MODULE 2

CHAPTER 1 –DATA LINK LAYER

CO – Students will be able to summarize the datalink layer responsibilities and protocols

Prepared By Mr. EBIN PM, Chandigarh University, Punjab

DLL DESIGN ISSUES

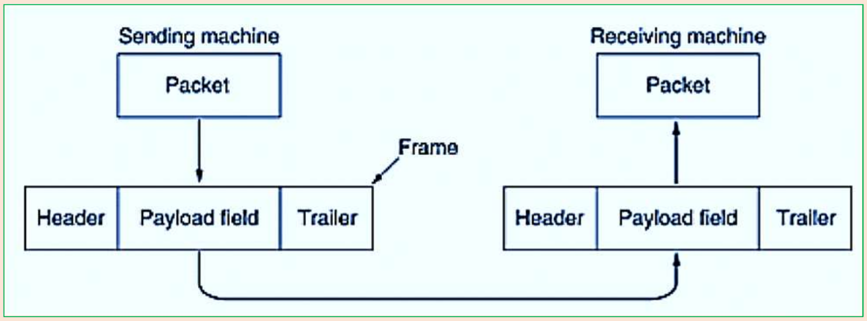
- Specific responsibilities of the data link layer include framing, addressing, flow control, error control, and media access control.

1. FRAMING

- The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame.
- Each frame contains a frame header, a payload field for holding the packet, and a frame trailer

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 2

Relationship between packets and frames.



❖**Fixed-Size Framing** - In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

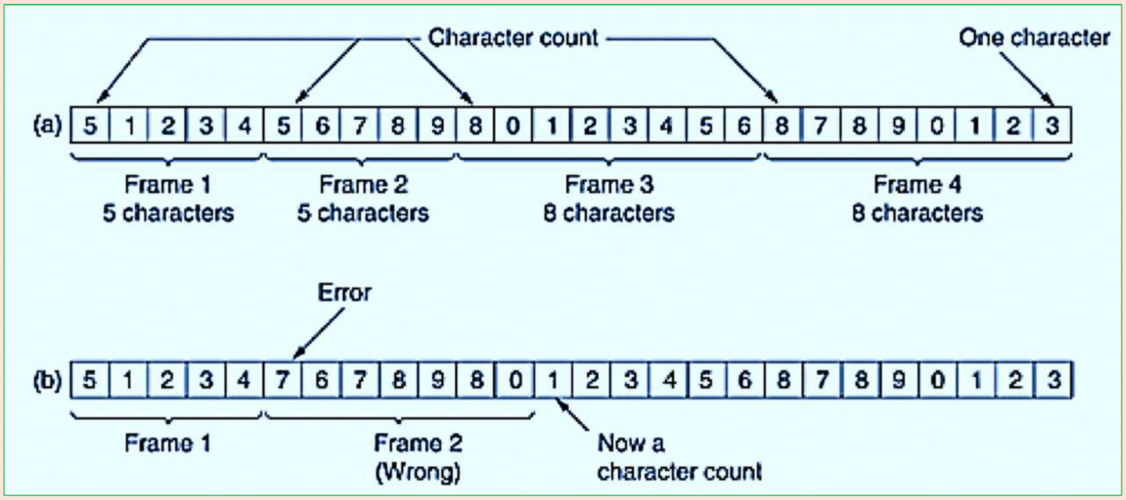
Eg: ATM wide-area network

❖Variable-Size Framing

- In variable-size framing, we need a way to define the end of the frame and the beginning of the next.
- The approaches were used for this purpose are:

A. Character Count

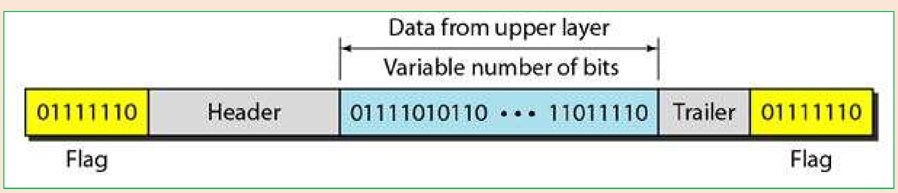
- It uses a field in the header to specify the number of characters in the frame.
- When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of the frame is.



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 5

B. Flag bytes with byte stuffing

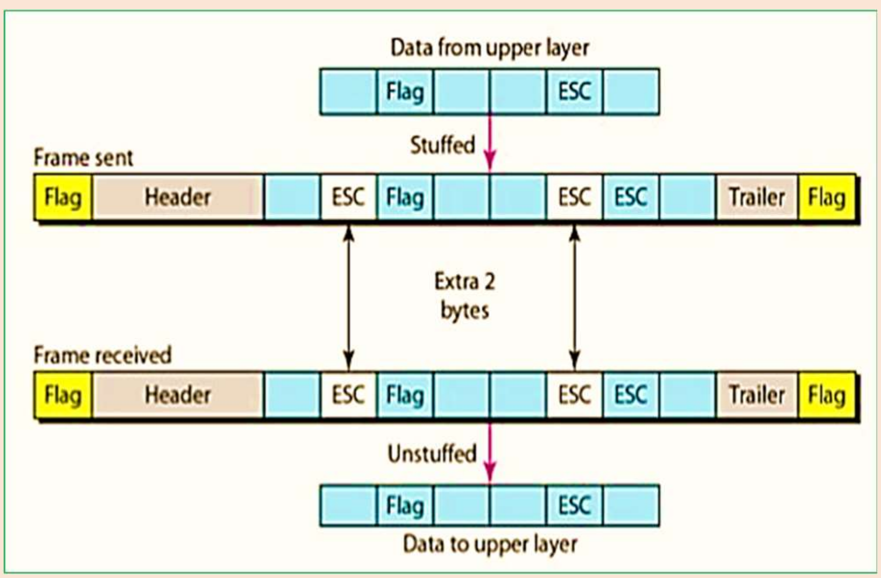
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.

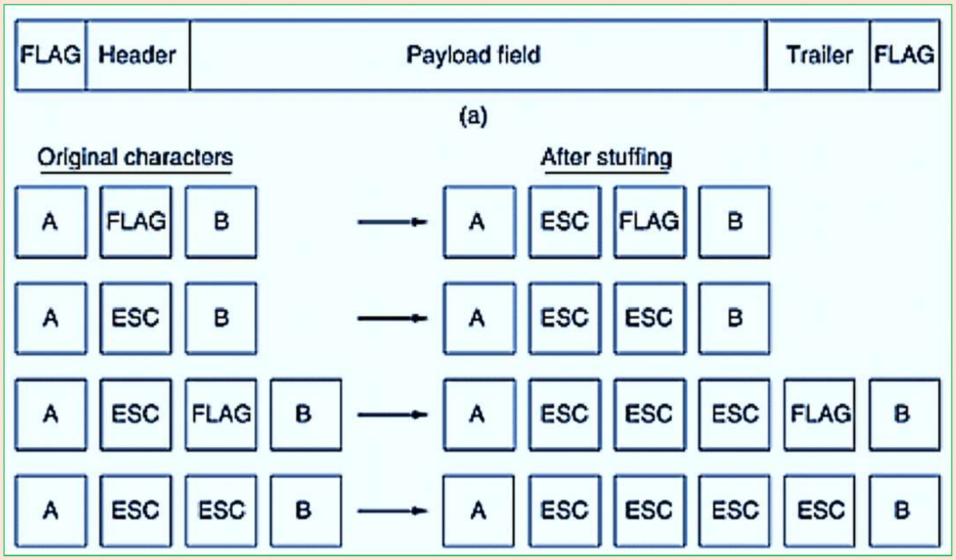


- Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame.
- To fix this problem, In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 6

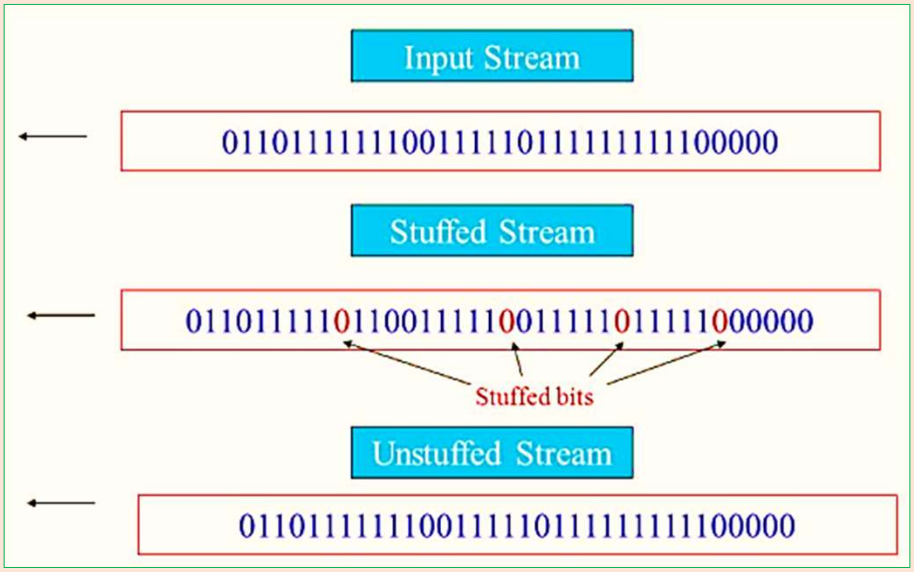
- This byte is usually called the escape character (ESC) which has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.
- If the text contains one or more escape characters followed by a flag, the receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame.
- To solve this problem, the escape characters that are part of the text must also be marked by another escape character.
- In other words, if the escape character is part of the text, an extra one is added to show that the second one is part of the text.





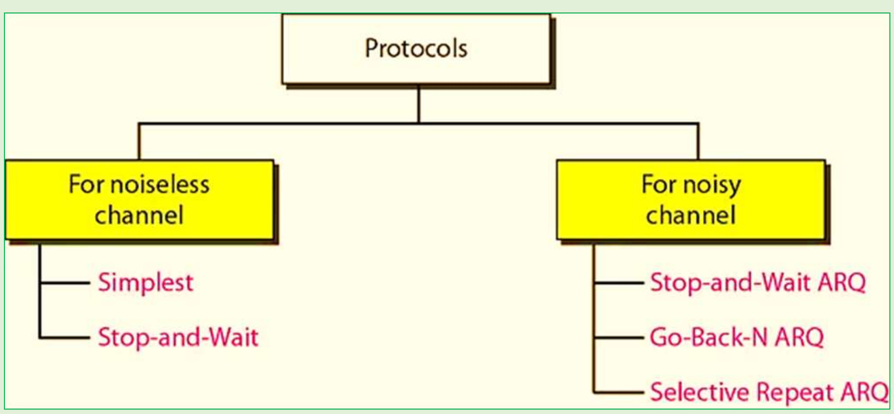
C. Bit Stuffing

- Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame
- That is, if the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame.
- We do this by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing.
- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.



2. ERROR CONTROL

- Error control is both error detection and error correction.
- Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

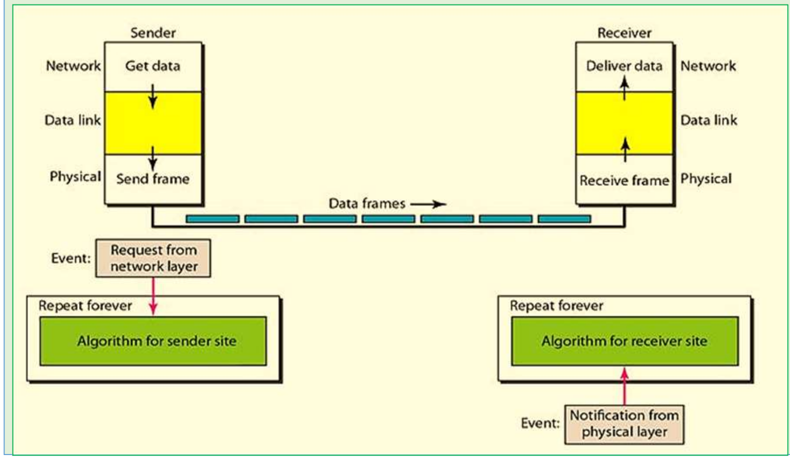


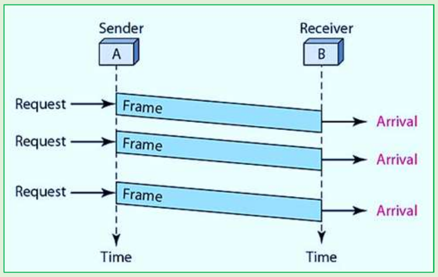
❖NOISELESS CHANNELS

1. Simplest Protocol

- No flow control and error control
- It is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver.
- There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it.
- The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer.

- The data link layers of the sender and receiver provide transmission services for their network layers. The data link layers use the services provided by their physical layers (such as signaling, multiplexing, and so on) for the physical transmission of bits.



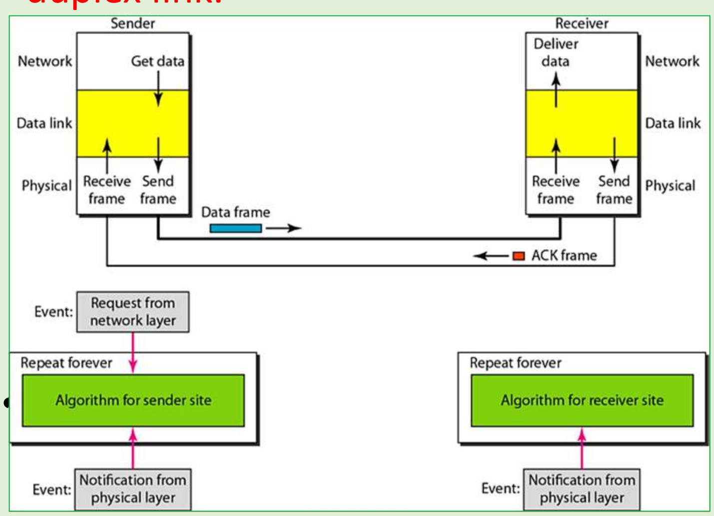


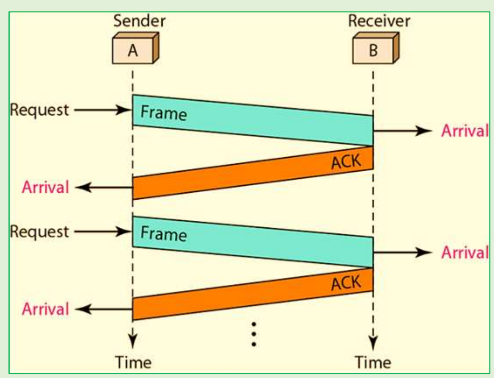
Flow Diagram

2. Stop-and-Wait Protocol

- To prevent the receiver from becoming overwhelmed with frames, we somehow need to tell the sender to slow down. There must be feedback from the receiver to the sender.
- In Stop-and-Wait Protocol , the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.
- We still have unidirectional communication for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction.
- We add flow control to our previous protocol. After a frame is sent, the algorithm must ignore another network layer request until that frame is acknowledged.

- At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. We therefore need a half-duplex link.





Flow Diagram

❖NOISY CHANNELS

1. Stop-and-Wait Automatic Repeat Request

- It adds a simple error control mechanism to the Stop-and-Wait Protocol
- To detect and correct corrupted frames, we need to add redundancy bits to our data frame .When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver.
- Lost frames are more difficult to handle than corrupted ones. The received frame could be the correct one, or a duplicate, or a frame out of order. The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.

- The lost frames need to be resent in this protocol. the sender keeps a copy of the sent frame. At the same time, it starts a timer.
- If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted.
- Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.
- Since an ACK frame can also be corrupted and lost, it too needs redundancy bits and a sequence number. The ACK frame for this protocol has a sequence number field. In this protocol, the sender simply discards a corrupted ACK frame or ignores an out-of-order one

➢Sequence Numbers

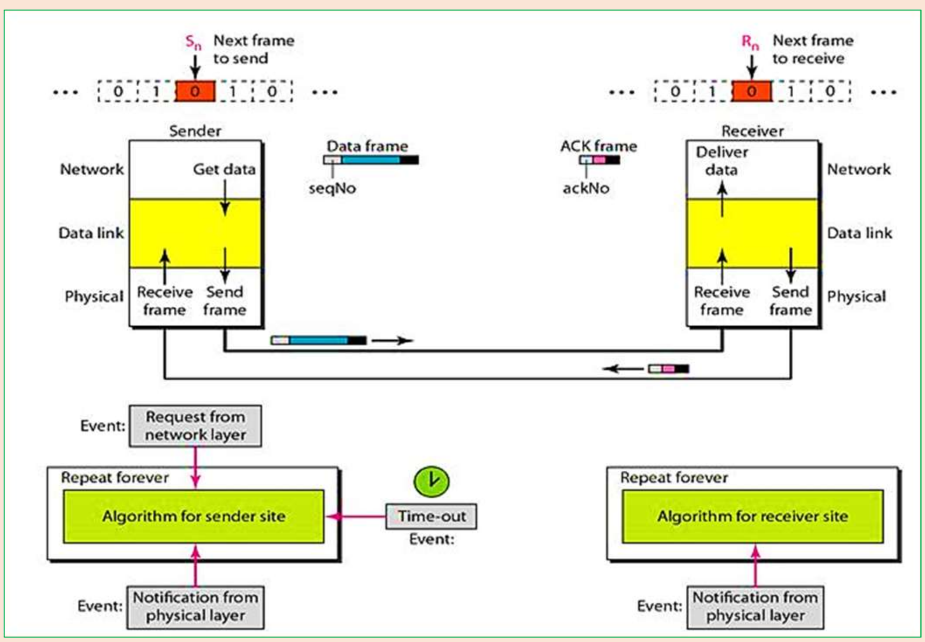
- The frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame.
- One important consideration is the range of the sequence numbers. Since we want to minimize the frame size, we look for the smallest range.
- Assume we have used **x** as a sequence number; we only need to use **x + 1** after that. There is no need for **x + 2**.
- To show this, assume that the sender has sent the frame numbered x. Three things can happen.

1. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment. The acknowledgment arrives at the sender site, causing the sender to send the next frame numbered x + 1.
2. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment, but the acknowledgment is corrupted or lost. The sender resends the frame (numbered x) after the time-out. Note that the frame here is a duplicate. The receiver can recognize this fact because it expects frame x + I but frame x was received.
3. The frame is corrupted or never arrives at the receiver site; the sender resends the frame (numbered x) after the time-out.

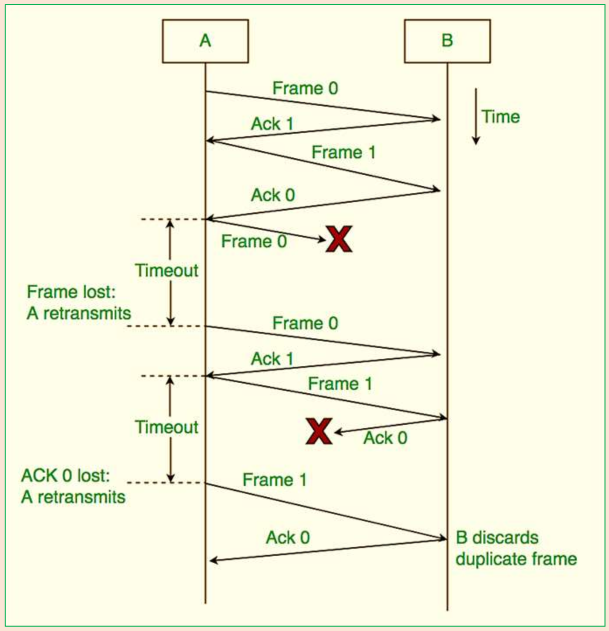
➢We can see that there is a need for sequence numbers x and x + I.

➢Acknowledgment Numbers

- The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver.
- For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next).



Flow diagram



2. Go-Back-N Automatic Repeat Request

- In this protocol we can send several frames before receiving acknowledgments.
- We keep a copy of these frames until the acknowledgments arrive.

➢ Sequence Numbers

- Frames from a sending station are numbered sequentially. Because we need to include the sequence number of each frame in the header, we need to set a limit.
- If the header of the frame allows m bits for the sequence number, the sequence numbers range from **0 to 2^m - 1**. For example, if m is 4, the only sequence numbers are 0 – 15. However, we can repeat the sequence. So the sequence numbers are

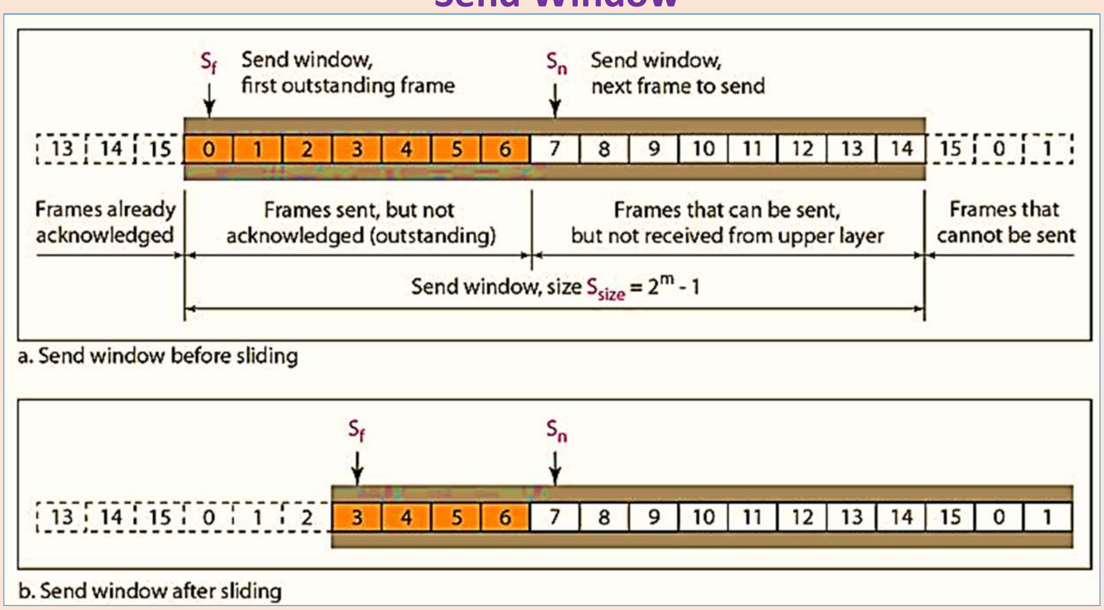
0, 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,0,1,2,3,4,5,6,7,8,9,10, 11, ...

- In the Go-Back-N Protocol, the sequence numbers are modulo 2^m , where m is the size of the sequence number field in bits.

➢Sliding Window

- The sliding window is an abstract concept that defines the range of sequence numbers .
- The sender and receiver need to deal with only part of the possible sequence numbers.
- The window at any time divides the possible sequence numbers into four regions

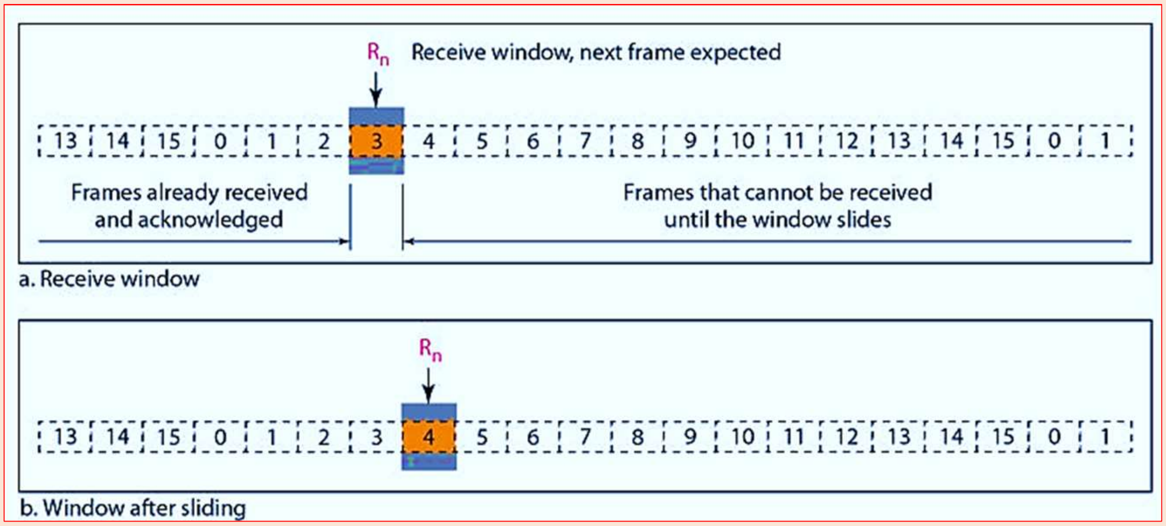
Send Window



- The window itself is an abstraction; three variables define its size and location at any time.
- **Sf**(send window, the first outstanding frame)
- **Sn** (send window, the next frame to be sent)
- **Ssize** (send window, size).
- The variable Sf defines the sequence number of the first (oldest) outstanding frame.
- The variable Sn holds the sequence number that will be assigned to the next frame to be sent.
- Finally, the variable Ssize defines the size of the window, which is fixed in our protocol.

- The acknowledgments in this protocol are cumulative, meaning that more than one frame can be acknowledged by an ACK frame.
- In Figure b, frames 0, I, and 2 are acknowledged, so the window has slide to the right three slots.
- The receive window makes sure that the correct data frames are received and that the correct acknowledgments are sent.
- The size of the receive window is always 1.
- The receiver is always looking for the arrival of a specific frame.
- Any frame arriving out of order is discarded and needs to be resent.

Receive Window



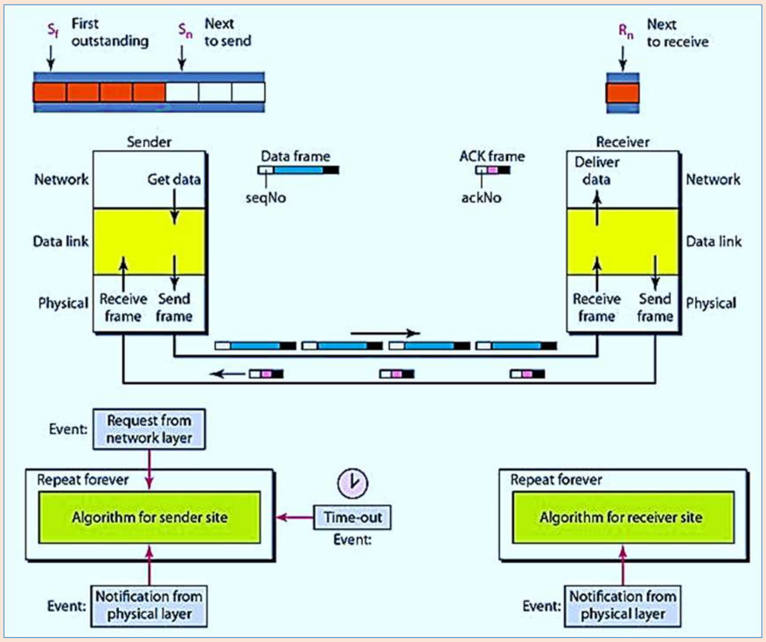
- we need only one variable Rn (receive window, next frame expected) to define this abstraction.
- The sequence numbers to the left of the window belong to the frames already received and acknowledged
- The sequence numbers to the right of this window define the frames that cannot be received. Any received frame with a sequence number in these two regions is discarded.
- Only a frame with a sequence number matching the value of Rn is accepted and acknowledged.
- The receive window also slides, but only one slot at a time. When a correct frame is received (and a frame is received only one at a time), the window slides.

➢Acknowledgment

- The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order.
- If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting.
- The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire. This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer.
- The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgment for several frames

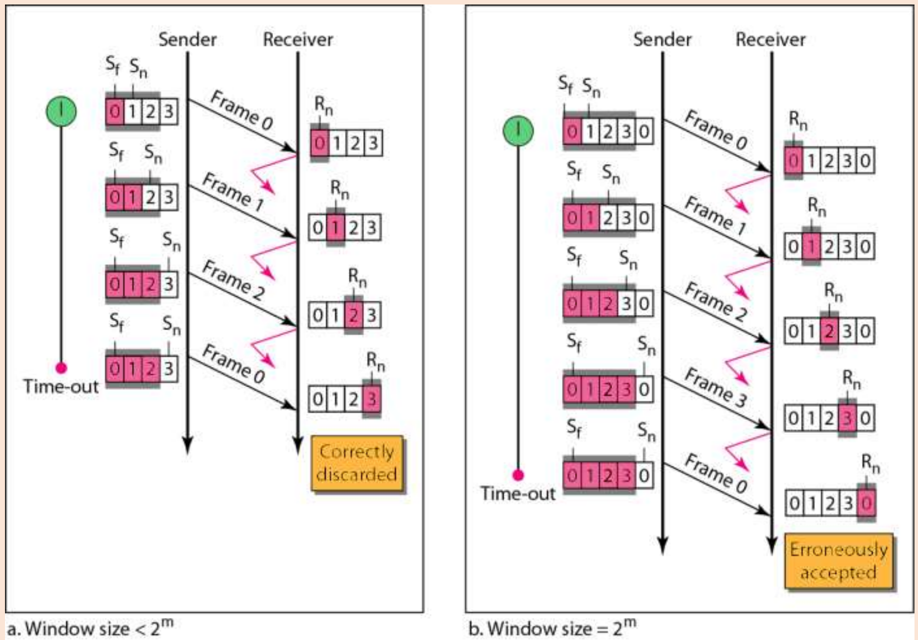
➢Resending a Frame

- When the timer expires, the sender resends all outstanding frames.
- For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4,5, and 6 again.
- That is why the protocol is called Go-Back-N ARQ.
- In Go-Back-N ARQ, the size of the send window must be **less than 2^m** and the size of the receiver window is always **1**



➤Send Window Size

- Suppose m =2, which means the size of the window can be 2^m - 1, or 3.
- If the size of the window is 3 (less than 2^2) and all three acknowledgments are lost, the frame timer expires and all three frames are resent.
- The receiver is now expecting frame 3, not frame 0, so the duplicate frame is correctly discarded.
- On the other hand, if the size of the window is 4 (equal to 2^2) and all acknowledgments are lost, the sender will send a duplicate of frame 0.
- However, this time the window of the receiver expects to receive frame 0, so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is an error.



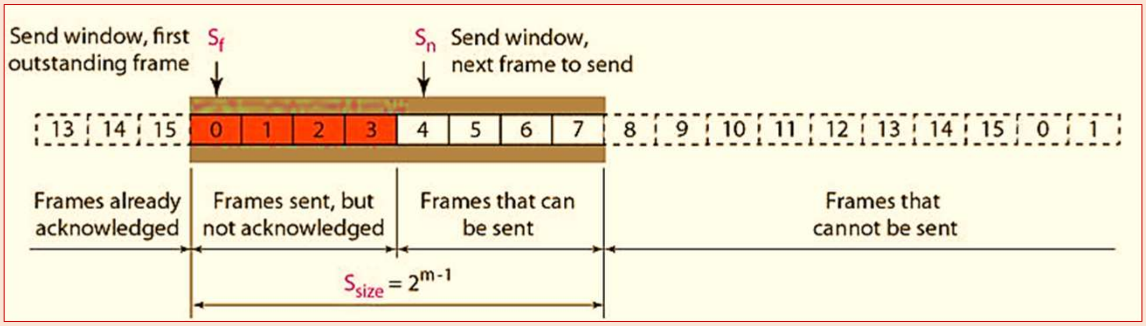
Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 35

3. Selective Repeat Automatic Repeat Request

- Go-Back-N ARQ resending of multiple frames.
- For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent.
- This mechanism is called Selective Repeat ARQ. It is more efficient for noisy links.
- The Selective Repeat Protocol also uses two windows: a send window and a receive window
- The size of the send window is much smaller; it is 2^{m-1}
- The receive window is the same size as the send window

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 36

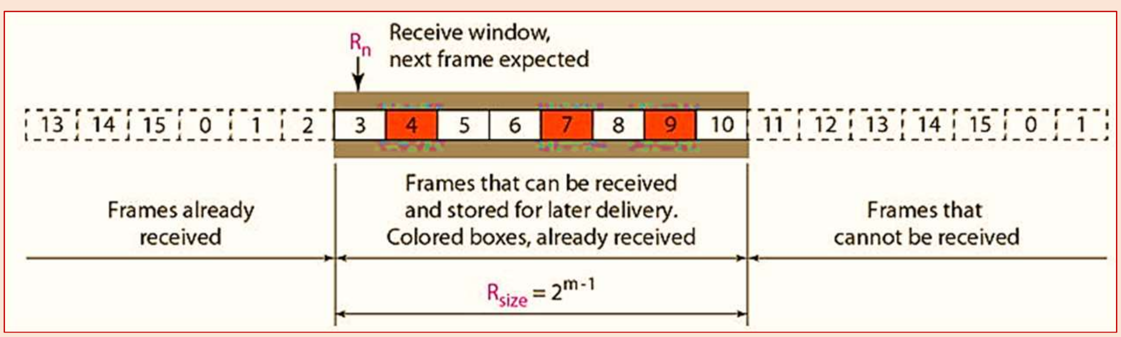
- If m = 4, the sequence numbers go from 0 to 15, but the size of the window is just 8 (it is 15 in the Go-Back-N Protocol).



- The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer.

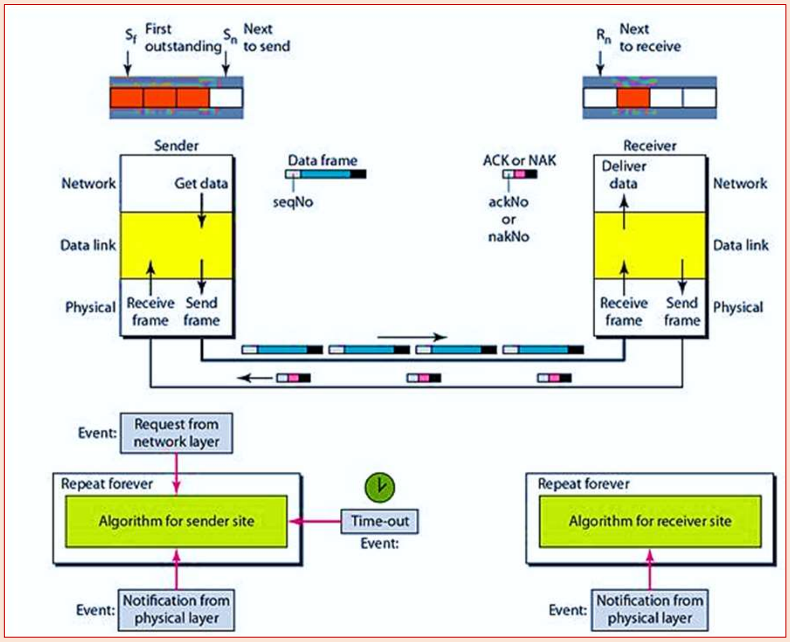
Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 37

- Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered

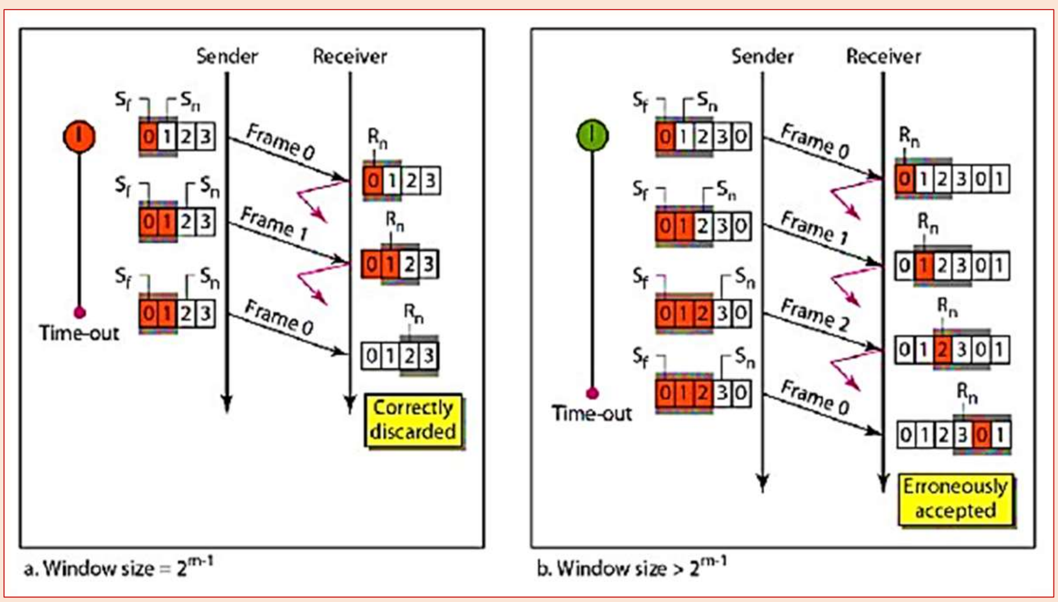


- Those slots inside the window that are colored define frames that have arrived out of order and are waiting for their neighbors to arrive before delivery to the network layer.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 38



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 39

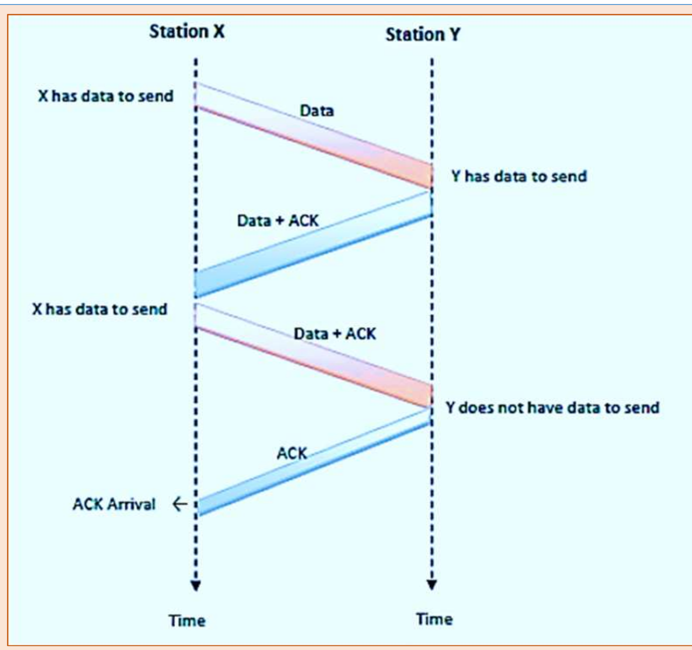


Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 40

❖Piggybacking

- Communications are mostly full – duplex in nature, i.e. data transmission occurs in both directions
- In reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.
- Piggybacking is used to improve the efficiency of the bidirectional protocols
- When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 41



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 42

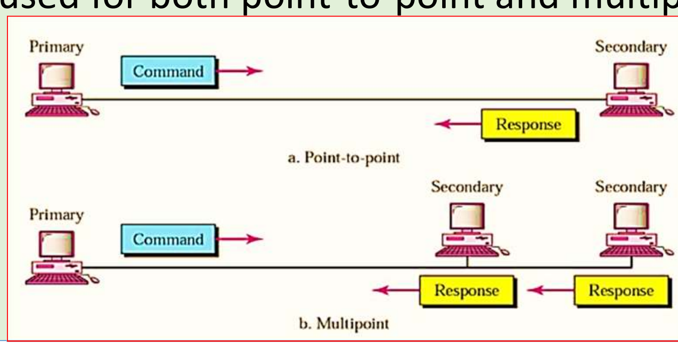
HDLC

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- It implements the ARQ mechanisms
- HDLC provides two common transfer modes that can be used in different configurations:

1. Normal Response Mode (NRM)
2. Asynchronous Balanced Mode (ABM).

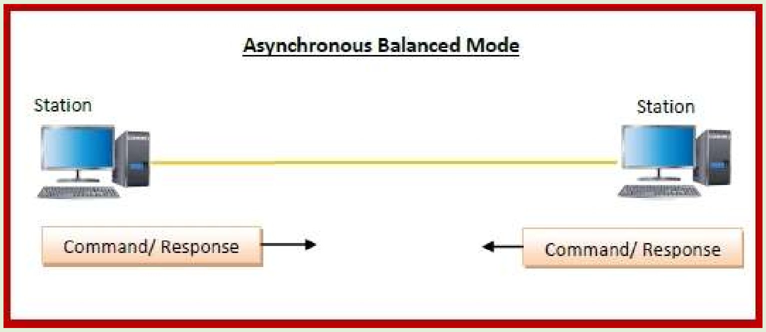
1. Normal Response Mode

- The station configuration is unbalanced.
- We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond.
- The NRM is used for both point-to-point and multiple-point links



2. Asynchronous Balanced Mode

- The configuration is balanced.
- The link is point-to-point, and each station can function as a primary and a secondary (acting as peers)
- This is the common mode today.



❖Frames

- HDLC defines three types of frames:

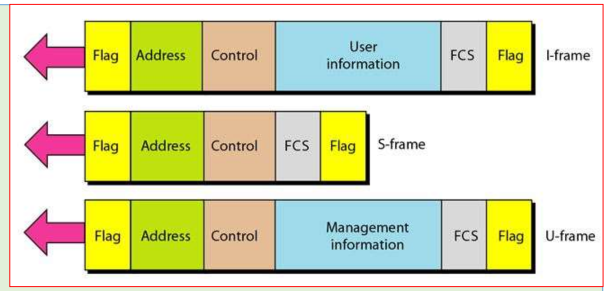
➢**Information frames (I-frames)**

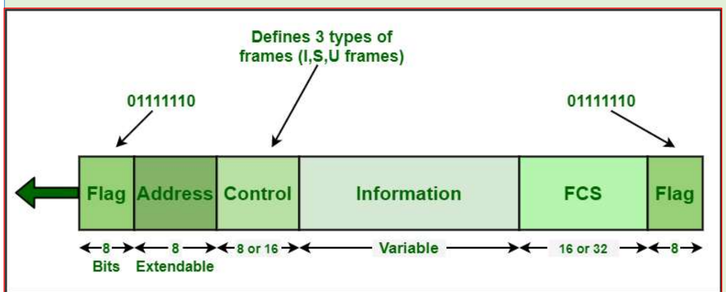
➢**Supervisory frames (S-frames)**

➢**Unnumbered frames (V-frames)**

- I-frames are used to transport user data and control information relating to user data (piggybacking).
- S-frames are used only to transport control information.
- V-frames are reserved for system management. Information carried by V-frames is intended for managing the link itself.

❖Frame Format





Basic Frame Structure

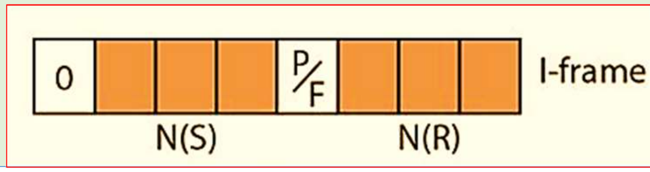
- **Flag field** - The bit pattern 01111110, that identifies both the beginning and the end of a frame
- **Address field** - Contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address.
- **Control field** - The control field is a 1 or 2 byte segment of the frame used for flow and error control.
- **Information field** - The information field contains the user's data from the network layer or management information
- **FCS field** - The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte ITU-T CRC

❖Control Field

- The control field determines the type of frame

➢Control Field for I-Frames

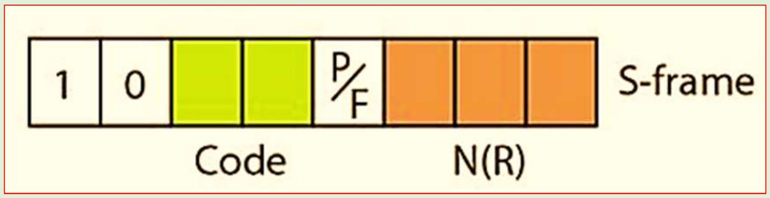
- I-frames are designed to carry user data from the network layer.
- They can include flow and error control information (piggybacking).
- The first bit defines the type. If the first bit of the control field is 0, this means the frame is an I-frame.
- The next 3 bits, called N(S),define the sequence number of the frame



- The last 3 bits, called N(R), correspond to the acknowledgment number when piggybacking is used
- The single bit between N(S) and N(R) is called the P/F bit.
- The P/F field is a single bit with a dual purpose. It has meaning only when it is set (bit = 1) and can mean Poll or Final. It means poll when the frame is sent by a primary station to a secondary (when the address field contains the address of the receiver). It means final when the frame is sent by a secondary to a primary (when the address field contains the address of the sender).

➢Control Field for S-Frames

- S-frames do not have information fields.
- If the first 2 bits of the control field is 10, this means the frame is an S-frame.
- The last 3 bits, called N(R), corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame



- The 2 bits called code is used to define the type of S-frame itself. With 2 bits, we can have four types of S-frames.

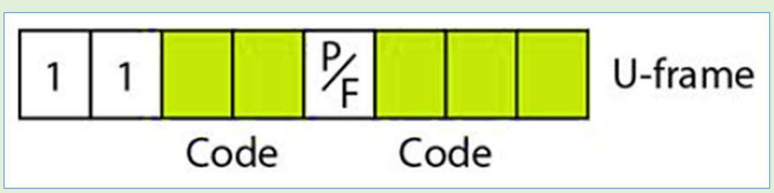
1. **Receive ready (RR)** - If the value of the code subfield is 00, it is an RR S-frame. This kind of frame acknowledges the receipt of a safe and sound frame or group of frames. In this case, the value N(R) field defines the acknowledgment number.
2. **Receive not ready (RNR)** - If the value of the code subfield is 10, it is an RNR S-frame. It announces that the receiver is busy and cannot receive more frames. It acts as a kind of congestion control mechanism by asking the sender to slow down. The value of N(R) is the acknowledgment number.

3. **Reject (REJ)** - If the value of the code subfield is 01, it is a REJ S-frame. This is a NAK frame. It is a NAK that can be used in Go-Back-N ARQ to improve the efficiency of the process by informing the sender, before the sender time expires, that the last frame is lost or damaged. The value of N(R) is the negative acknowledgment number.
4. **Selective reject (SREJ)** - If the value of the code subfield is 11, it is an SREJ S-frame. This is a NAK frame used in Selective Repeat ARQ. Note that the HDLC Protocol uses the term selective reject instead of selective repeat. The value of N(R) is the negative acknowledgment number

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 53

➢Control Field for U-Frames

- Unnumbered frames are used to exchange session management and control information between connected devices.
- 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.



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 54

U-frames Control Command and Response

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	DM	Set asynchronous balanced mode or disconnect mode
11110	SABME		Set asynchronous balanced mode, extended
00 000	UI	UI	Unnumbered information
00 110		UA	Unnumbered acknowledgment
00 010	DISC	RD	Disconnect or request disconnect
10 000	SIM	RIM	Set initialization mode or request information mode
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	XID	Exchange ID
10 001	FRMR	FRMR	Frame reject

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 55

MODULE 2

CHAPTER 2 – ERROR DETECTION & CORRECTION

Prepared By Mr. EBIN PM, Chandigarh University, Punjab 56

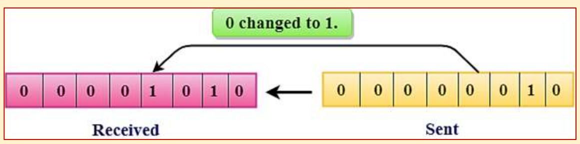
TYPES OF ERRORS

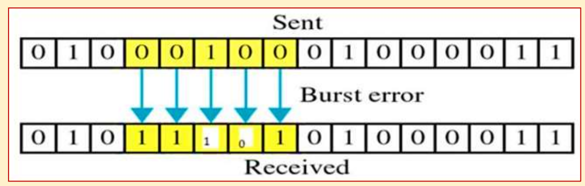
➢Single-Bit Error

- Only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.

➢Burst Error

- The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.





Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 57

❖REDUNDANCY

- The central concept in detecting or correcting errors is redundancy.
- To be able to detect or correct errors, we need to send some extra bits with our data.
- These redundant bits are added by the sender and removed by the receiver.
- Their presence allows the receiver to detect or correct corrupted bits.
- To detect or correct errors, we need to send extra (redundant) bits with data.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 58

❖Detection Versus Correction

- In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even interested in the number of errors.
- In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.
- The number of the errors and the size of the message are important factors.
- If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities.

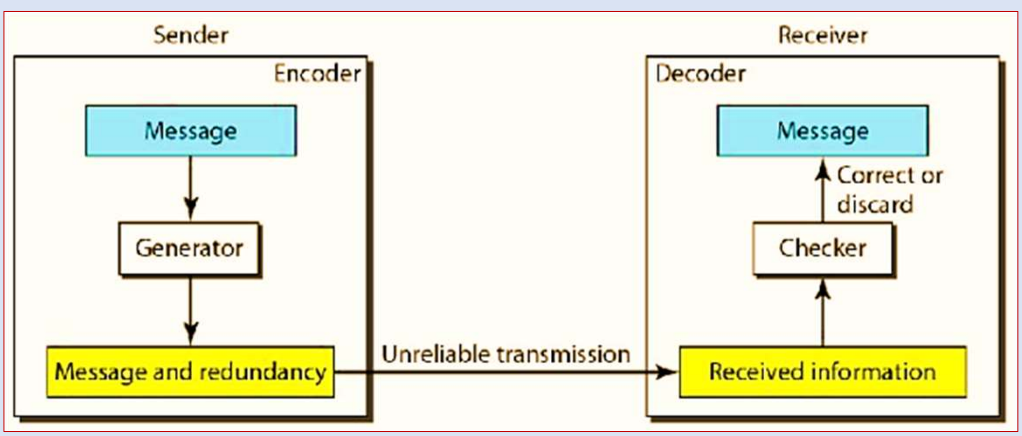
❖Forward Error Correction Versus Retransmission

- There are two main methods of error correction.
- Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the number of errors is small.
- Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message.
- Resending is repeated until a message arrives that the receiver believes is error-free (usually, not all errors can be detected).

CODING

- Redundancy is achieved through various coding schemes.
- The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.
- The receiver checks the relationships between the two sets of bits to detect or correct the errors.
- The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme.
- We can divide coding schemes into two broad categories: block coding and convolution coding.

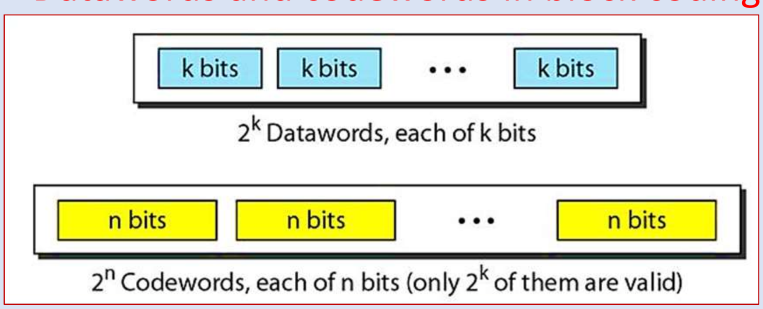
The structure of encoder and decoder



❖BLOCK CODING

- We divide our message into blocks, each of **k** bits, called **data words.**
- We add **r** redundant bits to each block to make the length **n = k + r.**
- The resulting n-bit blocks are called **code words**.
- we have a set of data words, each of size k, and a set of code words, each of size of n. With k bits, we can create a combination of 2k data words; with n bits, we can create a combination of 2n code words.
- Since n > k, the number of possible code words is larger than the number of possible data words.
- The block coding process is one-to-one; the same data word is always encoded as the same code word.

Datawords and codewords in block coding



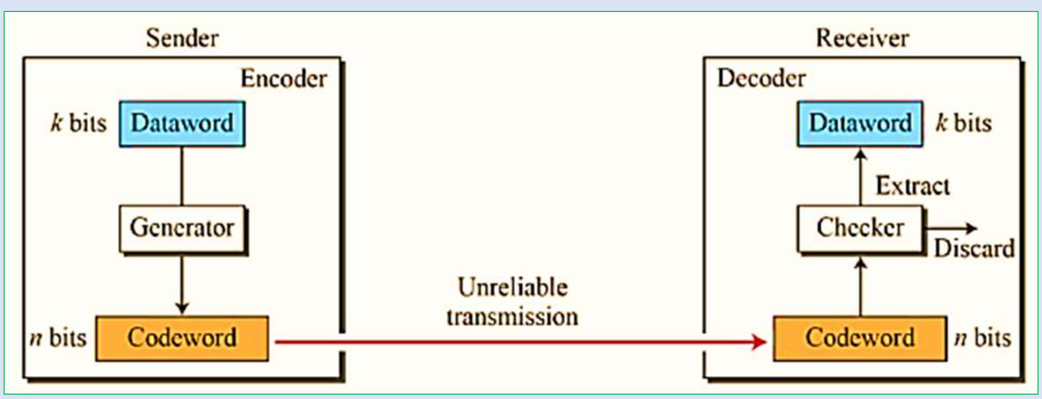
➢Error Detection

- If the following two conditions are met, the receiver can detect a change in the original codeword.

1. The receiver has (or can find) a list of valid codewords.
2. The original codeword has changed to an invalid one.

- The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding .
- Each codeword sent to the receiver may change during transmission.
- If the received codeword is the same as one of the valid codewords, the word is accepted; the corresponding dataword is extracted for use.
- If the received codeword is not valid, it is discarded.
- If the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.
- This type of coding can detect only single errors. Two or more errors may remain undetected.

Process of error detection in block coding



Let us assume that k =2 and n =3. Table shows the list of datawords and codewords.

Datawords	Codewords
00	000
01	011
10	101
11	110

- Assume the sender encodes the dataword 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it.
2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.

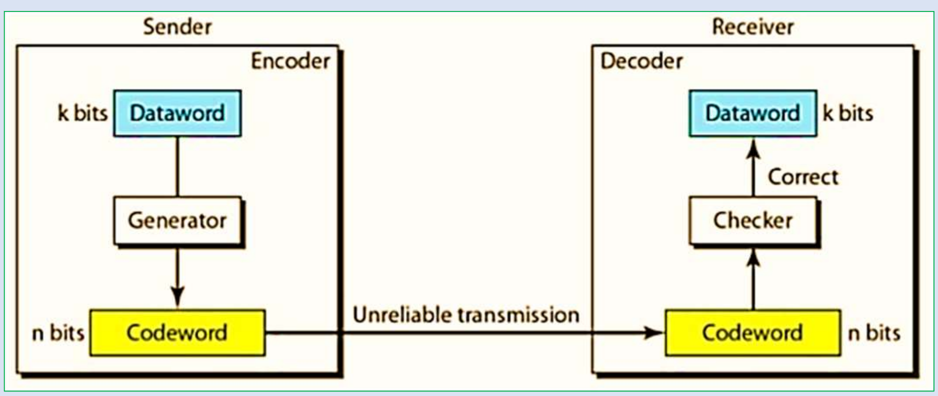
3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable.

➢ An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected.

➢Error Correction

- Error correction is much more difficult than error detection.
- In error detection, the receiver needs to know only that the received codeword is invalid
- In error correction the receiver needs to find (or guess) the original codeword sent.
- We can say that we need more redundant bits for error correction than for error detection.
- Following figure shows the role of block coding in error correction. The idea is the same as error detection but the checker functions are much more complex.

Structure of encoder and decoder in error correction



- Assume the dataword is 01.
- The sender consults the table (or uses an algorithm) to create the codeword 01011.
- The codeword is corrupted during transmission, and 01001 is received (error in the second bit from the right).
- First, the receiver finds that the received codeword is not in the table. This means an error has occurred. (Detection must come before correction.)
- The receiver, assuming that there is only 1 bit corrupted, uses the following strategy to guess the correct dataword.

A code for error correction

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

1. Comparing the received codeword with the first codeword in the table (01001 versus 00000), the receiver decides that the first codeword is not the one that was sent because there are two different bits.
2. By the same reasoning, the original codeword cannot be the third or fourth one in the table.
3. The original codeword must be the second one in the table because this is the only one that differs from the received codeword by 1 bit. The receiver replaces 01001 with 01011 and consults the table to find the dataword 01.

❖Hamming Distance

- The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits.
- The Hamming distance between two words x and y is represented as **d(x, y)**
- The Hamming distance can easily be found if we apply the XOR operation (⊕) on the two words and count the number of 1s in the result.
- The Hamming distance is a value greater than zero.
- **Eg:** The Hamming distance d(000, 011) is 2 because 000 ⊕ 011 is 011 (two 1s).
- **Eg:** The Hamming distance d(10101, 11110) is 3 because 10101 ⊕11110 is 01011 (three 1s).

- The **minimum Hamming distance** is the smallest Hamming distance between all possible pairs in a set of words.
- We use d_{min} to define the minimum Hamming distance in a coding scheme.
- Eg: We first find all the Hamming distances.

  d(00000, 01011) = 3

  d(01011, 10101) = 4

  d(00000, 10101) = 3

  d(01011, 11110) = 3

  d(00000, 11110) = 4

  The d_{min} in this case is **3**

Inputs		Output
A	B	X = A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

- Any coding scheme needs to have at least three parameters:

➢ The codeword size n

➢ The dataword size k

➢ The minimum Hamming distance d_{min}.

- A coding scheme C is written as C(n, k) with a separate expression for d_{min}

Eg: **C(5, 2) with d_{min}= 3.**

- The Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission. For example, if the codeword 00000 is sent and 01101 is received, 3 bits are in error and the Hamming distance between the two is d(00000, 01101) =3

- To guarantee the detection of up to ***s*** errors in all cases, the minimum Hamming distance in a block code must be d_{min} = ***S* + 1**
- To guarantee correction of up to **t** errors in all cases, the minimum Hamming distance in a block code must be d_{min} = **2t + 1**

❖ Parity bits

- A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data is even or odd.
- Parity bits are used for error detection.
- There are two types of parity bits:

Even parity bit and **Odd parity bit**

Even parity bit:

- In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.

Odd Parity bit :

- In the case of odd parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

LINEAR BLOCK CODE

- In a linear block code, the exclusive OR (XOR) of any two valid codewords creates another valid codeword

1. Simple Parity-Check Code

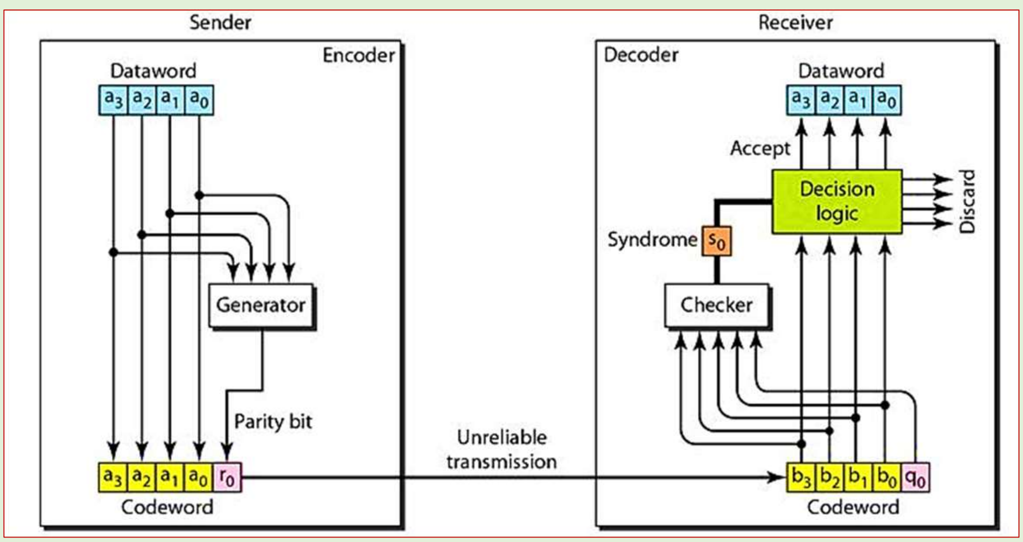
- A simple parity-check code is a single-bit error-detecting code
- In this code, a k-bit dataword is changed to an n-bit codeword where **n = k + 1**. The extra bit, called the **parity bit**, is selected to make the total number of 1s in the codeword even.
- The minimum Hamming distance for this category is d_{min} **=2** which means that the code is a single-bit error-detecting code; it cannot correct any error.

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

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 79

Encoder and decoder for simple parity-check code

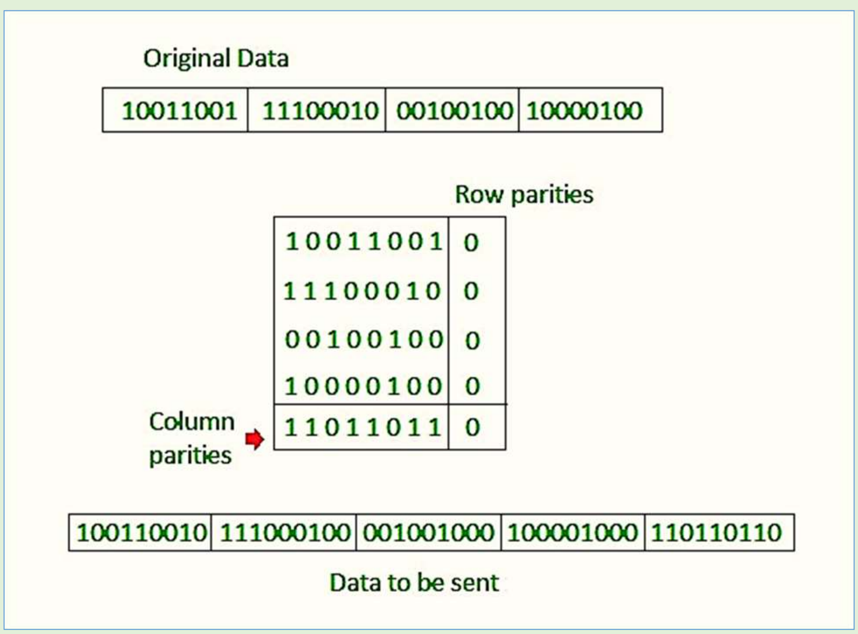


Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 80

2. Two-dimensional parity check

- In this method, the dataword is organized in a table (rows and columns)
- For each row and each column, 1 parity-check bit is calculated. The whole table is then sent to the receiver, which finds the syndrome for each row and each column.
- The two-dimensional parity check can detect up to three errors that occur anywhere in the table.
- Errors affecting 4 bits may not be detected

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 81



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 82

3. Hamming Codes

- Hamming codes are error-correcting codes
- These codes were originally designed with d_{min}= 3, which means that they can detect up to two errors or correct one single error.
- relationship between n and k in a Hamming code. We need to choose an integer m >= 3. The values of n and k are then calculated from mas n = 2^m -1 and k = n - m. The number of check bits r =m.
- For example, if m =3, then n =7 and k = 4. This is a Hamming code C(7, 4) with d_{min} =3.

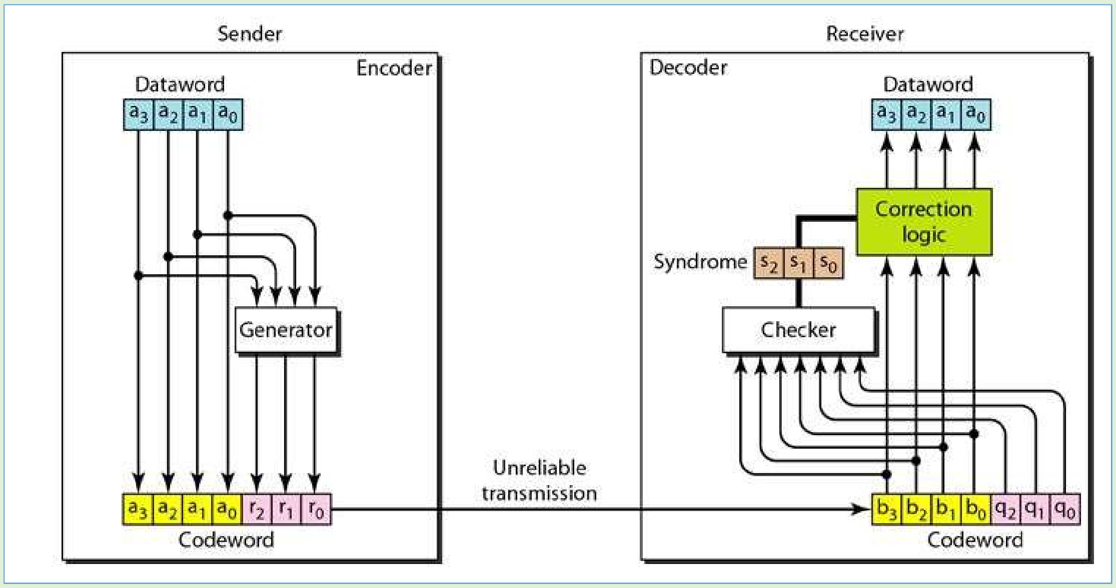
Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 83

Hamming code C(7, 4)

Datawords	*Codewords*	*Datawords*	*Codewords*
0000	0000000	1000	1000110
0001	0001101	1001	1001011
0010	0010111	1010	1010001
0011	0011010	1011	10111 00
0100	0100011	1100	1100101
0101	01011 10	1101	1101000
0110	0110100	1110	1110010
0111	0111001	1111	1111111

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 84

The structure of the encoder and decoder for a Hamming code



❖Hamming Code Structure

➢All the bit positions that are power of 2 are marked as parity bits (1,2,4,8,…..) and other bits are for data.

Eg: 7 bit hamming code

D7	**D6**	**D5**	**P4**	**D3**	**P2**	**P1**

Parity bit values :

Eg: 1101

D7	D6	D5	P4	D3	P2	P1
1	1	0	?	1	?	?

P1 : check 1 bit & skip 1bit (1,3,5,7,9,……)

P2 : check 2 bit & skip 2 bit (2,3,6,7,10,11,…)

P4 : check 4 bit & skip 4 bit (4,5,6,7,12,13,14,15,……)

D7	D6	D5	P4	D3	P2	P1
1	1	0		1		

P1 D3 D5 D7 ⟶ P1 101 ⟶ P1 = 0

P2 D3 D6 D7 ⟶ P2 111 ⟶ P2 =1

P4 D5 D6 D7 ⟶ P4 011 ⟶ P4 = 0

1	1	0	0	1	1	0

❖ *DETECTING & CORRECTING ERROR*

Suppose the receiver receives the data **1011011**

D7	D6	D5	P4	D3	P2	P1
1	0	1	1	0	1	1

Step 1: analyze bit 1,3,5,7 (for P1) = P1 D3 D5 D7 = 1011

Odd number of 1s. So error exist and we put **P1=1**

Step 2: analyze bit 2,3,6,7 (for P2) = P2 D3 D6 D7 = 1001

even number of 1s. So no error and we put **P2=0**

Step 3: analyze bit 4,5,6,7 (for P4) = P4 D5 D6 D7 = 1101

Odd number of 1s. So error exist and we put **P4=1**

Correcting Error

P4	P2	P1
1	0	1

- Error word E = 1 0 1
- Decimal value of the error E = 5 which shows that the 5th bit is in error.
- So we write the correct word by simply inverting only the 5th bit

D7	D6	D5	P4	D3	P2	P1
1	0	0	1	0	1	1

CYCLIC CODES

- Cyclic codes are special linear block codes with one extra property.
- In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.
- For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword
- cyclic codes have a very good performance in detecting single-bit errors, double errors, an odd number of errors, and burst errors.
- They can easily be implemented in hardware and software

❖Cyclic Redundancy Check

- Cyclic Redundancy Check (CRC) is used in networks such as LANs and WANs.
- It is an error detection method based on binary division.
- Here a sequence of redundant bits called CRC bits are appended to the end of data, so that the resulting data unit become exactly divisible by second predetermined binary number.
- At the destination side, the incoming data is divisible by the same number.
- If the remainder is 0, then the data is accepted , otherwise rejected.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 91

➢CRC generation at sender side

Step 1 : Find the length of the divisor "L"

Step 2 : Append "L-1" bits to the original message

Step 3 : Perform binary division (XOR) Operation

Step 4 : Remainder of the division = CRC

Eg : Find the CRC for the data block 100100 with the divisor 1101?

- Here L=4 . So 3 zeros will be append to the original message.
- So the data block become **100100000**

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 92

➢ **How receiver detect error using CRC**

CHECK SUM

- It is an error detection method .
- The checksum is used in the Internet by several protocols
- The checksum is based on the concept of redundancy
- Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers.
- For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12,0,6,36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum.

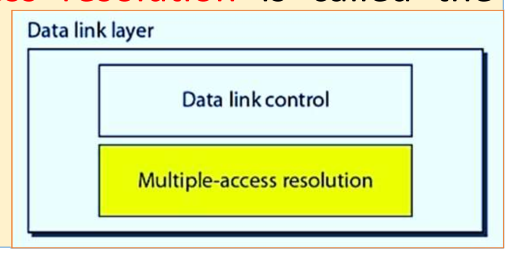
- If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.
- The Internet has been using a 16-bit checksum.

MODULE 2

CHAPTER 3 – MAC SUBLAYER

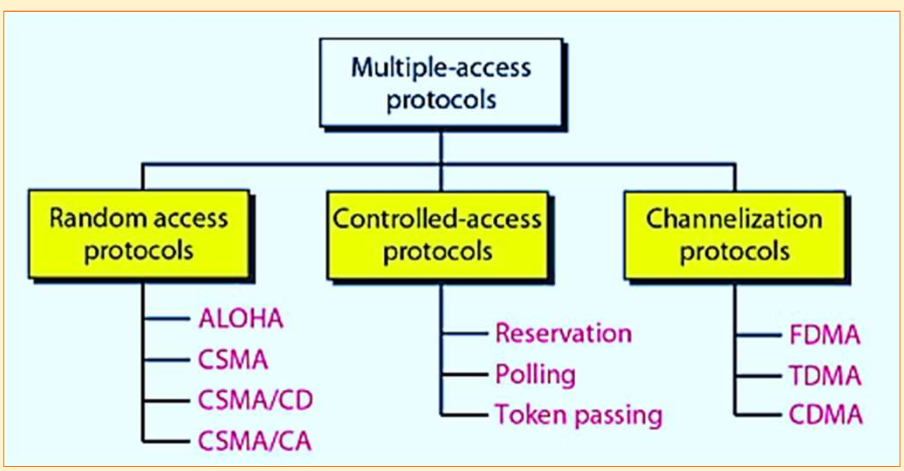
MULTIPLE ACCESS

- The data link layer as two sublayers.
- The upper sublayer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media.
- The upper sublayer that is responsible for flow and error control is called the logical link control (LLC) layer; the lower sublayer that is mostly responsible for multiple access resolution is called the media access control (MAC) layer.



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 97

- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link.



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 98

❖RANDOM ACCESS (contention method) PROTOCOLS

- There is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access.
- No rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.
- In a random access method, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified. To avoid access conflict or to resolve it when it happens, each station follows a procedure.

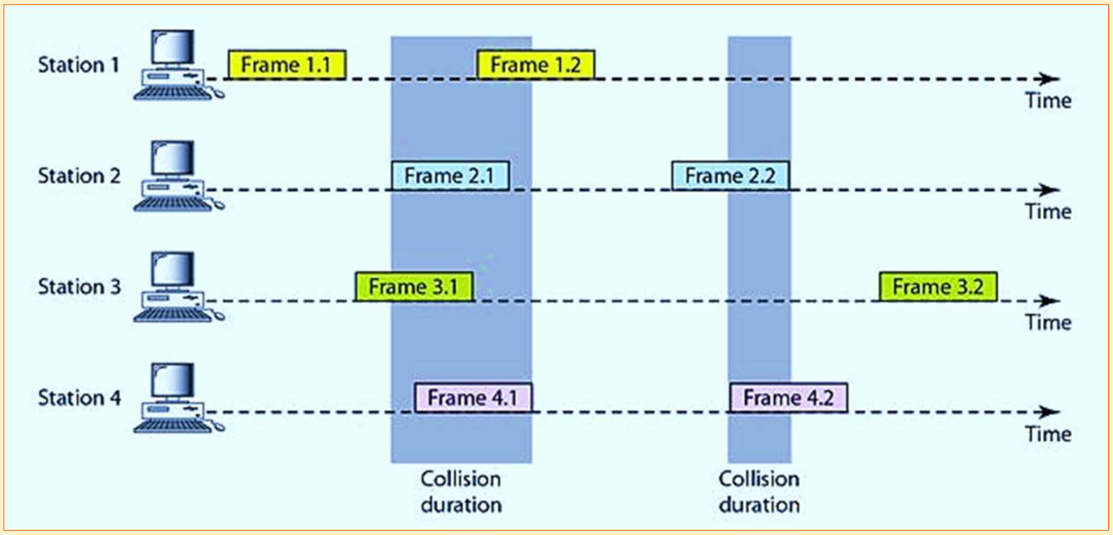
❖ALOHA

- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

1. Pure ALOHA

- The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol.
- The idea is that each station sends a frame whenever it has a frame to send.
- Since there is only one channel to share, there is the possibility of collision between frames from different stations.

Frames in a pure ALOHA network



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 101

- In the above figure , there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel.
- Only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3.
- Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.
- we need to resend the frames that have been destroyed during transmission.
- The pure ALOHA protocol relies on acknowledgments from the receiver

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 102

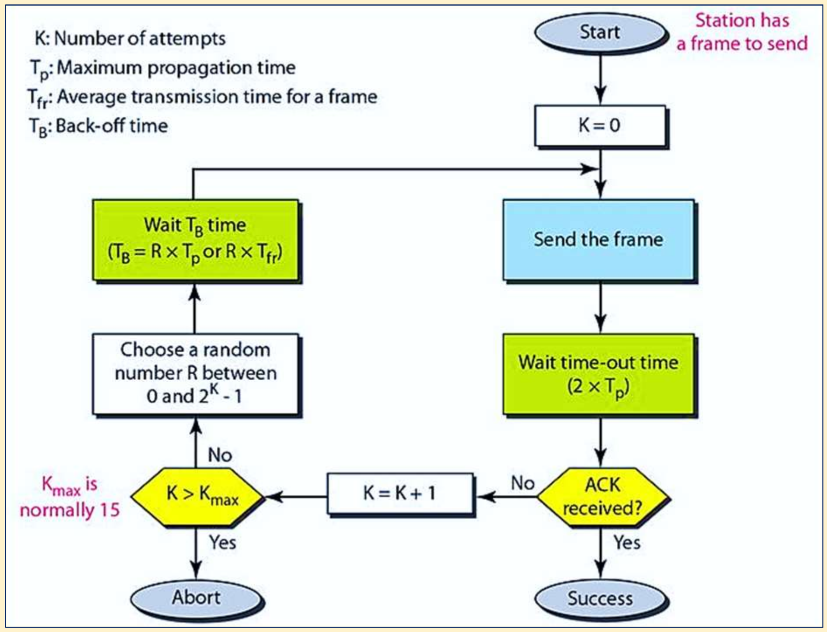
- When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame
- A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.
- In Pure ALOHA , when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the **back-off time TB.**

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 103

- Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax, a station must give up and try later.
- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (**2 × Tp).**
- The back-off time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions).
- for each retransmission, a multiplier R = 0 to 2^k-1 is randomly chosen and multiplied by Tp (maximum propagation time) or Tfr (the average time required to send out a frame) to find TB.

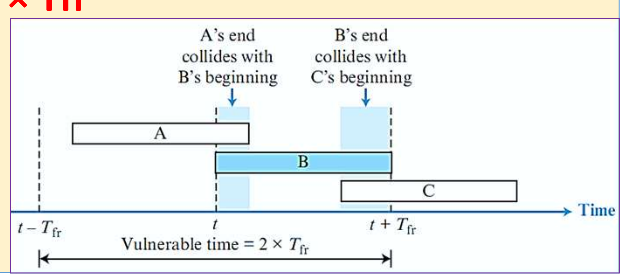
Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 104

Procedure for pure ALOHA protocol



➢Vulnerable time for pure ALOHA protocol

- Station B starts to send a frame at time t. Now imagine station A has started to send its frame after t – Tfr. This leads to a collision between the frames from station B and station A. On the other hand, suppose that station C starts to send a frame before time t + Tfr. Here, there is also a collision between frames from station B and station C
- Pure ALOHA vulnerable time = **2 × Tfr**



➢Throughput

- Let us call G the average number of frames generated by the system during one frame transmission time.
- Then it can be proven that the average number of successfully transmitted frames for pure ALOHA is

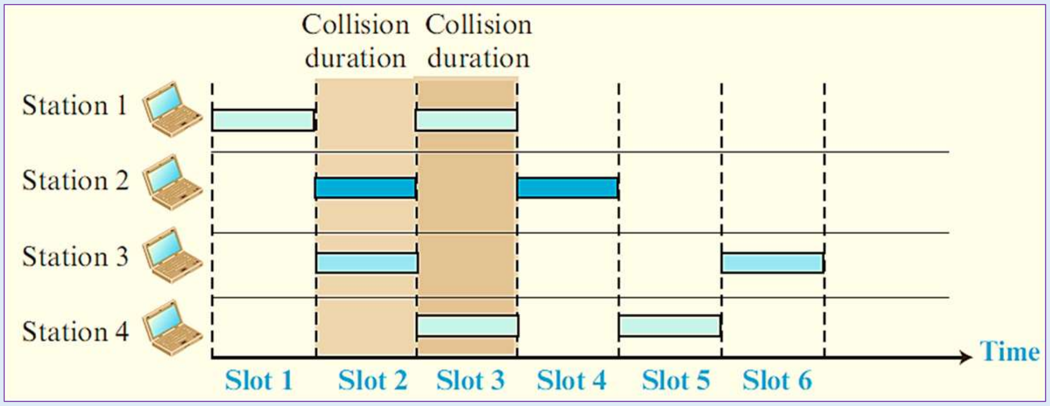
$$S = G \times e^{-2G}$$

- The maximum throughput Smax is **0.184**, for G = 1/2

2. Slotted ALOHA

- Pure ALOHA has a vulnerable time of 2 × Tfr. This is so because there is no rule that defines when the station can send.
- A station may send soon after another station has started or just before another station has finished.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA
- In slotted ALOHA we divide the time into slots of Tfr seconds and force the station to send only at the beginning of the time slot

Frames in a slotted ALOHA network



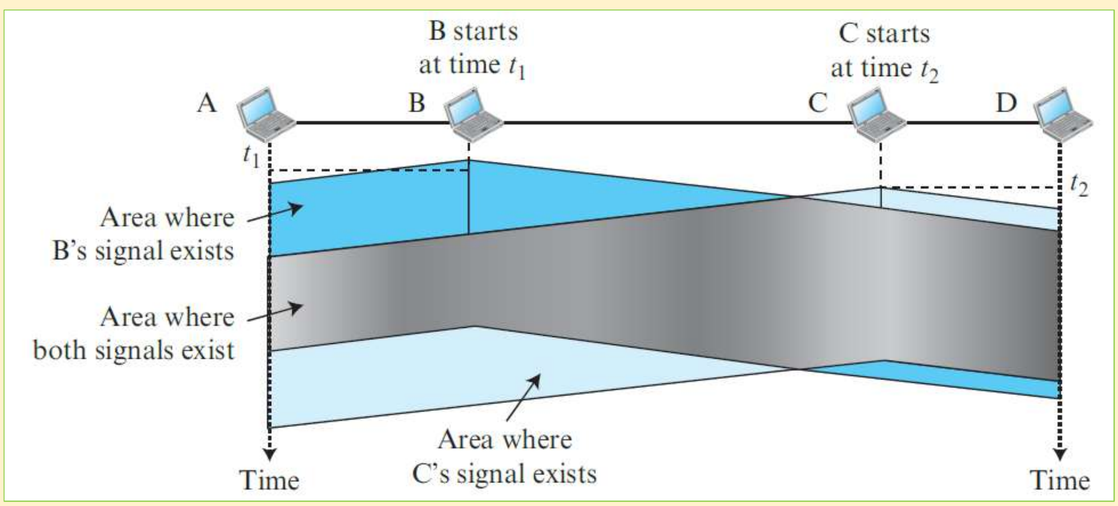
- Because a station is allowed to send only at the beginning of the synchronized timeslot; if a station misses this moment, it must wait until the beginning of the next timeslot.

- There is still the possibility of collision if two stations try to send at the beginning of the same time slot.
- However, the vulnerable time is now reduced to one-half, equal to Tfr.
- Slotted ALOHA vulnerable time = **Tfr**
- The throughput for slotted ALOHA is **S = G ×** e^{-G}
- The maximum throughput **Smax = 0.368** when G = 1.

❖Carrier Sense Multiple Access (CSMA)

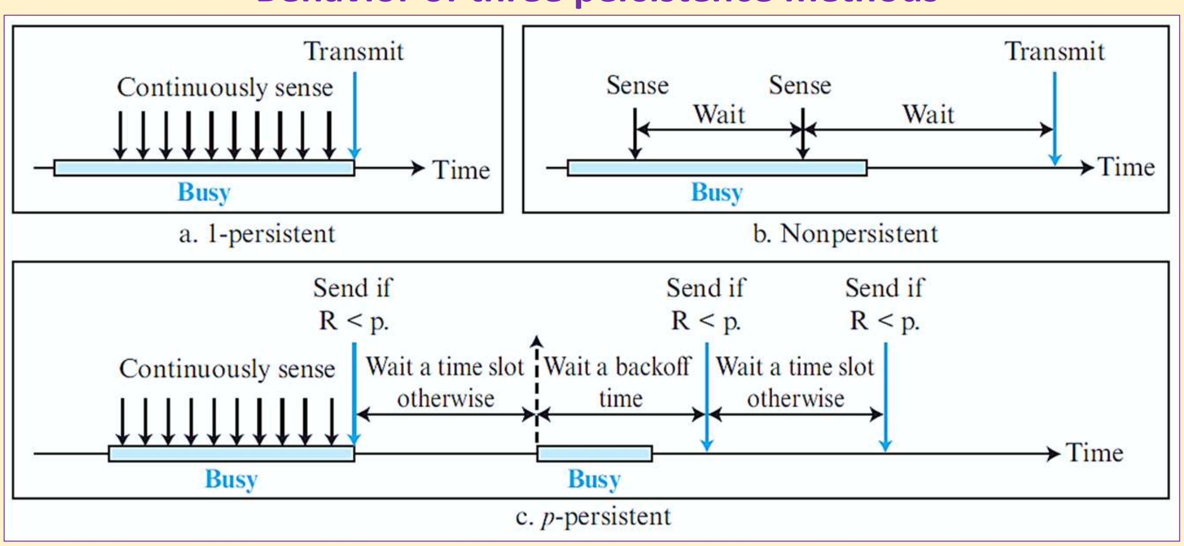
- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.
- In other words, CSMA is based on the principle “sense before transmit” or “listen before talk”.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

Space/time model of a collision in CSMA



- At time t1, station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2 > t1), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed
- **Vulnerable Time** - The vulnerable time for CSMA is the propagation time Tp. This is the time needed for a signal to propagate from one end of the medium to the other.
- **Persistence Methods** – shows the behavior of three persistence methods when a station finds a channel busy.

Behavior of three persistence methods



- R is a random number (R= 0 to 1)

➢1-Persistent

- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

➢Nonpersistent

- In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.

- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send

➢P-Persistent

- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.

- It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it

follows these steps:

1. With probability p, the station sends its frame.

2. With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again.

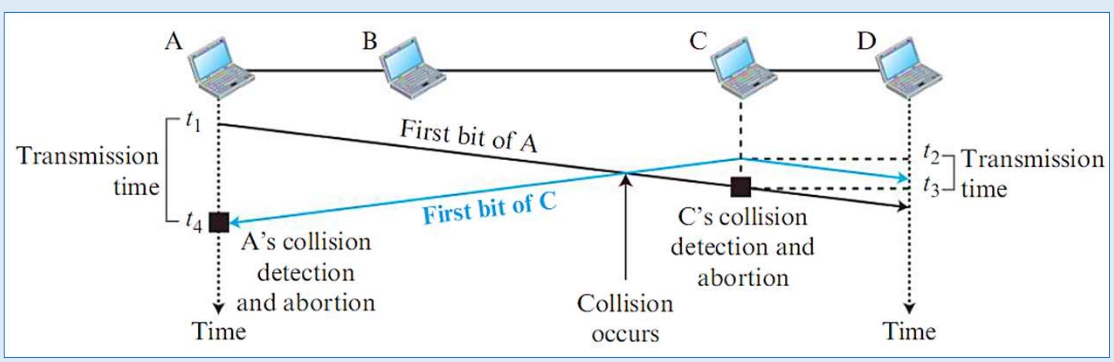
a. If the line is idle, it goes to step 1.

b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

❖CSMA/CD

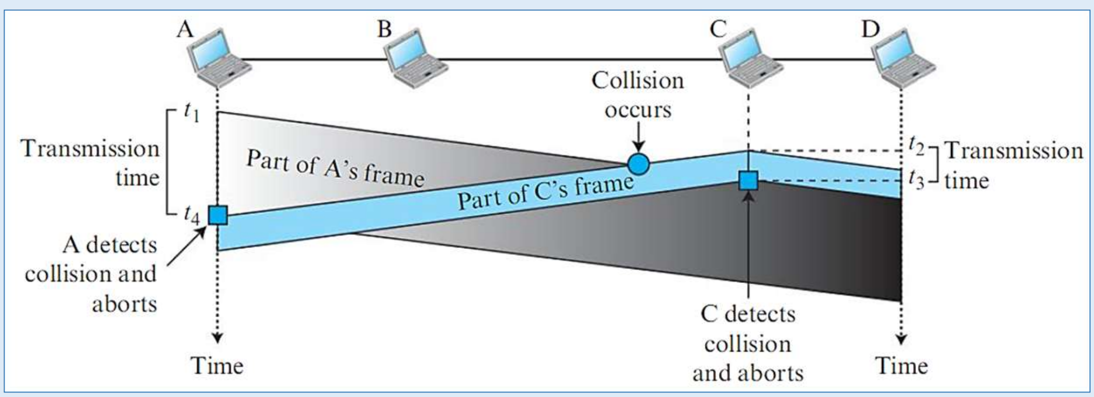
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

Collision of the first bits in CSMA/CD



- At time t1, station A has executed its persistence procedure and starts sending the bits of its frame.
- At time t2, station C has not yet sensed the first bit sent by A.
- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time t2. Station C detects a collision at time t3 when it receives the first bit of A's frame.
- Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.

Collision and abortion in CSMA/CD



- A transmits for the duration t4 − t1.
- C transmits for the duration t3 − t2.

➢Energy Level

- The level of energy in a channel can have three values: zero, normal, and abnormal.
- At the zero level, the channel is idle.
- At the normal level, a station has successfully captured the channel and is sending its frame.
- At the abnormal level, there is a collision and the level of the energy is twice the normal level.
- A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.

➢Throughput

- The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
- For the 1-persistent method, the maximum throughput is around 50 percent when G = 1.
- For the nonpersistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.
- Traditional Ethernet was a broadcast LAN that used 1-persistence method to control access to the common media.

❖CSMA/CA

- Since we need to avoid collisions on wireless networks because they cannot be detected.
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was invented for wireless network.
- Collisions are avoided through the use of CSMA/CA's three strategies:

1. The interframe space (IFS)
2. The contention window
3. Acknowledgments

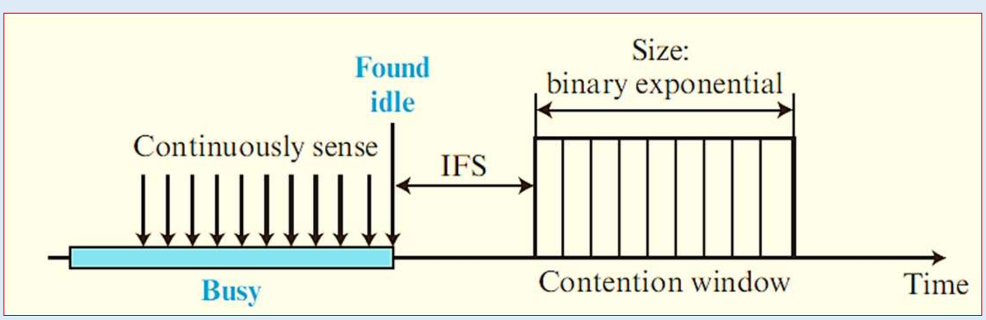
➢Interframe space (IFS)

- When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.
- Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.
- The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.

➢Contention Window

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy.
- This means that it is set to one slot the first time and then doubles each time if the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.

- One interesting point about the contention window is that the station needs to sense the channel after each time slot.
- However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.



➢Acknowledgment

- With all these precautions, there still may be a collision resulting in destroyed data.
- In addition, the data may be corrupted during the transmission.
- The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 127

❖CONTROLLED ACCESS PROTOCOLS

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.

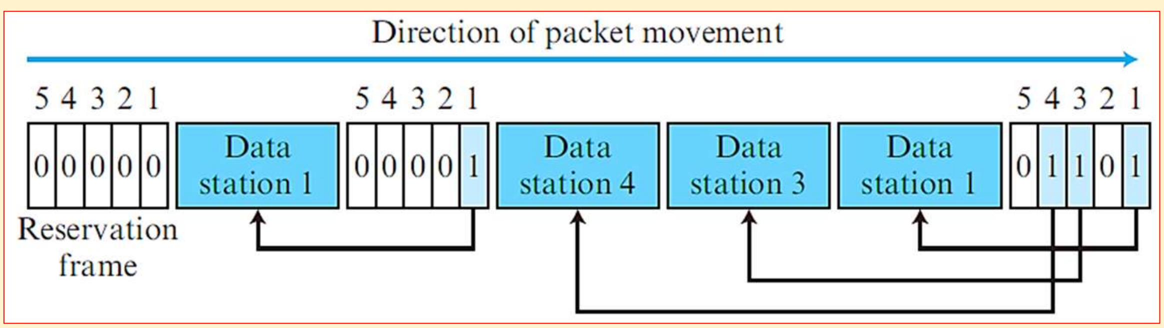
➢controlled-access methods

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

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 128

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



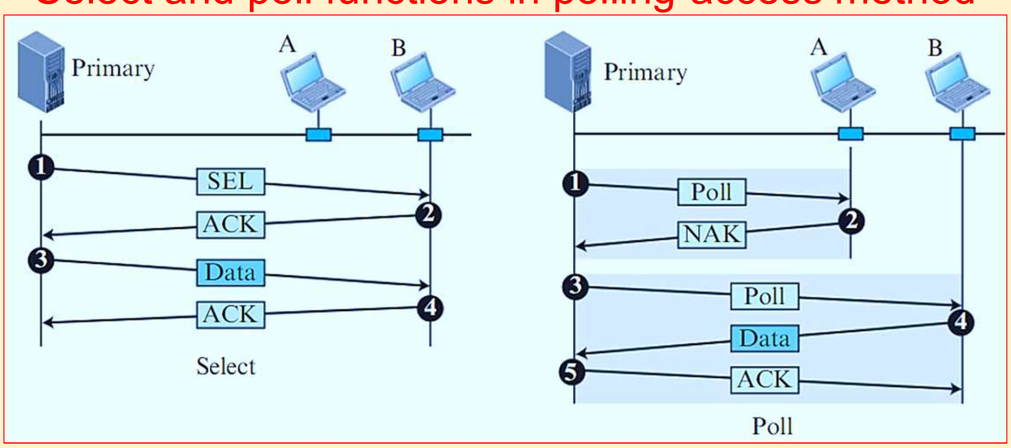
2. Polling

- 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

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 131

- This method uses **poll** and **select** functions to prevent collisions. However, the drawback is if the primary station fails, the system goes down.

Select and poll functions in polling-access method



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 132

➢Select

- The select function is used whenever the primary device has something to send. (the primary controls the link).
- What it does not know is whether the target device is prepared to receive. So the primary must alert the secondary to the upcoming transmission and wait for an acknowledgment of the secondary's ready status.
- Before sending data, the primary creates and transmits a select (SEL) frame, one field of which includes the address of the intended secondary

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 133

➢Poll

- The poll function is used by the primary device to solicit transmissions from the secondary devices.
- When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send.
- When the first secondary is approached, it responds either with a NAK frame if it has nothing to send or with data (in the form of a data frame) if it does.
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send.
- When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 134

3. Token Passing

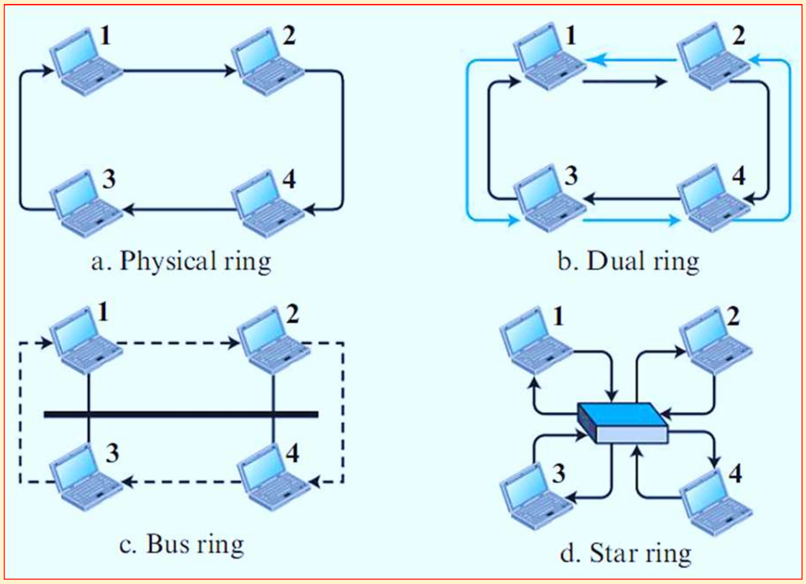
- In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor.
- The current station is the one that is accessing the channel now.
- In this method, a special packet called a **token** circulates through 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.
- Token management is needed for this access method. The token must be monitored to ensure it has not been lost or destroyed.
- Another function of token management is to assign priorities to the stations and to the types of data being transmitted.
- Token management is needed to make low-priority stations release the token to high-priority stations.

Logical Ring

- In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.

Logical ring and physical topology in token-passing access method



- **Physical ring topology**
- In the physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line.
- This means that the token does not have to have the address of the next successor. The problem with this topology is that if one of the links—the medium between two adjacent stations—fails, the whole system fails
- **Dual ring topology**
- The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring.

- The second ring is for emergencies only. If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring.
- After the failed link is restored, the auxiliary ring becomes idle again.
- For this topology to work, each station needs to have two transmitter ports and two receiver ports. The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.

Bus ring topology

- Also called a token bus, the stations are connected to a single cable called a bus.

- They make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes).
- When a station has finished sending its data, it releases the token and inserts the address of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media.
- The Token Bus LAN, standardized by IEEE, uses this topology.

Star ring topology

- In a star ring topology, the physical topology is a star. There is a **hub**, however, that acts as the connector.

- The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections.
- This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate.
- Adding and removing stations from the ring is easier.
- This topology is still used in the Token Ring LAN designed by IBM.

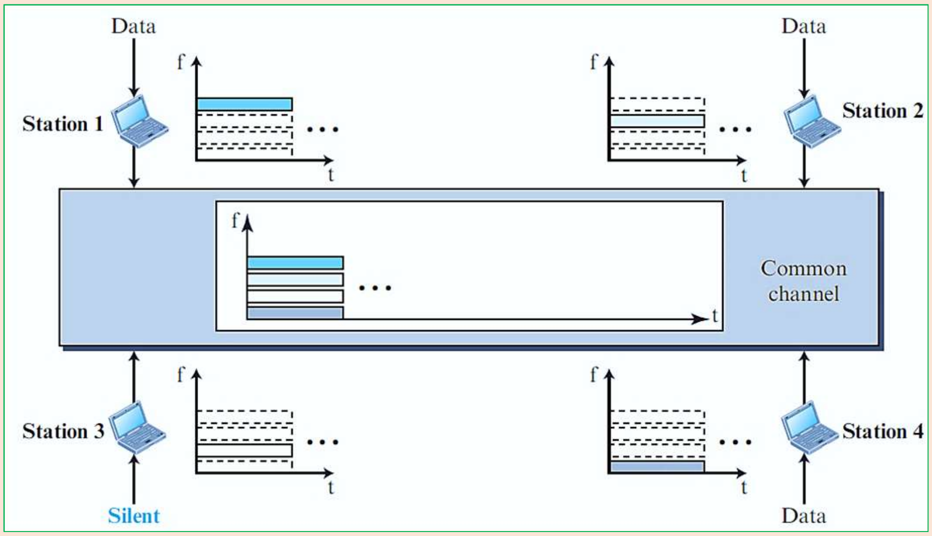
❖CHANNELIZATION PROTOCOLS

- Channelization (or channel partition) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

1. Frequency-Division Multiple Access (FDMA)

- The available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.
- Each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a band-pass filter to confine the transmitter frequencies.

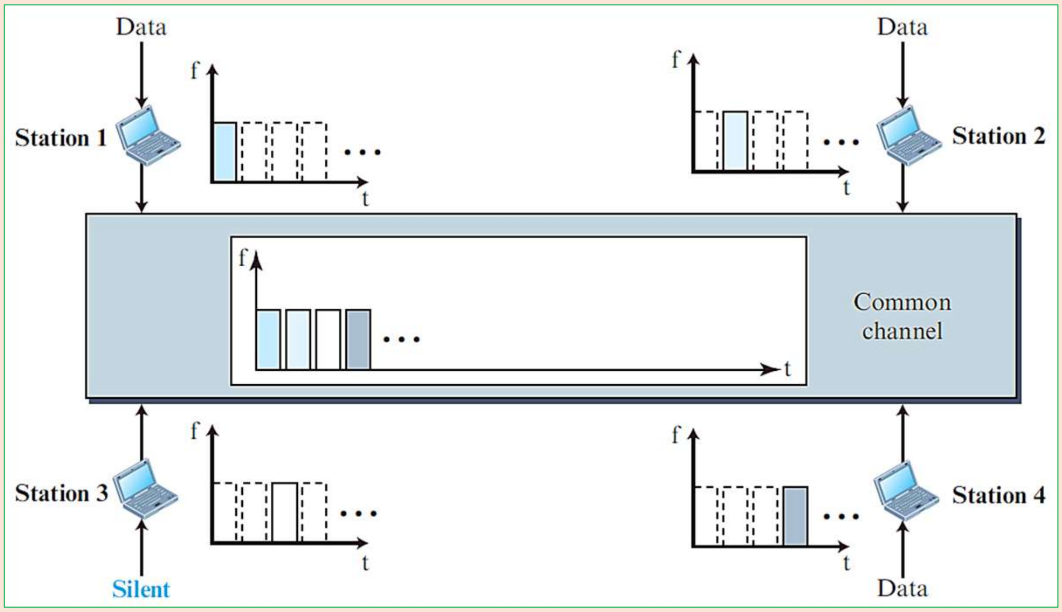
- To prevent station interferences, the allocated bands are separated from one another by small guard bands.



- FDMA specifies a predetermined frequency band for the entire period of communication.
- This means that stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA.
- This feature can be used in cellular telephone systems

2. Time-Division Multiple Access (TDMA)

- The stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data.
- Each station transmits its data in its assigned time slot.

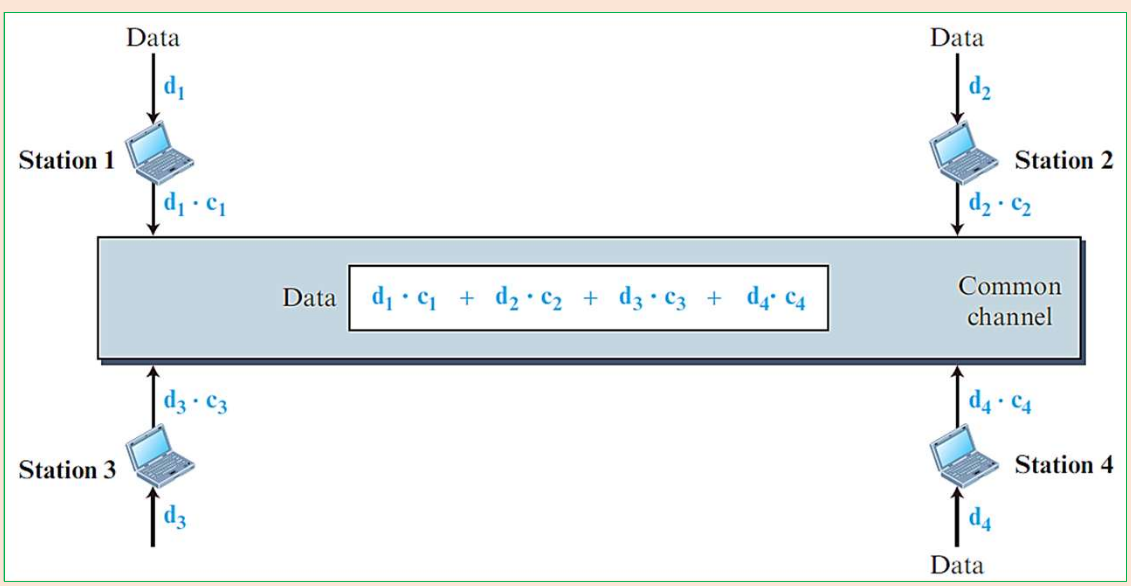


- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot. This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area.
- To compensate for the delays, we can insert guard times. Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.

3. Code-Division Multiple Access (CDMA)

- CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.
- It differs from TDMA because all stations can send data simultaneously; there is no time-sharing
- CDMA simply means communication with different codes.
- For example, in a large room with many people, two people can talk in English if nobody else understands English. Another two people can talk in Chinese if they are the only ones who understand Chinese, and so on.
- In other words, the common channel, the space of the room in this case, can easily allow communication between several couples, but in different languages (codes).

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 147



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 148

- Let us assume we have four stations, 1, 2, 3, and 4, connected to the same channel. The data from station 1 are d1, those from station 2 are d2, and so on.
- The code assigned to the first station is c1, to the second is c2, and so on.
- The assigned codes have two properties.

1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

- Station 1 multiplies (a special kind of multiplication) its data by its code to get $d1 \cdot c1$.
- Station 2 multiplies its data by its code to get $d2 \cdot c2$, and so on.

- The data that go on the channel are the sum of all these terms.
- Any station that wants to receive data from one of the other three stations multiplies the data on the channel by the code of the sender.
- For example, suppose stations 1 and 2 are talking to each other. Station 2 wants to hear what station 1 is saying. It multiplies the data on the channel by c1, the code of station 1.
- Because $(c1 \cdot c1)$ is 4, but $(c2 \cdot c1)$, $(c3 \cdot c1)$, and $(c4 \cdot c1)$ are all 0s, station 2 divides the result by 4 to get the data from station 1.

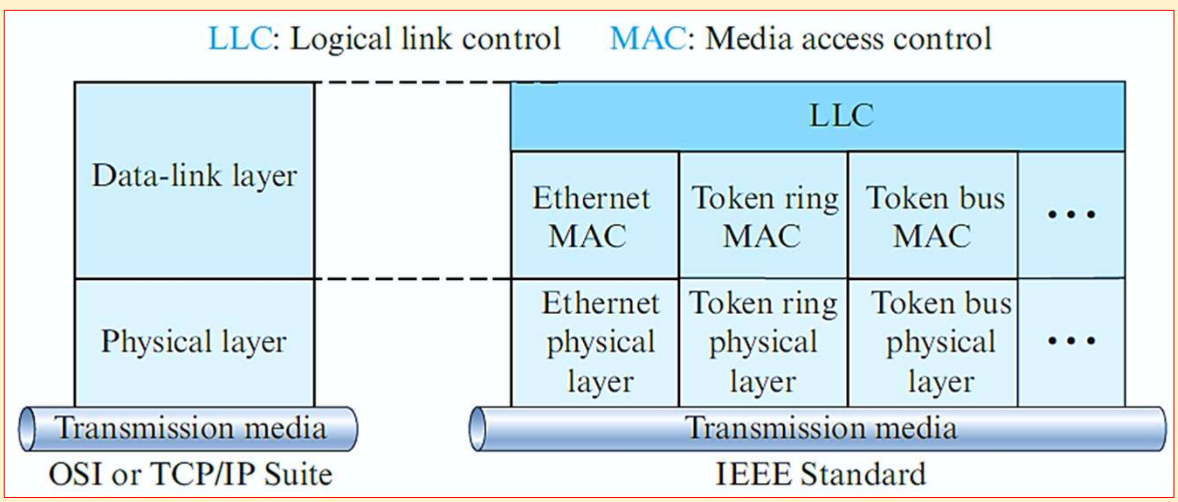
$$data = [(d1 \cdot c1 + d2 \cdot c2 + d3 \cdot c3 + d4 \cdot c4) \cdot c1] / 4 = [d1 \cdot c1 \cdot c1 + d2 \cdot c2 \cdot c1 + d3 \cdot c3 \cdot c1 + d4 \cdot c4 \cdot c1] / 4 = (4 \times d1) / 4 = \mathbf{d1}$$

ETHERNET – WIRED LANs

❖IEEE Project 802

- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.
- Project 802 specifying functions of the physical layer and the data-link layer of major LAN protocols.
- The IEEE has subdivided the data-link layer into two sublayers: logical link control (LLC) and media access control (MAC).
- IEEE has also created several physical-layer standards for different LAN protocols.

IEEE standard for LANs



➢ Logical Link Control (LLC)

- The data link control handles framing, flow control, and error control.
- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control (LLC).
- Framing is handled in both the LLC sublayer and the MAC sublayer.
- The LLC provides a single link-layer control protocol for all IEEE LANs. This means LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

➢ Media Access Control (MAC)

- IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- For example, it defines CSMA/CD as the media access method for Ethernet LANs and defines the token-passing method for Token Ring and Token Bus LANs.
- A part of the framing function is also handled by the MAC layer.

Generations:

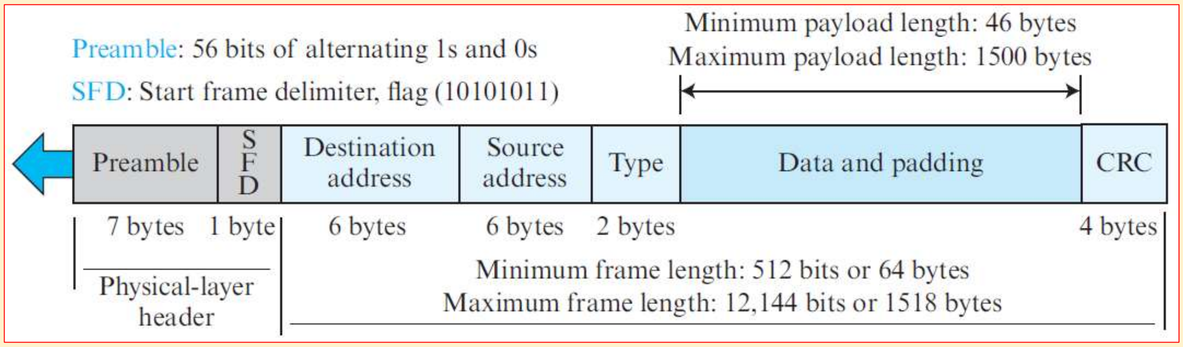
1. Standard Ethernet (10 Mbps)
2. Fast Ethernet (100 Mbps)
3. Gigabit Ethernet (1 Gbps)
4. 10 Gigabit Ethernet (10 Gbps).

1. Standard Ethernet

- We refer to the original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet.

▪ Frame Format

- The Ethernet frame contains seven fields



○Preamble.

- This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.
- The pattern provides only an alert and a timing pulse. The preamble is actually added at the physical layer and is not (formally) part of the frame.

○Start frame delimiter (SFD)

- This field (1 byte: 10101011) signals the beginning of the frame.
- This field is actually a flag that defines the beginning of the frame.
- The SFD field is also added a the physical layer.

○**Destination address (DA)**

- This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.
- When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upper layer protocol defined by the value of the type field.

○**Source address (SA)**

- This field is also six bytes and contains the link-layer address of the sender of the packet.

○**Type**

- This field defines the upper-layer protocol whose packet is encapsulated in the frame.
- This protocol can be IP, ARP, OSPF, and so on. It is used for multiplexing and demultiplexing.

○**Data**

- This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes.
- If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame.
- If it is less than 46 bytes, it needs to be padded with extra 0s.

- A padded data frame is delivered to the upper-layer protocol as it is (without removing the padding), which means that it is the responsibility of the upper layer to remove or add the padding.

○ **CRC**

- The last field contains error detection information, in this case a CRC-32.
- The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

➢ Connectionless and Unreliable Service

- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- Ethernet has no connection establishment or connection termination phases. The sender sends a frame whenever it has it; the receiver may or may not be ready for it.
- The sender may overwhelm the receiver with frames, which may result in dropping frames.
- If a frame drops, the sender will not know about it.
- Ethernet is also unreliable like IP and UDP.

- Minimum frame length: 64 bytes
- Maximum frame length: 1518 bytes
- Minimum data length: 46 bytes
- Maximum data length: 1500 bytes

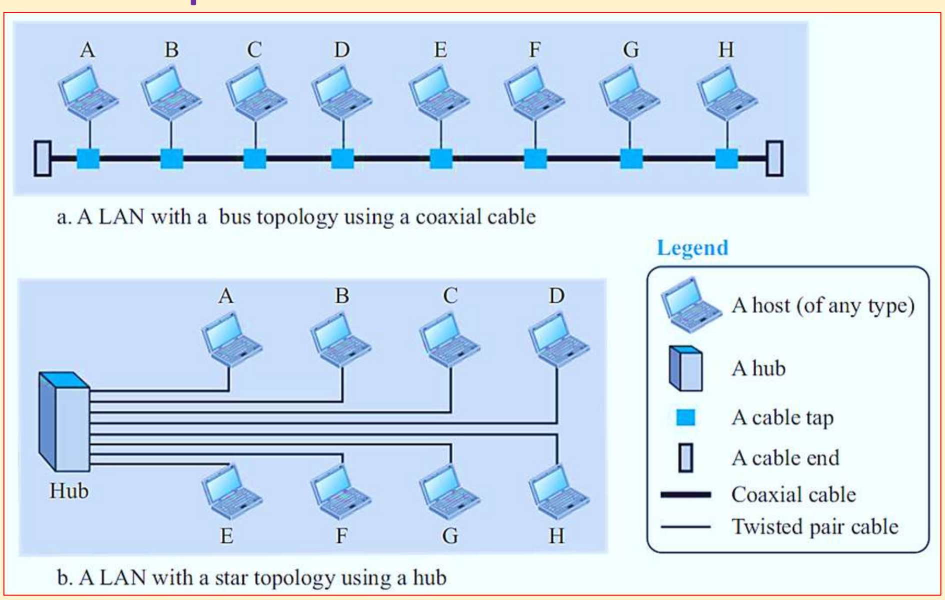
➢Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a link-layer address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 161

Implementation of standard Ethernet



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 162

➢Efficiency of Standard Ethernet

- Efficiency = **$1 / (1 + 6.4 \times a)$**
- The parameter **"a"** is the number of the frames that can fit on the medium.

  a = (propagation delay)/(transmission delay)
- If the length of the media is shorter or the frame size longer, the efficiency increases.
- In the ideal case, a = 0 and the efficiency is 1

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 163

➢Summary of Standard Ethernet implementations

- In the nomenclature **10BaseX**

➢ number defines the data rate (10 Mbps)

➢ Base means baseband (digital) signal

➢ X approximately defines either the maximum size of the cable in 100 meters or the type of the cable

➢T for unshielded twisted pair cable (UTP)

➢F for fiber-optic

- The standard Ethernet uses a baseband signal, which means that the bits are changed to a digital signal and directly sent on the line.
- All implementations use a Manchester encoding

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 164

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000	Manchester

2. Fast Ethernet (100 Mbps)

- The MAC sublayer was left unchanged, which meant the frame format and the maximum and minimum size could also remain unchanged.
- By increasing the transmission rate, features of the Standard Ethernet that depend on the transmission rate, access method and implementation, had to be reconsidered

➢Implementation

- Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
- The two-wire implementation can be either shielded twisted pair (STP), which is called 100Base-TX, or fiber-optic cable, which is called 100Base-FX.
- The four-wire implementation is designed only for unshielded twisted pair (UTP), which is called 100Base-T4.

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

1. Gigabit Ethernet

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps).
- The IEEE committee calls the Standard **802.3z**
- The goals of the Gigabit Ethernet were to upgrade the data rate to 1 Gbps, but keep the address length, the frame format, and the maximum and minimum frame length the same.
- Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full duplex.
- Almost all implementations of Gigabit Ethernet follow the full-duplex approach.

➢Implementation

- The following table is a summary of the Gigabit Ethernet implementations.
- S-W and L-W mean short wave and long wave respectively.

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

1. 10-Gigabit Ethernet

- The IEEE committee created 10-Gigabit Ethernet and called it Standard **802.3ae**
- The goals of the 10-Gigabit Ethernet design can be summarized as upgrading the data rate to 10 Gbps, keeping the same frame size and format, and allowing the interconnection of LANs, MANs, and WAN possible.
- This data rate is possible only with fiber-optic technology at this time. The standard defines two types of physical layers: LAN PHY and WAN PHY. The first is designed to support existing LANs; the second actually defines a WAN with links connected through SONET OC-192

➢Implementation

- 10-Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention
- CSMA/CD is not used in 10-Gigabit Ethernet.
- Four implementations are the most common: 10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4.

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

WIRELESS LANs (WiFi)

❖IEEE Project 802.11

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- In some countries, including the United States, the public uses the term **WiFi** (short for **wireless fidelity**) as a synonym for wireless LAN.
- WiFi, however, is a wireless LAN that is certified by the WiFi Alliance, a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.

➢Architecture

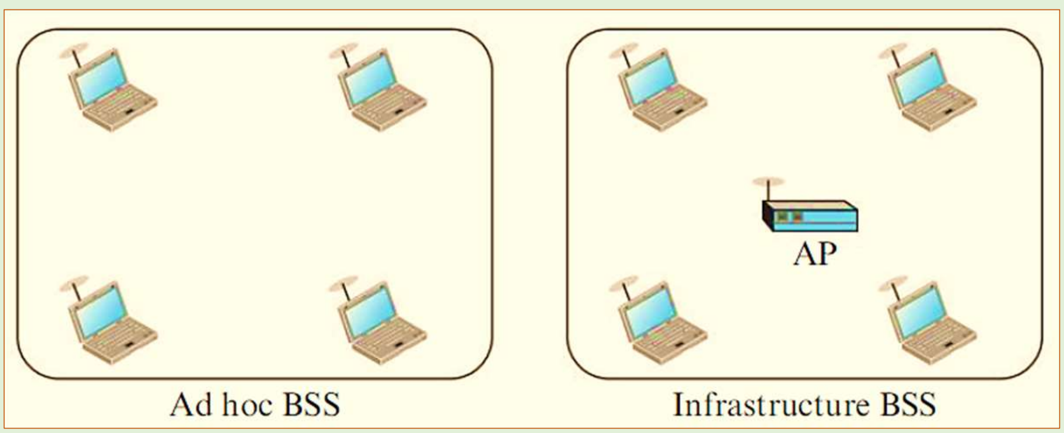
- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS)

▪ Basic Service Set

- IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an **ad hoc** architecture.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 173

- A BSS with an AP is sometimes referred to as an **infrastructure** BSS.



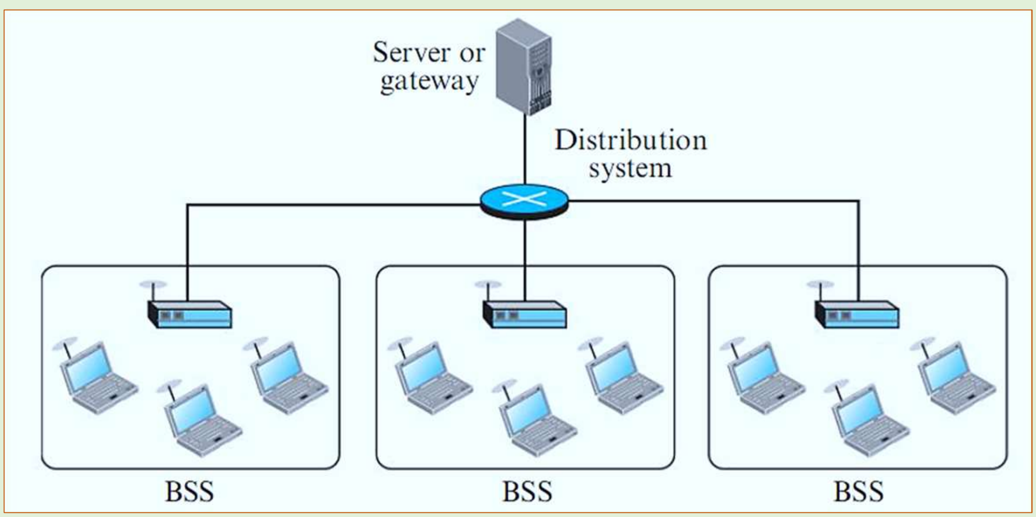
Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 174

Extended Service Set

- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a distribution system, which is a wired or a wireless network. The distribution system connects the APs in the BSSs.
- IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- Note that the extended service set uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN.

Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 175

Extended service set (ESS)



Prepared By Mr. EBIN PM, Chandigarh University, Punjab EDULINE 176

➢Station Types

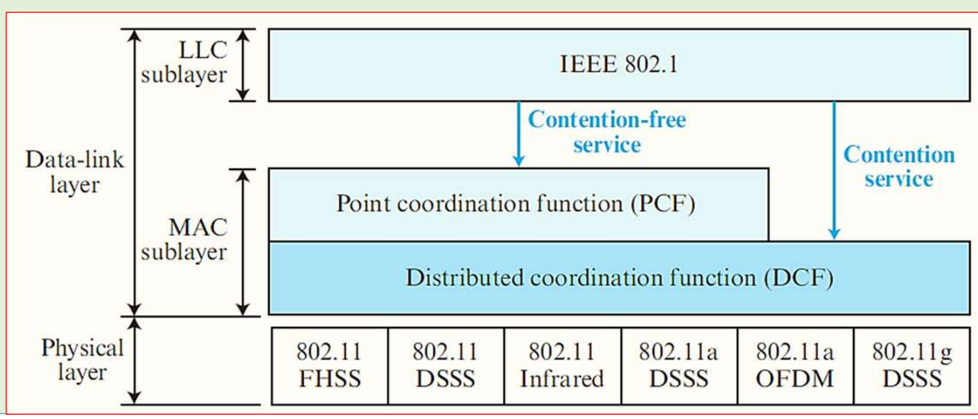
- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition , BSS-transition and ESS-transition mobility.
- A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS.
- A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- A station with ESS-transition mobility can move from one ESS to another.
- However, IEEE 802.11 does not guarantee that communication is continuous during the move.

➢MAC Sublayer

- IEEE 802.11 defines two MAC sublayers:

  Distributed Coordination Function (DCF)

  Point Coordination Function (PCF)



❖Distributed Coordination Function

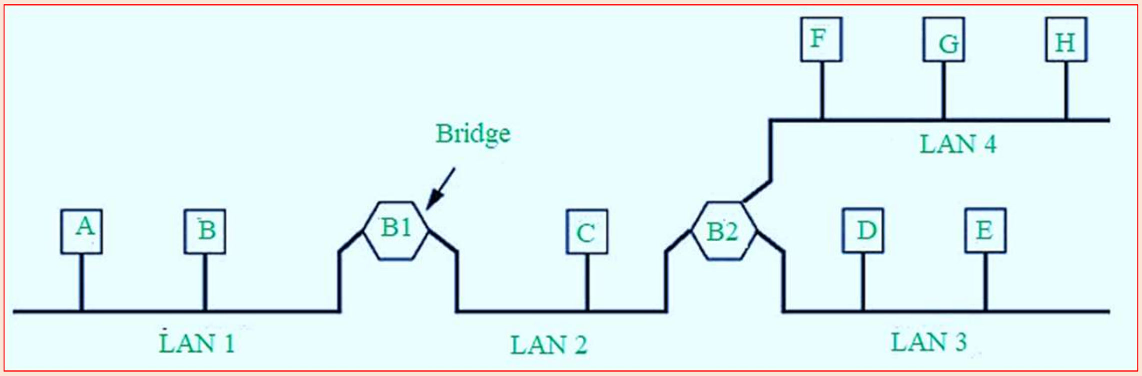
- It is a protocol defined by IEEE at the MAC sublayer
- DCF uses CSMA/CA as the access method

❖Point Coordination Function (PCF)

- The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network).
- It is used mostly for time-sensitive transmission.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

❖Bridges

- Bridges are a data link layer device and can connect to different networks as well as connect different networks of different types.
- Bridges from 802.x to 802.y where x & y may both be Ethernet or one can be Ethernet and other may be a token ring, etc.
- It locally connects small LANs, whereas if LANs are big then bridges can no longer handle them.
- Bridge follows a protocol in IEEE format execute 802.1 which is a spanning tree of bridges.
- It stores and forwards Ethernet frames, i.e., it has to do with the MAC address, they handle the hardware addresses.



- It also examine the frame header and selectively forward frames based on MAC destination address, such as in the given figure if Bridge 2 receives a packet then it will selectively decide whether to send it to LAN 3 or LAN 4.

- When a frame is to be forwarded in a segment it uses CSMA/CD to access the segment.
- The hosts are unaware of the presence of bridges, it appears to them as a single whole network.
- Bridges need not be configured they are plug-and-play and self-learning devices, i.e. a bridge has a learning table, they learn which hosts can be reached through which interfaces.
- At the physical level, the bridge boosts the signal strength like a repeater or completely regenerates the signal.