USN □□□□□□□□□□

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A++ GRADE BY NAAC

Internal Assessment Test 1 – November 2024

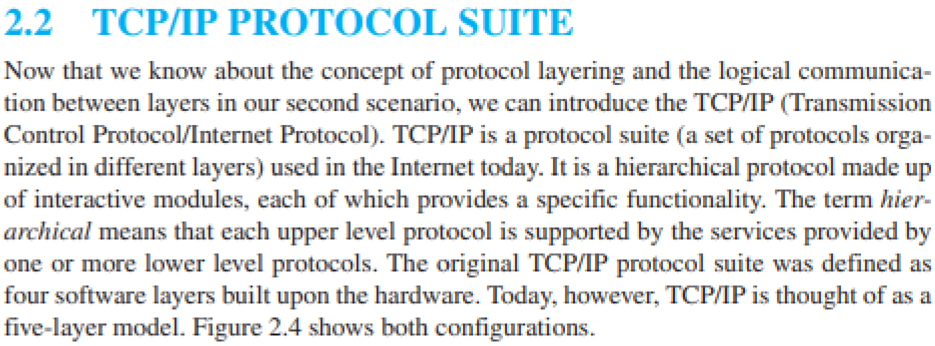
Sub:	Computer Networks				Sub Code:	BCS502	Branch:	CSE
Date:	08.11.2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	V (A, B & C)	OBE

<u>Answer any FIVE FULL Questions</u> MARKS CO RBT

		MARKS	CO	RBT
1 (a)	With the help of a neat diagram, explain the functionalities of each layer in TCP/IP Protocol.	7	CO2	L2

Layers and explanation - 5 Marks
Diagram - 2 Marks

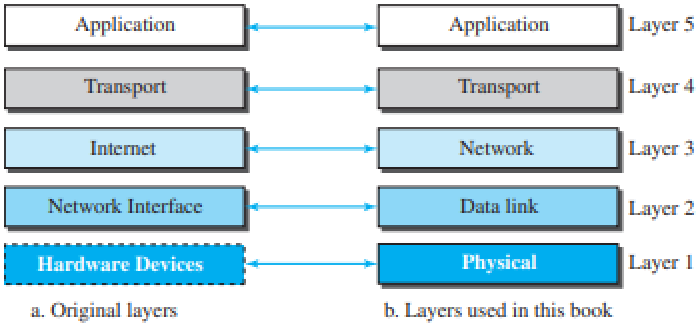
Solution



2.2 TCP/IP PROTOCOL SUITE

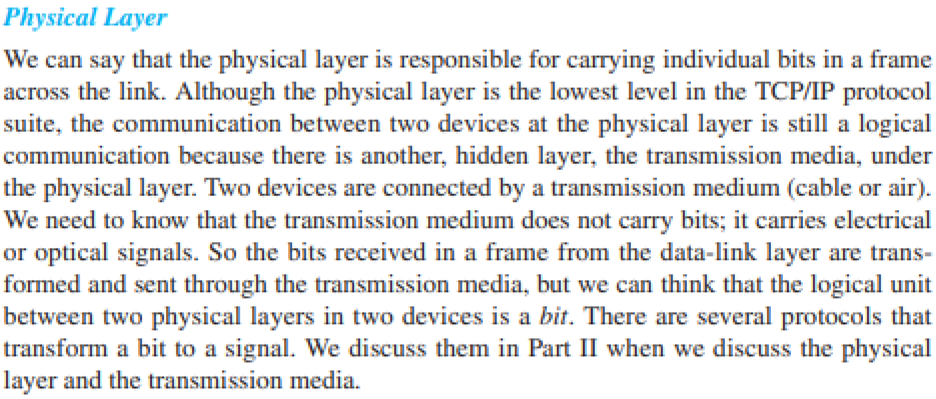
Now that we know about the concept of protocol layering and the logical communication between layers in our second scenario, we can introduce the TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term *hierarchical* means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model. Figure 2.4 shows both configurations.

Figure 2.4 *Layers in the TCP/IP protocol suite*



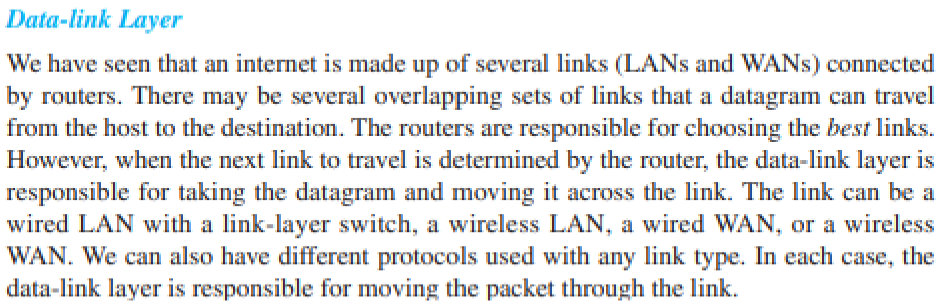
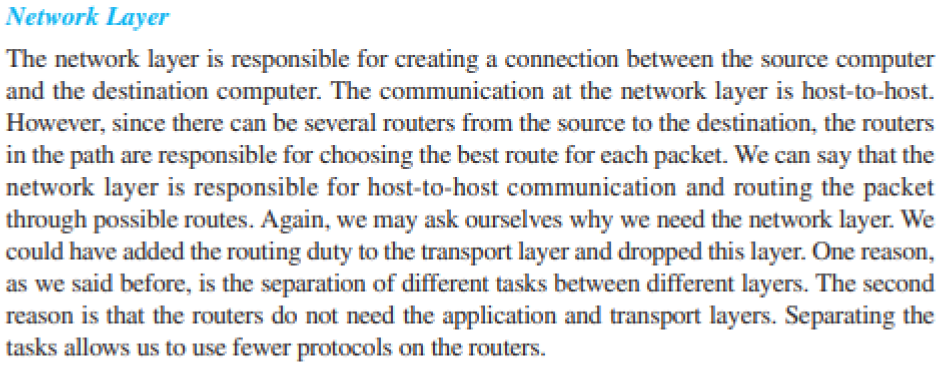
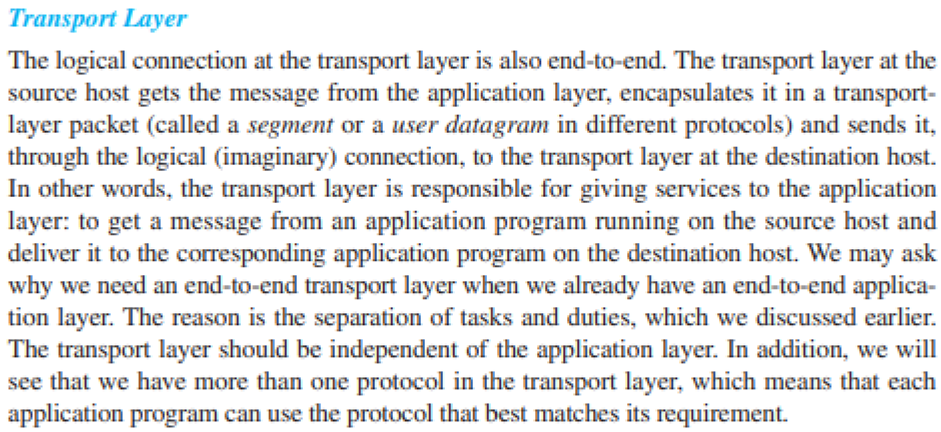
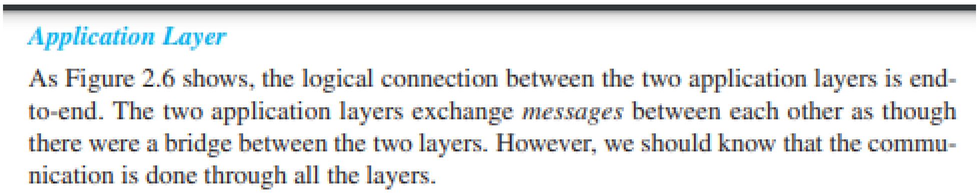
a. Original layers

b. Layers used in this book

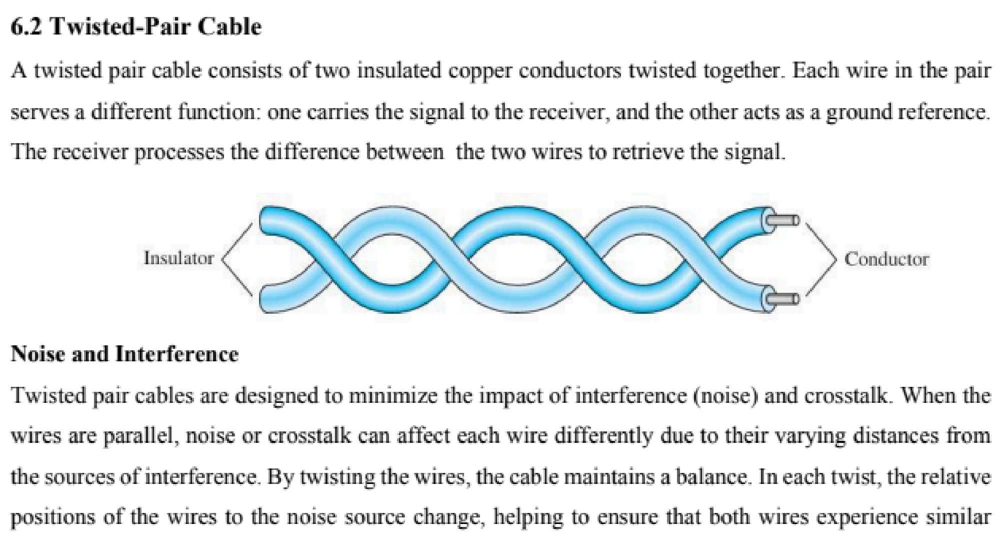


Physical Layer

We can say that the physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium (cable or air). We need to know that the transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a *bit*. There are several protocols that transform a bit to a signal. We discuss them in Part II when we discuss the physical layer and the transmission media.

	 *Data-link Layer* We have seen that an internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the *best* links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. We can also have different protocols used with any link type. In each case, the data-link layer is responsible for moving the packet through the link.  *Network Layer* The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet. We can say that the network layer is responsible for host-to-host communication and routing the packet through possible routes. Again, we may ask ourselves why we need the network layer. We could have added the routing duty to the transport layer and dropped this layer. One reason, as we said before, is the separation of different tasks between different layers. The second reason is that the routers do not need the application and transport layers. Separating the tasks allows us to use fewer protocols on the routers.  *Transport Layer* The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet (called a *segment* or a *user datagram* in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host. We may ask why we need an end-to-end transport layer when we already have an end-to-end application layer. The reason is the separation of tasks and duties, which we discussed earlier. The transport layer should be independent of the application layer. In addition, we will see that we have more than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement.  *Application Layer* As Figure 2.6 shows, the logical connection between the two application layers is end-to-end. The two application layers exchange *messages* between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers.			
1 (b)	Among circuit switched networks and packet switched networks, Identify the appropriate network to communicate the destination over a phone call. Provide proper justification for your answer. **Identifying the type of network - 1 Mark** **Justification - 2 Marks** **Solution** **The appropriate network to communicate the destination over a phone call is circuit switched network.** Circuit-switched networks establish a dedicated path for the entire duration of the call, ensuring a continuous and reliable connection. This dedicated line helps maintain real-time audio transmission with minimal latency and no interruptions, which is crucial for clear, seamless conversations. Unlike packet-switched networks that break data into packets sent independently (as seen in the Internet and VoIP),	3	CO1	L3

	circuit-switched networks offer consistent quality and steady bandwidth. This approach prevents packet loss, jitter, or delays that can degrade call quality. Hence, circuit-switched networks are optimal for traditional voice calls, providing the reliability and performance needed for uninterrupted communication.			
2 (a)	With a neat sketch explain Twisted pair cables, connectors of twisted pair cables. With a neat graph explain the performance of Twisted pair cables. **Twisted pair cables: 2 Marks** **Connectors : 2 Marks** **Performance : 2 Marks** **Solution**	6	CO1	L2



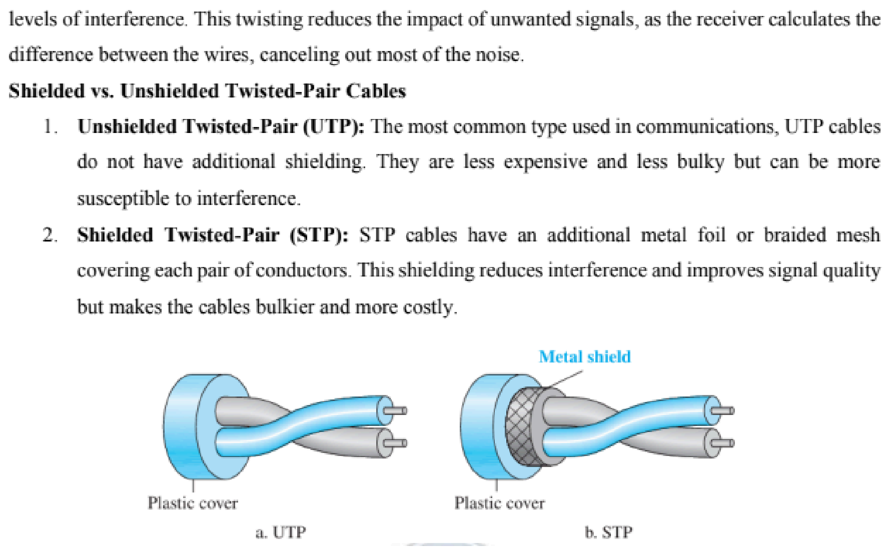
6.2 Twisted-Pair Cable

A twisted pair cable consists of two insulated copper conductors twisted together. Each wire in the pair serves a different function: one carries the signal to the receiver, and the other acts as a ground reference. The receiver processes the difference between the two wires to retrieve the signal.

Insulator
Conductor

Noise and Interference

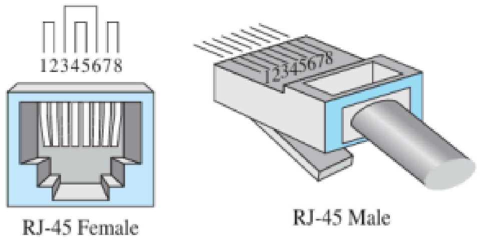
Twisted pair cables are designed to minimize the impact of interference (noise) and crosstalk. When the wires are parallel, noise or crosstalk can affect each wire differently due to their varying distances from the sources of interference. By twisting the wires, the cable maintains a balance. In each twist, the relative positions of the wires to the noise source change, helping to ensure that both wires experience similar

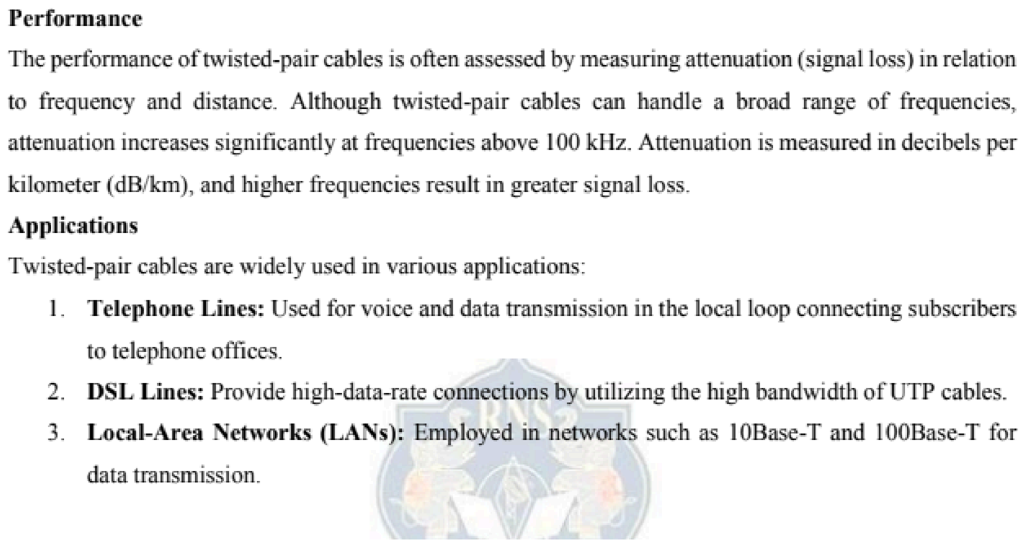


levels of interference. This twisting reduces the impact of unwanted signals, as the receiver calculates the difference between the wires, canceling out most of the noise.

Shielded vs. Unshielded Twisted-Pair Cables

1. **Unshielded Twisted-Pair (UTP):** The most common type used in communications, UTP cables do not have additional shielding. They are less expensive and less bulky but can be more susceptible to interference.
2. **Shielded Twisted-Pair (STP):** STP cables have an additional metal foil or braided mesh covering each pair of conductors. This shielding reduces interference and improves signal quality but makes the cables bulkier and more costly.





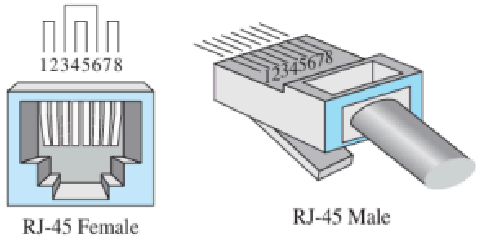
Performance

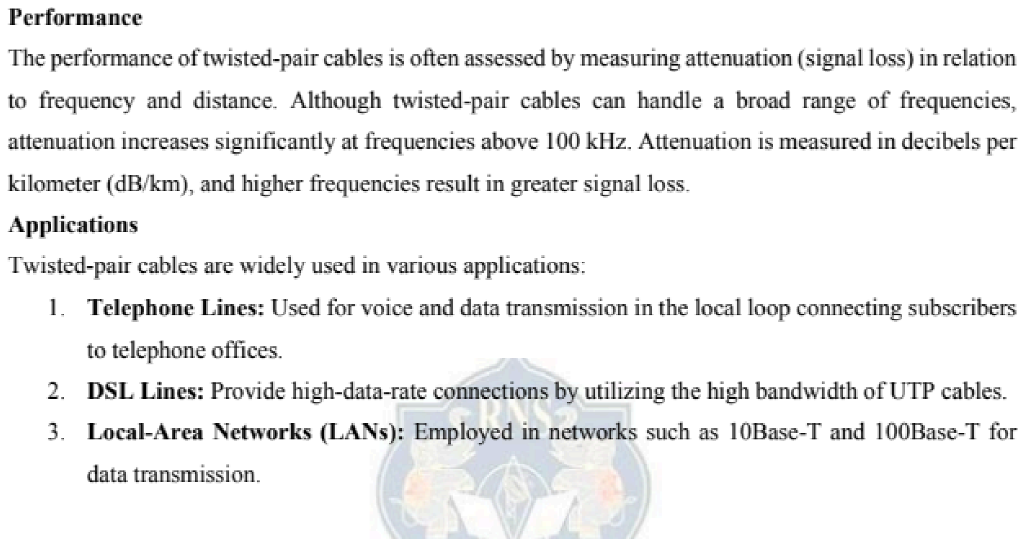
The performance of twisted-pair cables is often assessed by measuring attenuation (signal loss) in relation to frequency and distance. Although twisted-pair cables can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100 kHz. Attenuation is measured in decibels per kilometer (dB/km), and higher frequencies result in greater signal loss.

Applications

Twisted-pair cables are widely used in various applications:

1. **Telephone Lines:** Used for voice and data transmission in the local loop connecting subscribers to telephone offices.
2. **DSL Lines:** Provide high-data-rate connections by utilizing the high bandwidth of UTP cables.
3. **Local-Area Networks (LANs):** Employed in networks such as 10Base-T and 100Base-T for data transmission.





Performance

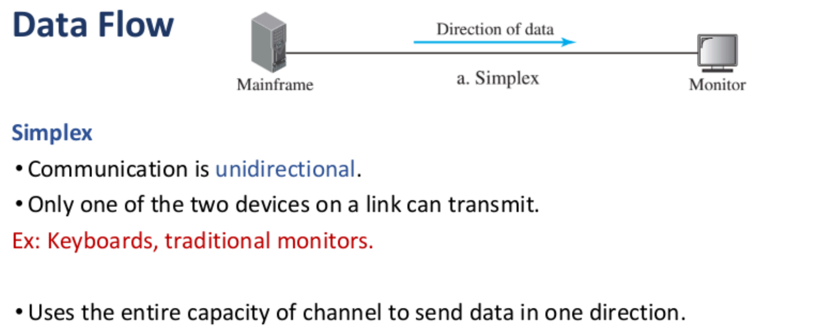
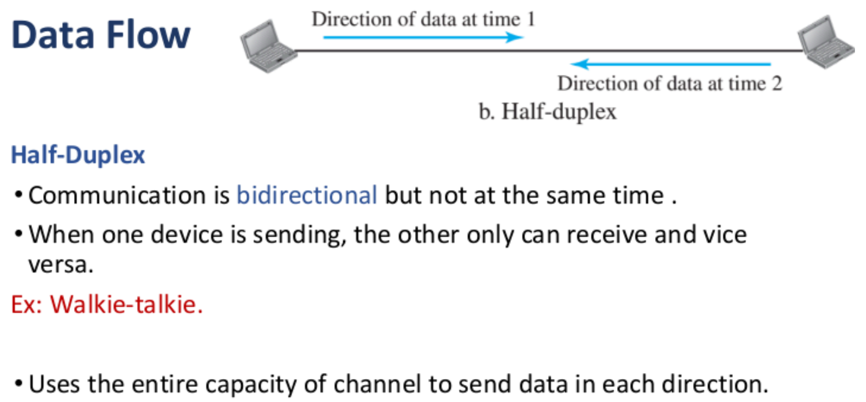
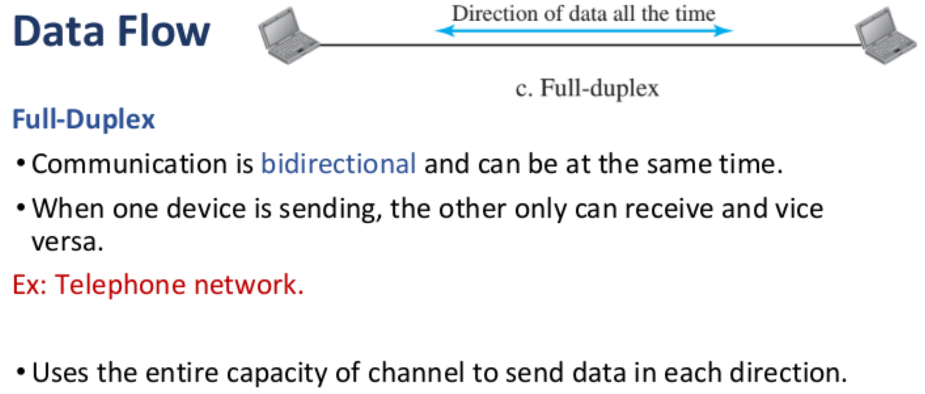
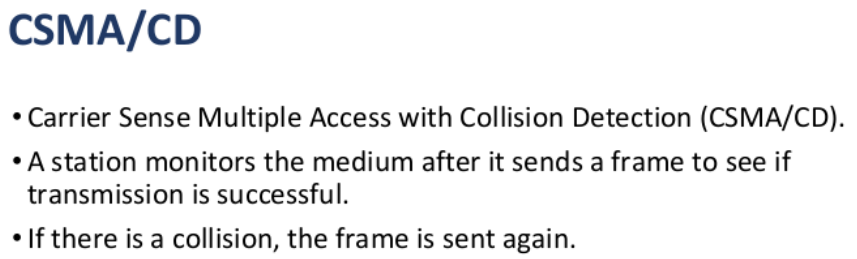
The performance of twisted-pair cables is often assessed by measuring attenuation (signal loss) in relation to frequency and distance. Although twisted-pair cables can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100 kHz. Attenuation is measured in decibels per kilometer (dB/km), and higher frequencies result in greater signal loss.

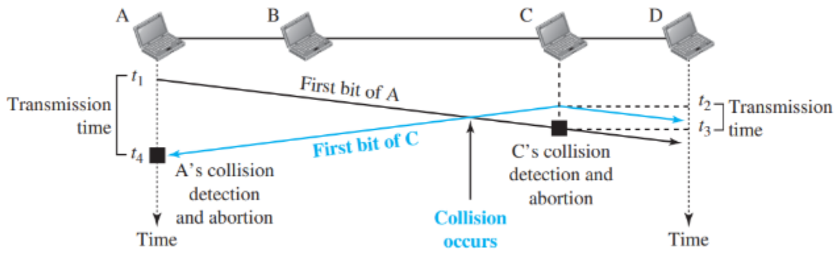
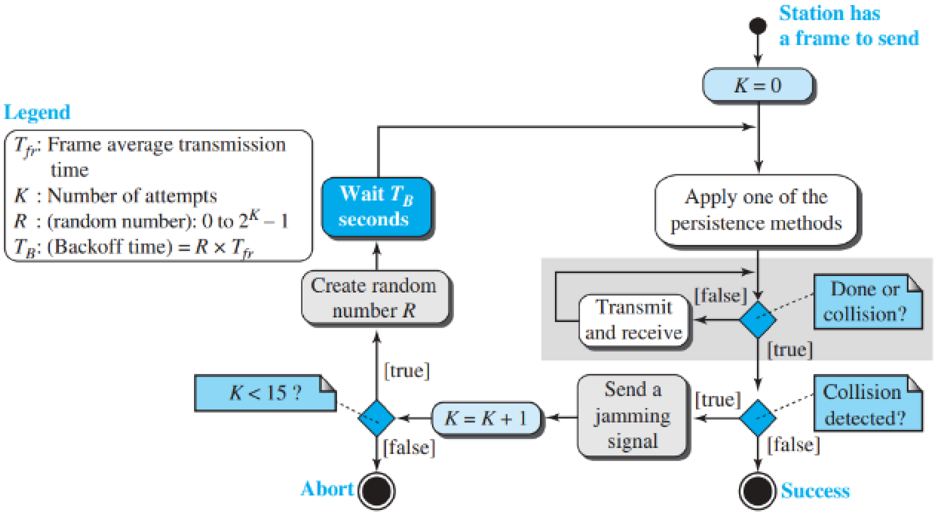
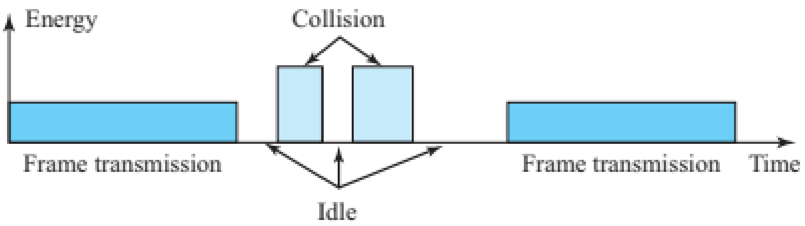
Applications

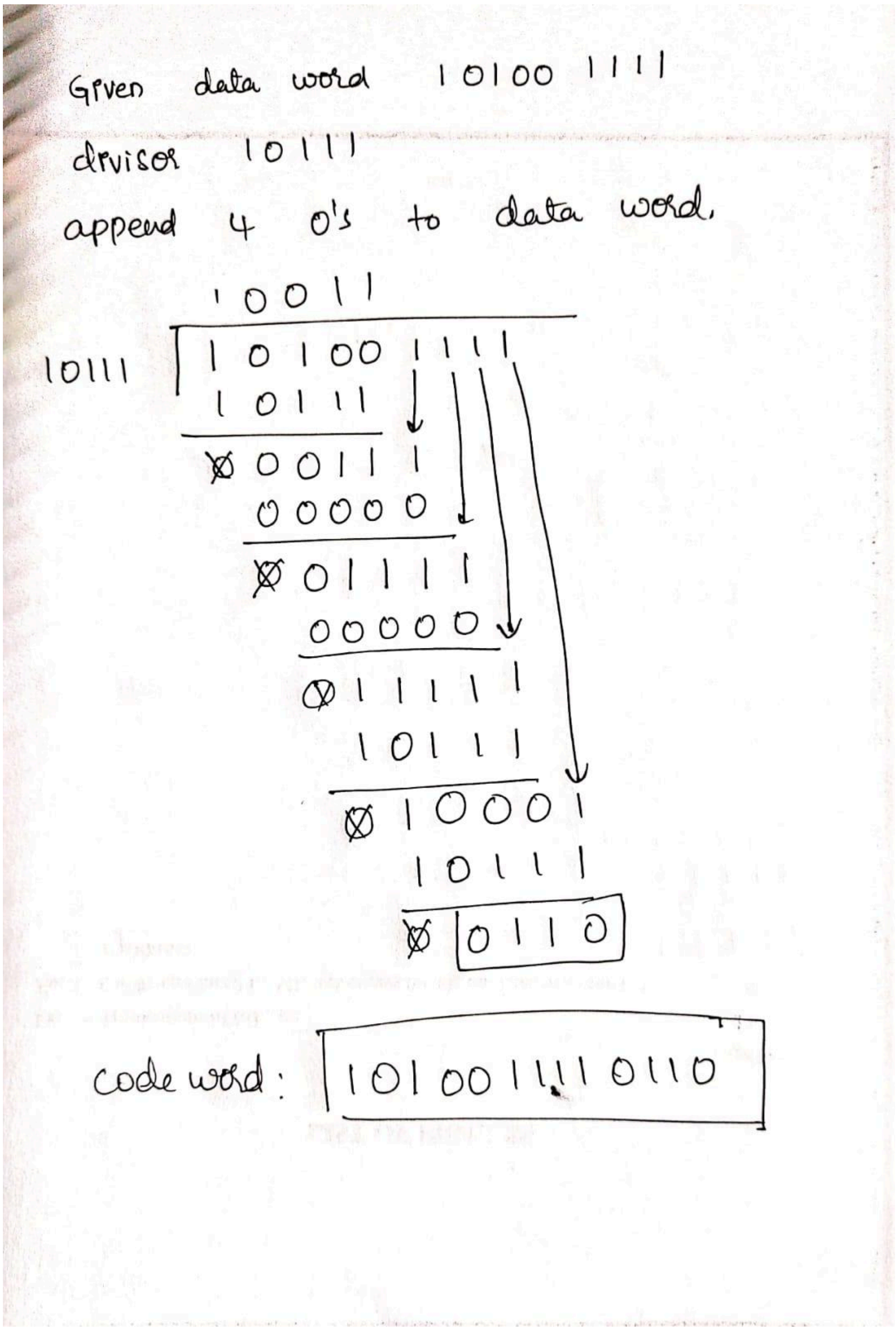
Twisted-pair cables are widely used in various applications:

1. **Telephone Lines:** Used for voice and data transmission in the local loop connecting subscribers to telephone offices.
2. **DSL Lines:** Provide high-data-rate connections by utilizing the high bandwidth of UTP cables.
3. **Local-Area Networks (LANs):** Employed in networks such as 10Base-T and 100Base-T for data transmission.

2 (b)	With the help of a neat diagram explain any two modes of data transmission/communication. **Any two modes = 2 + 2 Marks** **Solution**	2 + 2	CO1	L2

	 **Data Flow** **Simplex** - Communication is unidirectional. - Only one of the two devices on a link can transmit. Ex: Keyboards, traditional monitors. - Uses the entire capacity of channel to send data in one direction.  Direction of data at time 1 Direction of data at time 2 b. Half-duplex **Data Flow** **Half-Duplex** - Communication is bidirectional but not at the same time . - When one device is sending, the other only can receive and vice versa. Ex: Walkie-talkie. - Uses the entire capacity of channel to send data in each direction.  **Data Flow** **Full-Duplex** - Communication is bidirectional and can be at the same time. - When one device is sending, the other only can receive and vice versa. Ex: Telephone network. - Uses the entire capacity of channel to send data in each direction.			
3	Explain briefly the working of CSMA/CD for data transmission with the help of flow charts **Data Transmission - 2 Marks.** **Flow chart - 3 Marks.** **Explanation - 5 Marks.** **Solution**  **CSMA/CD** - Carrier Sense Multiple Access with Collision Detection (CSMA/CD). - A station monitors the medium after it sends a frame to see if transmission is successful. - If there is a collision, the frame is sent again.	10	CO1	L2

	The CSMA method does not specify the procedure following a collision. **Carrier sense multiple access with collision detection (CSMA/CD)** augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In Figure 12.11, stations A and C are involved in the collision. **Figure 12.11** *Collision of the first bits in CSMA/CD*  A B C D t_1 Transmission time t_4 First bit of A First bit of C t_2 t_3 Transmission time A's collision detection and abortion C's collision detection and abortion Collision occurs Time Time **Figure 12.13** *Flow diagram for the CSMA/CD*  Station has a frame to send $K = 0$ Legend T_{fr}: Frame average transmission time K : Number of attempts R : (random number): 0 to $2^K - 1$ T_B: (Backoff time) = $R \times T_{fr}$ Wait T_B seconds Apply one of the persistence methods Create random number R Transmit and receive [false] Done or collision? [true] $K < 15$? [true] $K = K + 1$ Send a jamming signal [true] Collision detected? [false] [false] Abort Success **Figure 12.14** *Energy level during transmission, idleness, or collision*  Energy Collision Frame transmission Frame transmission Time Idle			
4(a)	Given the data word 1 0 1 0 0 1 1 1 1 and the divisor 1 0 1 1, show the generation of CRC code word at the sender side. **Problem Solving : 4 Marks**	4	CO2	L3

	 Given data word 10100 1111 divisor 10111 append 4 0's to data word. 10011 10111) 1 0 1 00 1 1 1 1 1 0 1 11 Ø 0 0 1 1 1 0 0 0 0 0 Ø 0 1 1 1 1 0 0 0 0 0 Ø 1 1 1 1 1 1 0 1 1 1 Ø 1 0 0 0 1 1 0 1 1 1 Ø $\boxed{0110}$ code word: $\boxed{1010011110110}$			
4(b)	Explain briefly any two controlled access methods for data transmission **Any two methods = 3 + 3 Marks** **Solution**	6	CO2	L3

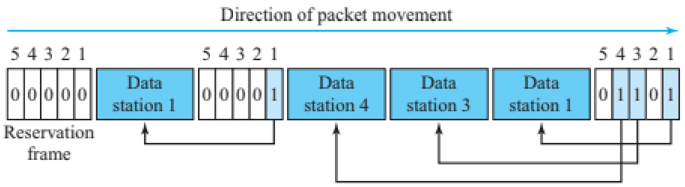
12.2.1 Reservation

In the **reservation** method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

If there are *N* stations in the system, there are exactly *N* reservation minislots in the reservation frame. Each minislot belongs to a station. When a station needs to send a data frame, it makes a reservation in its own minislot. The stations that have made reservations can send their data frames after the reservation frame.

Figure 12.18 shows a situation with five stations and a five-minislot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

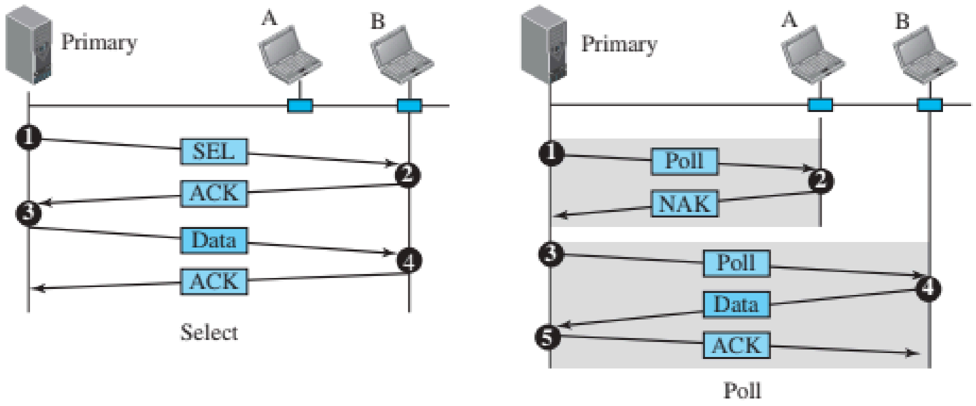
Figure 12.18 *Reservation access method*

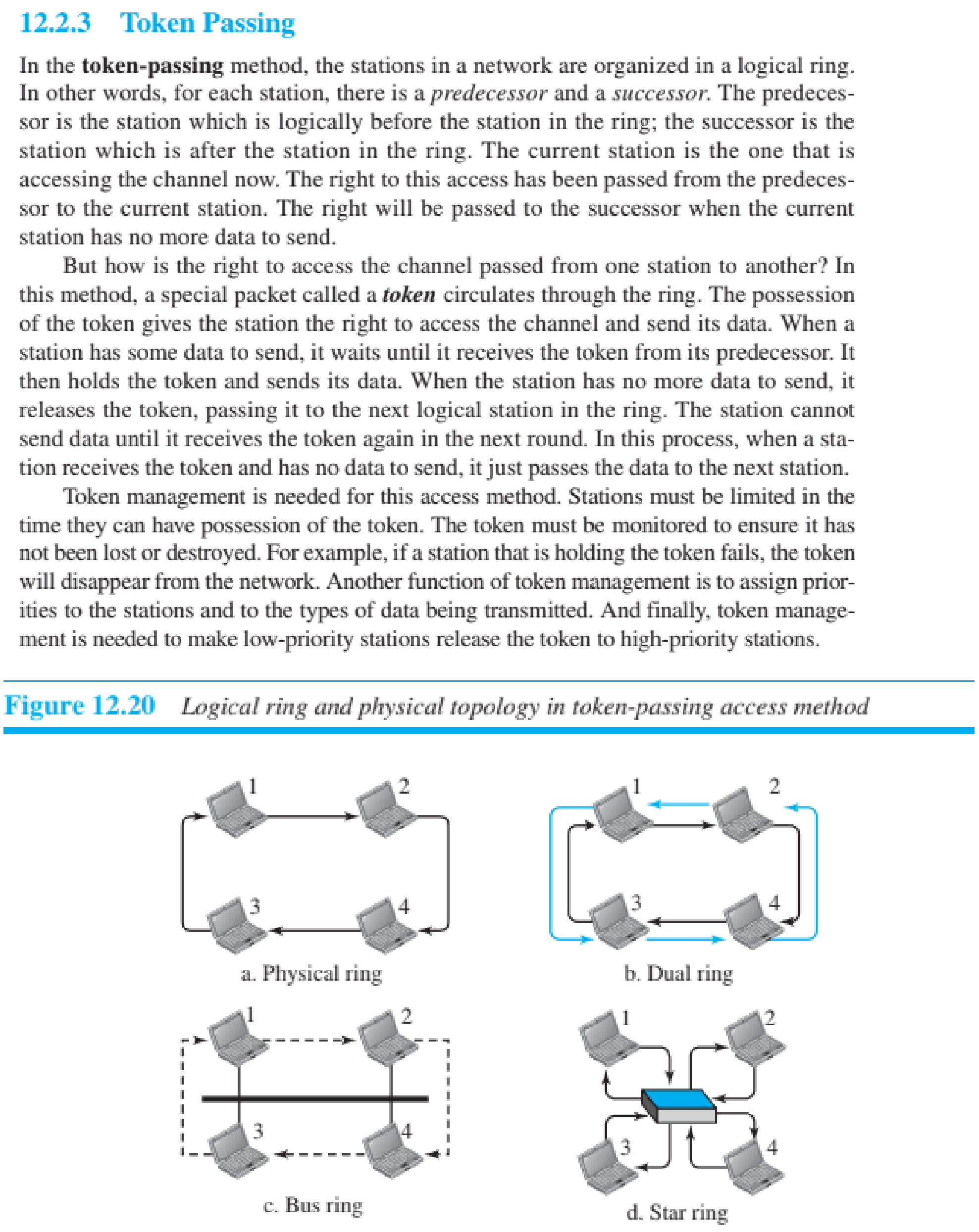


12.2.2 Polling

Polling works with topologies in which one device is designated as a ***primary station*** and the other devices are ***secondary stations***. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time. The primary device, therefore, is always the initiator of a session (see Figure 12.19). This method uses poll and select functions to prevent collisions. However, the drawback is if the primary station fails, the system goes down.

Figure 12.19 *Select and poll functions in polling-access method*





12.2.3 Token Passing

In the **token-passing** method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor* and a *successor*. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring. The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passed to the successor when the current station has no more data to send.

But how is the right to access the channel passed from one station to another? In this method, a special packet called a ***token*** circulates through the ring. The possession of the token gives the station the right to access the channel and send its data. When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring. The station cannot send data until it receives the token again in the next round. In this process, when a station receives the token and has no data to send, it just passes the data to the next station.

Token management is needed for this access method. Stations must be limited in the time they can have possession of the token. The token must be monitored to ensure it has not been lost or destroyed. For example, if a station that is holding the token fails, the token will disappear from the network. Another function of token management is to assign priorities to the stations and to the types of data being transmitted. And finally, token management is needed to make low-priority stations release the token to high-priority stations.

Figure 12.20 *Logical ring and physical topology in token-passing access method*

5	Define HDLC. Explain the frame format of HDLC with types. **Definition - 2 Marks** **Frame format - 4 Marks** **Types of Frames - 4 Marks** **Solution**	10	CO2	L2

HDLC

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- Implements stop and wait protocol.

HDLC provides two common transfer modes:

- Normal Response Mode (NRM)
- Asynchronous Balanced Mode (ABM)

Figure 11.14 *Normal response mode*

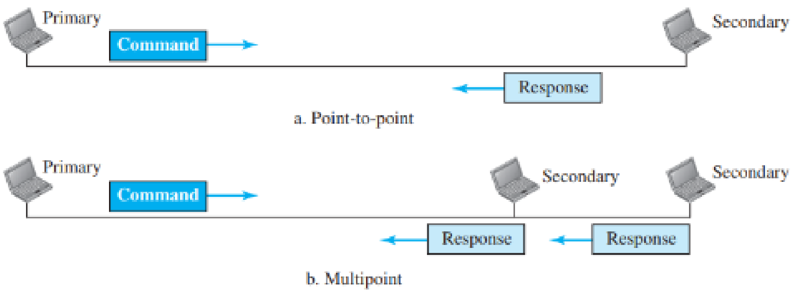
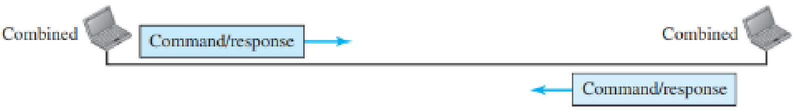


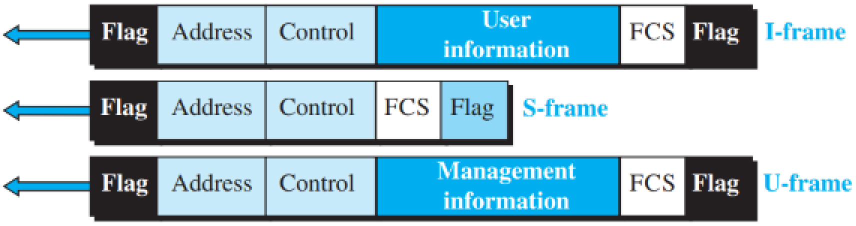
Figure 11.15 *Asynchronous balanced mode*



HDLC defines three types of frames:

- Information Frames (I-Frames)
- Supervisory frames (S-Frames)
- Unnumbered frames (U-Frames)

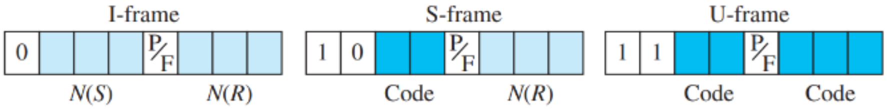
Figure 11.16 *HDLC frames*



Frames

- **Flag field:** Contains flag 01111110, which identifies both the beginning and the end of a frame.
- **Address field:** Contains the address of the secondary station.
- **Control Field**: One or two bytes used for flow or error control.
- **Information Field**: Contains the User's data from the network layer.
- **FCS Field**: Frame Check Sequence is the HDLC error detection field.

Figure 11.17 *Control field format for the different frame types*

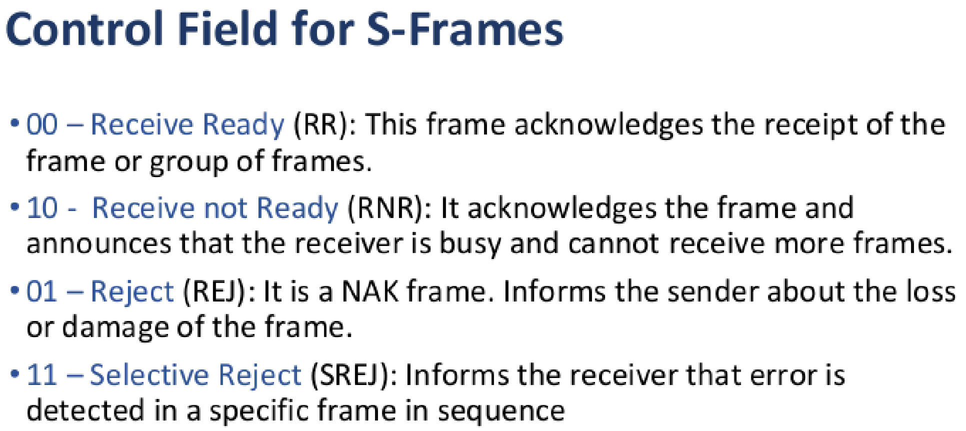
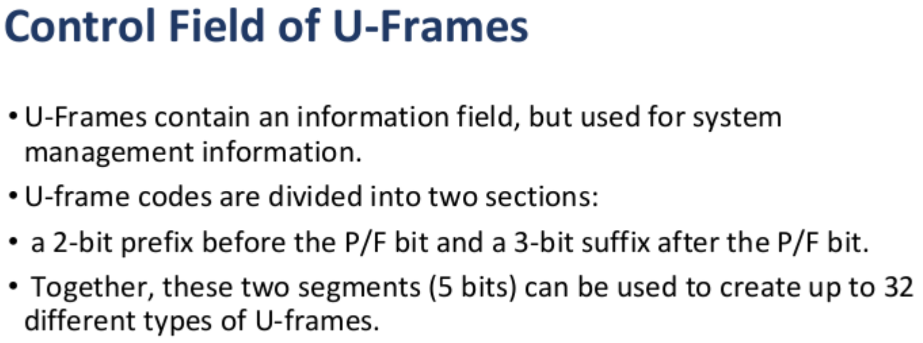
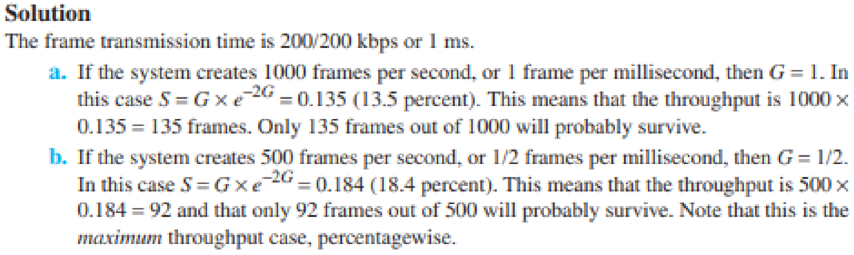
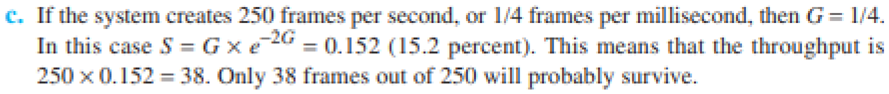


Control Field for I frames

- I-frames are designed to carry user data from network layer.
- First bit defines the type.
- If the first bit is 1, it is an I-Frame.
- Next 3 bits, defines a sequence number.
- Last N(R) corresponds to the acknowledgement number.
- P/F is poll or Final. If it is set to 1, it means frame is sent by primary to secondary.

Control Field for S-Frames

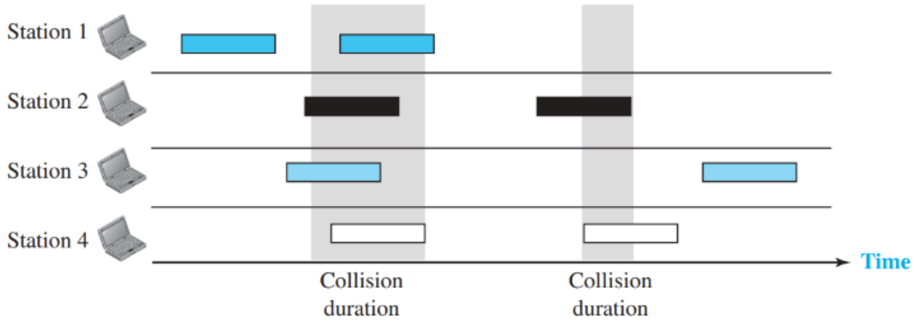
- Supervisory frames are used for flow and error control.
- S-Frames do not have information fields.
- If the first two bits are 10, then its an S-Frame.
- Last 3 bits, N(R) correspond to acknowledgement number (ACK) or NAK.
- The 2 bits called code are used to define S-Frame.

	 **Control Field for S-Frames** • 00 – Receive Ready (RR): This frame acknowledges the receipt of the frame or group of frames. • 10 - Receive not Ready (RNR): It acknowledges the frame and announces that the receiver is busy and cannot receive more frames. • 01 – Reject (REJ): It is a NAK frame. Informs the sender about the loss or damage of the frame. • 11 – Selective Reject (SREJ): Informs the receiver that error is detected in a specific frame in sequence  **Control Field of U-Frames** • U-Frames contain an information field, but used for system management information. • U-frame codes are divided into two sections: • a 2-bit prefix before the P/F bit and a 3-bit suffix after the P/F bit. • Together, these two segments (5 bits) can be used to create up to 32 different types of U-frames.			
6(a)	A pure ALOHA network transmits 200-bit frames on a shared channel of 200kbps. what is the throughput if the system produces : a. 1000 frames per second b. 500 frames per second c. 250 frames per second **Formula - 1 Mark** **Each problem - 1 Mark** **Solution**  **Solution** The frame transmission time is 200/200 kbps or 1 ms. **a.** If the system creates 1000 frames per second, or 1 frame per millisecond, then $G = 1$. In this case $S = G \times e^{-2G} = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive. **b.** If the system creates 500 frames per second, or 1/2 frames per millisecond, then $G = 1/2$. In this case $S = G \times e^{-2G} = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the *maximum* throughput case, percentagewise.  **c.** If the system creates 250 frames per second, or 1/4 frames per millisecond, then $G = 1/4$. In this case $S = G \times e^{-2G} = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.	4	CO2	L3
6 (b)	Briefly explain the working of pure ALOHA with the help of flow charts and also represent the vulnerable time with the help of neat graphs. **Flow chart - 2 Marks** **Explanation - 4 Marks**	6	CO2	L3

Solution

- ALOHA (Advocates of Linux Open-source Hawaii Association).
- Earliest Random Access method, developed in 1970 at university of Hawaii.
- The original ALOHA protocol is pure ALOHA.
- Idea is, each station sends a frame whenever it has a frame to send.
- Collision is possible due to single channel.

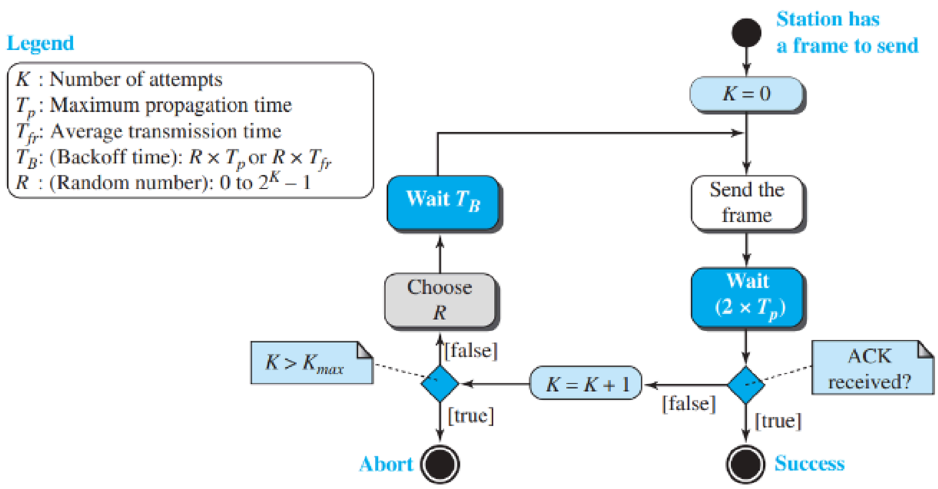
Figure 12.2 *Frames in a pure ALOHA network*



Pure ALOHA

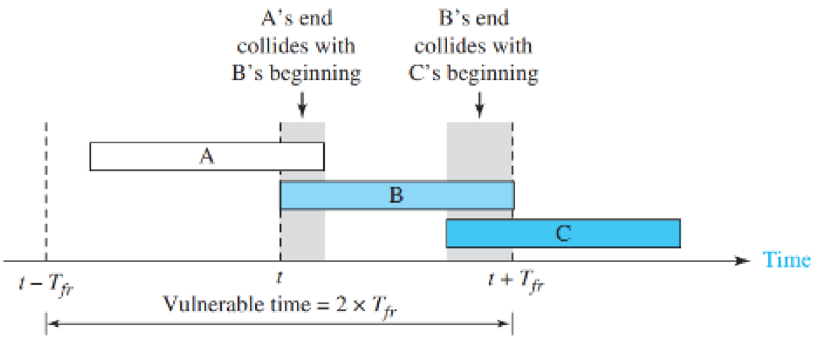
- Pure ALOHA protocol relies on acknowledgments from receiver.
- If acknowledgement is not received within the timer (time-out period), it resends the frame.
- If all stations resend the frames again, then collision happens.
- Each station waits a random amount of time before resending the frame.
- Backoff time T_B

Figure 12.3 *Procedure for pure ALOHA protocol*


Legend
K : Number of attempts
T_p : Maximum propagation time
T_{fr}: Average transmission time
T_B: (Backoff time): $R \times T_p$ or $R \times T_{fr}$
R : (Random number): 0 to $2^K - 1$
Station has a frame to send
$K = 0$
Send the frame
Wait $(2 \times T_p)$
ACK received?
[true]
Success
[false]
$K = K + 1$
$K > K_{max}$
[true]
Abort
[false]
Choose R
Wait T_B

- Length of time in which there is a possibility of collision.

Figure 12.4 *Vulnerable time for pure ALOHA protocol*



Throughput

- G is the average number of frames generated by the system during one frame transmission time.
- Successful transmissions are represented with S.
- Maximum throughput S_{max} is 0.184 where G = ½.

The throughput for pure ALOHA is $S = G \times e^{-2G}$.
The maximum throughput $S_{max} = 1/(2e) = 0.184$ when $G = (1/2)$.

CI **CCI** **HOD**