The scheme does not allow for frequency division multiplexing.

Broadband : The use of coaxial cable for providing data transfer by means of analog or radio-frequency signals. Digital signals are passed through the modem and trasmitted over one of the frequency bands of the cable.

Carrier : A continuous frequency capable of being modulated or impressed with the second (information carrying) signal.

Channel : A means for transporting information signals. Several channels can share the same media.

Channel Capacity : The maximum rate at which information can be transmitted over a given channel. It is normally measured in bauds but can be stated in bits per second.

Character Terminal : A terminal which cannot construct its packets, thus needs an additional device Packet Assembler and Disassembler (PAD) for connection to Packet Switched network.

Coaxial Cable : An electro-magnetic transmission medium consisting of a center conductor and an outer concentric conductor.

Connectivity : In a LAN, the ability of any device attached to distribution system to establish a session with any other device.

Data Link Layer : In a layered architecture, the data link protocol provides for channel level addressing, packet framing, and CRC check generation and application. It also serves as a channel bandwidth allocater using, for instance, distributed CSMA/CD control.

Ethernet : A local area network and its associated protocol developed for (but not limited to) Xerox Corporation. Ethernet is a baseband system.

Fiber Optics : A technology for transmitting the information via light waves moving through a fine filament. Signals are encoded by varying some characteristics of the light waves generated by low powered laser. Output is sent through light conducting fiber to a receiving device that encodes the signal.

Four Wire (4 Wire) Circuit: A two away circuit in which signals simultaneously follow separate and distinct paths in opposite directions in the transmission medium. It is called four wire because it uses a pair of wires in each direction in the most simple form.

Headend: A component of broadband network that translates the “transmit frequency band” to “receive frequency band”, thus, making it possible for a station to transmit and receive on a single cable network.

IEEE 802: A committee of IEEE organised to produce a LAN standard.

Logical Link Control: A protocol specified in IEEE 802.2 for data link level transmission control.

Medium Access Control (MAC): For bus, tree and ring topologies the method of determining which device has access to the transmission medium at any time. CSMA/CD and token are common access methods.

Message : A logically related collection of data to be moved.

Network Layer: Layer 3 of the OSI model. Responsible for routing data through a communication network.

Packet : A group of bits that includes data plus source and destination addresses. Generally refers to a network layer (layer 3) protocol.

Packet Assembler/Disassembler (PAD): A device used with an X.25 network to provide service to asynchronous terminals.

Packet Terminal: A terminal which can form its own packet. This terminal is also capable of interacting with a network character terminal.

Physical Layer: Layer 1 of the OSI model. Concerned with the electrical, mechanical and timing aspects of signal transmission over a medium.

Polling: A method of network control where nodes are instructed to transmit in turn, under the command of a master node.

Presentation Layer: Layer 6 of the OSI model. Concerned with data format and display.

Public Data Networks (PDN): A government controlled or national monopoly packet switched network. This service is publicity available to data processing users.

Public Switched Telephone Network (PSTN) : A telephone switching system that provides switching transmission facilities to customers.

Remote Terminal: A terminal connected via a data link to a system.

Repeater: A device that receives data on one communication link and transmits it, bit by bit, on another link as fast as it is received, without buffering. An integral part of the ring topology. Also used to connect linear segments in a baseband bus LAN.

Satellite Links: The links which are established using a satellite communication system.

Security: In computing it is Prevention/ Protection of information against retrieval, alteration or destruction by unauthorised user.

Session Layer: Layer 5 of the OSI model. This layer deals with active interconnections of one device to another over a communication system.

Teleprocessing: It refers to data processing combined with telecommunications.

Token: A special bit pattern, generally a 8 bit pattern e.g. 11111111, which ciruculates around the ring for control purposes. It helps in identifying the state of the ring i.e., idle or some station transmiting.

Token Bus: A medium access protocol technique for bus/tree. Stations form a logical ring around which token is passed. A station receiving a token may transmit data, and then must pass the token to the next station in the ring.

Token Ring: A medium access protocol technique for rings. A token circulates around the ring. A station may transmit by seizing the token, inserting the packet onto the ring and then transmitting the token.

Transport Layer: Layer 4 of the OSI model. Provides reliable, transparent transfer of data between endpoints.

VLSI : An abbreviation for Very Large Scale Integration, a fabrication technology in micro-electronics in which more than 1000 gates are integrated on a single silicon chip.

10.19. SELF-ASSESSMENT EXERCISES

1) What are the various kinds of network topologies?

2) Describe the types of switching available in networks.

3) Describe the various applications to which networks can be put.

10.20 FURTHER READINGS

Indira Gandhi National Open University, School of Engineering and Technology, *Modern Office, Block-1, Communication in the Office,* Units 2B and 3.