CN Module 2 Important Topics

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

Fixed Size framing

- No Boundary for the frames

Variable Size framing

- Define end of the frame and beginning of the next

Approaches

- Character Count
- Flag bytes with byte stuffing
- Bit Stuffing

Stop and wait Automatic Repeat Request

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

Stop and wait ARQ

Stop and wait ARQ adds a simple error control mechanism to the Stop-and-Wait Protocol

Corrupted frames

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

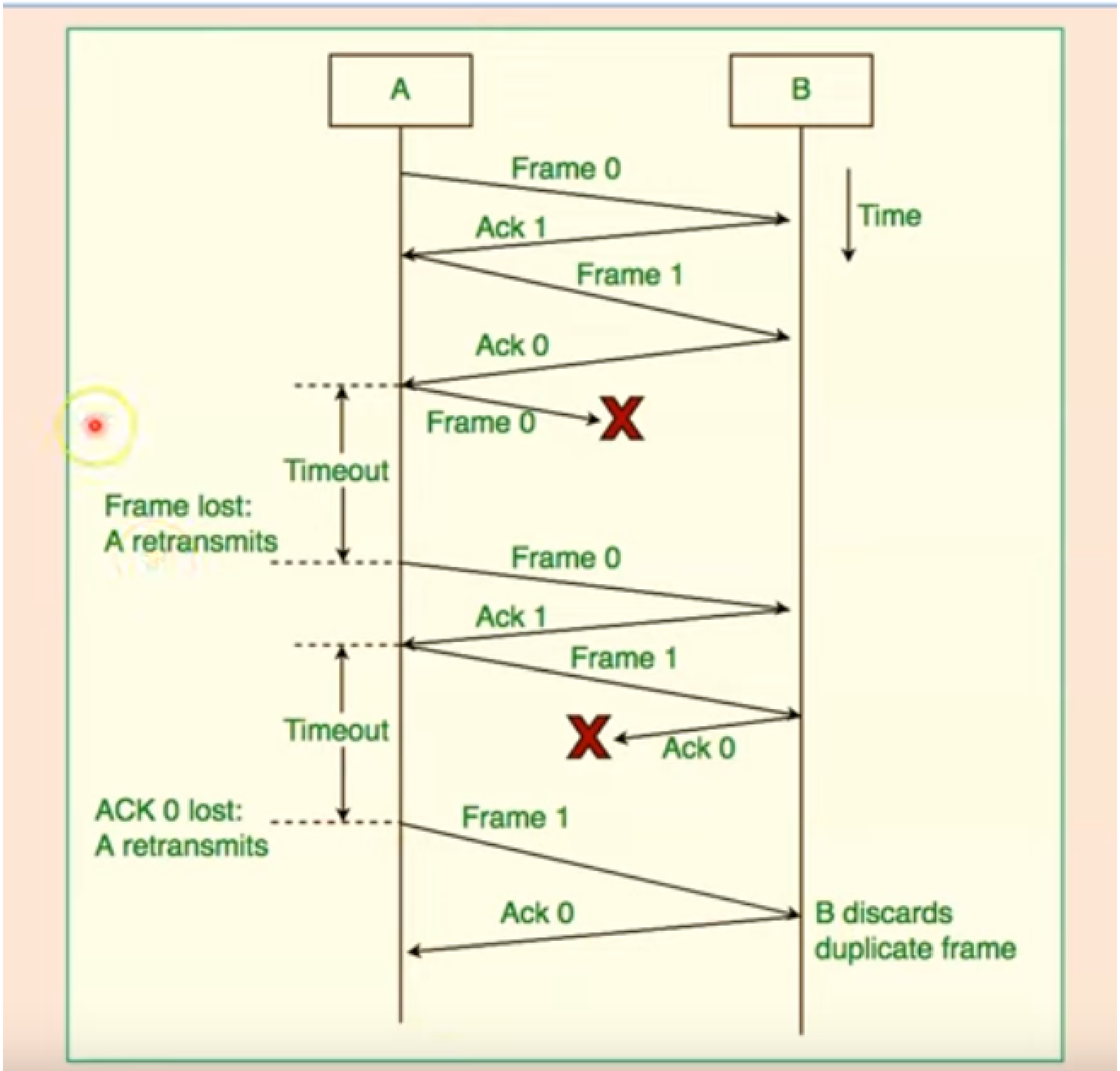
- Lost frames are more difficult to handle than corrupted ones.
- The received frame could be the correct one, or a duplicate, or a frame out of order.
- The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.
- 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.

Sequence Numbering

- 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.
        1. 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.

Acknowledgement 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).



- Frame 0 is sent
- Gets acknowledgement
- Frame 1 is sent
- Gets acknowledgment
- Frame 0 is sent
    - It failed
    - Waited until timeout

- After timeout
  - Frame 0 is sent
  - Acknowledgement is received
  - Frame 1 is sent
  - Ack 0 is failed to be received
- Timeout
- After timeout, Frame 1 is retransmitted

Go back N ARQ

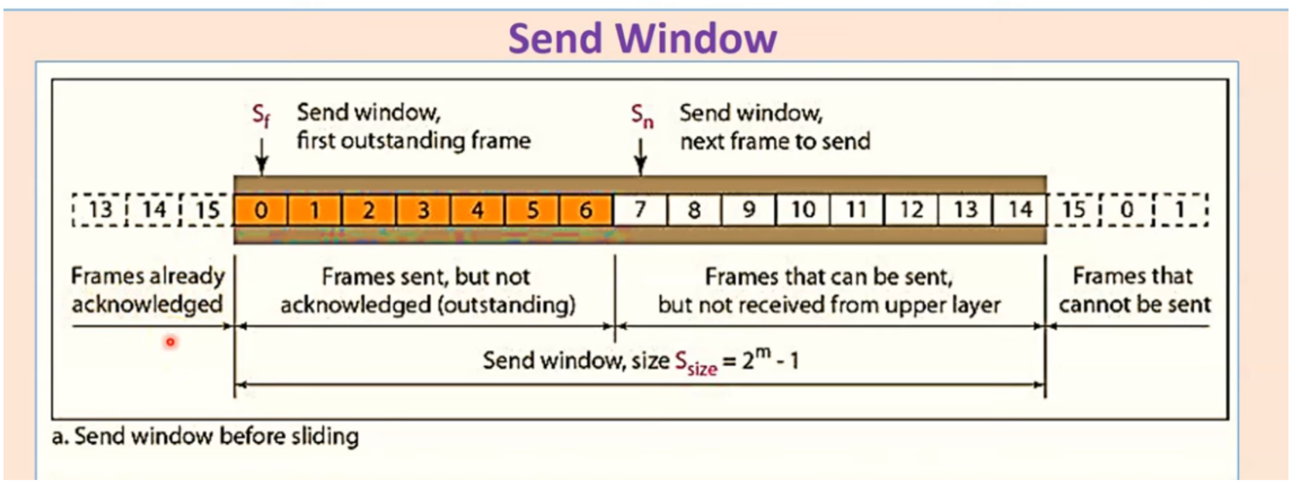
- In this protocol we can send several frames before receiving acknowledgments

Sequence numbers

- Frames from a sending station are numbered sequentially.
- If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to $2m$ - 1.
- or example, if m is 4, the only sequence numbers are 0 – 15.

Sliding window

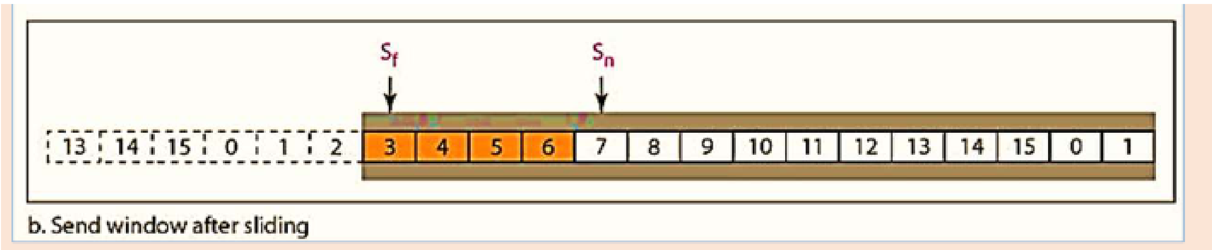
- The sliding window at any time divides the possible sequence numbers into four regions



Send Window

- The four regions are
  - Frames already acknowledged
    - 13,14,15

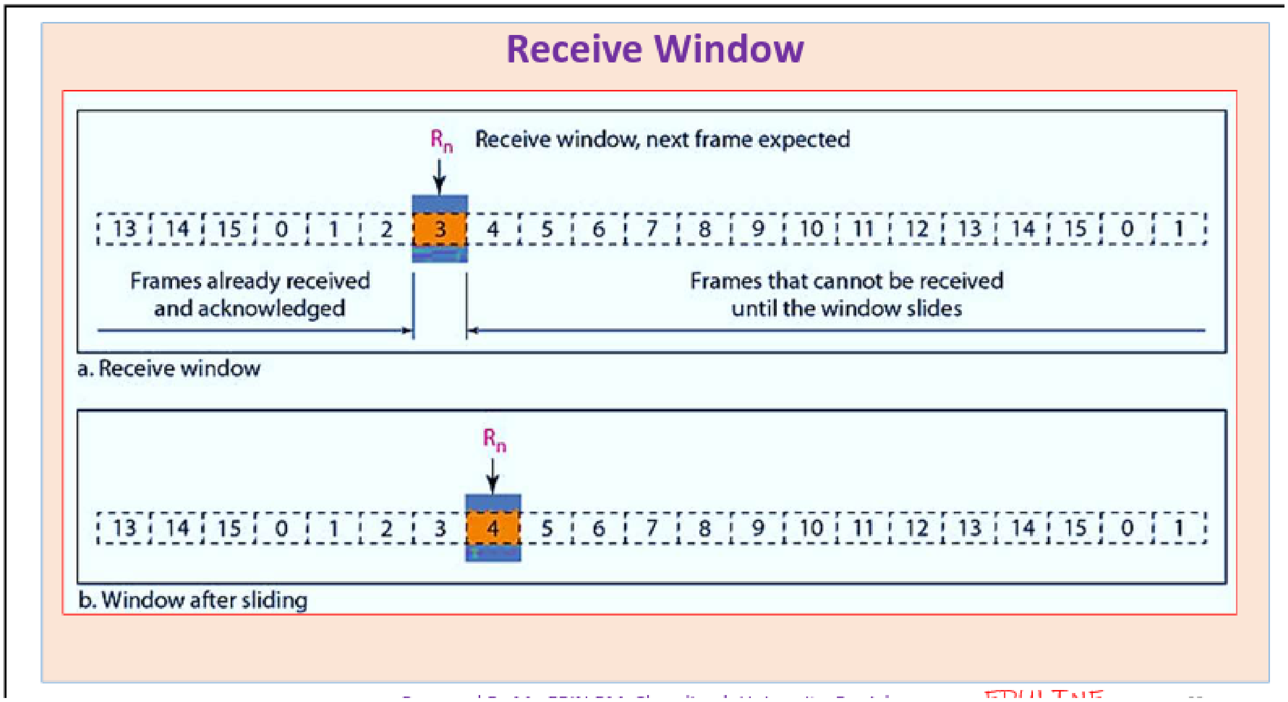
- Frames sent but not acknowledged
- Frames that can be sent but not received from upper layer
    - Here upperlayer = Network Layer, which is the layer above Data link layer
- Frames that cannot be sent

- There are 3 variables with the sliding window
    - Sf -> send window, first outstanding frame (Frames which are sent but not acknowledged)
        - Defines Sequence number for the first outstanding frame
    - sn -> Send window next frame to be sent
        - Sequence number that will be assigned to the next frame to be sent
        -
    - SSize -> Send window size
- The Acknowledgements are cumulative
    - With one ACK we can acknowledge multiple frames, In this example, frames 0,1 and 2 are acknowledged
    - 

    - the Sf is also slided accordingly, to 3 positions

Receive Window

- Size of receive window is 1

- 

- 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

Receiver Acknowledgement

- The receiver sends a positive acknowledgement 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 time
- The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgment for several frames

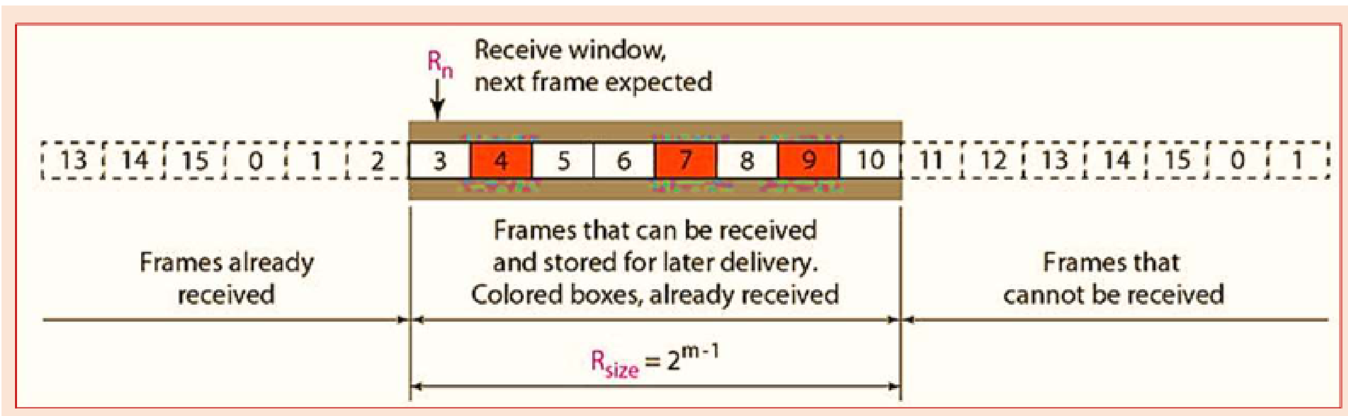
Resending a frame

- 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.

Selective repeat ARQ

- Go Back N ARQ sends multiple frames
- does not resend N frames when just one frame is damaged; only the damaged frame is resent.
- The Selective Repeat Protocol also uses two windows: a send window and a receive window
- In Send window the size is of the window is $2^{(m-1)}$
- Receive window is the same size of send window

Out of order receive



- Out of order will wait for their neighbours to finish, and then be received

---

Hamming distance & Hamming code (Problem)

Hamming distance

- The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits.
- 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.
  - XOR -> Same values = 0
  - XOR -> Different Values = 1
- 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 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

Detection

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

Correction

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

Hamming code

- 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.

Hamming code structure

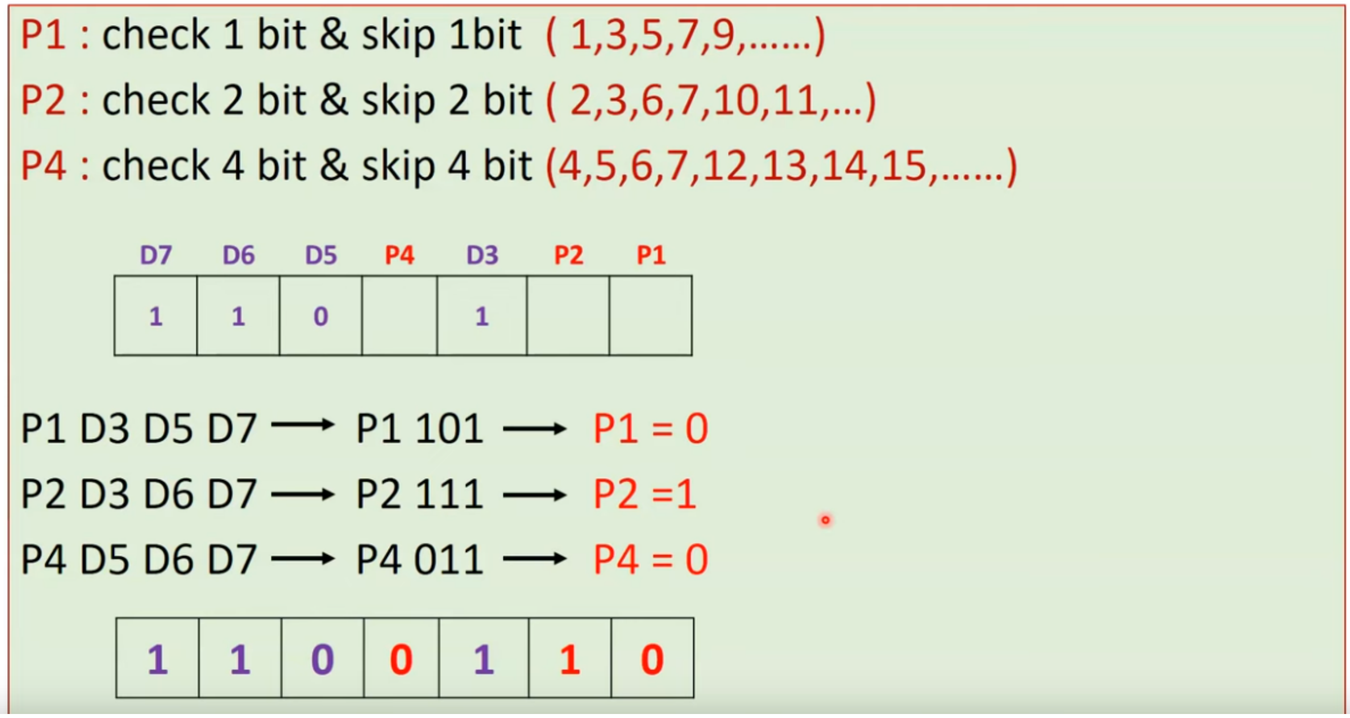
- Bit positions which are power of 2 are parity bit positions
- ➢All the bit positions that are power of 2 are marked as parity bits (1,2,4,8,.....) and other bits are for data.

  Eg: 7 bit hamming code

D7	D6	D5	P4	D3	P2	P1

- Here P1, P2, P4 are parity bits
  - occupies 1,2 and 4 positions = Power of 2
- D3,D5,D6,D7 are Data bits

Finding The parity value

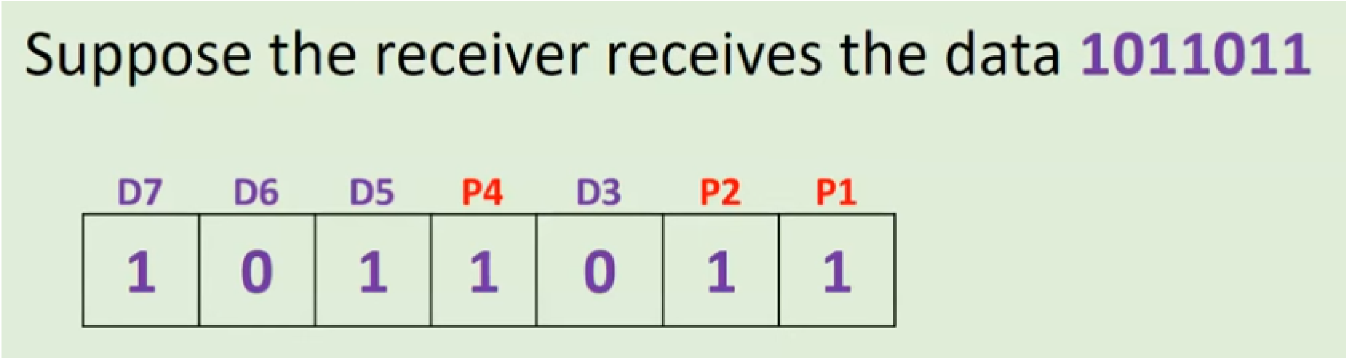


- Finding P1,P2,P4
    - The values available = 1,3,5,7,9..
    - P1, D3,D5,D7 ->P1 101
        - Values of D3,D5,D7 are 1,0 and 1
    - P2 D3,D6,D7 -> P2 111
        - Values are 111
    - P4 D5 D6 D7
        - Values are P4 011
- From the values
    - We have
        - P1 101
            - Number of 1's = 2 -> Even parity -> 0
        - P2 111
            - Number of 1's =3 -> Odd Parity -> 1
        - P4 011
            - Number of 1's = 2 -> Even parity -> 0

So we have

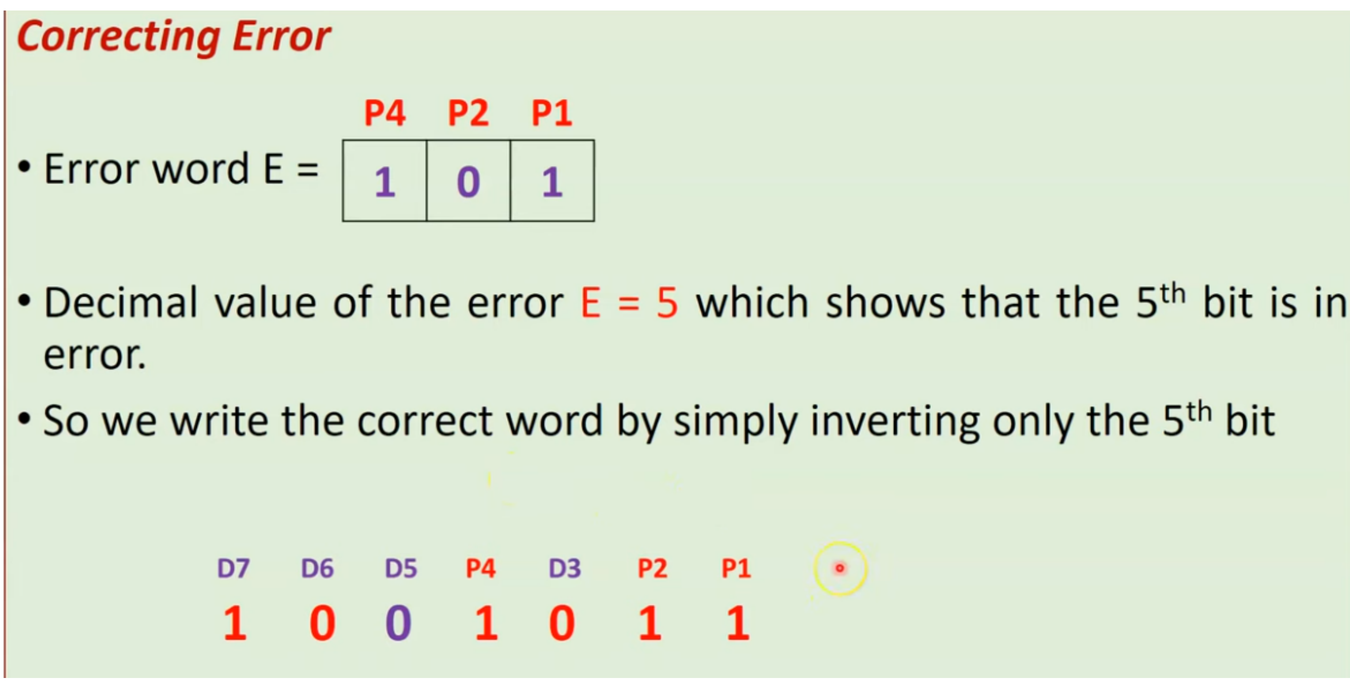
- P1 = 0
- P2 = 1
- P4 = 0

Detecting Error

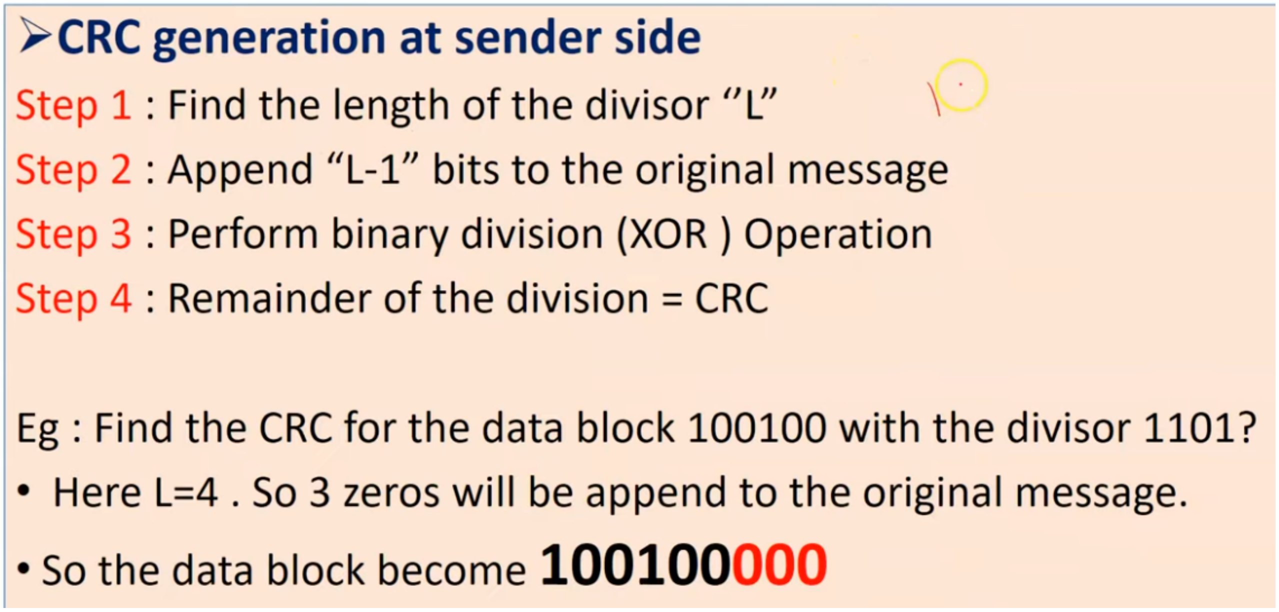


1. Analyse P1
    1. Since its P1, Check one bit, Skip one bit, Repeat
        1. Bits -> 1,3,5,7 ->1,0,1,1
        2. 1011 -> number of 1's = odd -> Error is there -> Set P1 = 1
2. Analyze P2
    1. Since its P2, Check 2 bits, skip 2 bits, repeat
        1. Bits = 2,3,6,7
        2. 1001 -> Number of 1's =2 = even -> Error is no there -> Set P2 = 0
3. Analyse P4
    1. SInce its P3, Check 4 bits, skip 4 bits, Repeat
    2. Bits = 4,5,6,7
    3. 1101 -> Number of 1's = 3 -> Odd -> Error is there

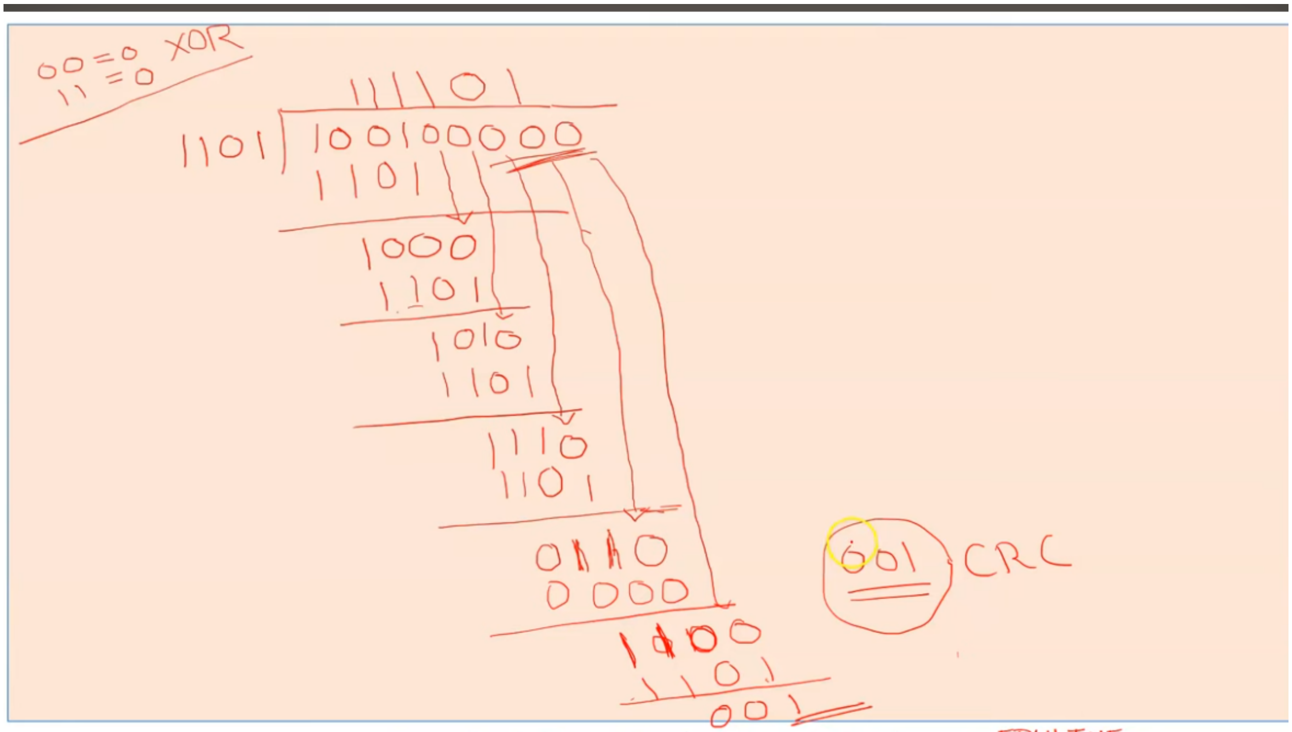
Correcting Error



CRC - Problem

- Cyclic Redundancy Check (CRC) is used in networks such as LANs and WANs.
- It is an error detection method based on binary division
- 

- Here the divisors length is 4
- L-1 = 4-1 bits = 3 bits are appended to original message
  - 100100 -> 100100000
- Perform Binary Division (XOR)
  - 1 and 1 = 0, 0 and 0 = 0, 1 and 0 = 1

- 

- Remainder is 001
- Replace the last 000 we have appended earlier with the CRC

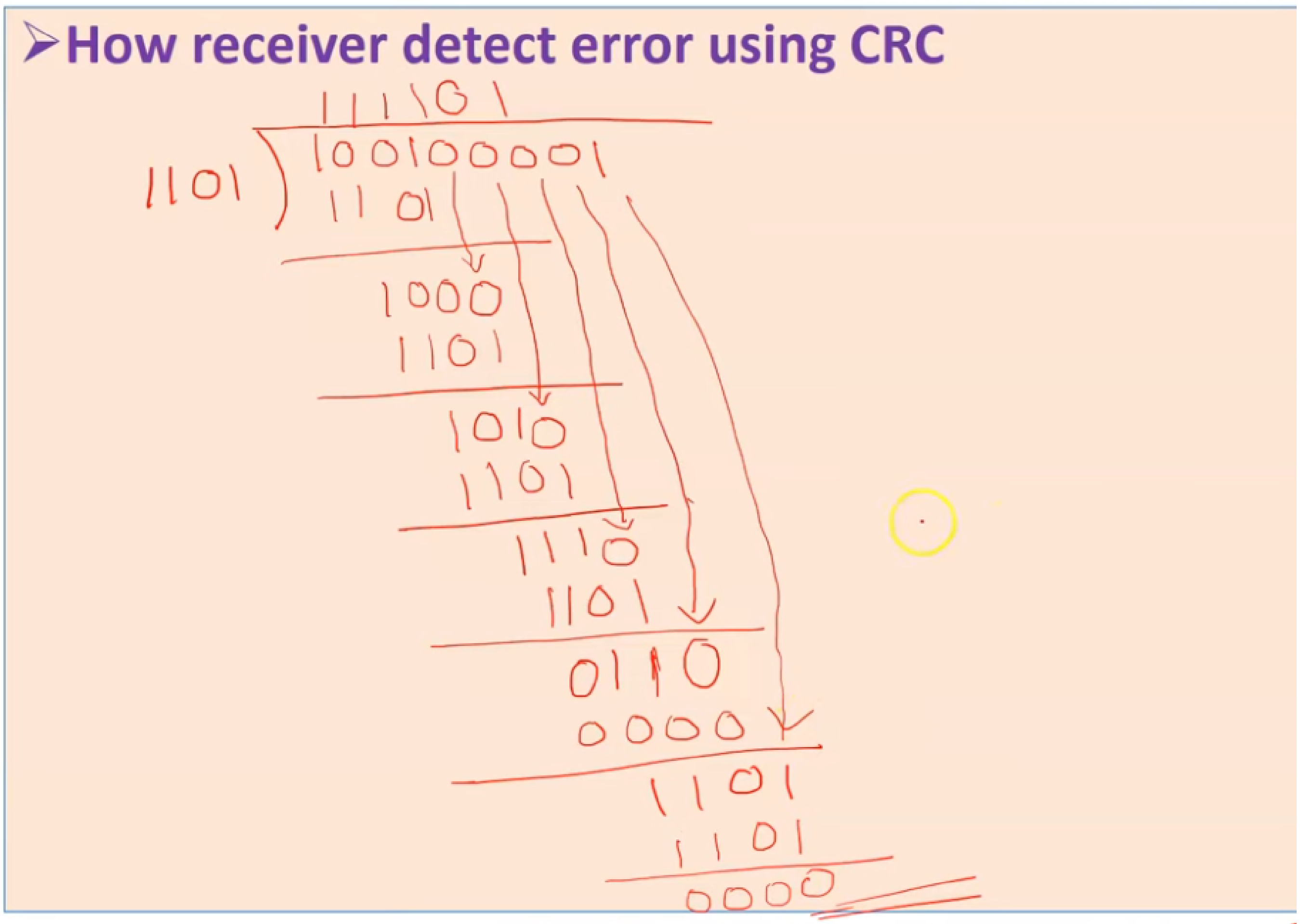
- Now it becomes
  - 100100 -> 100100000 -> 100100001

Sometimes the given divisor will be in polynomial form, we need to convert it

Example

- x^3+x^2+1 = 1101 ->x is not present, so that position is marked as 0
- x^2+x^1+1 = 111

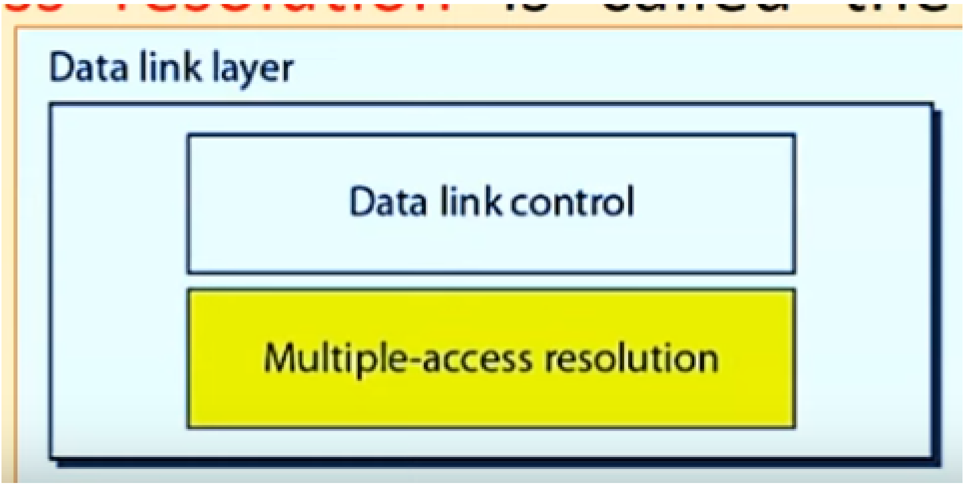
If Remainder is 0, then theres no errors



Multiple access protocols

- The data link layer has 2 sublayers
- Upper sublayer = data link control

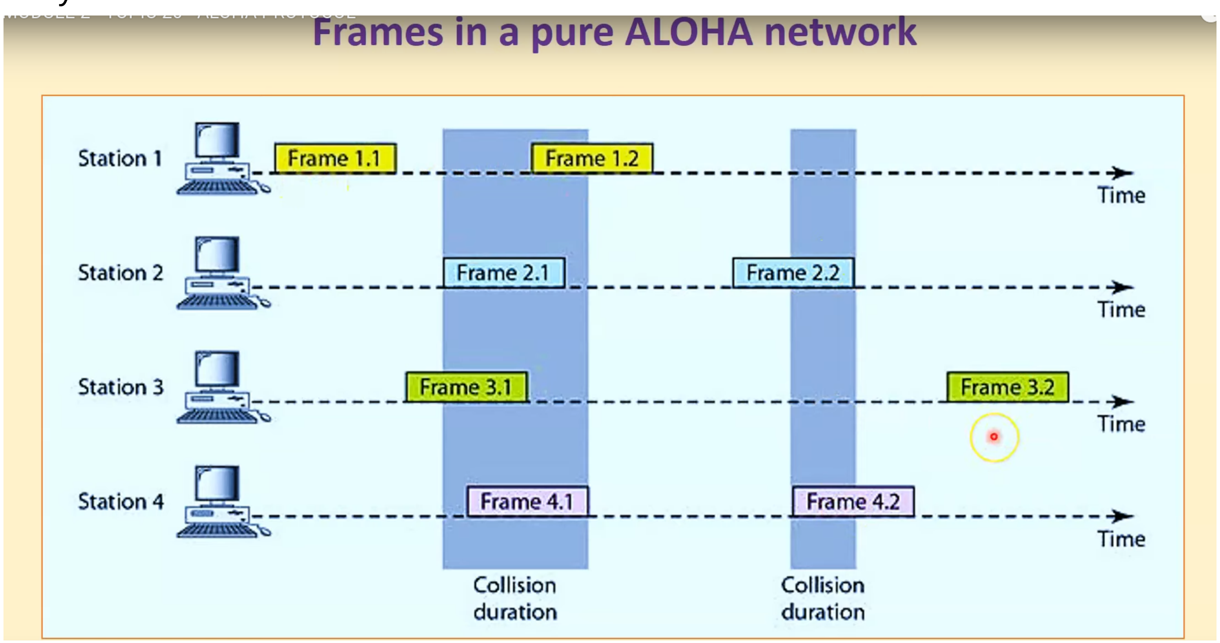
- Lower sublayer = Access to the shared media



Random access Protocols

- No scheduled time for a station to transmit
  - Thats why its called random access
- Stations compete with each other to access the medium

ALOHA

- It was designed for Radio(Wireless) LAN, can be used on any shared medium
- Each Station sends a frame whenever it has a frame to send
- Possibility of collision from different stations are there
  - 

  - Here, Frame 1.2,2.1,3.1 and 4.1 are having collision
  - Frame 2.2, 4.2 Also has collission
  - When collision happens these frames will be destroyed

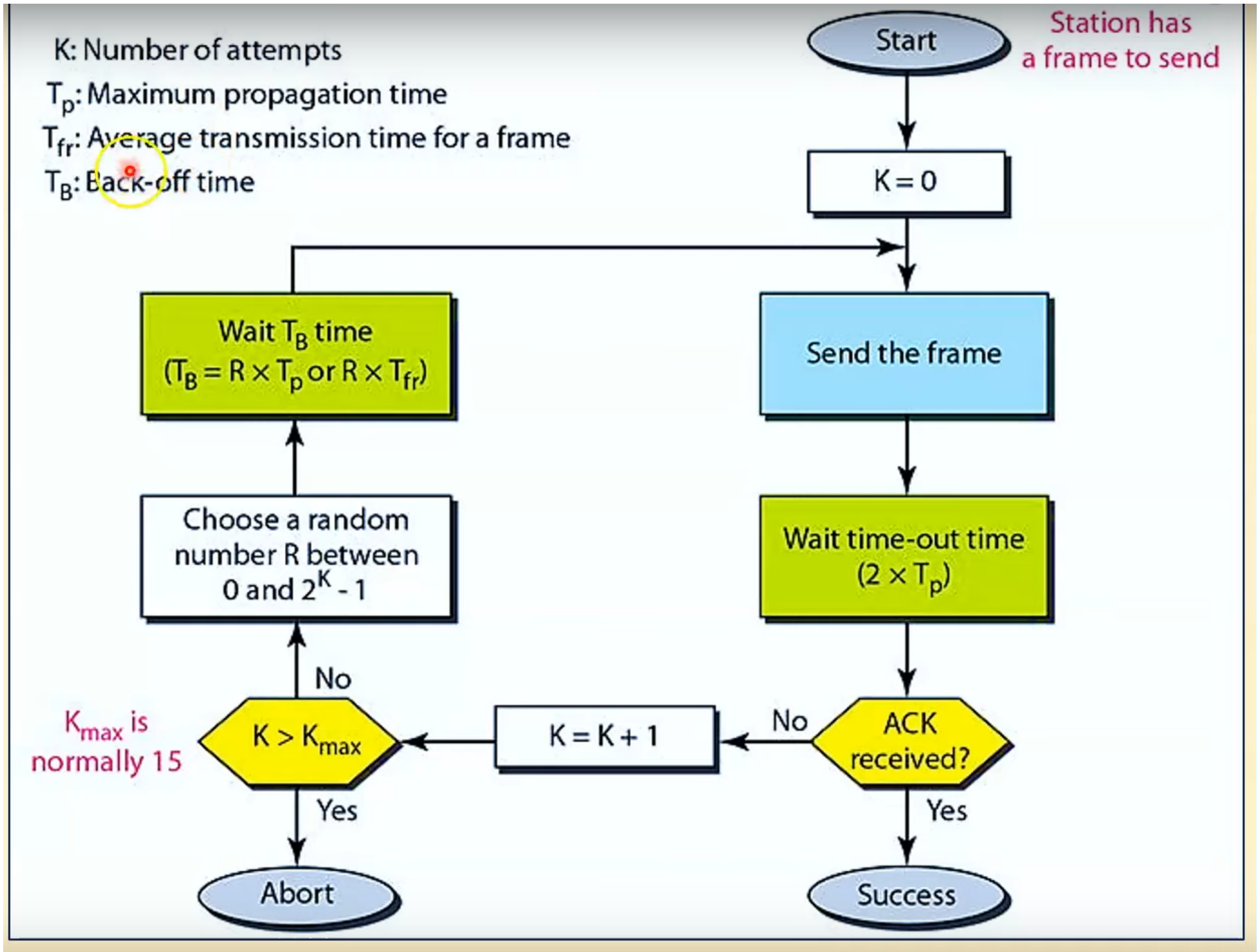
        - The destroyed frames need to be resent
    - So, only 2 Frames survive(The ones that didnt have any collision)
        - Frame 1.1 and 3.2
- ALOHA Relies on acknowledgements from the receiver
    - It expects the receiver to send an acknowledgement
    - If the acknowledgement doesnt appear after timeout
        - Sender assumes the frame is destroyed and resends the frame
- Theres another problem
    - If these frames for example 1.2,2.1,3.1 and 4.1 are Collided and their frames are resent at the same time, Then a similar collision will happen again
    - To solve this issue, ALOHA waits a random amount of time before resending a frame, so that no collision will occur
        - This time is called backoff time TB
        - • 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.
    - Another solution is
        - A retransmission limit
            - After this limit, the station must give up and try later

Procedure for pure ALOHA

1. Start
2. K=0 (K=Number of attempts)
3. Send the frame
4. Wait for the time out(Timeout = 2xtp) (tp = Maximum propogation time)
5. If acknowledgment is received
    1. Success
6. Else
    1. If number of attempts > Max Attempts (K>Kmax)
        1. Abort
    2. Else
        1. Choose a random number R between 0 and 2^k-1
        2. Wait for the backoff time
            1. Backoff time = R x Maximum Propogation Time or R x Average transmission time

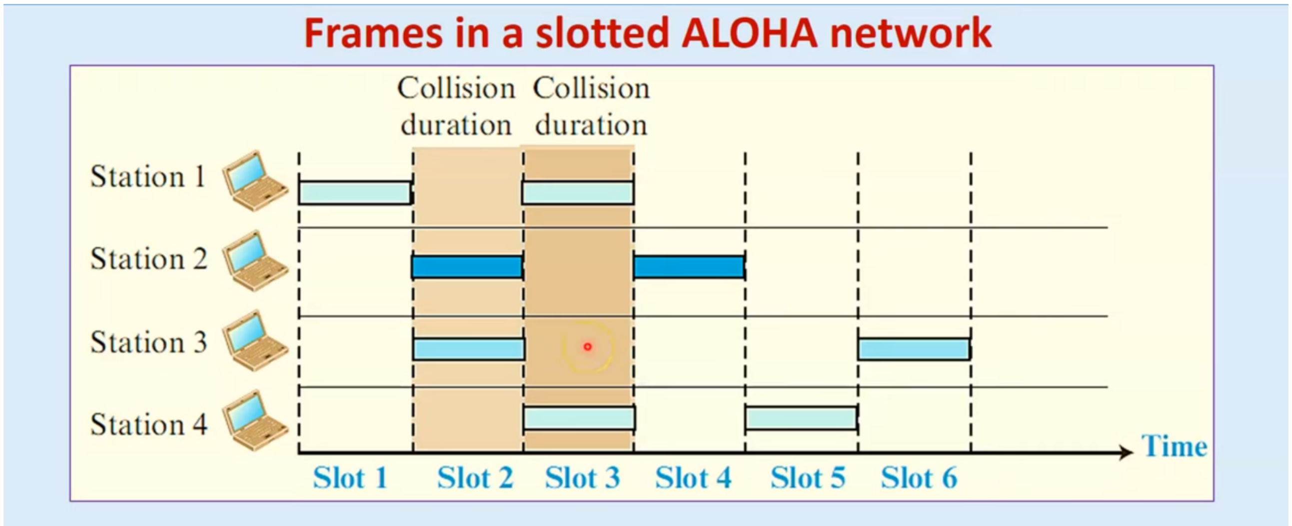
3. Go to step 3



Vulnerable time for Pure ALOHA = 2 x Tfr

Slotted ALOHA

- Invented to imprve efficiency of pure ALOHA
- Time is divided into slots
  - Each slot is of Tfr seconds
- Station is only allowed to send at the beginning of each slot
- If it misses the beginning, it needs to wait for the next slot

- 

Slotted ALOHA Vulnerable time = Tfr

CSMA (Carrier Sense Multiple Access)

- CSMA was developed to minimise collission
- CSMA Requires each station must listen to the medium or check state of medium before sending
- Can reduce collision but not eliminate it

Vulnerable time of CSMA = Propogation time

Persistence methods

Methods when station finds a channel busy

1 Persistent

- If a station finds a channel idle, it sends frame immediately
  - Highest chance of collission because multiple stations will think the channel is idle and send together

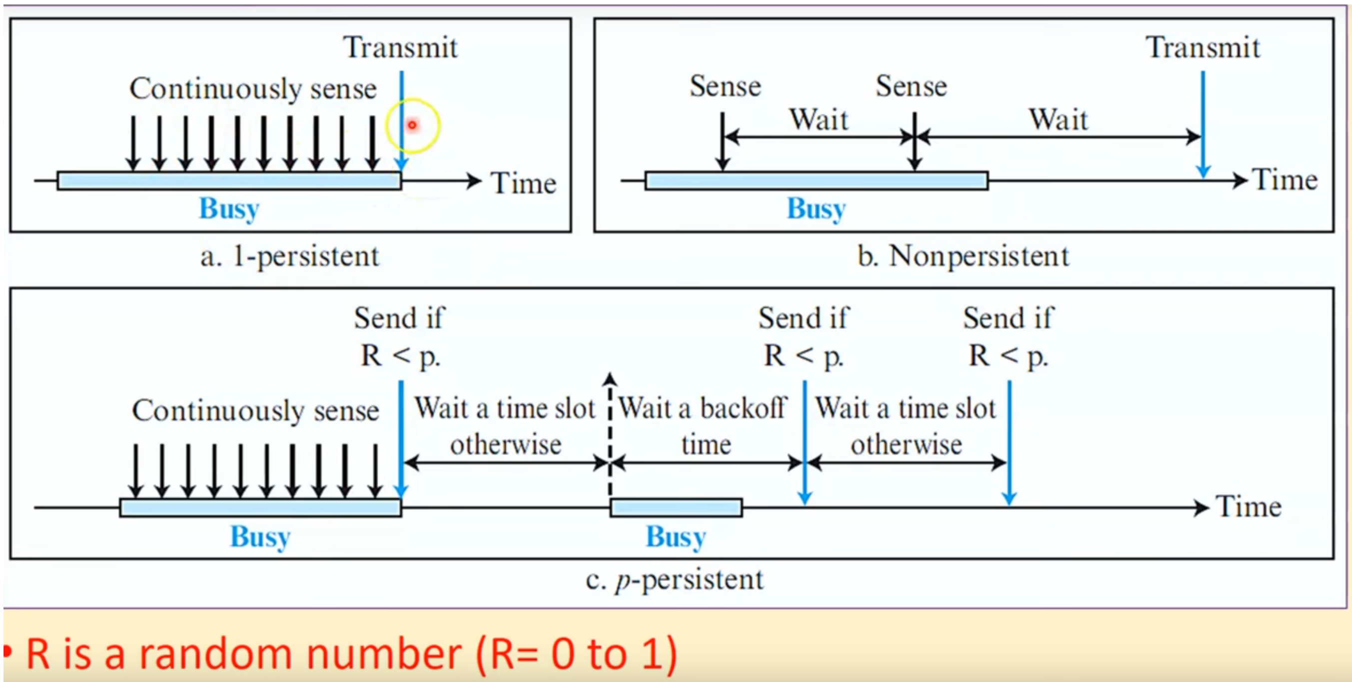
Non Persistent

- Senses the line, if idle, sends the frame immediately
- If not idle, waits a random time and senses again

P-Persistent

- Reduces chance of collission and improves efficiency
- Station wants to send a frame

  - When its idle, it sends the frame
  - If its busy
    - Waits for the beginning of the next time slot
      - if its idle
        - Send the frame
      - If its busy
        - act like collission has occured and do the backoff procedure



CSMA /CD (Carrier Sense Multiple Access, with collision detection)

- Station monitors the medium after it sends a frame to see if tranmission was successful
- If theres collission the frame is sent again
- Monitoring is done using Energy Levels

Energy Levels

- Zero Level
  - Idle
- Normal Level
  - Successfully captured channel and sending frame
- Abnormal Level
  - Collission is there and Energy is twice the normal
- CSMA/CD has higher throughput than Pure/Slotted ALOHA

CSMA /CD (Carrier Sense Multiple Access, with collision avoidance)

- Invented for wireless network
- Collissions are avoided using 3 strategies
  - The interframe space
  - The contention window
  - Acknowledgment

The interframe Space

- When an idle frame is found, station doesnt send immediately, it waits for a period of time called IFS
- If after IFS time, its still idle, it needs to wait till contention time

Contention window

- Amount of time divided into slots
  - A station that is ready to send, will choose a random slot from this contention window
  - Number of slots depends on the backoff strategy
    - its set to one slot, then doubles if station cant find idle

Acknowledgment

- Positive acknowledgement and timeout timer can help guarantee receiver has recieved the frame

Controlled access protocols

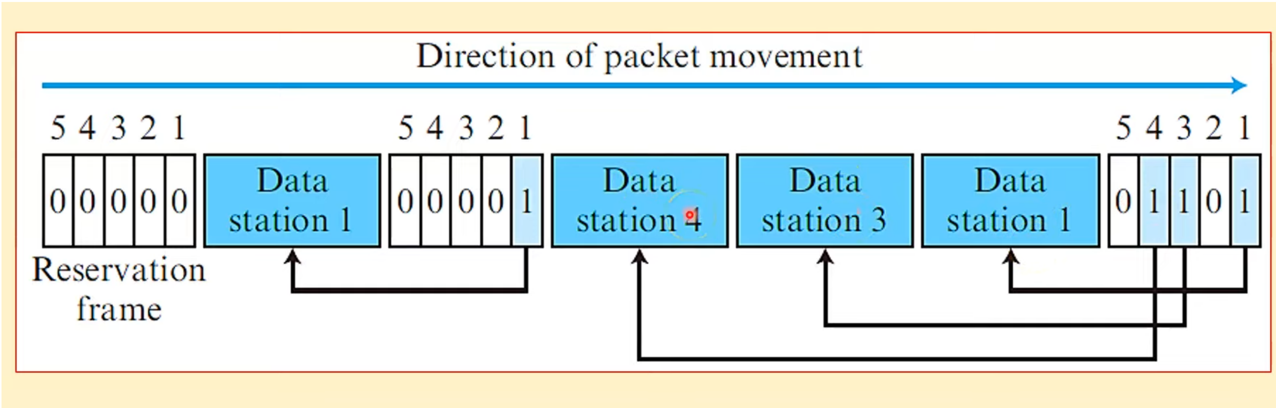
- The stations consult one another to find which station has the right to send'
- A station cannot send unless its authorized by other stations

Controlled Access Methods

Reservation

- In 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



- 5 Slots means 5 stations
- See the rightmost reservation frame
  - 0 1 1 0 1
  - 1,3,4 are sending the frames thats why they are 1

Polling

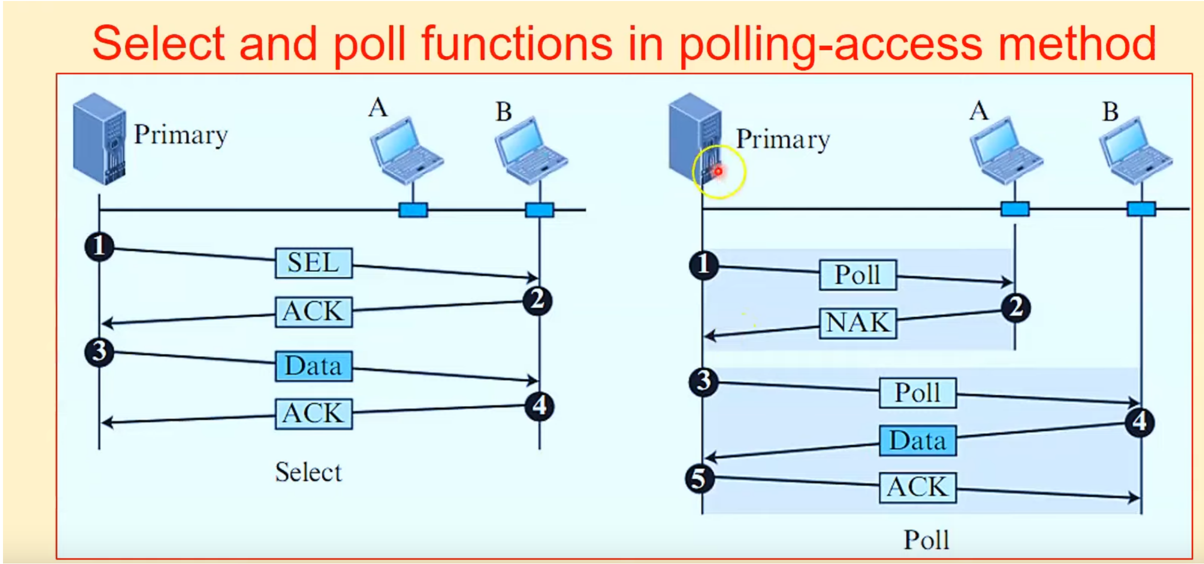
- Works on topologies where one device is designated as a primary station and other devices, secondary stations
- All data exchanges through primary device
- Primary device decides which machine uses the channel at a given time
- Uses select and poll functions to prevent collisions
- The drawback is that, if primary device fails, the whole system goes down

Select Function

- Used when Primary device has something to send
- Transmits Select frame to get acknowledgement from target secondary device

Poll Function

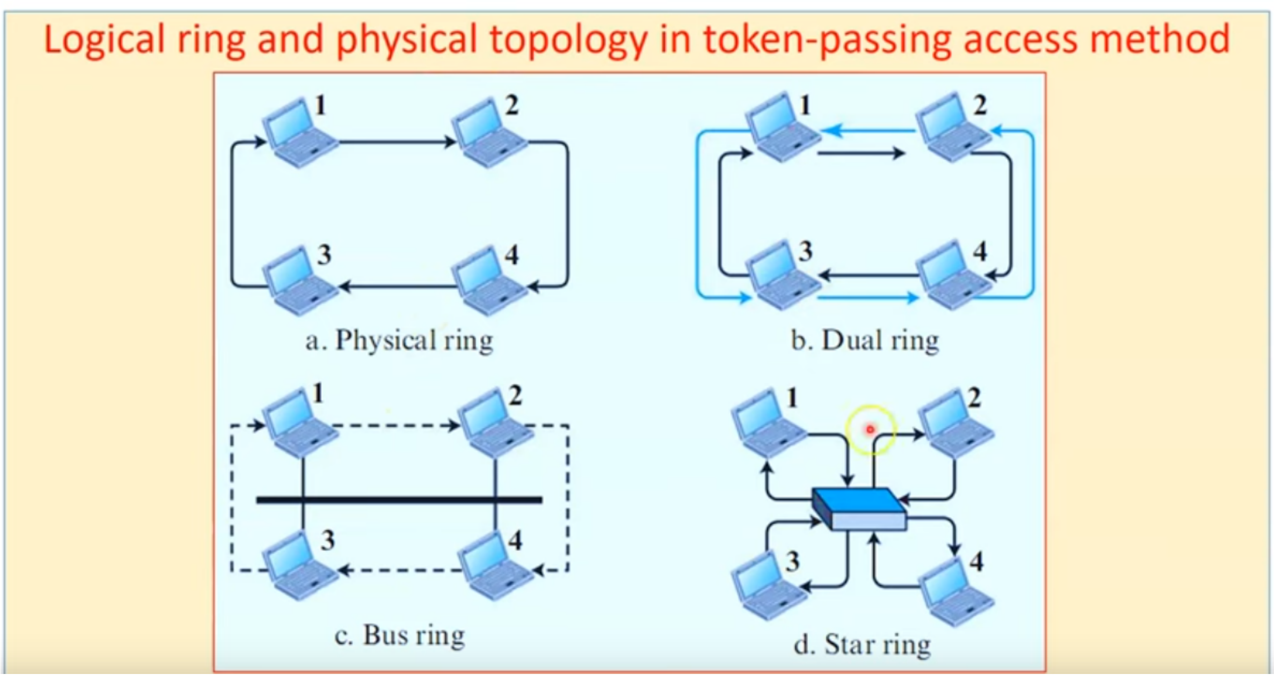
- When primary device is ready to receive data
  - It Asks (Poll) each device to see if theres anything to send
  - if nothing is to be sent, secondary device gives out NAK. otherwise it sends a data frame

- 

-

Token Passing

- The stations in the network are organized in a logical ring
  - For each station there is a predecessor and successor
- Special packet called token circulates through the ring
- Possession of this token gives the station the right to access the channel and send data
- When station has a data to send, it waits until it receives token from predecessor
- When it has no more data to send, it sends the token to the successor



Channelization protocols

- Available bandwidth of a link is shared in time

Frequency-Division Multiple Access (FDMA)

- Available bandwidth is divided into frequency Bands
- Each station is allocated a band to send data
- Bands are separated by guardbands to prevent interference
- Stream data can be used with FDMA
- Used in cellular telephone systems

Time Division Multiple Access (TDMA)

- Share the bandwidth in time
- Allocated a timeslot
- Transmits data in its timeslot

Code division multiple access (CDMA)

- All stations can send simultaneously
- Communication with different codes

Bridge

Ethernet & WiFi