Don Bosco Institute of Technology

INTERNAL ASSESSMENT TEST II SOLUTION

CPC304: Computer Network | Max marks:20
18/8/16 | Time: 9:30 AM-10:30AM

- Attempt any five from 1a and 1f
- Attempt any one subquestion from the remaining two questions

<table>
<tr><td>Q.No.</td><td>Question</td></tr>
<tr><td>1 a</td><td>What is the position of transmission media in the OSI model or Internet Model? Classify transmission media.</td></tr>
<tr><td>Ans:</td><td>The transmission media is situated at the physical layer of the OSI model or Internet Model as shown in the Figure 1.

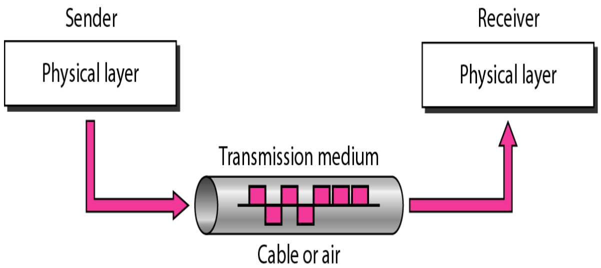


Figure 1: Transmission media and physical layer

Classification of transmission media is shown in Figure 2.

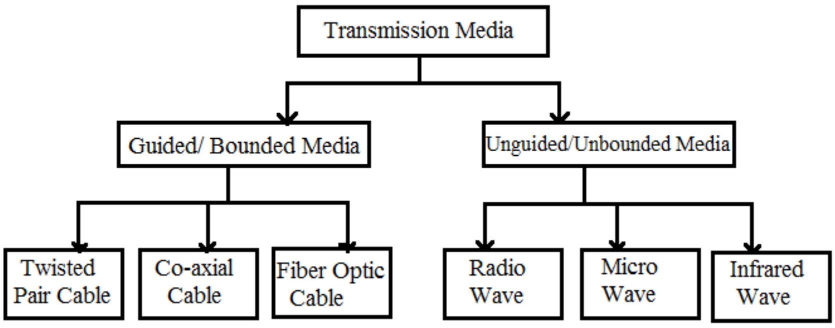
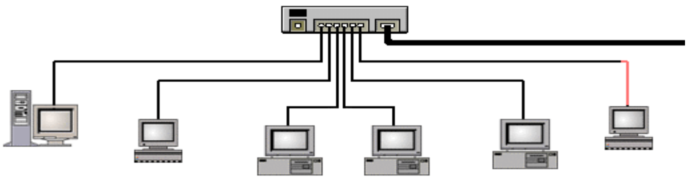
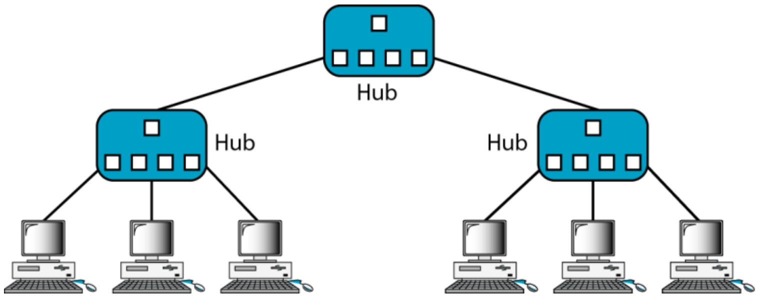


Figure 2: Classification of transmission media</td></tr>
<tr><td>1 b</td><td>Identify the purpose and function of the following networking devices and relate them to the OSI layer.

1. Hubs</td></tr>
</table>

	2. Routers
Ans	Hubs: Hubs are classified as passive hubs and active hubs. Passive hubs: A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.  **Figure 3 : Passive Hub** Active Hub: An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. hubs can also be used to create multiple levels of hierarchy, as shown in Figure 4. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).  **Figure 4 : Hierarchy of Hubs**
1 c	How many types of networks are defined by the bluetooth? Sketch the two types of network and discuss them.
Ans.	There are two types of networks defied by bluetooth as Piconet and Scatternet.

Piconet:

- A Bluetooth network is called a piconet, or a small net.
- It can have up to eight stations, one of which is called the master; the rest are called slaves.
- Maximum of seven slaves. Only one master.
- Slaves synchronize their clocks and hopping sequence with the master.
- But an additional eight slaves can stay in parked state, which means they can be synchronized with the master but cannot take part in communication until it is moved from the parked state.

Piconet is shown in Figure 5.

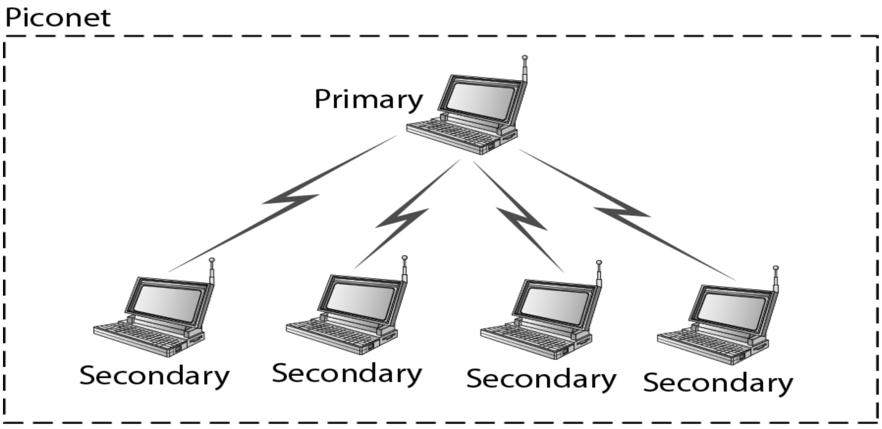
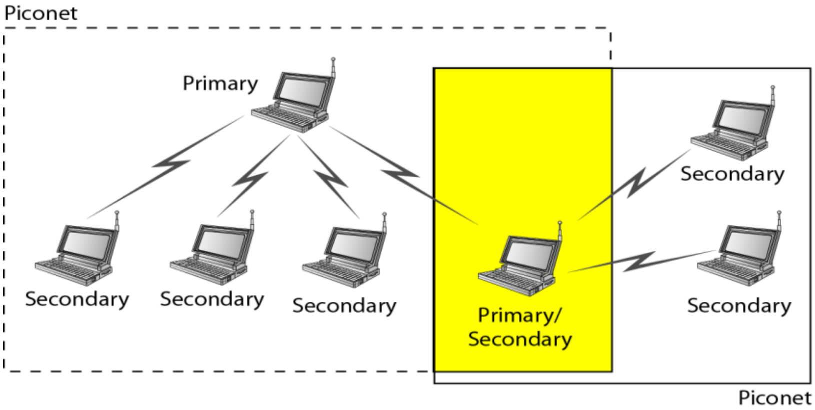
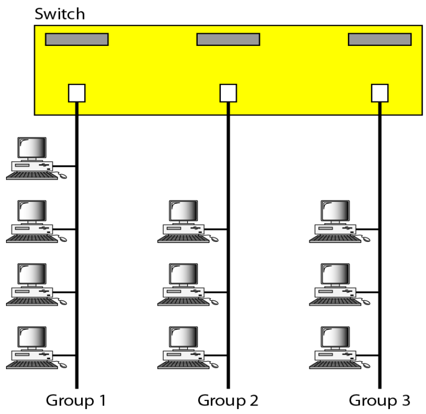


Figure 5: Piconet

Scatternet:

- Piconets can be combined to form what is called a scatternet.
- A slave station in one piconet can become the master in another piconet.
- Bluetooth devices has a built-in short-range radio transmitter.
- Scatternet is shown in Figure 6.

	 **Figure 6: Scatternet**
1 d	The figure shows a switched LAN in an engineering firm in which 10 stations are connected by a switch. The first four engineers work together as a first group, next three engineers works as the second group and the last three engineers works as a third group.  Figure 1 : Switch connecting three LANs The administrator needs to move two engineers from first group. to the third group to speed up the project being done by the third group. With repect to the above scenario state whether the following statement is True or False: VLAN can help adminstrator to perform the above task without physical rewiring. Justify your answer.
Ans.	With repect to the stated scenario the statement “VLAN can help adminstrator to perform the above task without physical rewiring.” is True. **Justification:**

If the administrators needed to move two engineers from the first group to the third group, to speed up the project being done by the third group? The LAN configuration would need to be changed. The network technician must rewire. The problem is repeated if, in another week, the two engineers move back to their previous group. In a switched LAN, changes in the work group mean physical changes in the network configuration.

Figure 7 shows the same switched LAN divided into VLANs. The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments. A LAN can be divided into several logical LANs called VLANs. Each VLAN is a work

group in the organization. If a person moves from one group to another, there is no need to change the physical configuration. The group membership in VLANs is defined by software, not hardware. Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN.

This means if a station moves from VLAN 1 to VLAN 2, it receives broadcast messages sent to VLAN 2, but no longer receives broadcast messages sent to VLAN 1. It is obvious that the problem in our previous example can easily be solved by using VLANs. Moving engineers from one group to another through software is easier than changing the configuration of the physical network.

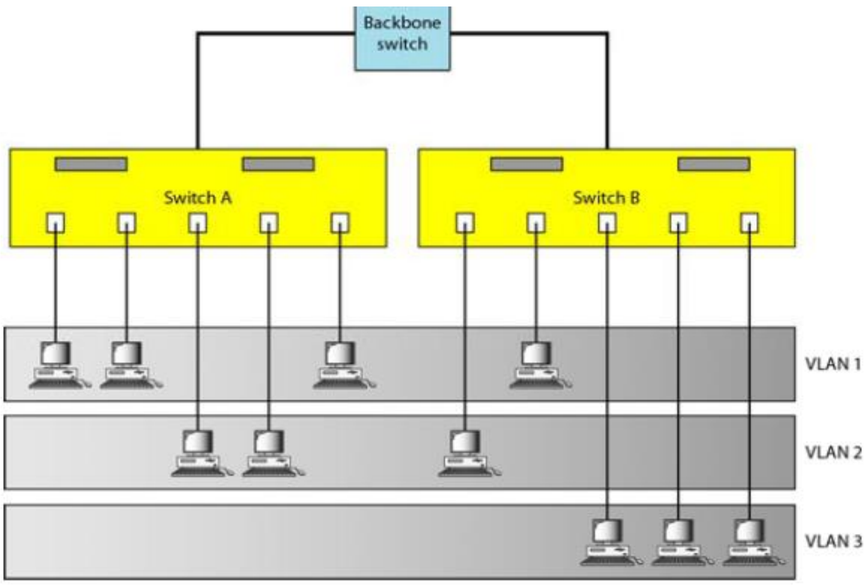


Figure 7: Two switches in a backbone using VLAN software

1 e	How does sky propagation is different from line of sight propagation? Sketch the both.

Ans. Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure 8.

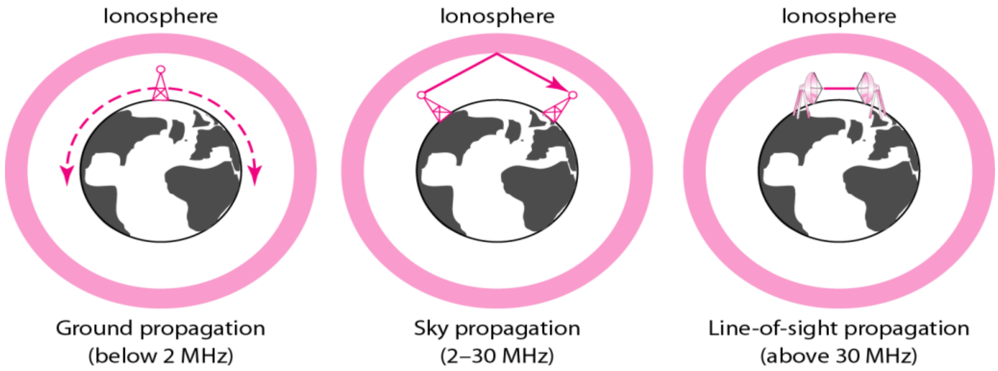


Figure 8: Propagation Methods

In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power. In line-or-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmission can not be completely focused.

1 f Differentiate between coaxial cable and fibre optic cable.

Ans Table 1 shows the difference between Coaxial cable and Fibre optic cable.

Table 1 : Difference between Coaxial cable and Fibre optic cable

Sr. No.	Coaxial Cable	Fibre Optic Cable
1	In coaxial cable, transmission of signal takes place in the electronic form over the inner conductor of the cable .	In Fibre optic cable, signal transmission takes place in an optical form over a glass fibre .
2	Coaxial having higher noise immunity than twisted pair cable.	Fibre optical fibre has highest noise immunity as the light rays are unaffected bv the ele3ctric noise.

	3	Coaxial cable is less affected due to external magnetic field.	Fibre optic cable is not affected by external magnetic field.
	4	Coaxial cable is moderate expensive.	Fibre optic cable is expensive.
	5	Coaxial cable has moderately high bandwidth.	Fibre optic cable has very high bandwidth.
	6	Coaxial cable has low attenuation.	Fibre optic cable has very low attenuation.
	7	Installation of coaxial cable is fairly easy.	Installation of fibre optic cable is difficult.

2 a	Identify the OSI layers that handles each of the following: 1. Dividing the transmitted bit stream into frames. 2. Determining which route through the subnet to use. Discuss these layers in detail in details. Also sketch the OSI/ISO layer and show the position of the identified layer in this diagram.
Ans	1. Dividing the transmitted bits into frames. This is handled by the data link layer. The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Other responsibilities of the data link layer include the following: Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames. Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one. Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver. Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame. Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

2. Determining which route through the subnet to use.
This is handled by the network layer. The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Other responsibilities of the network layer include the following:

Logical addressing: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

Routing: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

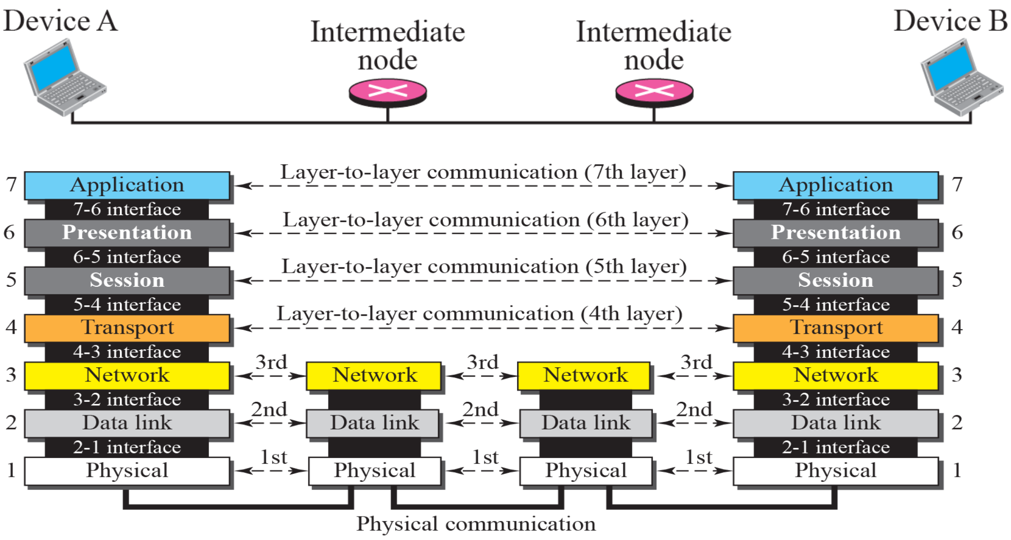


Figure 9 : OSI layer with data link layer and network layer

Figure 9 shows OSI layers with data link layer and network layer.

2 b Identify the topologies for the following scenario. Sketch the identified topologies with 4 devices. Discuss the topologies with advantages and disadvantages.

<table>
<tr><td></td><td>

1. In this topology every device has a dedicated point-to-point link to every other device.
2. In this topology each device has a a dedicated point-to-point connection with only the two devices on either side of it.

</td></tr>
<tr><td>Ans</td><td>

1. In this topology every device has a dedicated point-to-point link to every other device.

This is mesh topology.

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n (n - 1)$ physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. To accommodate that many links, every device on the network must have $n - 1$ input/output ports (see Figure 1.5) to be connected to the other $n - 1$ stations. Figure 10 shows mesh topology with 4 devices.

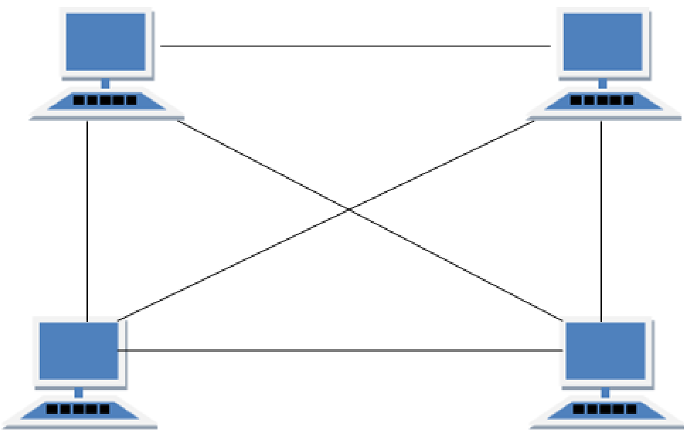


Figure 10: Mesh topology

Advantages of Mesh topology:

1. Yield the greatest amount of redundancy in the event that one of the nodes fails where network traffic can be redirected to another node.
2. Point-to-point link makes fault isolation easy.
3. Privacy between computers is maintained as messages travel along dedicated path.
4. Network problems are easier to diagnose.

Disadvantages of Mesh topology:

1. The amount of cabling required is high.

</td></tr>
</table>

2. A large number of I/O (input/output) ports are required.

2. In this topology each device has a a dedicated point-to-point connection with only the two devices on either side of it.

This is ring topology.

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. Figure 11 shows ring topology with 4 devices.

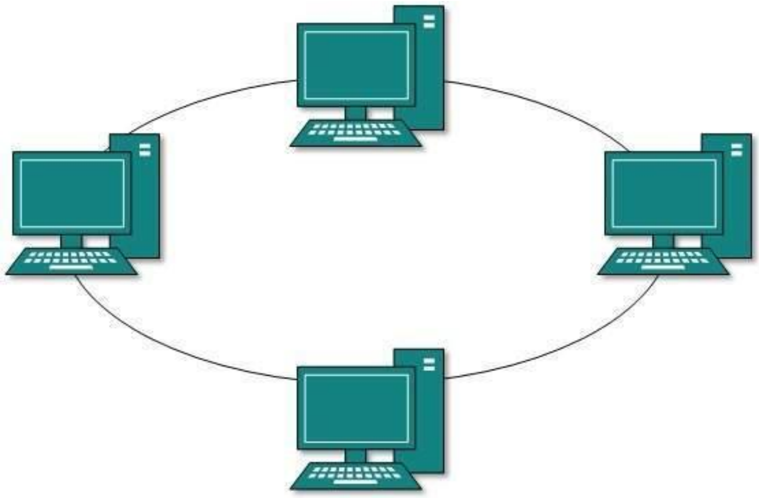


Figure 11: Mesh topology

Advantages of ring topology:

1. Ring networks offer high performance for a small number of workstations or for larger networks where each station has a similar workload.
2. Ring networks can span longer distances than other types of networks.
3. Ring networks are easily extendable.
4. Unlike Bus topology, there is no signal loss in Ring topology because the tokens are data packets that are re-generated at each node.

Disadvantages of ring topology:

1. Relatively expensive and difficult to install
2. Failure of one computer on the network can affect the whole network.
3. It is difficult to find fault in a ring network.
4. Adding or removing computers can disrupt the network.
5. It is much slower than an Ethernet network under normal load.

3 a	Calculate simple parity check code C(5,4) where data word size is 4 bits and codeword size is 5 bits. Assume the sender sends the data word 1011. The correct codeword is created from this data word and is sent to the receiver. Examine the following scenario and show which data word is created. i. No error occurred. ii. One single bit error changes a1
Ans	The most familiar error-detecting code is the simple parity-check code. In this code, a k-bit dataword is changed to an n-bit codeword where $n = k + 1$. The extra bit, called the parity bit, is selected to make the total number of 1s in the codeword even. Although some implementations specify an odd number of 1s, we discuss the even case. The minimum Hamming distance for this category is $d_{min} = 2$, which means that the code is a single-bit error-detecting code; it cannot correct any error. Table 2 is also a parity-check code with $k = 4$ and $n = 5$.

Table 2: Simple Parity Check code C(5,4)

Datawords	Codewords	Datawords	Codewords
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

The encoder uses a generator that takes a copy of a 4-bit dataword *(a0, a1, a2, a3)* and generates a parity bit *r0*. The dataword bits and the parity bit create the 5-bit codeword. The parity bit that is added makes the number of 1s in the codeword even. This is normally done by adding the 4 bits of the dataword (modulo-2); the result is the parity bit. In other words,

$$r_0 = a_3 + a_2 + a_1 + a_0 \qquad \text{(modulo-2)}$$

If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1. In both cases, the total number of 1s in the codeword is even.

The sender sends the codeword which may be corrupted during transmission. The receiver

	receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of Is in the received codeword is even; otherwise, it is 1. $s_0 = b_3 + b_2 + b_1 + b_0 + q_0 \quad \text{(modulo-2)}$ The syndrome is passed to the decision logic analyzer. If the syndrome is 0, there is no error in the received codeword; the data portion of the received codeword is accepted as the dataword; if the syndrome is 1, the data portion of the received codeword is discarded. The dataword is not created. Assume the sender sends the dataword 1011. The codeword created from this dataword is 10111, which is sent to the receiver. i. No error occurs; the received codeword is 10111. The syndrome is 0. The dataword 1011 is created. ii. One single-bit error changes aI' The received codeword is 10011. The syndrome is 1. No dataword is created.
3 b	Calculate the minimum hamming distance for coding scheme in the following Tables (Table 1 and Table 2). <table><tr><td>Dataword</td><td>Codeword</td></tr><tr><td>00</td><td>000</td></tr><tr><td>01</td><td>011</td></tr><tr><td>10</td><td>101</td></tr><tr><td>11</td><td>110</td></tr></table>**Table 1: Coding scheme 1** <table><tr><td>Dataword</td><td>Codeword</td></tr><tr><td>00</td><td>00000</td></tr><tr><td>01</td><td>01011</td></tr><tr><td>10</td><td>10101</td></tr><tr><td>11</td><td>11110</td></tr></table>**Table 2: Coding scheme 2** Discuss the relationship between the Hamming distance and error occuring during transmission.
Ans	The minimum hamming distance for coding scheme for the Table 1 is calculated as follows: <table><tr><td>Dataword</td><td>Codeword</td></tr><tr><td>00</td><td>000</td></tr><tr><td>01</td><td>011</td></tr></table>

10	101
11	110

Table 1 : Coding Scheme 1

$d(000, 011) = 2$ $d(000, 101) = 2$ $d(000, 110) = 2$ $d(011, 101) = 2$
$d(011, 110) = 2$ $d(101, 110) = 2$

The minimum hamming distance for Table 1 is dmin =2.

The minimum hamming distance for coding scheme for the Table 2 is calculated as follows:

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

Table 2 : Coding Scheme 2

$d(00000, 01011) = 3$ $d(00000, 10101) = 3$ $d(00000, 11110) = 4$
$d(01011, 10101) = 4$ $d(01011, 11110) = 3$ $d(10101, 11110) = 3$

The minimum hamming distance for Table 1 is dmin=3.

To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be dmin = s + 1.