UNIT 8 NETWORK TOPOLOGY

Structure

8.0 OBJECTIVES

After going through this Unit, you will be able to understand and appreciate:

- What is meant by network topology;
- Difference between physical and logical topologies;
- Basic topologies like star, bus, ring, tree and hybrid;
- Why star topology is popular;
- Topology related network components like hubs and switches;
- Different logical topologies;
- Ethernet and token passing ring protocols;
- Merits and demerits of Ethernet and token passing ring protocols;
- Why address resolution is required and how it is performed;

- Purpose of domain name servers an address resolution protocol;
- The need for encapsulation;
- Router connectivity and the functioning of routers in Internet; and
- Routing algorithms and the associated performance parameters.

8.1 INTRODUCTION

As you are aware, computers world over are interconnected via the Internet. The connection to the Internet happens in a variety of ways. For example, a home computer is usually stand-alone computer connected to the Internet via a dial up telephone line. In homes where there is more than one computer, they may be interconnected to form a home computer network. In such cases, one of the computers acts as the Internet link. It is called a proxy Internet server. Other computers access the Internet via the proxy server. The home proxy server also accesses the Internet via dial up line usually. In some rare cases, a home may use a leased line to access Internet. Computers in organisations and offices are generally interconnected locally. The local network, called Local Area Network (LAN) is then connected to the Internet via a gateway using a leased line. The gateway may be a firewall or a proxy server. There are a variety of ways in which LAN computers may be interconnected.

Network topology refers to the study of geometric properties of the way in which the computers in a network are interconnected. A generalised network connection is shown in Fig. 8.1. Here four computers are attached to what is called a network cloud. The network cloud is a graphic symbol that denotes a network without specifying the geometry or other interconnection details. Network cloud is a black box that hides the interconnection details from the viewer.

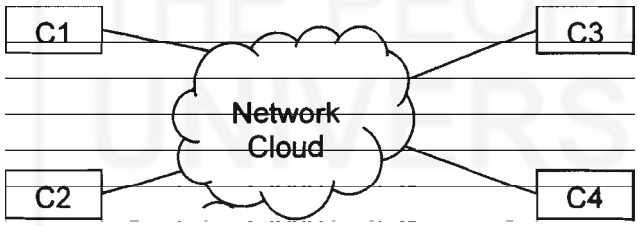


Fig. 8.1: A network cloud

There are a variety of ways in which these computers or nodes, as they are often called, can be interconnected physically inside the network cloud. For example, they may be interconnected as a daisy chain; say, C1-C2-C4-C3; or to a central switch as in the case of telephones being connected to an exchange. In a daisy chain connection, information moves from node to node in the order in which the chain is formed. In the above example, data moves from C1 to C2, C2 to C4 and C4 to C3 and vice versa for reverse flow. When a switch is used, a direct connection between two computers is established as in the case of calling and called subscribers in telephone communication. Network topology deals with the study of the way in which the computers are connected inside network cloud.

8.2 PHYSICAL AND LOGICAL TOPOLOGIES

You may be aware that in data networks like the Internet, data moves in packets. A long string of text is spilt into small packets, say 1024 bytes long, and sent over the network hopping from node to node. Accordingly, these networks are called packet

switched networks or packet data networks (PDNs). Interestingly, the way in which packets move in a network may not correspond to the way in which the computers are physically connected for a variety of reasons. One important reason is traffic management and routing. The idea is very similar to the vehicular traffic management. If a road is congested and there is traffic jam, one tends to take a different route even though the alternative route may be longer. Depending on the jam, the traffic may be diverted for quite sometime. Similarly, if a link is congested in a network, an alternative route may be chosen to forward the packets. Route is chosen independently for every packet depending on the traffic conditions. The path taken by a packet for traversing form a source computer to a destination computer is known as logical path. Obviously, there may be a number of logical paths in a network. The collection of all such paths is called the logical topology of the network. The physical links constitute the physical topology of the network. In essence, the logical topology refers to the way in which packets travel from a source to a destination, whereas the physical topology refers to the actual physical interconnection of the computers in the network. Physical topology is also referred to as *real* topology and the logical one as *virtual* topology.

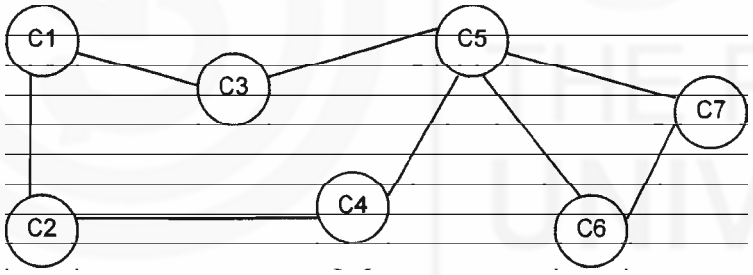
Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

1) A packet switched network uses a packet size of 2^{11} bytes. Determine the number of packets to be transmitted to transfer a file of size 1 MB.

2) Consider the physical topology given below:



Enumerate the number of logical paths between C1 and C7.

3) Can the packets of the same file travel via different logical paths? Do you foresee any problem in this case?

.....

.....

.....

.....

8.3 FULLY CONNECTED TOPOLOGY

Data communication involves computers in one part of the world being able to contact and communicate with computers in other parts of the world. For example, a home computer connects to different websites at different times. It is not just fixed one-to-one connection. It is multi-point communication connecting different to destinations at different times. For this purpose, a computer needs access to all the other computers that need to be contacted. One way of achieving this is to establish direct connections

between the source computer and all the destination computers. In this case, we need as many links as there are destination computers. For example, if a home computer were to connect to 10 different web sites, then we would need 10 different links connecting the home computer to each web site. As you know, this obviously is not the case. However, if every computer in the world were to be connected to every other computer like this, then we need a very large number of links. A network formed this way for five computers is illustrated in Fig. 8.2. Here, every computer is directly connected to every other computer. Networks with this kind of connectivity are said to have fully connected topology. There are 10 links in Fig. 8.2. The links are assumed to be full duplex in the sense that they are capable of transporting information both ways. If the links were unidirectional (half-duplex) as in the case of optical fibres, we would need twice the number of links for two-way communication. The number of links required in a fully connected network becomes very large even with moderate number of computers. For example, we require 1225 links for fully interconnecting 50 computers.

In a general case with N computers, $N(N-1)/2$ links are required as reasoned in the following.

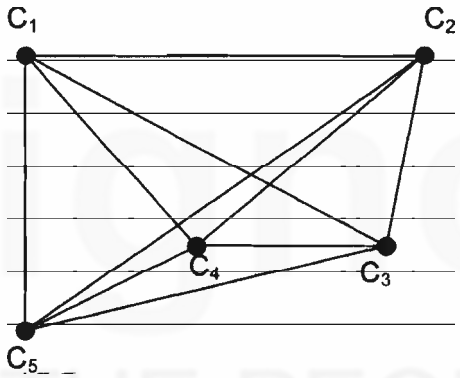


Fig. 8.2: Fully connected topology for five computers

Let us consider the N computers in some order. In order to connect the first computer to all other computers, we require $(N-1)$ links. With this, the second computer is already connected to the first. We now need $(N-2)$ links to connect the second computer to the others. For the third computer, we need $(N-3)$ links, for the fourth $(N-4)$ links, and so on. The total number of links N works out as follows:

$$L = (N-1) + (N-2) + \ldots + 1 + 0 = N(N-1)/2$$

Establishing separate and direct communication links connecting each computer to every other computer as shown in Fig. 8.2 is very expensive and is impracticable. Hence, this is just not done.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

4) How many half-duplex communication links are required for fully connected topology with 10 computers supporting full-duplex communication?

5) Draw a fully connected topology for two-way communication with four computers using fibre optic links. How many links are there in your network?

.....

.....

.....

.....

8.4 STAR TOPOLOGY

Star Topology is basically a physical topology. As the name implies, the topology looks like a star in the sky with rays emanating from the central point in all directions. It is a centralised topology where all computers are connected to a central point, which we call as *star point.* The topology is depicted in Fig. 8.3. This topology is easy to administer and maintain. The links can be tested and repaired from the central star point. This is one of biggest advantages of star topology. The topology is also a robust one. If a link or a computer fails, the rest of the network is not affected. As a result, this topology is very popular and is used extensively.

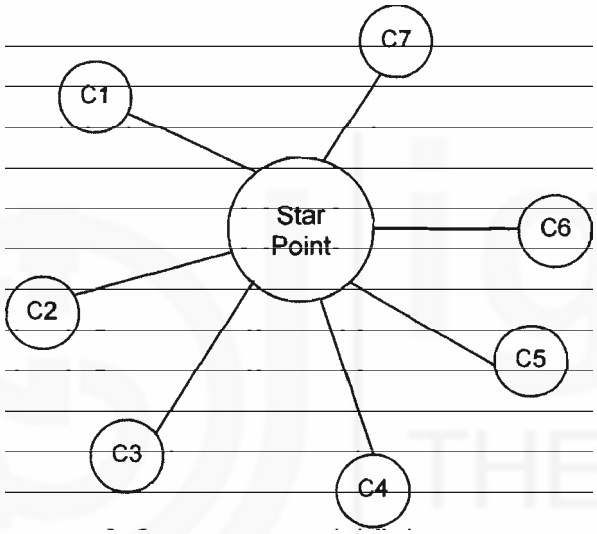


Fig. 8.3: Star topology

However, if the star point fails, the whole network fails. This is a disadvantage. Special care is taken at the time of designing the star point to make it very reliable.

Strictly speaking, physical star topology does not imply any logical topology. The logical topology is dependent on how the star point has been designed. This, in fact, makes this topology very attractive as it offers the flexibility of easy maintenance on the one hand and permits different logical topologies to be implemented on the other. Logical topology, as we mentioned earlier, defines the way in which a packet traverses form a source computer to a destination computer. Usually, there is set of rules that govern the exchange of packets between computers. Such a set of rules is called a protocol. There are many protocols used in networks. We learn more about protocols later in this unit. The star point of star topology can be designed to implement a variety of protocols such as Ethernet protocol, token ring protocol and a switch. Usually, either a hub that implements Ethernet protocol or a switch that permits switched connections is used as the star point. We learn about hubs and switches in the next section.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

6) Enumerate the advantages of star topology.

.....

.....

.....

.....

8.5 HUBS AND SWITCHES

As mentioned in the previous section, hubs and switches are used to implement logical topology in a physical star topology. Hub is a terminology used in several contexts in networks. In satellite networks, hub means a special ground station with which small satellite terminals communicate. In the context of LAN, hubs are used to implement two different logical topologies: Ethernet and token ring. But in most of the textbooks, the word hub is used to denote Ethernet hub, i.e. the hub that implements Ethernet logical topology. You must, however, be aware of the existence of different types of hubs. A hub is sometimes loosely called a concentrator as it connects to all computers in a network in star configuration. Ethernet is also implemented in bus physical topology that we discuss in the next section. Discussions on Ethernet in this section also apply to bus topology implementation. In fact, Ethernet was first implemented using bus topology. Later, it was implemented using hubs in star topology. At present, most of the Ethernet implementations are based on star physical topology using hubs.

Recall that logical topology corresponds to the way packets are transported within a network. Ethernet transports packets in much the same way information is exchanged in a group discussion among people. What happens in a group discussion? One who has something to say starts speaking and others listen. In the same way, in Ethernet topology, a computer starts transmitting whenever it has a packet to send. Other computers listen. Since any computer in the network can start a transmission Ethernet is called multiple access (MA) scheme. As happens in a group discussion, sometimes more than one computer may start a transmission simultaneously. What happens when two persons start speaking? Both of them go quiet and one among them starts afresh? Similar thing happens in Ethernet. When more than one computer start transmission simultaneously, we say that a collision has occurred. The computers that transmit simultaneously detect the collision, go quiet and follow a predetermined procedure to start the transmission afresh. Hence, Ethernet is a collision detection (CD) scheme. In a group discussion, if someone is already speaking, another person does not start to speak. Similar thing happens in Ethernet where detection of an ongoing transmission is called carrier sense (CS). On the whole Ethernet is a CSMA/CD scheme.

Let us now see how a hub helps implement Ethernet. Hubs come in 4, 8, 16, 24 and 48-port configurations. One computer can be attached to each port. Each port has provision for input/output and power connections. At the computer end there is a network interface card (NIC) that connects to the hub port. One of the ports is specially designed to be able to attach to another hub, thus allowing cascading of hubs. Cascading is useful when clusters of computer are located in nearby geographical areas. For example, an organisation spread over multiple floors of a multi-storey building, may use one hub per floor and cascade them so that computers in different floors can communicate with each other. Fig 8.4 shows a schematic of cascaded hubs with four ports each. Port 4 is specially designed to connect to another hub. Port 4 of the hub in Floor 1 is connected to Port 1 of the hub in Floor 2. Port 4 of the hub in Floor 2 is connected to Port 1 of the hub in Floor 3. Thus all the three hubs are cascaded in a daisy chain fashion. You may note that only two computers can be connected to the hub in Floor 2. If no cascading

is used, the special port can be used to connect a computer. This is shown in the hub in Floor 3. Hubs that have provision for cascading are also called *stackable hubs*.

The internal mechanism of an Ethernet hub forwards any incoming packet from any computer to the output lines of all other computers as well as to the output line of the sending computer. In this sense, the hub acts as a broadcaster.

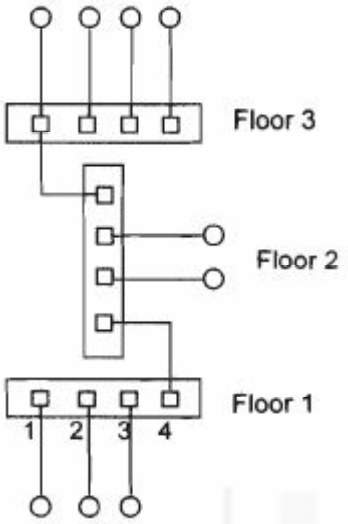


Fig. 8.4: 4-port cascaded hubs

This broadcast allows all the other computers and the transmitting computer to listen to the ongoing transmission. The transmitting computer is able to detect a collision by monitoring its own output line. If a bit received on its output line is not the same as the one sent by it, the computer knows that a collision has occurred. The Ethernet NIC in the computer senses carrier and detects collision. The hub enables multiple access feature as all the computers are connected to it and anyone can start a transmission. This is Ethernet hub implements CSMA/CD protocol. An important requirement of a hub-based design is that all computers connected to the hub must operate at the same speed.

The star point of star topology could be a switch. A switch is like a telephone exchange. The switch examines the destination address in an incoming packet and routes the packet to the appropriate outlet much as the telephone exchange examines the dialled number and routes the call to the appropriate destination. Much as the way telephone exchanges are interconnected, switches can be interconnected to route packets to computers that are not local. In fact, this is how most of the Internet connections work. An important advantage of the switch when compared to hub is that different computers can operate at different speeds. Of course, the source and the destination computer pair must operate at the same speed.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

7) What are the different logical topologies that can be implemented by hub?

.....

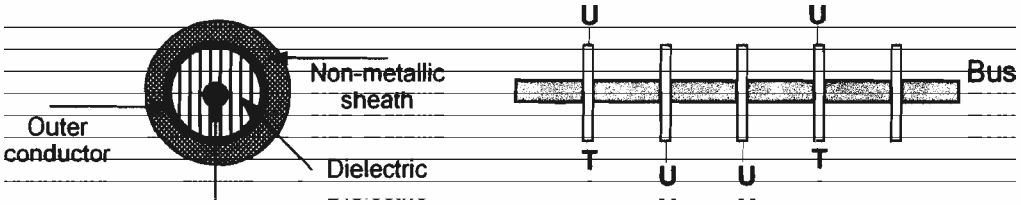
.....

.....

.....

8.6 BUS TOPOLOGY

Bus is a cable laid linearly. Imagine a coil of cable unrolled, stretched and laid from end-to-end in a linear fashion and it becomes a bus. The cable is of coaxial type. Coaxial cable has one central conductor with a surrounding metallic shield. The central conductor and the shield are separated by a dielectric medium. Dielectric, as you may know is an insulator that electrically separates the inner conductor and the outer metallic shield. A thick non-metallic sheath further protects the central conductor and the shield. Fig 8.5(a) depicts a coaxial cable. The outer conductor (the metallic shield) is usually grounded and acts as an electromagnetic shield.



Inner central conductor — U = User node T = Tap

(a) Coaxial cable — (b) Bus topology

Fig. 8.5: Coaxial cable and the bus topology

With the outer conductor grounded, the cable essentially has one single conductor that carries current. When laid out as bus, the central conductor is like broadcast medium. Since the central conductor acts as a broadcast medium, it is called ether, the space, and the network as Ethernet. The bus topology is shown in Fig. 8.5(b). The bus cable is open at both ends and needs to be terminated with suitable terminations for proper electrical operation. Taps are essentially screws driven halfway into the central conductor. Taps are connected to the NICs of user nodes or computers. Thus, all computers are connected to the central conductor. Tap connection to the central conductor is passive and failure, if any, in one of the computers does not affect others in the network. But if the cable breaks at any point, the entire system is affected. It is not easy to detect and locate the cable break and a special device called *time domain reflectometer* is used for this purpose.

The NIC implements CSMA/CD protocol described in the previous section. Since all NICs are connected to the central conductor, there is multiple access (MA). They are able to sense (Carrier Sense) and listen to the transmission that is taking place on the bus. Any collision can be detected (CD) and necessary action taken to resolve the same.

The first version of Ethernet was implemented using a thick coaxial cable specified as 10Base5. The specification 10Base5 means the cable operates at 10 Mbps speed, uses what is called baseband modulation and can have a maximum length of 500 meters. This Ethernet version was called thick Ethernet. True to its name, the cable was thick and difficult to handle. Later another version called thin Ethernet was introduced with the cable specification as 10Base2. This cable was more flexible and easier to handle. Bus based Ethernet is the forerunner of hub based Ethernet. Because of the problems faced in the maintenance of thick and thin Ethernet, hub based solution was invented. The cable used in hub based system is a twisted pair and the specification is 10BaseT. Twisted pair cables cover a maximum length of 100 m. They are like telephone cables and are easier to handle. Some high-speed implementations of Ethernet used optical fibre. Then, the system specification is like 100BaseF. Optical fibres cover a distance of about 2000 m.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

8) What is the operating speed and the maximum distance covered by 20Base3 Ethernet system?

.....

.....

.....

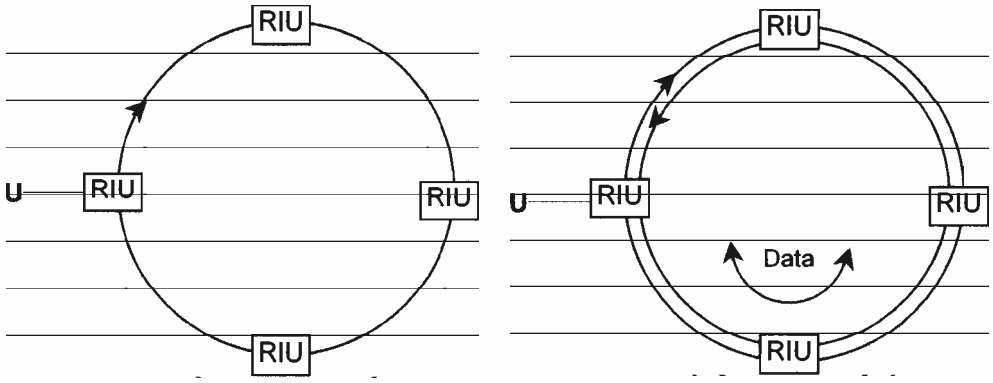
8.7 RING TOPOLOGY

In ring topology, a physical ring is formed by making point-to-point connection between computers. The computers themselves may not physically appear to be in the form of a ring, but electrically they form a ring. For example, two computers placed in adjacent rooms may be part of the ring. There is a circular communication path. Ring topology may be built around a single ring or two rings (dual ring).

Ring topologies are depicted in Fig. 8.6. The equivalent of tap in bus topology is Ring Interface Unit (RIU) in ring topology. User computers are attached to the RIUs. Unlike passive bus taps, RIUs are active units. Being active units, their failure rate is higher than passive taps. If a bus tap fails, only the concerned computer is affected. But if a RIU fails, the entire ring operation is affected. Hence, special considerations are required in ring topology to handle failures. In fact, failure management complicates the ring design and for this reason ring topology is not very popular.

Single ring topology shown in Fig. 8.6(a) usually uses bi-directional medium like copper wire. In case a segment of the ring or a RIU fails, the ring is folded back by the two end RIUs and the ring form of functioning continues. Dual ring configuration shown in Fig. 8.6(b) is generally adopted in the case of optical fibre design. As you may know, optical communication is naturally unidirectional as light that acts as the carrier of information is launched at one end of the fibre and received at the other. In dual ring, information travels in opposite directions in the two rings.

As in the case of bus topology, it is difficult to implement and maintain a ring structure physically. Hence, logical ring structure is often implemented using a ring hub in physical star topology. The logical topology in a ring network is called token passing ring or simply token ring.



(a) Single ring (b) Dual ring

Fig. 8.6: Ring Topology

A token circulates on the ring when it is idle. Token is a special bit pattern like 01111111 (zero followed by 7 ones). It is ensured that this pattern does not occur in the data transmitted by the computers. A special coding scheme is used to prevent the occurrence of token pattern in the data. A computer that has data to transmit seizes the token and starts transmitting the data. Imagine a circular formation of people around a round table participating in a group discussion. A ball is given to the group. The ball is passed around from one person to the next. The rule is that a person can speak only when he/she holds the ball. When a person wants to speak, he/she retains the ball when received and starts speaking. Once finished speaking, he/she passes the ball to the next person in the circular formation. The token ring scheme functions in a similar fashion. Two observations are important. First there is no collision in this scheme. Hence, the token ring functions more efficiently than Ethernet. However, Ethernet is more popular. Second, every station gets a chance to transmit as the token goes around. In Ethernet this is not the case. An unlucky station may keep on colliding again and again and may get a chance to transmit for quite some time.

On the ring, when a station starts transmission, the stations (computers) downstream listen to the transmission and monitor the destination address. If the destination address does not match one's own address, it passed to the next station as it is. When the data reaches the destination computer, the station copies and drains (takes away) the data from the ring. Thus a connection is established between the source and destination stations. After the source station has transmitted all data, it reintroduces the token on the ring. The token may now be seized by another station that has data to send. Obviously, the station next to the source station is the first one that can seize the token. Because of the use of token, the logical topology is called token passing ring. In optical fibre implementation, the logical topology is called Fibre Distributed Data Interface (FDDI). Ring networks operate at speeds of 10 Mbps to 1000 Mbps.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

9) Discuss the problem that would arise if a station on the ring seizes the token but fails to reintroduce the same on the ring after completing the data transmission. Suggest a mechanism to overcome such a problem.

.....

.....

.....

.....

8.8 MESH TOPOLOGY

Mesh is a complex interlaced structure realised by a bunch of point-to-point interconnections. Computers are interconnected without any geometric shape in mind. They are connected depending on the demand. They are somewhat like fully connected networks with some links missing. Therefore, they are sometimes referred to as partially connected topology. Mesh topology is illustrated in Fig. 8.7. In this topology, some of the nodes of the network are connected to more than one node by point-to-point links.

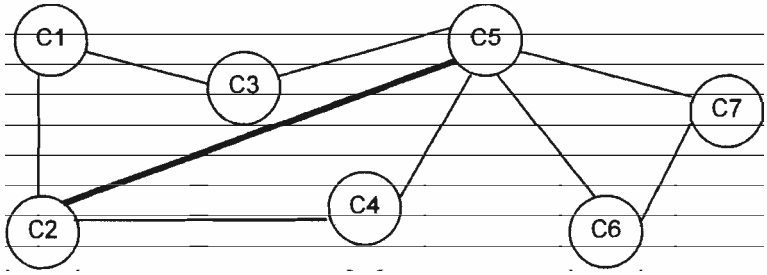


Fig. 8.7: Mesh Topology

Mesh is the actual topology that connects the wide area Internet all over the world. The nodes on the Internet invariably have mesh connectivity, i.e. multiple point-to-point links. Each node is connected to more than one node. The point-to-point links are established based on two considerations:

- Traffic between nodes
- Redundant routes.

Wherever heavy traffic is envisaged between two nodes, a direct link is established. Such links are sometimes called high usage routes. For example in Fig. 8.7, the link between node 2 and 5 is a high-capacity link to cater for heavy traffic between the two nodes. In addition, there must be at least one alternative route between a given source and destination i.e. a primary route and a secondary route. For example, the secondary route between C3 and C5 is via C3-C1-C2-C5. The secondary route may be used when C3-C5 link is broken. Often, there are many alternative routes between a source and destination. In such a case, the source and intermediate nodes must have some kind of intelligence to make a routing decision to select the best route at a given time. Most of the nodes on the Internet are routers that are capable of selecting the best possible route. Routing decisions take a definite amount of time. Hence, more is the number of intermediate nodes more is the time taken for the information to reach the destination. Usually, the shortest path with minimum number of intermediate nodes is chosen as the primary route. Only when that route is heavily loaded with traffic or unavailable for some other reason, an alternative route is chosen. We discuss routing and routing algorithms in more details in Sections 8.13 and 8.14 respectively.

8.9 TREE TOPOLOGY

Tree topology is also called hierarchical topology. In this topology, there is a clear hierarchy amongst the nodes. This is similar to a hierarchical structure in an organisation where there is a Chief Executive Officer (CEO) at the top, many senior level executives under him/her, junior executives reporting to seniors and so on. There are levels of responsibility and a clear reporting structure. Tree topology is modelled along the same lines. It is shown in Fig. 8.8. Strictly speaking, the structure is an inverted tree with the root node at the top and the branch and leaf nodes below the root.

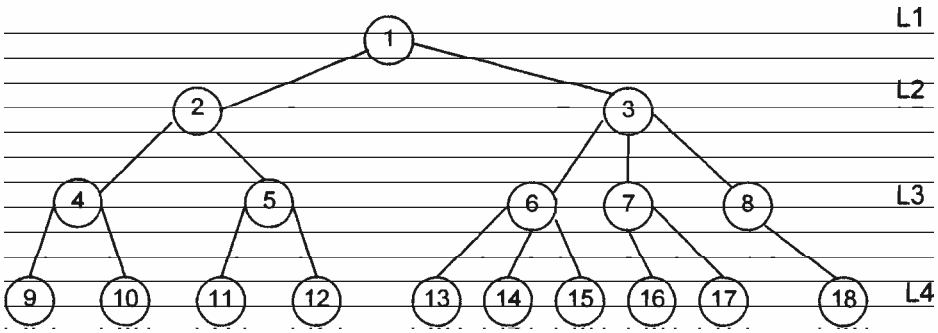


Fig. 8.8: Tree Topology

Four levels are shown in Fig. 8.8. The number of levels in a tree is called its depth. The top level node (Level 1) is called the root node and the bottom level nodes (level 4) as leaf nodes. The intermediate level nodes are called branch nodes at the designated levels. Each node except the root node has one point-to-point link connecting itself to the higher level node. Each node except leaf nodes has as many point-to-point links as there are braches attached to it. Leaf nodes, being at the bottom level have no branches. There is an interesting relationship between the number of nodes and the number of point-to-point links in a tree. The number of links is always one less than the number of nodes. Verify this in Fig. 8.8.

The number of branches that emanate from a node is called the branching factor (BF) of that node. If the branching factor is uniformly two for all the nodes, then the tree is called a binary tree. In Fig. 8.8, the left portion of the tree is shown to be binary. The tree itself is not binary as there are portions with branching factors that are not two. If all the nodes (except leaf nodes) in a tree have the same branching factor, then the same may be called the BF of the tree. If the BF of a tree is one, then the tree reduces to linear topology. The extreme right portion of Fig. 8.8 comprising nodes 8 and 18 represents the linear topology.

There is strict hierarchy of interaction amongst the nodes. Two nodes at the same level emanating from the same branch node above interact through that branch node. For example, nodes 6 and 7 in Fig. 8.8 communicate via node 3. If the nodes are attached to different branches, then the communication proceeds by traversing up the tree as much as required. For example, the communication between nodes 9 and 12 takes place via the route 9-4-2-5-12.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

10) What is the branching factor of a leaf node?

11) How many nodes and point-to-point links are there in a binary tree of depth 5?

12) Why is it a tree topology is also called a hierarchical topology?

.....

.....

.....

.....

8.10 HYBRID TOPOLOGY

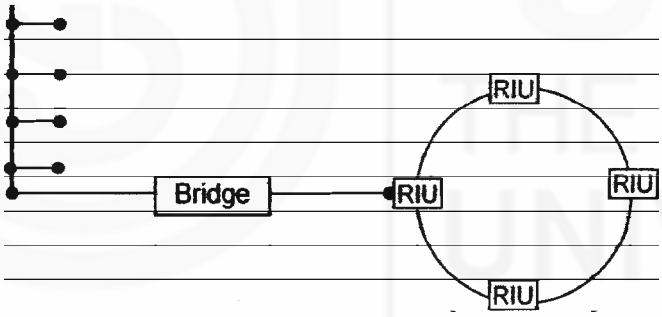
A hybrid topology is a combination topology in which two or more of the topologies discussed above coexist and work together. Figure 8.9 shows two example hybrid topologies. A large variety of hybrid topologies are possible. In Fig. 8.9(a), two star topologies are interconnected by a bus topology. This implementation is typical in campus networks like in a university. Each department may have star implementation while a bus or ring network may interconnect the departments. In general, such an implementation is adopted wherever the facilities that need to be interconnected are dispersed. For example, an office that is situated in different floors of a multi-storey building may use a hybrid structure. Computers in each floor may use Ethernet hub based star structure

and the different floors may be interconnected by a bus structure. It is important to note that the entire set up works on the logical topology of Ethernet. Hence, interconnection of star with bus is seamless with no intermediate device.

Figure 8.9(b) shows a hybrid topology interconnecting a bus topology and a ring topology. In this case an intermediate device called a bridge is required. This is because the two topologies implement different logical protocols, viz. Ethernet and token ring. Bridge is an intelligent device. It implements two different logical topologies or protocols. In Fig. 8.9(b) it implements Ethernet on one side and token ring on the other. It appears like Ethernet NIC for the bus topology and as a token ring station attached to a RIU on the ring topology side. It is capable of recognising addresses at the logical level and mule *packets 1mm* one LAN to the other, it converts (reformats) packets of one protocol to that of another.

In some organisations, same topology is implemented in segments in geographical locations that are far apart All segments together are considered as one LAN.

Bus (a) Star-Bus-Star Hybrid Topology



(b) Bus-Ring Hybrid Topology

Fig. 8.9: Hybrid Topologies

In such cases, the signal from one segment to another traverses a long distance. In the process the signal level may be attenuated and may become too low to be recognised properly at the destination. To avoid this, devices called repeaters are used in between the segments. Repeaters are non-intelligent devices. They just amplify the signal level and make the signals strong so mat destination may recognise them property. In some cases, bridges may be used in place of repeaters for better management of LAN segments. Since, the bridges transform packets from one topology level to another, they automatically amplify the signals.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

13) In a university, LIS department has implemented star Ethernet LAN and the computer science (CS) department bus Ethernet LAN. The two departments are

in two different buildings that are far apart. How would you interconnect the two LANs?

14) In Question 13, how would your interconnection strategy change if the CS department had ring LAN? Explain the function of the device used.

15) Compare the features of bridges and repeaters.

.....

.....

.....

.....

8.11 MEDIA ACCESS CONTROL PROTOCOLS

Ethernet and token ring are two media access control (MAC) protocols that we have already studied briefly. In this section, we learn more details about them. Bus is a medium and so is ring, single or dual. Many computers are connected to these media. Any of the computers can access the medium that it is connected to. Since many computers access the same medium, we need some kind of protocol (a set of rules) so that there is an orderly access to the medium. Actually the access takes place in a controlled manner. Hence, the nomenclature MAC protocol is used.

In bus topology, Ethernet protocol is used. In ring topology, token passing ring protocol is used. Both these protocols are called multiple access protocols as they define sets of rules for multiple computers to access a medium. In hub based star implementations, the protocol depends on the type of hub used. The hub may be Ethernet hub or token ring hub.

Let us first see more details of Ethernet. As you already know, the Ethernet protocol rules are summarised in the acronym CSMA/CD. Consider the case when there is an ongoing transmission on the bus. The protocol must ensure that no new transmission starts at this stage. If it does, it will collide with the ongoing transmission and both transmissions will fail. No new transmission while there is an ongoing transmission is ensured by carrier sense (CS) mechanism. You may be aware that carrier refers to a high frequency transmission that carries the information signal. We have carrier frequencies in AM/FM radio broadcast. For example, 92.5 MHz is the carrier frequency of a FM radio station. The music signal is superimposed on this frequency and broadcast. Similarly, in LANs, information bits are superimposed over a carrier. The presence of carrier on the bus implies that there is a live transmission on the bus. Hence, any computer that has data to transmit will first sense the bus to see if the carrier is present. This process is aptly described as 'Listen before talking'. The rule specifies that a station can transmit only if there is no carrier present on the bus, i.e. the bus is idle or free.

There may be more than one station ready to transmit at any point of time. All such stations will start transmitting as soon as they find the bus idle. There is multiple access (MA) that results in collision. Let us what a collision is and how it is detected. If a computer is transmitting bit '0' and that gets changed to bit T on the bus or vice versa (bit T changes to bit '0'), then a collision is said to have occurred. The transmitting station is continuously listening to its own transmission on the bus and detects such a collision. When it finds a T changed to '0' or vice versa, it knows that a collision has occurred. Continuous comparison of what is transmitted and received on the bus is the collision detection (CD) mechanism. This process is often called as 'Listen while talking'.

Once a collision is detected, what do the stations do? They wait for random times and retransmit again. One station may wait for one millisecond, another for two and so on. Since the wait time is random for each station, it is likely that each station waits for different time and then attempts retransmission. The collision is resolved in this manner. Since the wait time is random for each station, it is possible that two or more stations wait for the same random time. In such a case, there will be a collision again during the retransmission attempt. If this happens, the same process of waiting for random times is repeated until the collision is finally resolved.

Now let us look at the details of token passing ring protocol. This protocol is relatively simple when compared to Ethernet. However, certain types of failures need to be taken care of in this protocol. As mentioned earlier, a token circulates on the ring whenever there is no data transmission on the ring. A token is a particular bit pattern and is recognised by this pattern. When a station has data to send it seizes the token and starts its own transmission. By seizing we mean that the station changes the token bit pattern such that it is no longer recognised as token. Instead, the pattern corresponds to one that indicates the beginning of transmission of data. Following this pattern, the destination and source addresses are sent. Whenever a station sees the beginning pattern, it examines the destination address to determine if the data is destined for itself. If so, it copies the data. When the data transmission is complete, the source station reintroduces a token on the ring. If any other station has data to send, it follows a similar procedure. To avoid a station holding the ring for a very long time, an upper limit is set for the size of data packet that can be transmitted at a time. If a station has large data to send, it needs to break down the same into a number of packets and transmit. After sending one packet, the station will have to wait for its turn to get the token. Only when it gets the token again, it can transmit another packet. This ensures that every station gets a fair chance to transmit.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

16) What is a carrier in LAN?

17) Find out and record the carrier frequency of a nearby AM radiobroadcast station.

18) What are the reasons due to which an Ethernet station experiences a collision during a retransmission attempt?

19) What is a token in token ring protocol?

20) In some token ring implementation, the destination station, instead of source station, reintroduces the token. What difference does it make?

.....

.....

.....

.....

.....

.....

8.12 ADDRESS RESOLUTION

In data networks, destination addresses have different formats at different levels. This is required for easy implementation of a complex system. For example, at user level, we need easy to remember addresses like names. Such user addresses are not transmittable as such. The network needs numerical addresses specified in bits. The name addresses provided by the user are decoded and the user data packet is encapsulated with decoded numerical addresses. The process of converting the addresses from one format to another is known as address resolution. Encapsulation takes place at several levels in a hierarchical structure for packet transmission. Three addresses and two levels of encapsulation are important to understand although there may be as many as six addresses encapsulated often. We study the important ones now.

Consider the case of a user sending e-mail. He/she uses a destination address something like *james_bond@mgm.co.uk.* The sending computer cannot use this address as it is because every computer on the Internet is addressed by a 32/128-bit number. The server mgm.co.uk is known on the network by a number assigned to it and not by its alphabet description. The 32/128-bit number is called Internet Protocol (IP) address. IP address has two versions: IPv4 and IPv6. IPv4 uses 32-bit address and IPv6 128-bit. IPv4 has been in use for a very long time, over 30 years, and most of the computers on the Internet have IPv4 addresses as of now. IPv6 has been introduced recently. Over the years, IPv6 is expected to replace IPv4 addresses.

The first step in packet transmission is to resolve the string address to numerical IP address. This is done with the help of Domain Name Servers (DNS) that are located in a hierarchical structure throughout the Internet. DNS have a table of string addresses with the corresponding numerical IP address. Usually, the table in one DNS is only partial and the entire set of addresses is covered by the complete hierarchical structure of the DNS. To start with, the sending computer accesses the nearest DNS by sending it the character string address provided by the user. If the DNS has the particular string stored in its table, it returns the numerical IP address. Otherwise it accesses another DNS that is in the hierarchy. This process is continued until a DNS is found that has the particular string address and its corresponding numerical address in its table. This process constitutes the first level of address resolution.

Once the sending computer receives the numerical IP address, it encapsulates the user message with numerical addresses. The numerical address received from DNS is used as the destination address and its own numerical address as the source address. This is the first level of encapsulation. The next level takes place in LANs.

You are aware of the use of NIC in bus LANs and RIU in ring LANs. These interface units have their own unique addresses assigned by the manufacturer. They are accessed by these addresses only. These addresses are 48-bit long. The destination and source stations are identified by 48-bit interface addresses on the LAN. The computers in which the interface units are housed are identified by their IP addresses. IP addresses are not recognised by the interface units. We now have two addresses: 32/128-bit IP address for the computer and the 48-bit interface address. We need to resolve the destination IP address to destination interface address before the data transmission can take place on the LAN. This is the second level of address resolution, in bus LAN, this address resolution is done by using a protocol called Address Resolution Protocol (ARP). Let us now see how ARP works. In all LANs, there is provision to broadcast information. This is usually done by reserving a special broadcast address. On bus LANs using ARP, the sending computer broadcasts the destination IP address received

as part of the first-level encapsulated packet. All other stations (NIC) read this broadcast. Whichever NIC is attached to the computer that has this IP address responds in reply. The sending computer now knows the NIC address to which the user information should be forwarded. It now encapsulates the user packet with the received NIC address as destination and its own NIC address as source and transmits the packet. This is the second level of encapsulation.

Thus address resolution and encapsulation are two important functions carried out in data networks at different levels.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

21) Why do we need address resolution in data networks?

22) What is the function of DNS?

23) How does ARP resolve IP addresses?

.....

.....

.....

.....

8.13 ROUTERS

A router is a device that forms one of the basic building blocks of Internet. Internet cannot function without routers. You are already familiar with repeaters and bridges. Router is a higher-level device that performs the functions of a bridge and a repeater and more. The primary function of router is to direct the user packets encapsulated with IP addresses in the direction of the destination. In this sense, the routers are much like telephone exchanges for the data networks. Telephone exchanges route the phone calls to the appropriate destination. Similarly, routers forward the data packets towards the destination. The telephone exchanges examine the number dialled to determine the destination. Routers examine the destination IP address in the incoming packets to decide the destination route. For this purpose, routers maintain what are called routing tables that contain entries relating to a destination addresses and the corresponding output that should be used to route the incoming packet.

Consider a user connected to a bus LAN in an institution in Delhi wanting to send a file to a user connected to a bus LAN in an institution in New York. Both LANs are connected to Internet via routers. The routers are connected to the LAN on one side and to the internet on the other as shown in Fig. 8.10. They are recognised both as a local machine and an Internet machine. They have unique Internet IP addresses as wet as local LAW addresses.

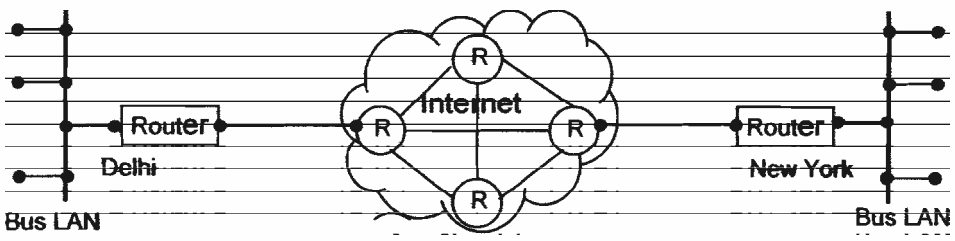


Fig. 8.10: Routers Use

There are also routers on the Internet that connect to other Internet routers in a mesh fashion. Whenever the destination IP address in a packet originating on the LAN does not point to a machine on one's own local network, as is the case in our example of Delhi sending to New York, the packet is forwarded to the router. This is done by a protocol called Transmission Control Protocol (TCP) mat runs on every LAN machine. We team about TCP HI Unit 9. The router forwards the same to another appropriate router on me Internet The packet travels via a number of routers on the Internet until it finally reaches the concerned router in New York that semis the packet to me appropriate machine on the LAN.

As you may observe, on me internet we have a number of possible routes that can be taken to reach the packet to New York. A typical route in our case is Delhi-Mumbai-Arnsterdam-London-New York. At every stage, the concerned router makes a routing decision as to which of the output ink must be chosen to forward the packet. The routing decision is taken according to the routing algorithm (software program) used by the router. Routing algorithm are discussed in the next section.

The routers shown at Delhi and New York institutions may also have multiple output links connecting to different routers on the Internet. It means that the concerned institutions have more than one Internet link. For example, if the packet were destined to Japan, the route chosen could be different if multiple paths were available.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

24) "Routers to data networks are Bee exchanges in telephone networks" Discuss.

.....

.....

.....

.....

8.14 ROUTING ALGORITHMS

As you may be aware, an algorithm is a step-by-step procedure to execute a task especially in a computer. Software programs implement algorithms to perform various tasks. Routing algorithms are procedures to make routing decisions. Routers execute routing algorithms to make routing decisions. Routing algorithms may be placed under two broad categories:

- Adaptive or dynamic algorithms
- Fixed or static algorithms

Dynamic algorithms adapt themselves to changing traffic conditions and network availability. For example, traffic may suddenly increase in a particular segment. As a result, tong queues of packets may build up stowing down the delivery to the destination. An adaptive algorithm may find an alternative route that may be longer but faster. Static algorithms use fixed routes for relatively long time durations. There could be more than one fixed route defined for a given destination in order of priority. Static algorithms do not monitor traffic conditions or the time to deliver. They are relatively easier to implement when compared to dynamic algorithms. They also need less processing power, i.e. CPU time.

Routing algorithms are designed to satisfy certain performance parameters. Some of the important parameters are:

1) Minimum delay for delivery

2) Minimum number of hops to reach the destination

3) Robustness

4) Stability

5) Fairness

Minimum delay may be local or global. By local we mean that the packet does not stay in the router for long. The output queue small and the packet leaves the router quickly. By global we mean tile delay in reaching tire destination. A packet may leave a router quickly but may get stuck later, tit such a case, it is better to route the packet by an alternative route even though the local delay may be longer.

A packet traversing a router is said to have done a hop. In other words, a packet hops from router to router on its way to the destination. As you are aware, every router examines the destination address in the header portion of every incoming packet. There is computational time overhead associate with this activity. Hence, it is desirable to have minimum number of routers or hops on the way to the destination.

Robustness means the ability to reach tile destination even when part of the network fails. A router should not forward a packet to a dead router on the way. In that case, the packet would never reach the destination. A robust routing algorithm would ensure that a packet is delivered to the destination at all costs. In other words there is guaranteed delivery.

Stability refers to the ability to deliver the packet as quickly as possible without the packet wandering here and mere. Sometimes loops may be formed in a network that packets may go round and round without moving forward towards the destination. A loop in the network is an unstable condition. Routing algorithms must ensure that no loops are formed. And if formed, they must be detected quickly and remedial action taken.

Fairness means delivery in a reasonable time for all types of packets. Sometimes, networks may receive high priority packets. In such case, other packets are delayed and the high priority ones are forwarded first. But such an action should not result in low priority or normal packets being delayed indefinitely. This criterion is called fairness.

There are many routing algorithms that are designed to implement one or more of the performance parameters discussed above. Some of the important algorithms are:

- Shortest path routing
- Flooding
- Hierarchical routing
- Broadcast routing

A shortest path may be determined based on one or more of the following factors:

- Link length
- Minimum local delay

- Minimum global delay
- Minimum cost
- Minimum number of hops.

Shortest path algorithm is one of the most popularly used ones. Flooding is a robust algorithm and is often used in military applications where delivery is critical. It is also very simple to implement. In flooding, an incoming packet is forwarded on all outgoing links except the one on which it arrived. The idea is that the packet will definitely be delivered to the destination via one of all the possible available routes. Hence, the algorithm is robust. Flooding generates a vast number of duplicate packets and can choke me network unless controlled. It can also cause loops easily. One of the reasons why a packet is not forwarded on the incoming link is to avoid looping. A variation of flooding is called controlled flooding. Here, a router remembers at the packets that it has forwarded. If the same packet returns to it, it is discarded straight away or after forwarding one or two more times. This is the control exercised.

Hierarchical routing maps the network in a hierarchy and forwards the packets via the appropriate hierarchical route. Broadcast routing is like flooding where the packet is sent even on the incoming route.

Self-Check Exercise

Note: i) Write your answers in the space given below.

ii) Check your answers with the answers given at the end of this Unit.

25) Distinguish between dynamic and static routing.

26) What is robustness in routing? Which algorithm is designed to meet robustness requirement?

.....

.....

.....

.....

8.15 SUMMARY

This unit deals with four basic aspects of data networks, viz. topology, media access control (MAC) protocols, address resolution and routing. Data networks are designed in different geometrical shapes. The geometrical shape of the network is called the topology of the network. There are a variety of topologies in use. This unit discusses the main topologies. These include star, bus ring, mesh, tree and hybrid topologies. The way data travels in a network need not necessarily correspond to the physical topology of the network. Data travel often defines its own topology and this is called the logical topology of the network. Logical topology is generally defined by way of set of rules called protocols. Two important protocols, viz. Ethernet and token passing ring have been discussed in detail. The merit of implementing these protocols using star physical topology has been explained. Certain bask: devices that are required to build topologies and interconnecting them have been described. These include hubs, switches, repeaters, bridges, and routers.

All data packets that traverse a network carry the source and destination addresses.

These addresses use different formats at different levels. When moving from one level to another, addresses have to be translated from one format to another. This function called address resolution is required at different levels in networks. Three important address formats and the techniques for their resolution are discussed in detail. User level name addresses are resolved to IP addresses by domain name servers (DNS). IP addresses are resolved to hardware interface unit addresses by address resolution protocols (ARP). After addresses are resolved, encapsulation is required before data transmission.

Finally, the functioning of routers and the features of some of the important routing protocols have been discussed. A router is one of the basic building blocks of Internet. Internet cannot function without routers. Local routers connect to LANs on the one side and the Internet on the other. Internet routers connect to other routers in the Internet. The connectivity is such that there are at least two routes to reach a destination. Routers execute routing algorithms to make routing decisions.

Routing algorithms may be dynamic or static. Dynamic algorithms adapt themselves to changing traffic conditions and network availability. Static algorithms use fixed routes for relatively long time durations. Static algorithms are relatively easy to implement. Routing algorithms are designed to satisfy certain performance parameters. They include minimum delay, minimum number of hope, robustness, stability and fairness. Routing protocols that satisfy one or more of the performance have been discussed briefly. They include shortest path routing, flooding, controlled flooding and hierarchical routing algorithms. Shortest path algorithm is the most widely used one. It takes into factors like minimum local and global delay, minimum number of hops to the destination etc.

8.16 ANSWERS TO SELF-CHECK EXERCISES

1) Packet size is 2^{11} bytes. File size is 1 MB, i.e. 2^{20} bytes. Therefore the number of packets to be transmitted is $2^{20}/2^{11} = 2^9$, i.e. 512 packets.

2) The logical paths through which packets can travel from C1 to C7 are:

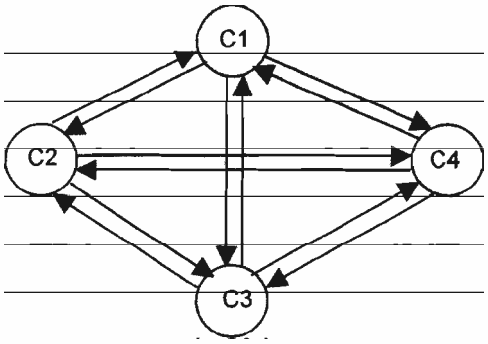
   - C1-C3-C5-C7
   - C1-C3-C5-C6-C7
   - C1-C2-C4-C5-C7
   - C1-C2-C4-C5-C6-C7

   There are a total of 4 logical paths constituting the logical topology of the network. The packet should not travel from C5 to C4, as it would result the packet going back to C1 and thus looping forever.

3) Yes. The packets of the same file may travel via different logical paths, as routing decision is taken for every packet independently. The problem that may arise is that the packets may arrive out of sequence at the destination. For example, consider a file having 10 packets. Packet 4 may be routed via longer route and Packet 5 via a shorter route. In such case, it is possible that Packet 5 arrives at the destination before Packet 4. The destination will have to take care of proper sequencing of the packets. For this purpose, whenever two or more packets of the same file are transmitted, the packets are tagged with a sequence number at the source so that the destination can sequence them properly. Packet numbering at the source and sequencing at the destination are taken care of high level protocols.

4) Half-duplex links carry information in only one direction. To support full-duplex communication, i.e. communication in both directions, we need two half-duplex links between every pair of computers. For a fully connected network with N computers, we need a total of N(N - 1)/2 full-duplex links or 2 x N(N -1)/2 half-duplex links. For 10 computers we need:

   2 x 10(10 -1)/2 = 2 x (10 x 9)/2 = 90 half-duplex links.



5) Fibre optic links are one-way (half-duplex) communication links. For two-way (full-duplex) communication, we need two optical fibre links between ever source and destination pair. The fully connected topology for four computers is shown in the Figure below. There are 12 links in the network. The formula

   N(N -1) links applies, i.e. 4 x 3 = 12.

6) The advantages of star topology are:

   - Ease of implementation
   - Ease of maintenance
   - Ease of administration: connection, disconnection etc.
   - It is a robust topology. If a link or a computer fails, the rest of the network is not affected
   - Flexibility for implementing different logical topologies, i.e. protocols including Ethernet protocol, token ring protocol and a switch.

7) The different logical topologies (or protocols) that can be implemented by a hub are Ethernet and token ring.

8) 20Base3 Ethernet system means an operating speed of 20 Mbps (mega bits per second) and the maximum distance covered is 300 meters.

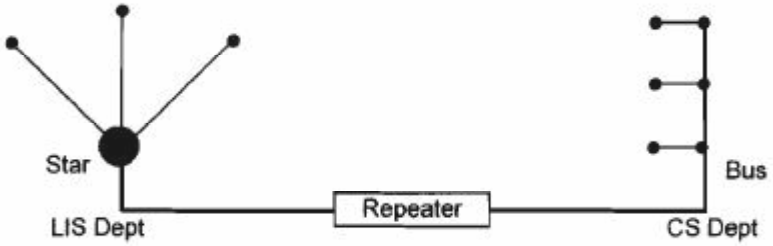
9) A station that seizes the token is expected to reintroduce the token on the ring after completing the data transmission. But it fails to so. In such a case, there will be no token on the ring. The token is said to have been lost. No other station can now transmit data and the ring is as good as 'dead'. Such a situation can be handled in the following way. When a station has data to send and finds no token or traffic on the ring for quite sometime, say 5 seconds, can introduce a new token on the ring. The new token can now be seized and new data transmissions can start.

10) Leaf nodes have no branches. Hence, the branching factor of leaf node is zero.

11) The number of nodes in a binary tree of depth 5 is (23 - 1) = 31. The number of point-to-point links is one less than the number of nodes, i.e. 30.

12) In tree topology, communication between adjacent nodes takes place by following a strict hierarchy. Hence, it is also called a hierarchical topology.

13) Both LIS and CS departments have Ethernet LAN, i.e. the same logical topology but different physical topologies. Since the departments are geographically far apart, signals will be attenuated. Hence, a repeater may be placed between the two buildings to boost the signal level as shown below.



14) If the CS department has a ring LAN, then the two protocols or the logical topologies are different. We need an intelligent device to transform packets from one format to another. Hence, we use a bridge instead of a repeater to interconnect the two departments. The bridge implements Ethernet protocol for the LIS department and the token ring protocol for the CS department. It performs necessary format conversion.

15) Comparison of repeaters and bridges:

Features	Repeater	Bridge
Signal amplification	Yes	Yes
Intelligent Device	No	Yes
Address Recognition	No	Yes
Packet Reformatting	No	Yes
Same Multiple Interfaces	Yes	Yes
Different Multiple Interfaces	No	Yes
Multiple Protocols	No	Yes

16) Carrier is a high frequency signal over which the data signals are superimposed.

17) AM broadcast frequencies lie in the range of 550 kHz to 1500 kHz. The AM Rajdhani channel in Delhi has a broadcast frequency of 666 kHz. Student is required to find out the broadcast frequency of an AM station nearby his/her city/town and record the answer.

18) There are two reasons as to why a collision may occur during retransmission attempt in Ethernet:

- The random wait time generated by two or more colliding stations might have been the same. For example, if two colliding stations generate random wait time as 0.1 sec by chance, then a collision will occur during retransmission attempt.
- A new station may join and start transmission at the same time when an old station is making a retransmission attempt.

19) A token is a specific bit pattern, say 7 ones and one zero (11111110). This pattern is unique such that it is not allowed to appear in the data.

20) Consider a token ring with 10 stations serially numbered. Let Station 2 seize the token and transmit data to Station 6. If Station 2 reintroduces the token, then the next station that would get the opportunity to transmit is Station 3. But if Station 6 reintroduces the token, then the next station that would get the opportunity to transmit is Station 7. Thus, the next station that gets opportunity to transmit changes in the two cases.

21) In data networks, destination addresses have different formats at different levels. This is required for easy implementation of a complex system. Address resolution is required to change addresses from one format to another.

22) Domain Name Server (DNS) resolves name string address provided by the user into a numerical IP address.

23) In all LANs, there is provision to broadcast information. On bus LANs using ARP the sending computer broadcasts the destination IP address of the packet. All other stations (NIC) on the LAN read this broadcast. Whichever NIC is attached to the computer that has mis IP address responds in reply. The sending computer now knows the NIC address to which the user information should be forwarded. Thus an IP address is resolved to NIC address.

24) The primary function of a router is to direct the user packets encapsulated with IP addresses in the direction of the destination. In this sense, the routers are much like telephone exchanges for the data networks. Telephone exchanges route the phone calls to the appropriate destination. Similarly, routers forward the data packets towards the destination. The telephone exchanges examine the number dialled to determine the destination. Routers examine the destination IP address in the incoming packets to decide the destination route.

25) Dynamic algorithms adapt themselves to changing traffic conditions and network availability. For example, traffic may suddenly increase in a particular segment. As a result, long queues of packets may build up slowing down the delivery to the destination. An adaptive algorithm may find an alternative route that may be longer but faster. Static algorithms use fixed routes for relatively long time durations. They do not monitor traffic conditions or the time to deliver. Static algorithms are relatively easier to implement when compared to dynamic algorithms. They also need less processing power, i.e. CPU time.

26) Robustness means the ability to reach the destination even when part of the network fails. A router should not forward a packet to a dead router on the way. In that case, the packet would never reach the destination. A robust routing algorithm would ensure that a packet is delivered to the destination at all costs. In other words there is guaranteed delivery. Flooding and controlled flooding are the routing algorithms designed to implement robustness.

8.17 KEYWORDS

Address Resolution : Given an address in one format, the process of obtaining the equivalent in another format

Algorithm : A step-by-step procedure for performing a task in a computer program

ARP : Address Resolution Protocol used to resolve IP addresses to NIC addresses in Ethernet LAN

Bridge : An intelligent device capable of interconnecting two dissimilar networks

Bus : A laid out open cable to which LAN computers are connected

Carrier Sensing : The process of checking whether a transmission is in progress on the bus of Ethernet LAN

Coaxial cable : A cable with an inner and an outer conductor placed coaxially and separated by insulating material. The overall structure is covered by a sheath

Collision Detection : The process of finding out if two or more stations are transmitting at the same time on one common medium

DNS : Domain Name Server used to resolve name string addresses into IP addresses.

Ethernet : A protocol used for exchange of information in bus or hub LAN

Flooding : A routing protocol that is robust

Hub : A device used in star configuration implementing one of the LAN protocols

Hybrid Topology : A network topology comprising two or more dissimilar network segments

LAN : Local Area Network

Media Access Control : A technique or protocol for controlling access to a common medium by multiple computers

Mesh : A network topology where computers are interconnected without any particular geometric shape in mind.

Multiple Access : Refers to where multiple computers access a common medium

NIC : Network Interface Card used in Ethernet LAN

Packet : A segment of information with specified length and structure

Protocol : A set of rules that govern the exchange of packets between computers

Repeater : A passive device that amplifies the signal level

Ring : LAN topology where computers are connected in the form of a ring

RIU : Ring Interface Unit used in ring LAN

Robustness : The ability of a routing algorithm to reach the destination even when part of the network fails

Router : A fundamental networking device used extensively in Internet to route packets towards their destination

Stability in Routing : The ability of routing algorithm to deliver packets as quickly as possible without the packets wandering here and there

Star : LAN topology configured with a central unit called hub

Switch : Networking device that switches incoming packets to output lines leading to their destinations

Token : A specific bit pattern use in token ring LAN

Token Ring : A LAN protocol for multiple access in the common ring

Tree : Network topology configured in the form of an inverted tree with the root at the top and the branches spanning downwards.

8.18 REFERENCES AND FURTHER READING

Mansfield, Kenneth C and Antonakos, James L. *An Introduction to Computer Networking*. New Delhi: Prentice Hall of India, 2002. Print

Tanenbaum. A. S. *Computer Networks*. 4th Ed. New Delhi: Prentice Hall of India, 2002. Print

Viswanathan. Thiagarajan. *Telecommunications Switching Systems and Networks*. New Delhi: Prentice Hall of India, 2008. Print

www.en.wikipedia.org/wiki