SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

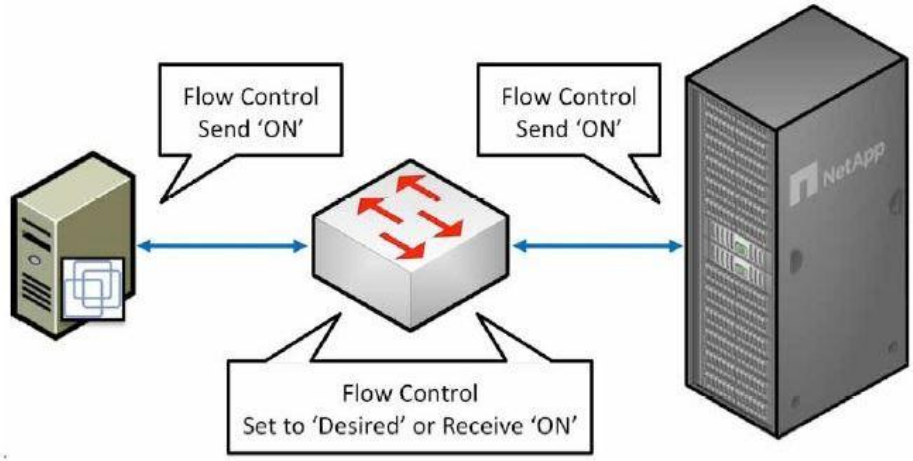
UNIT IV

Flow Control, Error Detection & Correction, CSMA, CSMA/CD, HDLC and PPP

Agenda

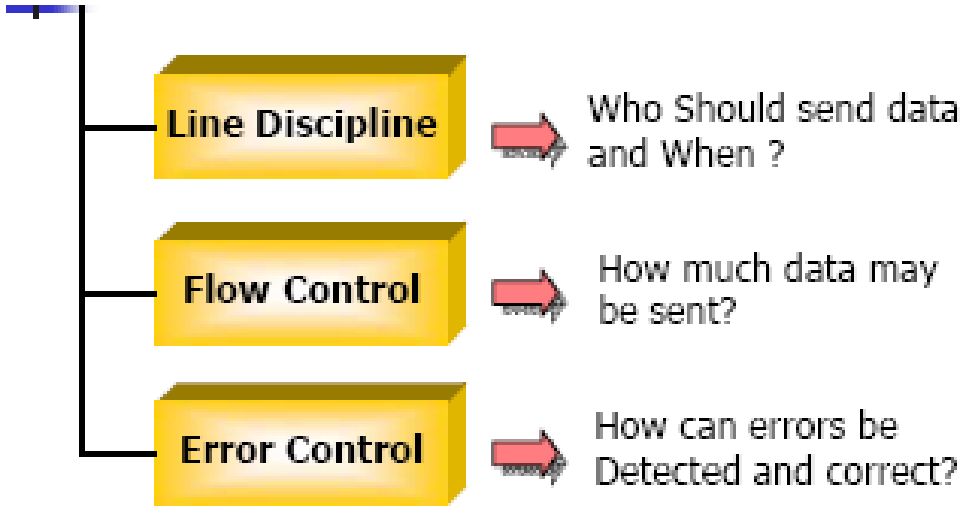
- **Framing, Flow Control Mechanisms**
- **Stop Wait Protocol**
- **Goback N ARQ, Selective Reject ARQ**
- **CRC, Checksum**
- **Types of Errors**
- **Error Correction**
- **CSMA, CSMA/CD**
- **HDLC**
- **PPP**

Flow & Error Control



Data Link Control

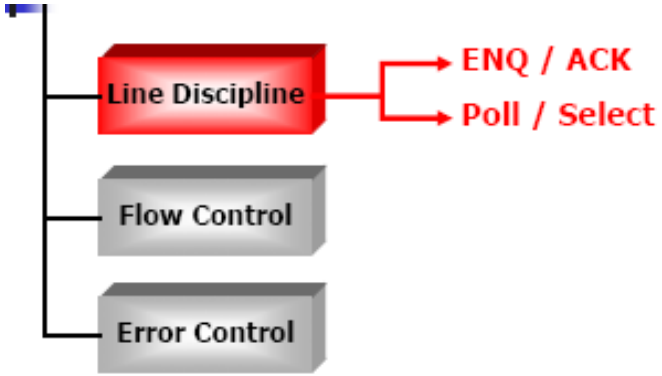
- **Line Discipline: Determines which device can send and when it can send**
- **Flow Control: Coordinates the amount of data that can be sent before receiving acknowledgement. Linked with error control**
- **Error Control: Allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates retransmission of those frames by the sender**



Line Discipline

- In Line discipline whatever the system is, no device should be allowed to transmit until that device has evidence that the intended receiver is ready to receive the transmission
- Line discipline can be done in two ways:

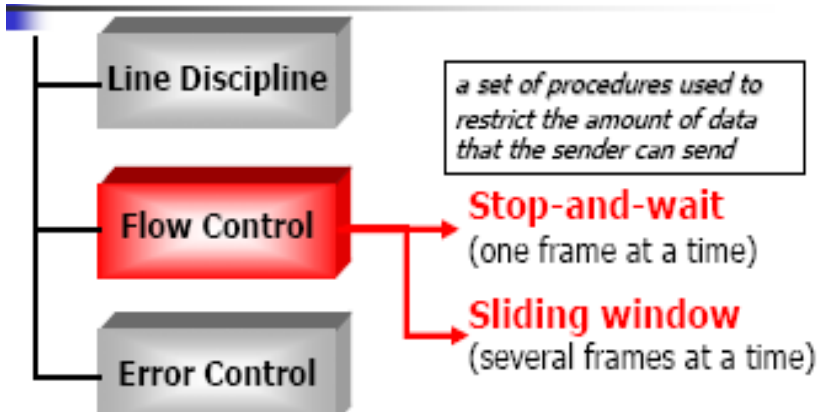
  - Enquiry/Acknowledgment (ENQ/ACK)
  - Poll/Select



Flow Control

- Second aspect of Data link control- Flow Control
- Set of procedures that tells the sender as how much data it can transmit before waiting for an acknowledgment from the receiver.
- Receiver got set of memory blocks called the BUFFER that store the incoming data before they are processed.
- If buffer begins to fill up, receiver must be able to tell the sender to send fewer data frames or halt the transmission until the buffer is free to accept the data frame again.
- Under this we got two techniques:

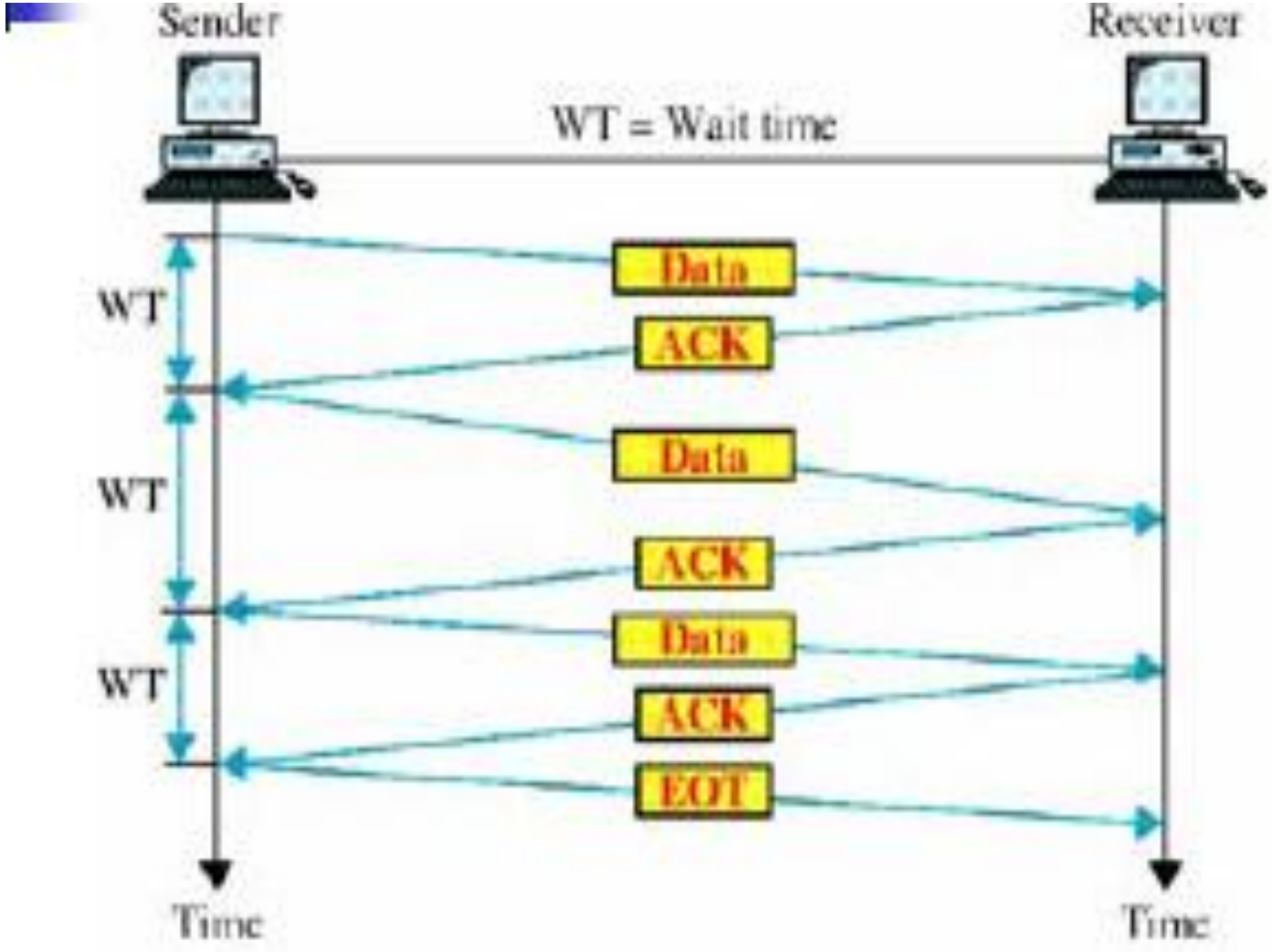
  - Stop- and Wait
  - Sliding Window



Stop and Wait

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- In stop- and- wait flow control, the sender waits for an acknowledgment after every data frame it sends.
- Only when acknowledgement has been received, the next data frame is sent.
- The process of alternatively sending and waiting repeats until the sender transmits an end of transmission frame
- Advantage: of stop and wait flow control is simplicity as each frame is checked and acknowledged before transmitting next frame
- Disadvantage: It is very slow as each frame must travel all the way to the receiver and acknowledgement must travel all the way back before the next frame can be sent.
- If distance between the devices are too long, time spent waiting for ACKs between each frame can add to the transmission time.


Sender
Receiver
WT = Wait time
WT
WT
WT
Data
ACK
Data
ACK
Data
ACK
EOT
Time
Time

Sliding Window

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- In Sliding window, the sender can transmit several data frames before needing an acknowledgment
- Frames can be sent one after another i.e. link can carry several frames at once and its capacity can be used efficiently
- The receiver acknowledges only some of the frames using a simple ACK to confirm the receipt of multiple data frames
- Sliding window is like an imaginary boxes at both the sender and receiver side
- These windows can hold the data frames and provides the upper limit on the number of data frames that can be transmitted before receiving an acknowledgement.

- Frames may be transmitted to the receiver as long as window is not full.

- The frames are numbered 0 to n-1 . For example if n=8, frames are numbered 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1……

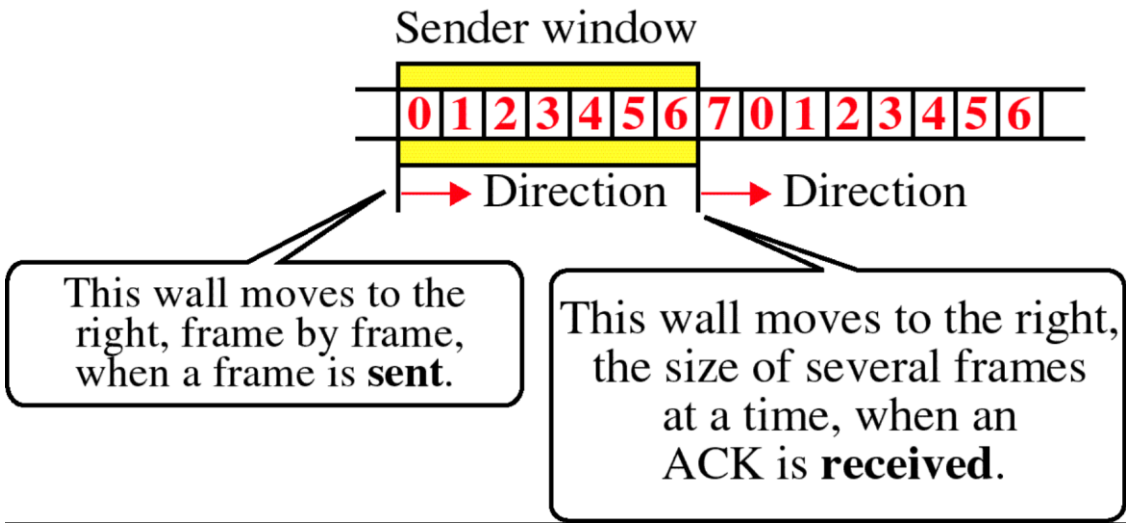
- The size of the window is n-1. Window always cover n-1 data frames and not n data frames.
- When the receiver sends an ACK it can include the number of next frame it is expected to receive. For example when the sender sees an ACK with number 5, it means all frames upto 4 (0 to 4) has been received.

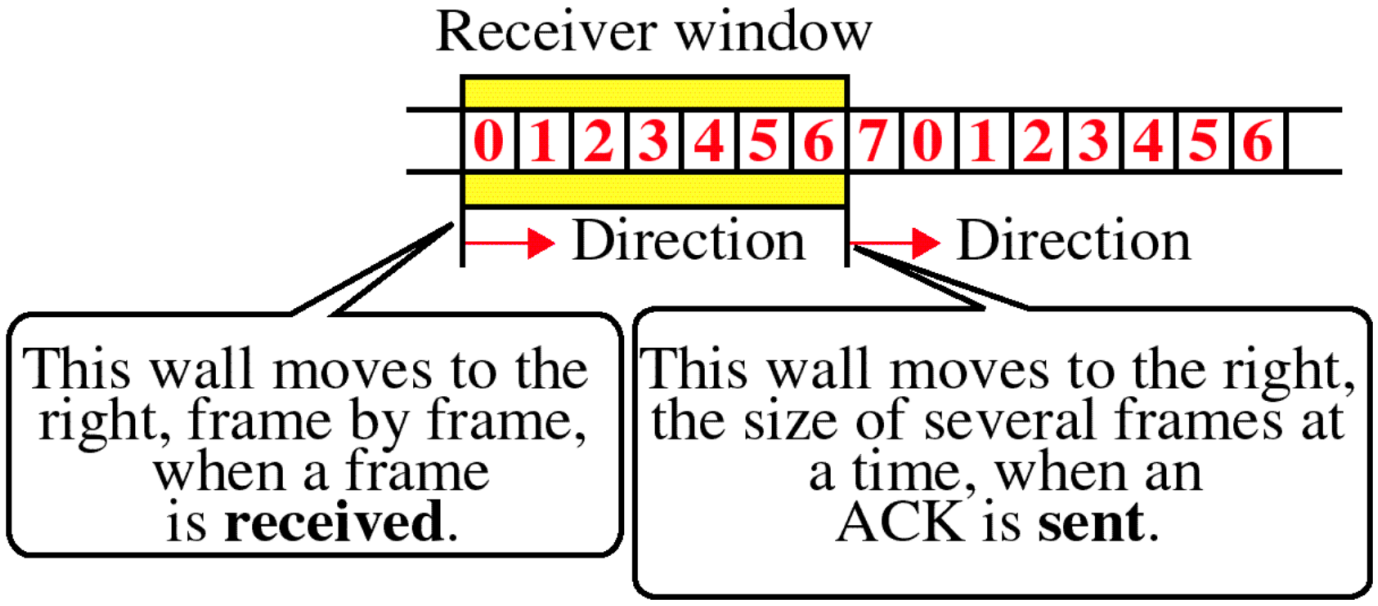
Sender Window

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- At the beginning of transmission sender's window contains n-1 data frames.
- As frames are sent out, left boundary of window moves inward shrinking the size of the window
- Given a window size w, if three frames have been transmitted since last ACK, number of frames left in window is **w-3**
- For example say we have a window of size 7. (0 to 6)
- Say Frames 0 through 3 have been sent and no ACK have been received, sender's window contains only 4,5 & 6.
- Once ACK is received with number 4, then four frames have been received (0 through 3) and sender's window expands to include next four frames in buffer to contain totally 6 frames as 4,5,6,7,0,1,2.
- If say received ACK is numbered 2, the sender's window would have been expanded only by two frames to contain totally 6 as 2,3,4,5,6,7,0 only.

Sender & Receiver Window

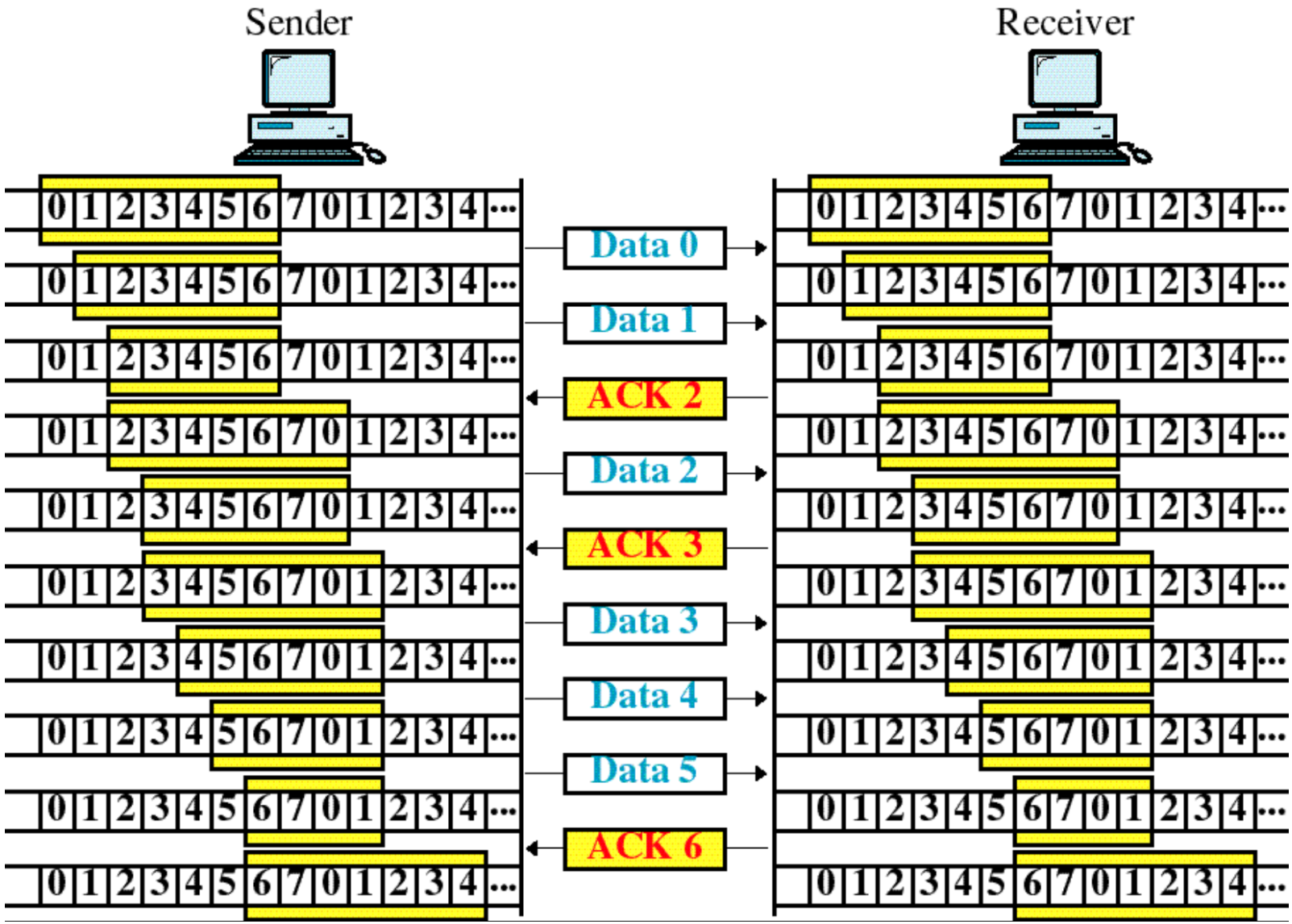




Receiver Window

- At receiver we got not n-1 data frames but n-1 spaces for frames
- As new frames come in the size of the receiver window shrinks
- Receiver window does not represent number of frames received but number of frames that may still be received before an ACK can be sent.
- If a receiver got a window size of w, if three frames are received without being acknowledged , number of spaces in window is w-3.
- As soon as ACK is received , the window expands to include more spaces for number of frames equal to number of frames acknowledged
- Let us take the receiving window of size 7 i.e 0 through 6
- With the arrival of data frame 0, receiving window shrinks moving from 0 to 1 and receiver window has now shrunk to six frames before sending an ACK
- Once say frames 0 through 3 are received without sending an ACK, receiving window now shrinks to 3 frame spaces.

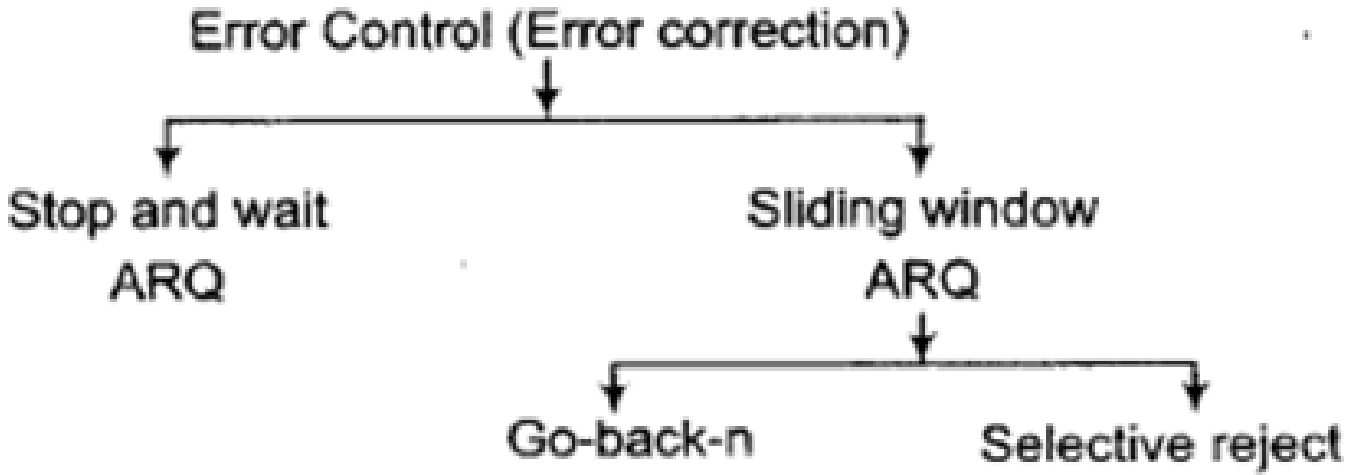
Sliding Window



Automatic Repeat Request (ARQ)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Error correction in data link layer is implemented simply: anytime an error is detected in an exchange, a negative acknowledgement (NAK) is received and specified frames are transmitted- ARQ
- Frame is so damaged because of noise and receiver cannot recognize the frame, ARQ allows us to say that the frame has been lost.
- Other function of ARQ is retransmission of last frames including lost acknowledgement
- Stop and wait is implemented as Stop and Wait ARQ
- Sliding window is implemented as sliding window ARQ which comes under two variants: Go-back-n and Selective Reject



Error correction classification

Stop and Wait ARQ

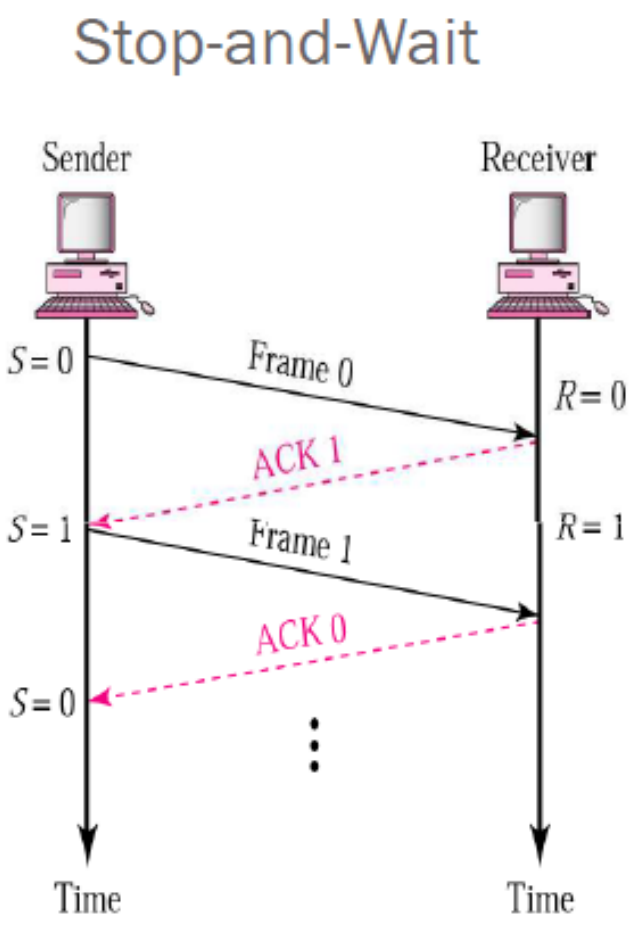
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- It is an extension of Stop-and –wait flow control to include retransmission of data in case of lost or damaged frames. For retransmission to work, four features are added:
- Sending device keeps track of last frames transmitted until it receives an acknowledgment for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly
- For identification purposes both data and ACK frames are numbered alternatively 0 and 1.
- If an error is discovered in a data frame, indicating that it has been corrupted in a transit, a NAK frame is returned. When an NAK frame is returned, it resends the frame transmitted after the last acknowledgement irrespective of the number
- Sending device is equipped with a timer. If an expected acknowledgment is not received within a allotted time period, sender assumes that last data was lost in transit and send it again

Damaged Frames

- when a frame is discovered by the receiver to be an error, it returns an NAK frame and sender retransmits the last frame again.
- Let us take for example a sender transmits data frame and one of it is found to be an error.
- Sender transmits data frame 0 and receives an acknowledgment ACK1 indicating it is expecting data 1
- Now sends data 1 and receives acknowledgment ACK0
- Sender now transmits next frame data 0 . Receiver discovers an error in it and returns an NAK
- Sender retransmits data 0 again and receives ACK1.

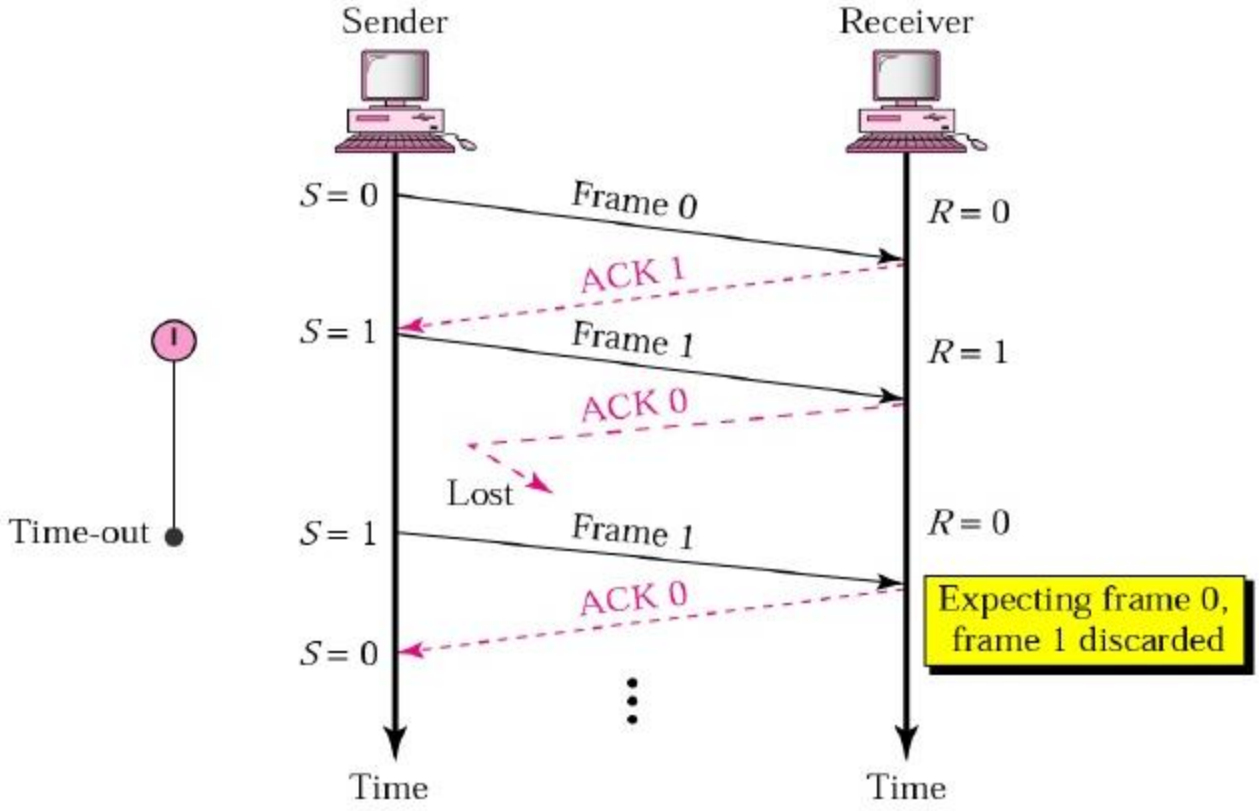
Damaged Frames



- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control variable ® that holds the number of the next frame expected (0 or 1).
- Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it
- Receiver send only positive ACK if the frame is intact.
- ACK number always defines the number of the next expected frame

ARQ- Lost Frames

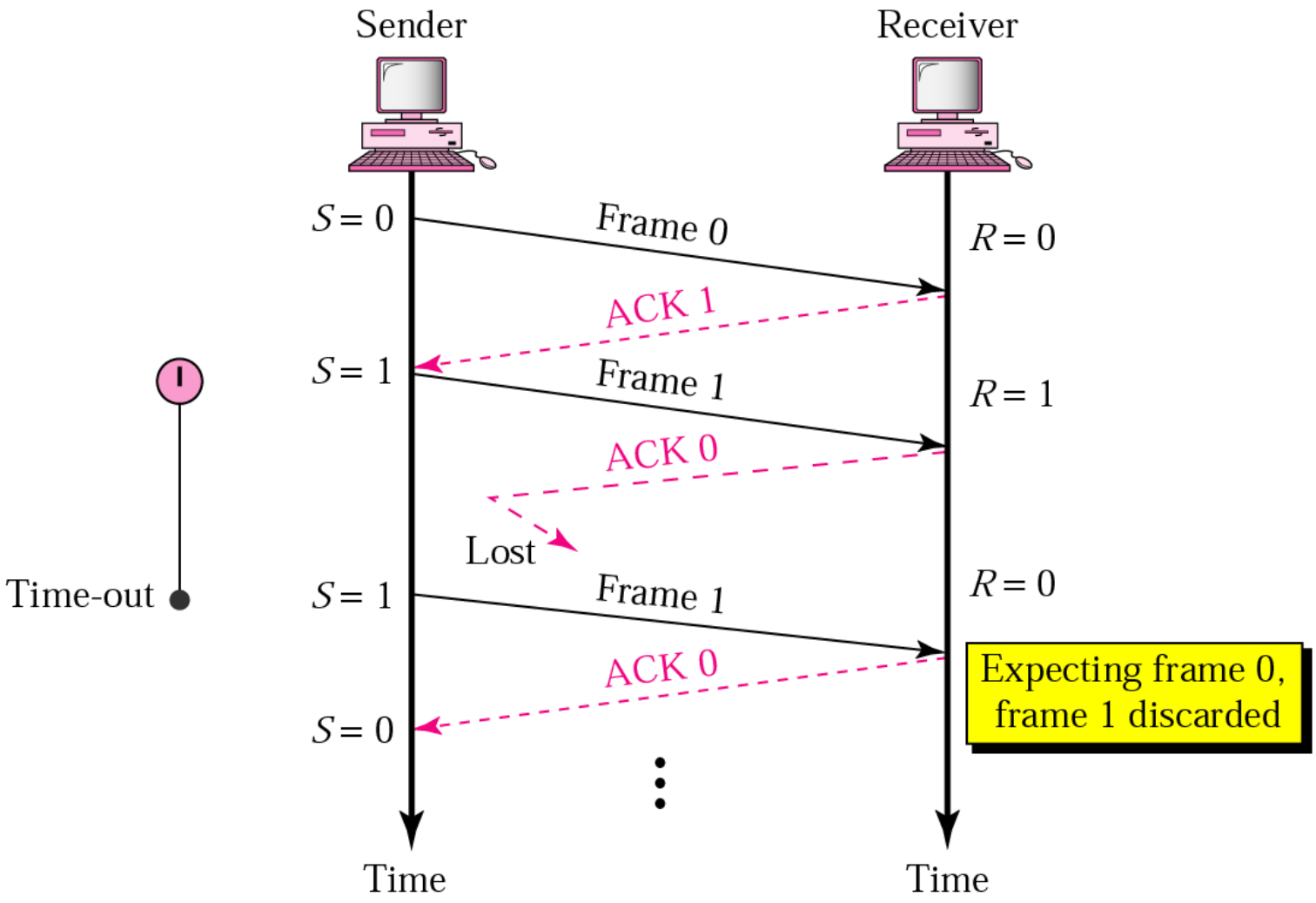
- Sender is equipped with a timer that starts every time the data frame is transmitted
- If the frame never makes it to the receiver , the receiver can neither acknowledge it positively or negatively
- Sending devices waits for an ACK or NAK until the timer goes off at which point it tries again
- Now it retransmits the data frame and starts the timer once again and wait for an acknowledgement



ARQ- Lost Acknowledgement

- Here data frame has made it to the receiver has been found as either acceptable or not acceptable
- But the ACK or NAK frame returned by receiver has been found to be lost in transit
- Now the sending device waits until the timer goes off, then retransmits the data frame again.
- Receiver here checks the number of new data frame.
- If lost frame was a NAK, the receiver accepts the new copy and returns an ACK for it
- If lost frame was an ACK, the receiver recognizes the new copy as a duplicate, acknowledges its receipt, discards the frame and waits for next frame.

ARQ Lost Acknowledgement

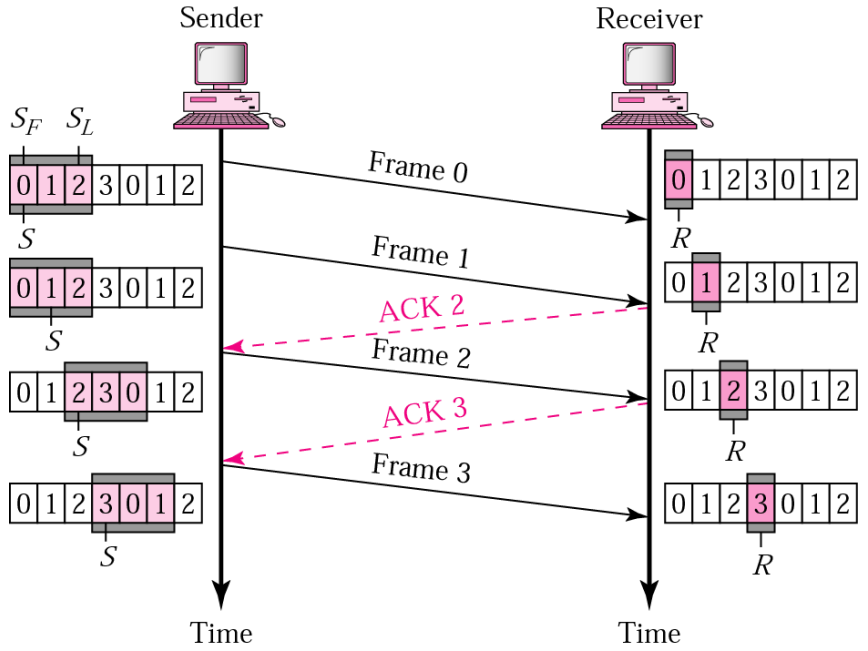


Disadvantage of Stop-and-Wait

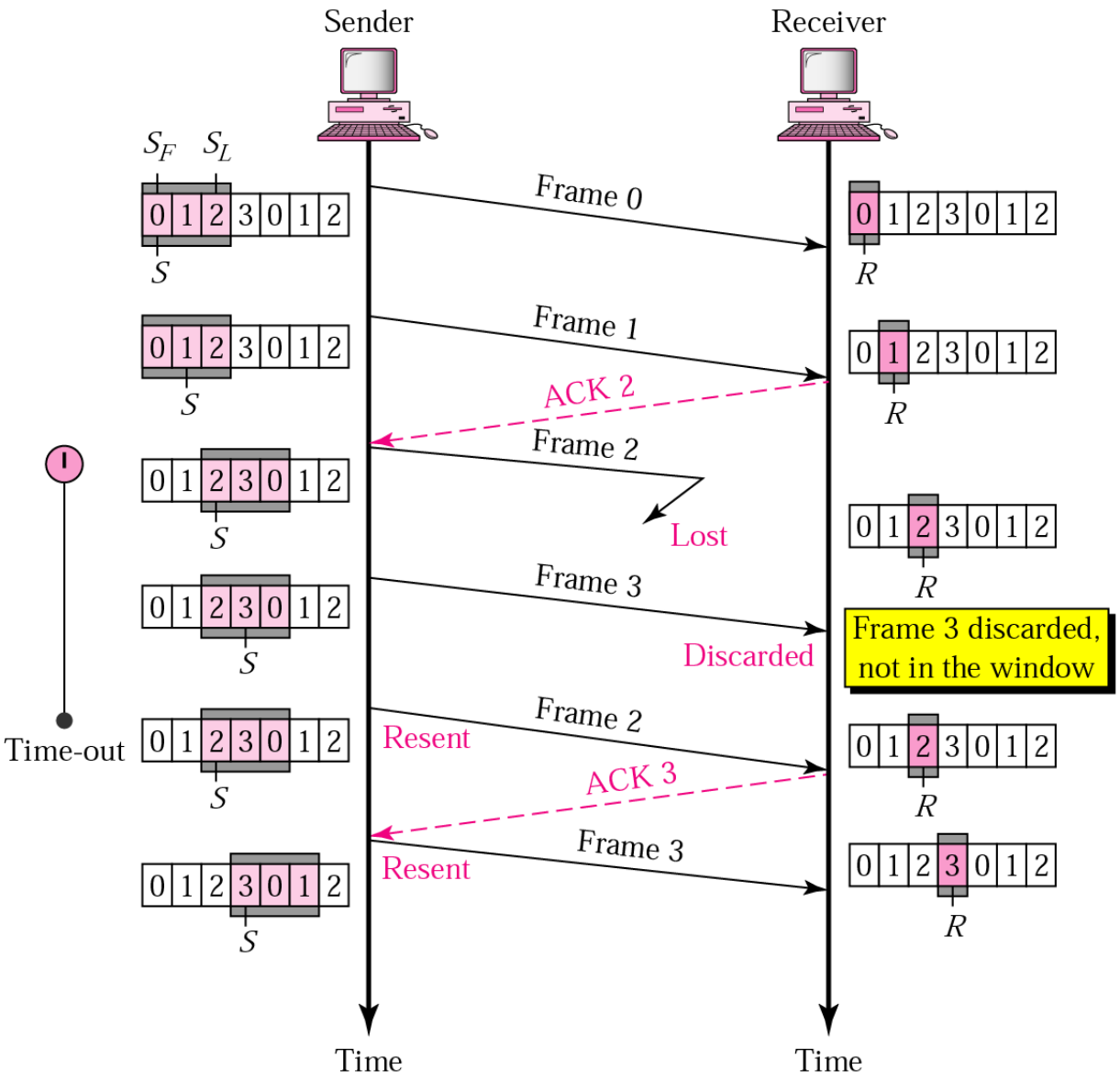
- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.
- Two protocol use the above concept,
  - **Go-Back-N ARQ**
  - **Selective Repeat ARQ**

Go Back N ARQ

- In Go-back-n ARQ, if a frame is lost or damaged all frames sent since last frame acknowledged are retransmitted
- Similarly if an acknowledgment is lost, sliding window waits for the acknowledgement for some specified time. If acknowledgement does not arrive within the time, the data is retransmitted again

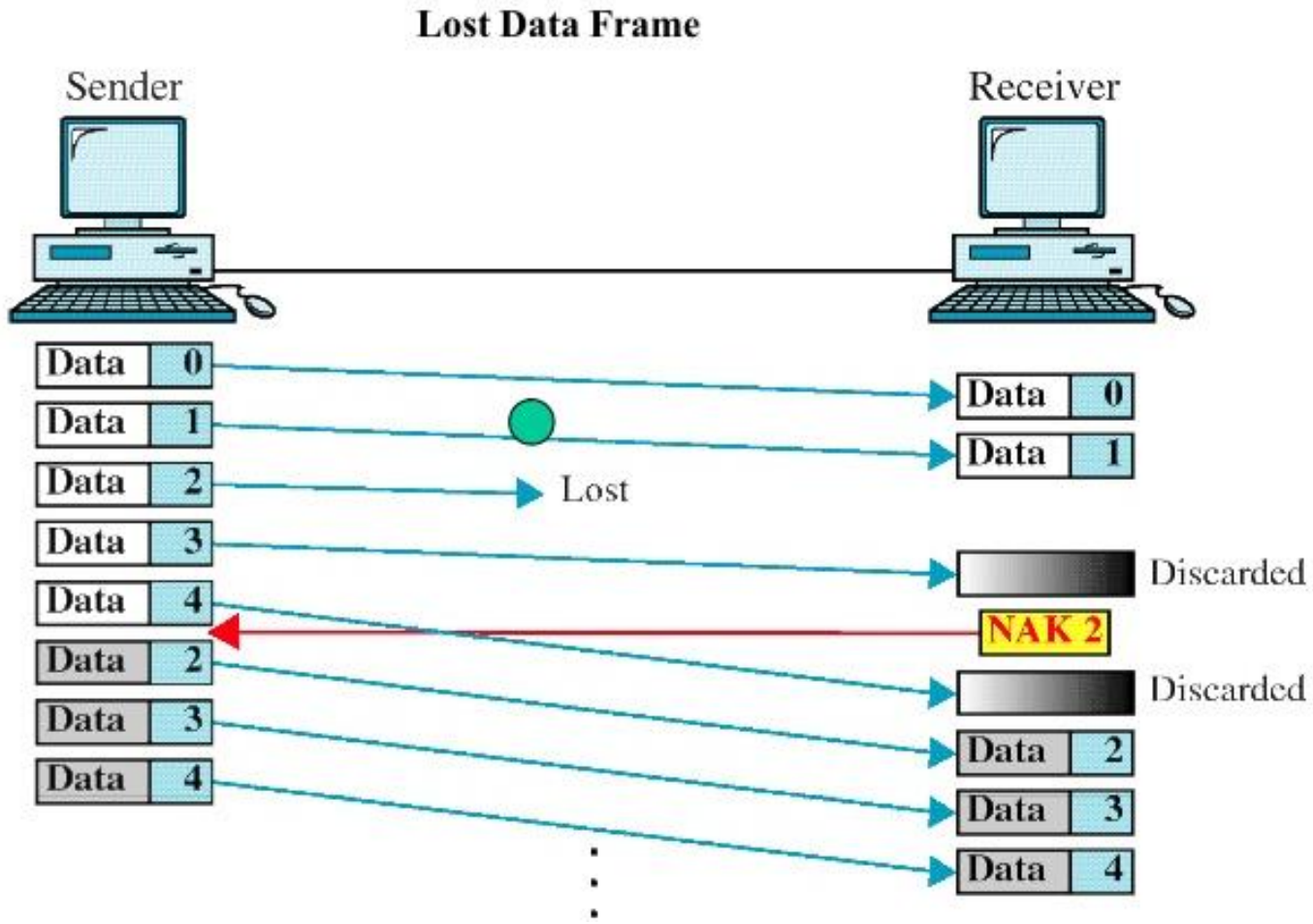


Go-back-n: Damaged Frame



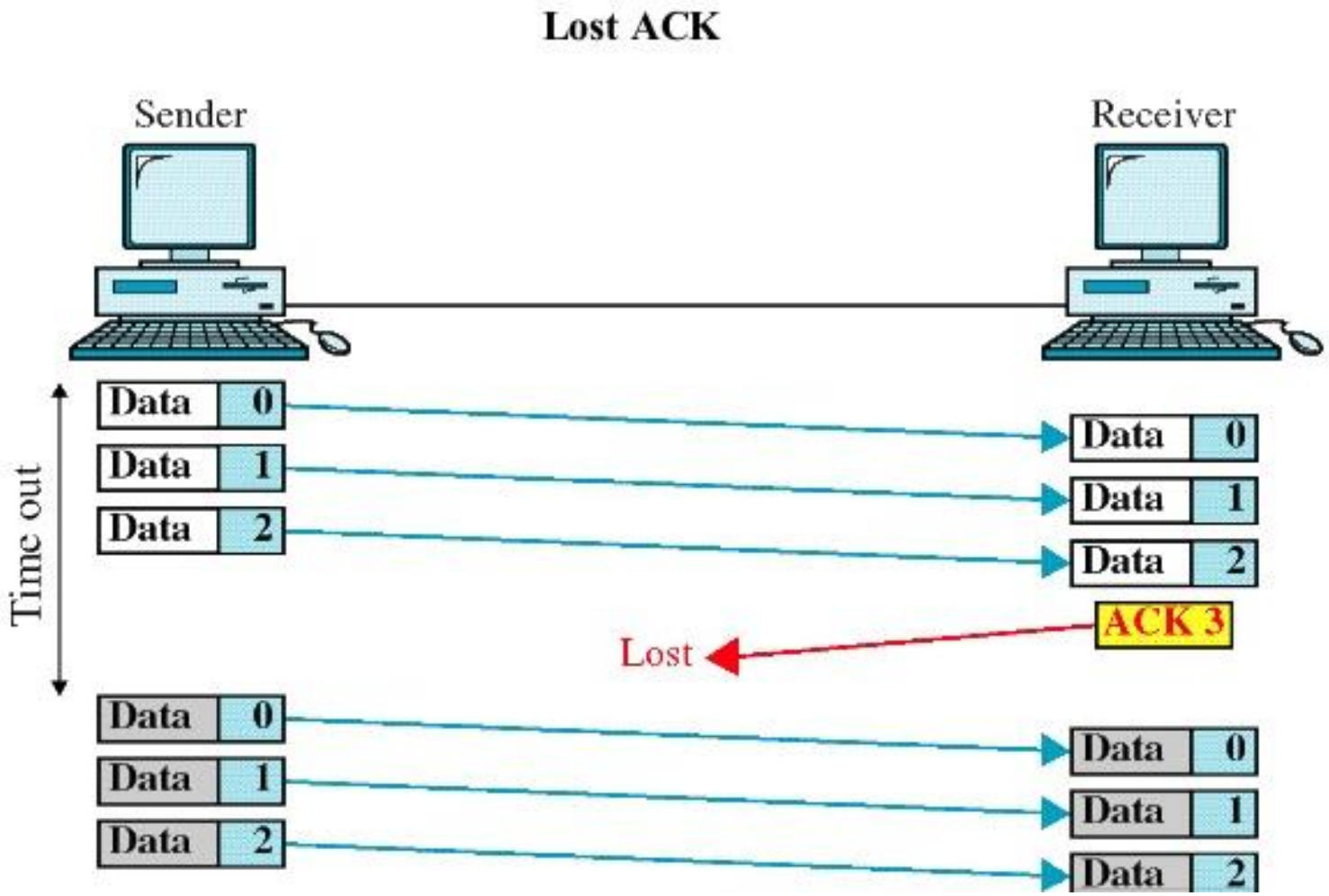
- We can see that six frames Frame 0,1,2,3,4,5 are being transmitted before an error is discovered in frame 3.
- An ACK3 has been returned by receiver showing that frames 0,1,2 have been received undamaged. The ACK3 has been sent before data 3 has arrived
- Data 3 is found to be damaged and so NAK3 has been sent immediately and frames 4 and 5 are discarded
- Sending device now retransmits all frames 3,4,5 sent since last acknowledgement and process continues
- Receiver discards frames 4 and 5 till it receive data 3 undamaged.

Go-back-n: Lost Data Frame



- In this send five data frames 0 through 4 are transferred.
- Two data frames data 0 and data 1 arrive intact but data 2 is lost
- Next frame expected at the receiver is data 3.
- Receiver is now expecting data 2 and so considers data3 to be an error and sends an NAK 2 indicating that 0 and 1 have been accepted but 2 is lost.
- Data 4 is transmitted before receiving NAK2 which is out of sequence and is therefore discarded.
- Once NAK2 is received, sender now retransmits 2,3,4.

Go-back-n: Lost Acknowledgement

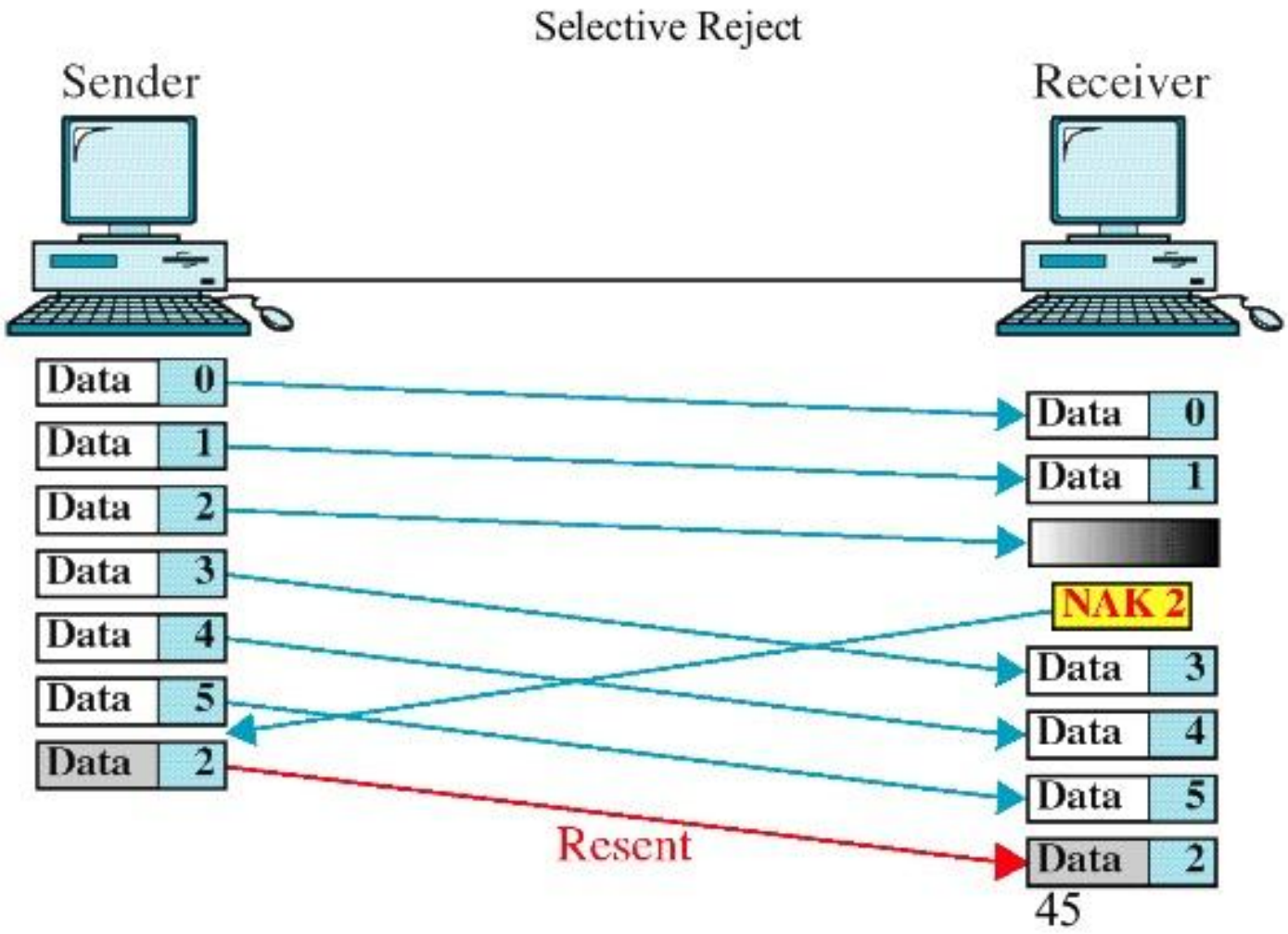


- In here the sender have transmitted first three frames 0 through 2.
- An acknowledgment ACK3 is now being sent to the sender saying three data frames have been received.
- The sender now waits a predetermined amount of time for an acknowledgment of three frames sent.
- Once ACK3 is not received within this time, all data frames are retransmitted again.

Selective Reject ARQ

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- In selective reject ARQ, only specific damaged or lost frame is retransmitted
- If a frame is corrupted in transit, NAK is returned and frame is resent out of sequence
- Receiving device must be able to sort the frames it has and insert the transmitted frames into proper place in sequence


Selective Reject
Sender
Receiver
Data 0
Data 1
Data 2
Data 3
Data 4
Data 5
Data 2
NAK 2
Data 0
Data 1
Data 3
Data 4
Data 5
Data 2
Resent

- The sender transmits 6 data frames 0 through 5
- Once data frames 0 and 1 arrives it is not acknowledged.
- Once data 2 is found be damaged, NAK2 is sent which acknowledges that previously unacknowledged data frames that have arrived intact and current data frame is found to be damaged
- NAK2 here tells that data 0 and 1 have been accepted and only data 2 has to be resent being damaged unlike go-back-n
- Frames received after the damaged frames cannot be acknowledged until the damaged frames have been retransmitted
- Receiver accepts data 3,4 5 while waiting for a new copy of data 2.
- Once data 2 arrives undamaged, ACK5 can be sent acknowledging new data 2 and original data frames 3,4 and 5.
- Logic is needed by the receiver to sort out of sequence transmission and keep track of frames are still missing and which have not yet been acknowledged

Go Back N Vs Selective Reject ARQ

- Though retransmitting a specific damaged frame seem to be more efficient than resending all frames
- Because of Complexity of storing and sorting required by the receiver and extra logic needed by sender to select specific frames for retransmission, Selective reject ARQ is expensive and not often used
- Selective reject ARQ gives better performance but in practice it is usually discarded in favour of go-back-n for simplicity of implementation

Error Detection & Correction

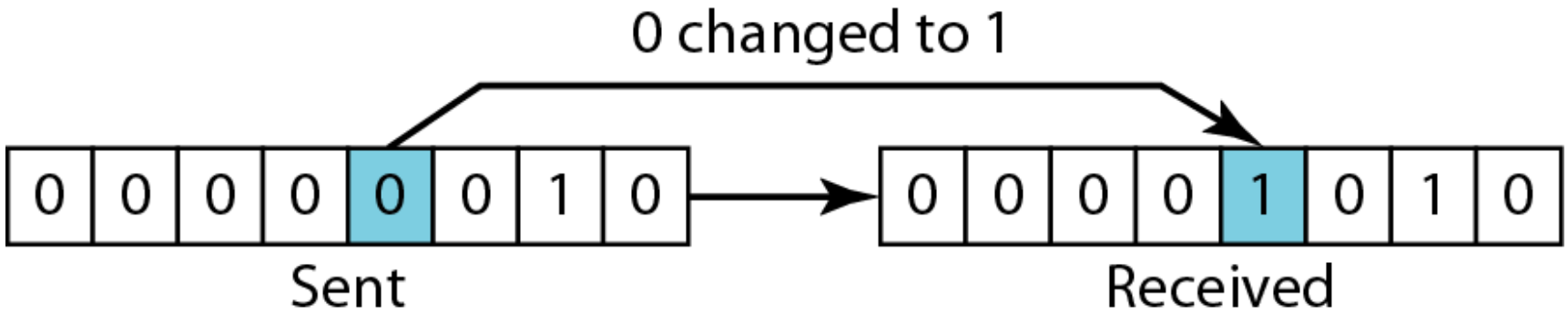
Error Detection & Correction

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

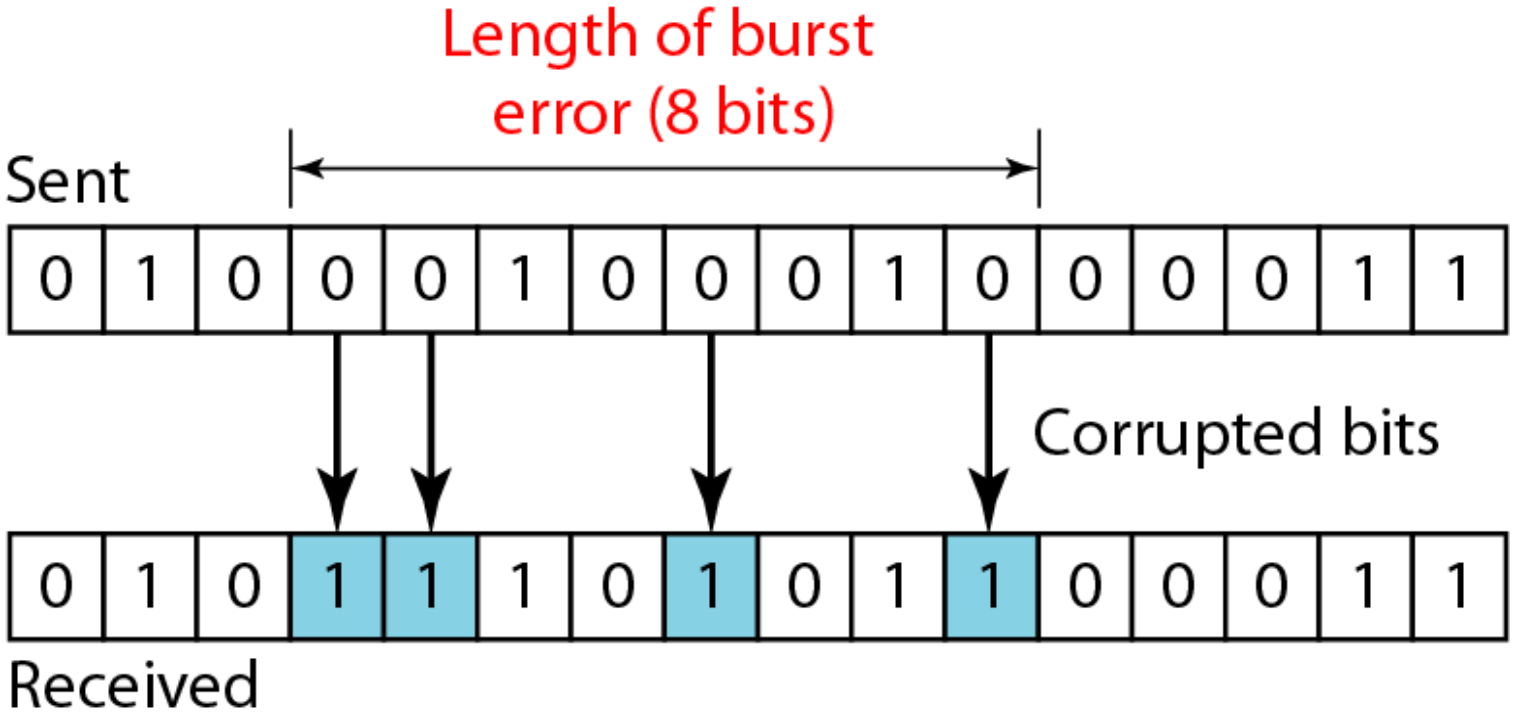
- When an electromagnetic signal flows from one point to another it is subject to interference from heat, magnetism and other forms of electricity
- This interference can change the shape of signal
- When these signals is carrying binary data, such changes can alter meaning of data resulting in error.
- Error when we say can be classified into two types- Single bit and Burst

- **Single bit error**: Error where only one bit of given data unit such as byte, character or packet is changed from 0 to 1.
- **Burst Error** : Error where two or more bits in a given data unit have changed from 1 to 0 or 0 to 1.

Single Bit Error



Burst Error


Length of burst error (8 bits)
Sent
0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1
Corrupted bits
0 1 0 1 1 1 0 1 0 1 1 0 0 0 1 1
Received

Error Detection Techniques

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

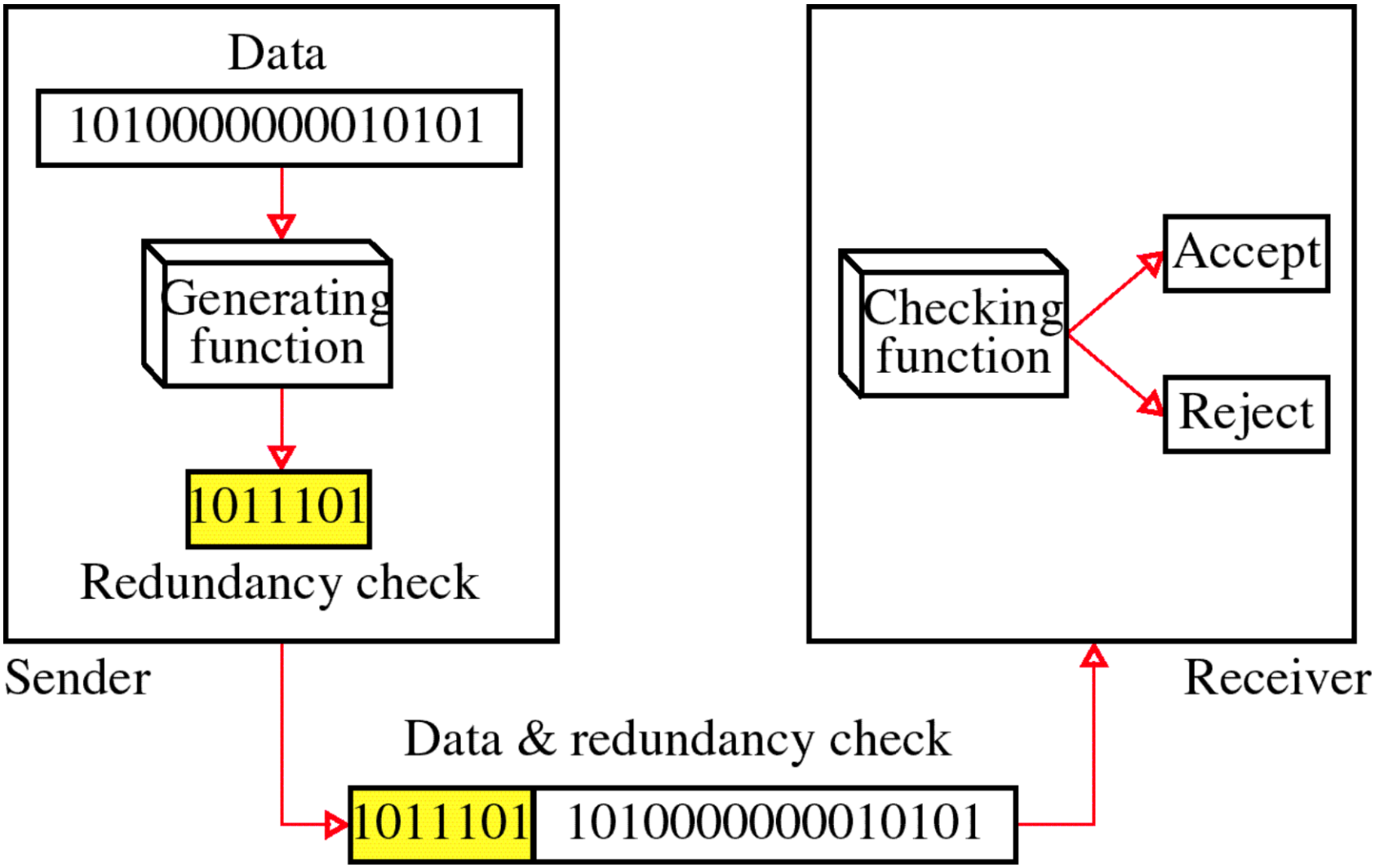
- Once a data is transmitted from sender to receiver, we need to check whether data received is error free or not.
- For that we got some Error detection methods that is been used.
- Some of them are :

- **Cyclic Redundancy Check (CRC)**
- **Checksum**

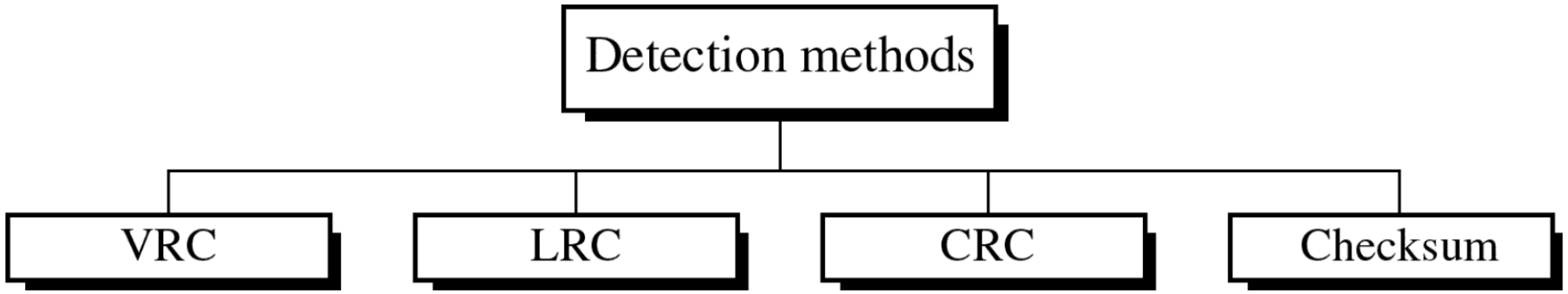
- Cyclic Redundancy Check
  - Used in HDLC, DDCMP, CSMA/CD, Token Ring
- Checksum
  - Used in IP

Redundancy

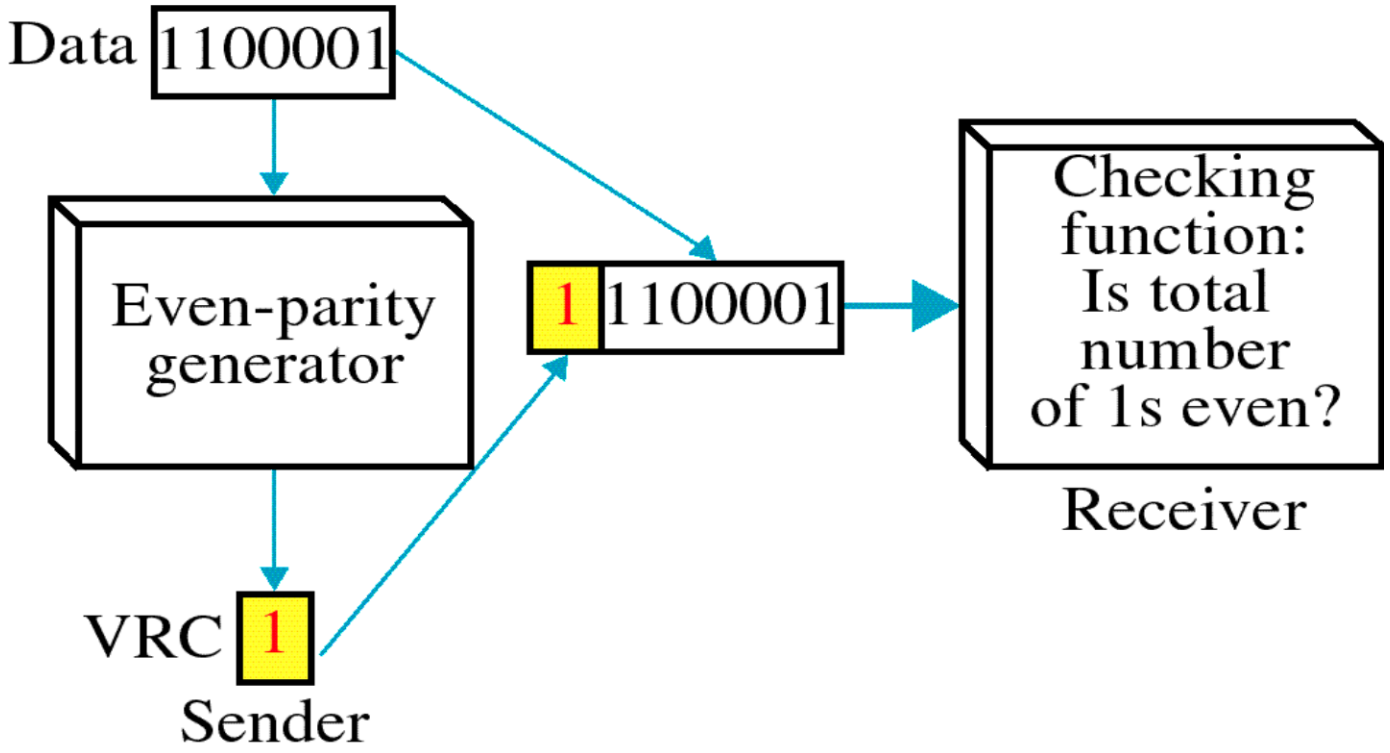
- Most basic method of error detection is to send every data unit twice
- Receiving device would compare both versions of data unit
- Any discrepancy would indicate an error and an appropriate correction mechanism could be set in place
- This mechanism would be completely accurate but it would be slow.
- This would double the transmission time and time it takes to compare bit by bit also must be added.
- An improvement of this method is to include EXTRA INFORMATION FOR PURPOSE OF COMPARISON.
- This technique is called Redundancy as extra bits are redundant to the information and discarded as soon as the accuracy of information is determined


Data
1010000000010101
Generating function
1011101
Redundancy check
Sender
Checking function
Accept
Reject
Receiver
Data & redundancy check
1011101
1010000000010101

Four types of redundancy checks are used in data communications



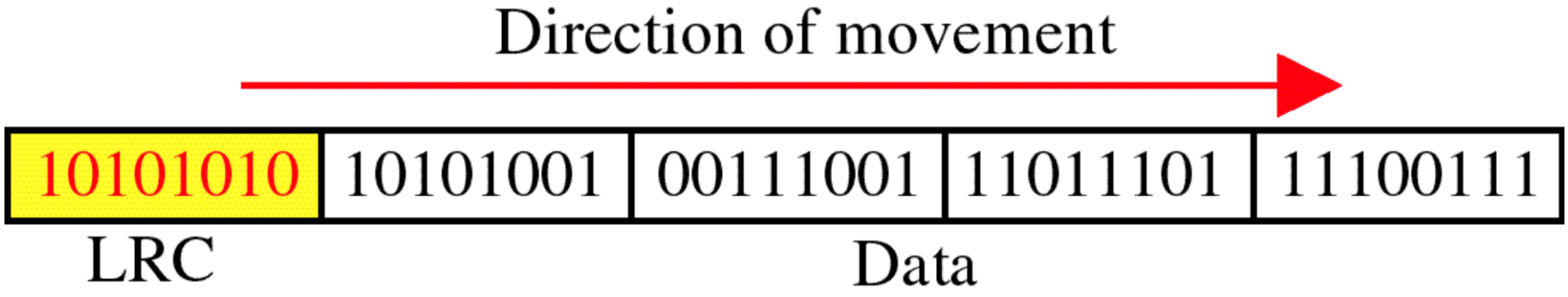
Vertical Redundancy Check - VRC



Performance

- It can detect single bit error
- It can detect burst errors only if the total number of errors is odd.

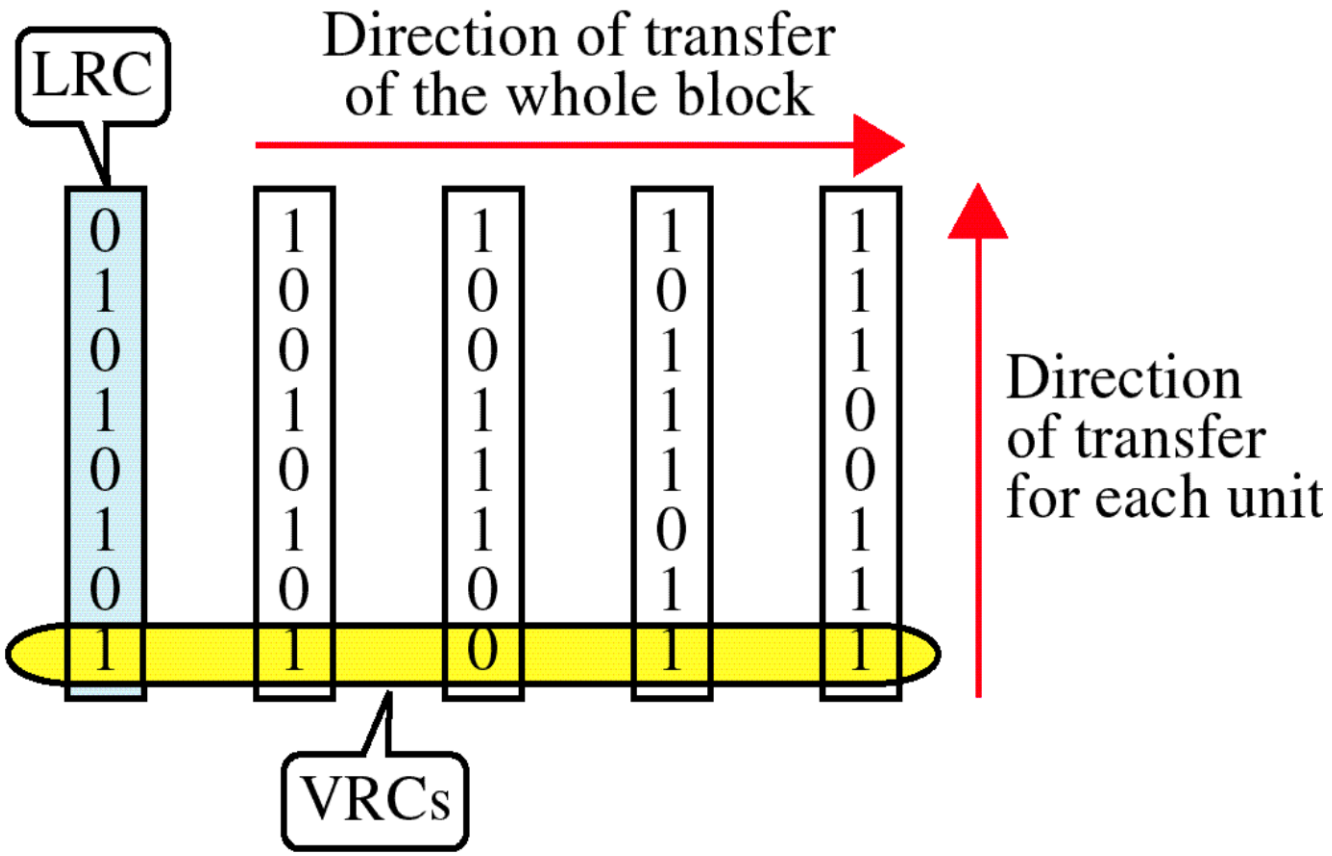
Longitudinal Redundancy Check - LRC



Performance

- **LCR increases the likelihood of detecting burst errors.**
- **If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.**

VRC and LRC

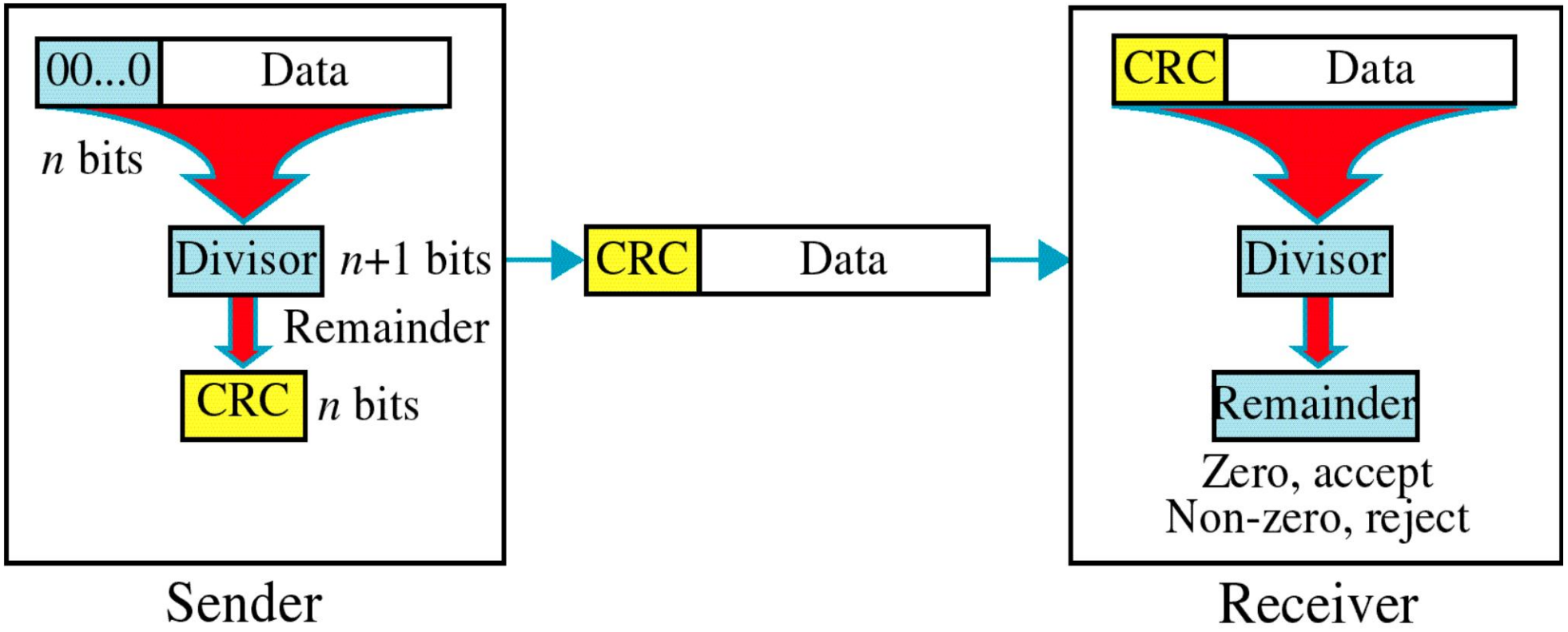

LRC
Direction of transfer
of the whole block
0 1 0 1 0 1 0 1
1 0 0 1 0 1 0 0
1 0 0 1 1 1 1 0
1 0 1 1 1 0 1 1
1 1 1 0 0 1 1 1
1 1 0 1 1
Direction
of transfer
for each unit
VRCs

Cyclic Redundancy Check (CRC)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- The most powerful redundancy checking technique is CRC
- This method uses binary division unlike LRC and VRC which uses binary addition.
- In CRC instead of adding bits together to achieve a desired parity, Sequence of redundant bits called CRC or CRC remainder is appended to the end of data unit so the resultant data unit becomes exactly divisible by second predetermined number which is the divisor.
- At receiver, incoming data unit is divided by the same divisor
- If there is no remainder, data unit is assumed to be intact and accepted.
- If there is a remainder it means data is been damaged in transit and must be rejected.

CRC


00...0
Data
n bits
Divisor
n+1 bits
Remainder
CRC
n bits
Sender
CRC
Data
CRC
Data
Divisor
Remainder
Zero, accept
Non-zero, reject
Receiver

CRC Algorithm

- First a string of 0's appended to data unit. The number n is less than the number of bits in the divisor which is n+1
- Secondly new elongated data is divided by the divisor using a process of modulo 2 binary division
- Remainder resulting from division is CRC
- CRC of n bits derived which is the remainder is appended to the data unit by replacing the appended 0's
- This data unit arrives at the receiver followed by CRC
- Now the receiver divides the data unit by the same divisor to find the remainder
- If remainder is 0 it means data is error free and is accepted
- If remainder is non zero, data got error and is rejected.

CRC Generator

- CRC generator i.e. divisor is often represented as a string of 1s and 0s but as algebraic polynomial
- Polynomial is represented as $x^7+ x^6+ x^4 +x^3 +x +1$
- Relationship of polynomial to corresponding binary representation is 11011011
- Standard CRC polynomials are CRC-12, CRC-16, CRC-ITU-T and CRC-32

CRC-12

$$x^{12}+x^{11}+x^3+x+1$$

CRC-16

$$x^{16}+x^{15}+x^2+1$$

CRC-ITU

$$x^{16}+x^{12}+x^5+1$$

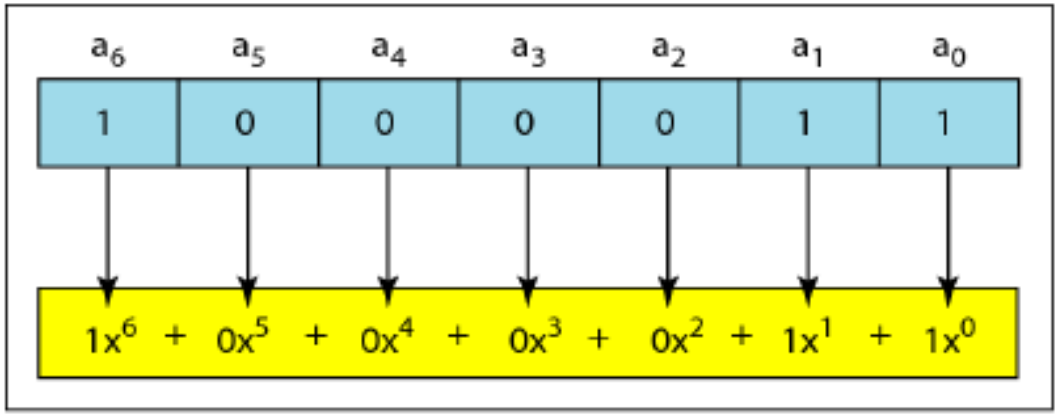
CRC-32

$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$$

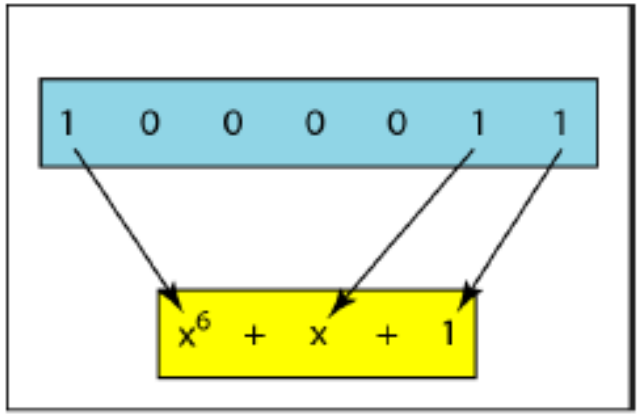
Standard Polynomials

Name	*Polynomial*	*Application*
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
CRC-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

Polynomial Representation of a binary word



a. Binary pattern and polynomial

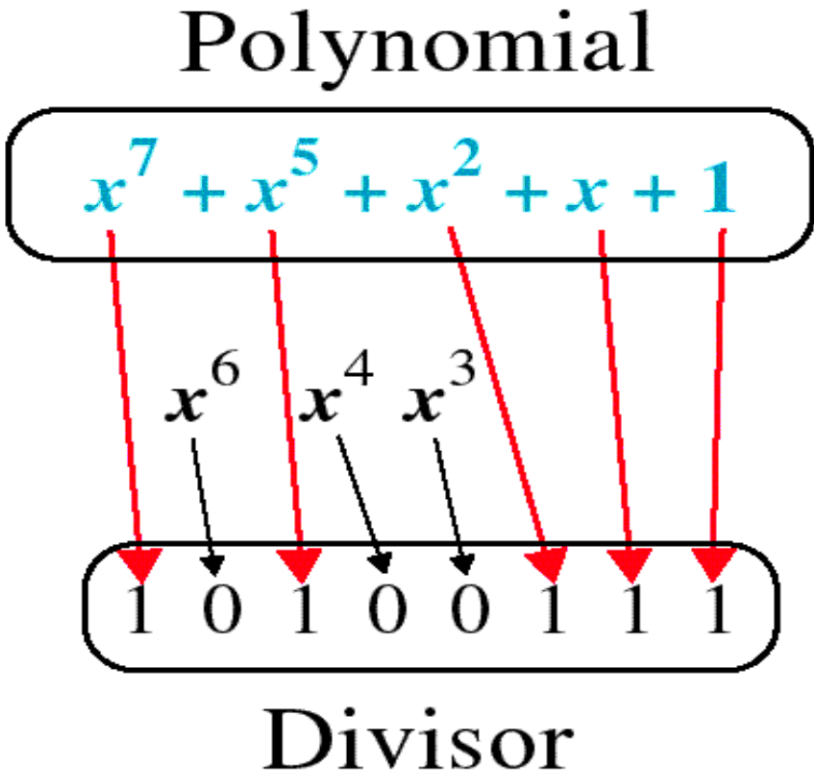


b. Short form

Polynomial

$$x^7 + x^5 + x^2 + x + 1$$

Polynomial and Divisor



CRC Example

Example: Suppose sender want to transmit the information string: 1111101. The receiver and sender decide to use the (arbitrary) polynomial pattern, 1101 which is the divisor

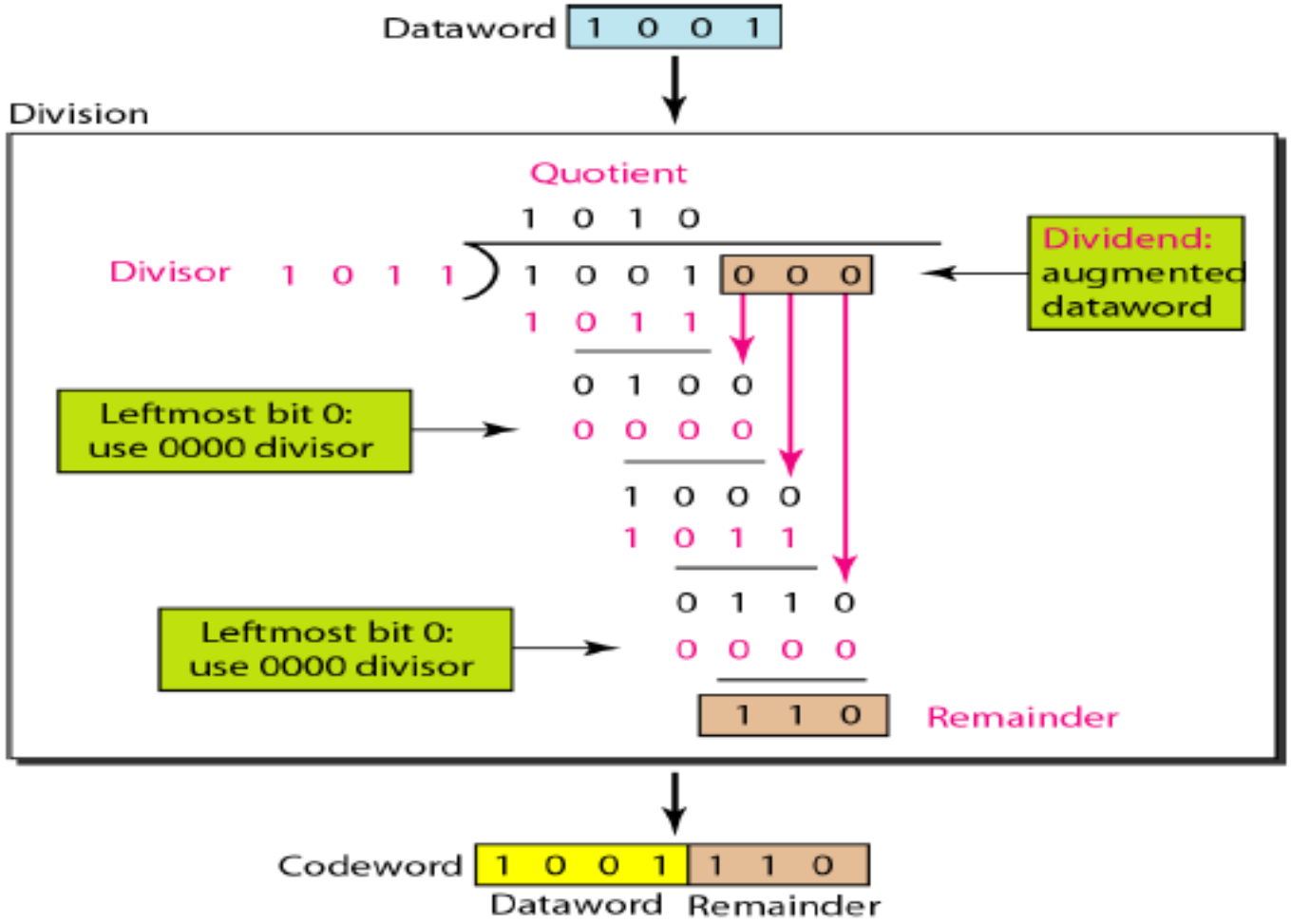
```
          1011011
      ------------
1101 ) 1111101000
       1101
       ----
       001010
          1101
          ----
          01111
            1101
            ----
            001000
               1101
               ----
               01010
                 1101
                 ----
                 0111
```

CRC

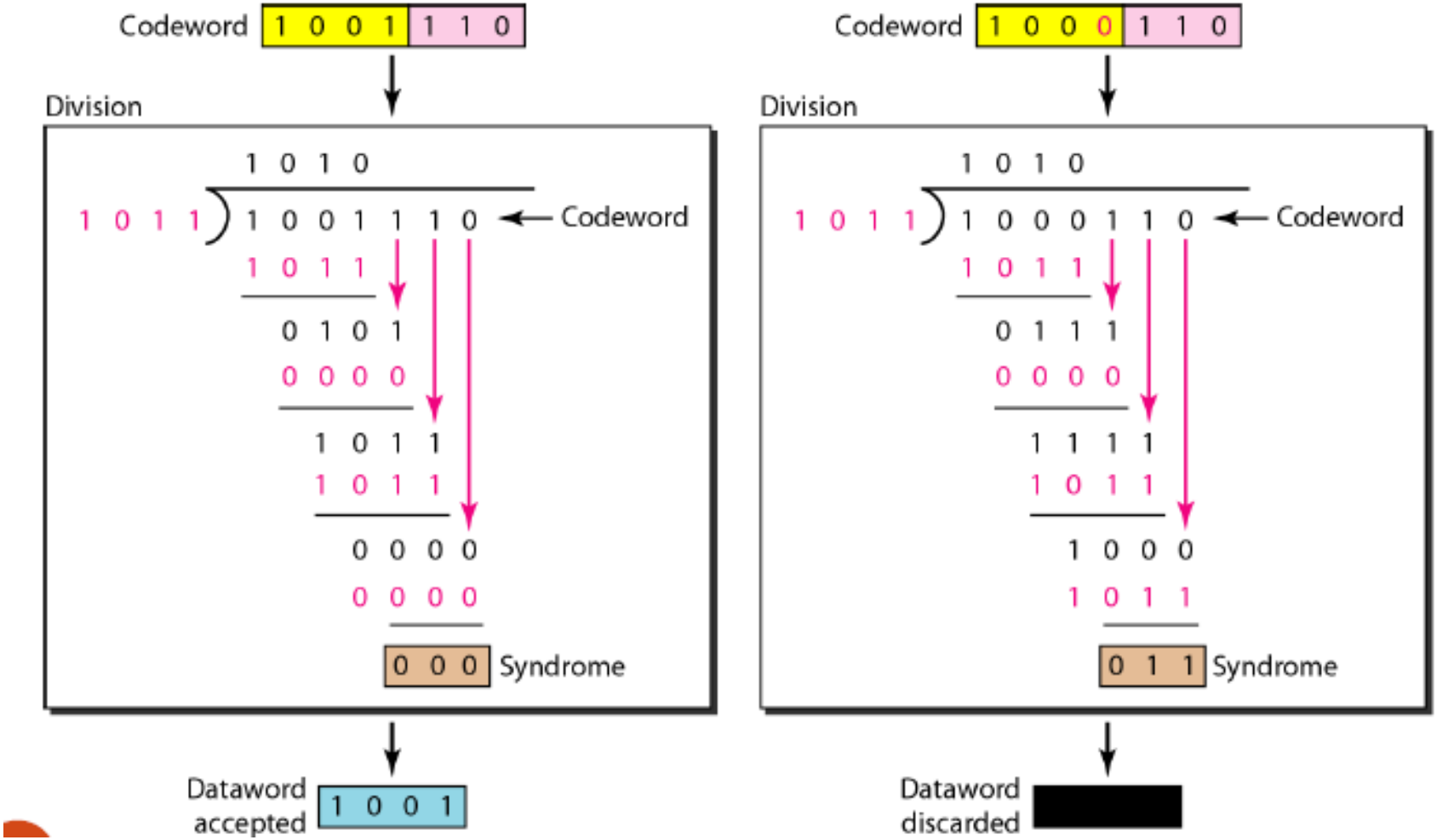
- Remainder is 0111 through modulo 2 division which is added to the data unit by replacing the appended 0's to get 1111101000+ 0111= 1111101111
- Receiver divides the appended data unit by the divisor to see if remainder is zero. If zero it is error free

```
          1011011
     ----------------
1101 ) 1111101111
       1101
       ----
       0010100
          1101
          ----
          01111
            1101
            ----
            001011
               1101
               ----
               01101
                 1101
                 ----
                 0000
```

Division in CRC sender



Division in CRC Receiver



Checksum

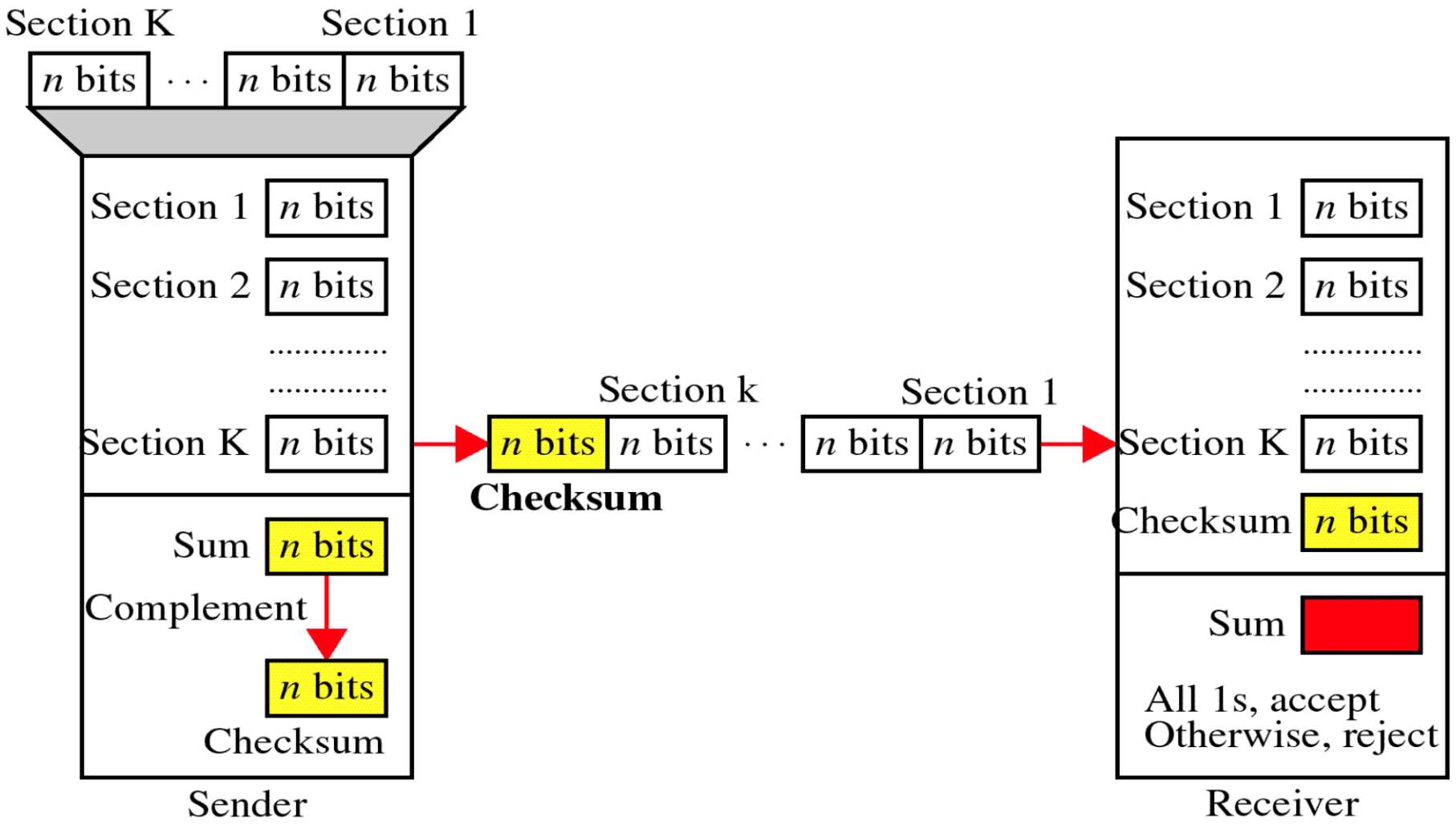
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Error detection used by higher layer protocols is Checksum
- Checksum also is based on the concept of redundancy

Check sum Generator :

- In sender, checksum generator subdivides the data unit into equal segments of n bits usually 16
- These segments are added together using one's complement arithmetic so that total is also n bits long
- The total is then complemented and appended to the end of the original data unit as redundancy bits called checksum bits

Checksum


Section K
Section 1
n bits
n bits
n bits
Section 1
n bits
Section 2
n bits
Section K
n bits
Sum
n bits
Complement
n bits
Checksum
Sender
Section k
Section 1
n bits
n bits
n bits
n bits
Checksum
Section 1
n bits
Section 2
n bits
Section K
n bits
Checksum
n bits
Sum
All 1s, accept
Otherwise, reject
Receiver

At the sender

- **The unit is divided into *k* sections, each of *n* bits.**
- **All sections are added together using one's complement to get the sum.**
- **The sum is complemented and becomes the checksum.**
- **The checksum is sent with the data**

At the Receiver

- **The unit is divided into *k* sections, each of *n* bits.**
- **All sections are added together using one's complement to get the sum.**
- **The sum is complemented.**
- **If the result is zero, the data are accepted: otherwise, they are rejected.**

Performance

- **The checksum detects all errors involving an odd number of bits.**
- **It detects most errors involving an even number of bits.**
- **If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.**

Data Unit and Checksum

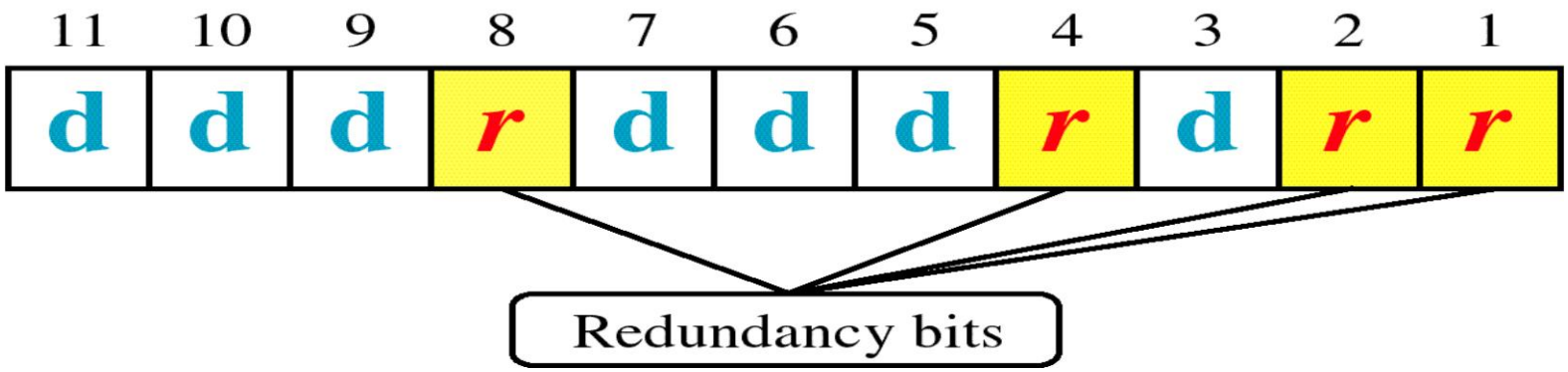
The receiver adds the data unit and the checksum field. If the result is all 1s, the data unit is accepted; otherwise it is discarded.

Error Correction

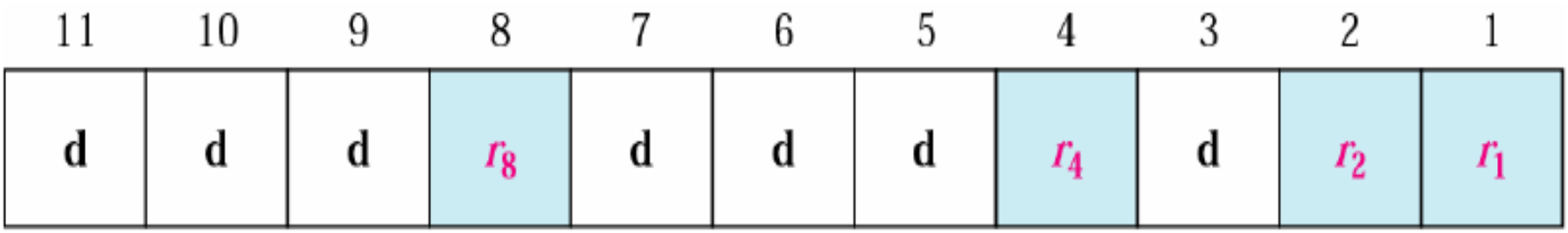
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Mechanisms covered till now would detect errors but not correct them
- One method is when an error is detected by the receiver, the receiver can have the sender retransmit the entire data unit
- Another technique is to have error correcting codes by the receiver.
- These Error correcting codes are efficient to correct single bit error only
- Not efficient in correcting a burst errors.
- Based on this we will now see one of the famous Error correcting code- **Hamming Code**

Hamming Code

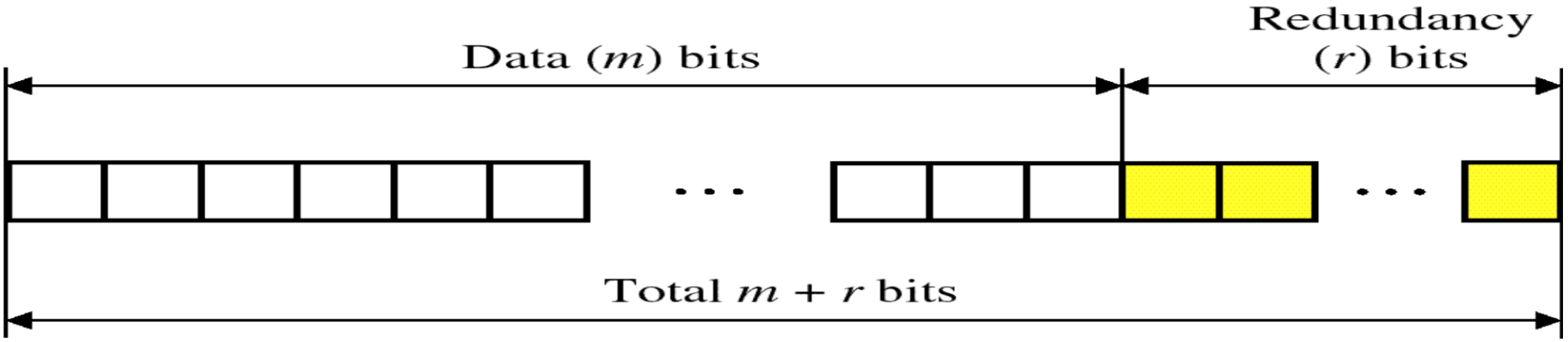


Error Correction



Hamming Code

- Technique developed by R.W. Hamming
- Applied to data units of any length and uses the relation ship between data and redundancy as $2^r >= m+r+1$ where m is the data unit, r redundancy bit.
- For example a 7 bit data would need $2^4 >= 7+4+1$
- Redundancy bits are placed in positions which are powers of 2
- Position of redundancy bits in hamming code for m +r bits i.e 7+4= 11 bit data



- Example: Let us say data is 7 bit word which is 1001101
- We would now apply hamming code technique to see which bit got error.
- Steps are:

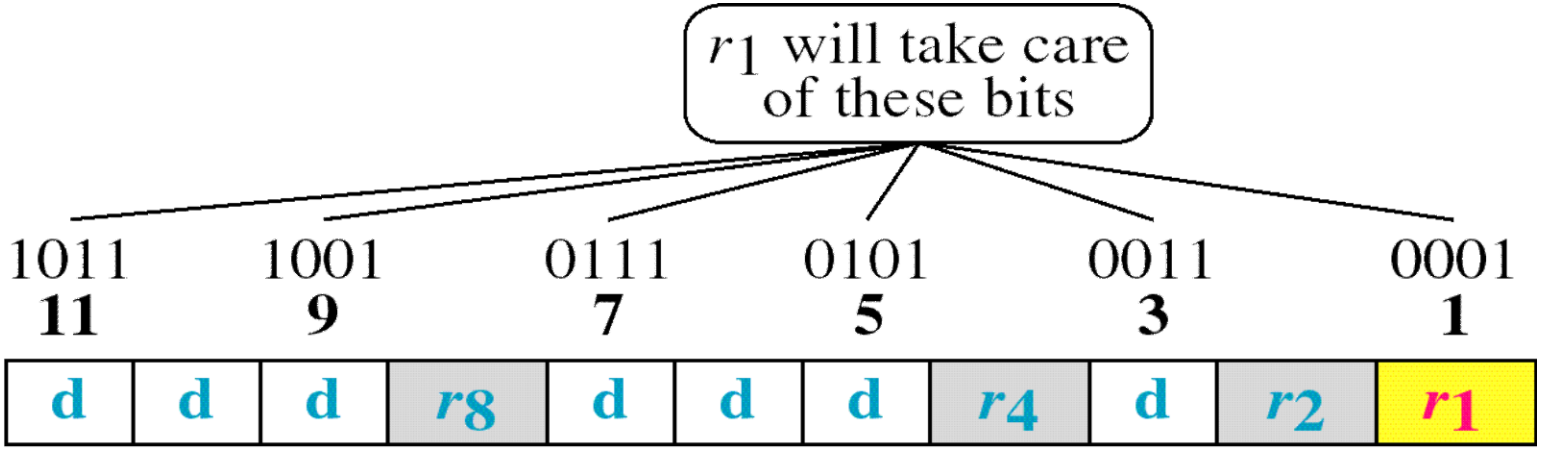
- Determine the number of redundancy/ check bits which is given as $2^4 >= 7+4+1$. so we used four parity bits
- Number the n bits left to right

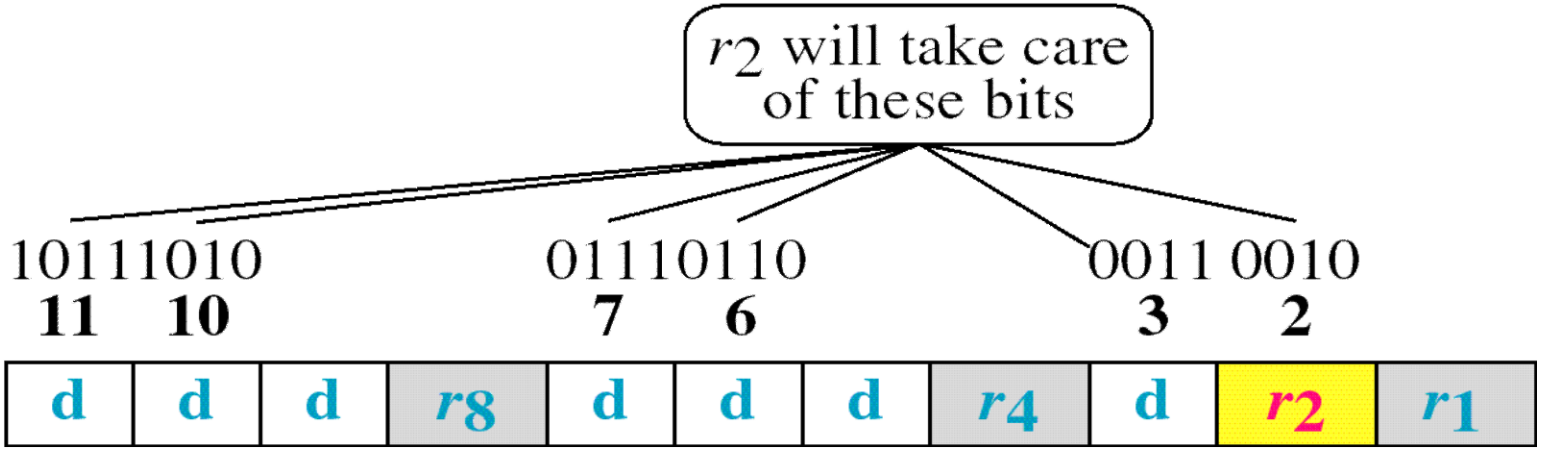
  1 0 0 r_8 1 1 0 r_4 1 r_2 r_1
- We got to now calculate the combination of the four r values for a seven bit data sequence
- For that we first write all bit positions as sums of those numbers that are powers of 2

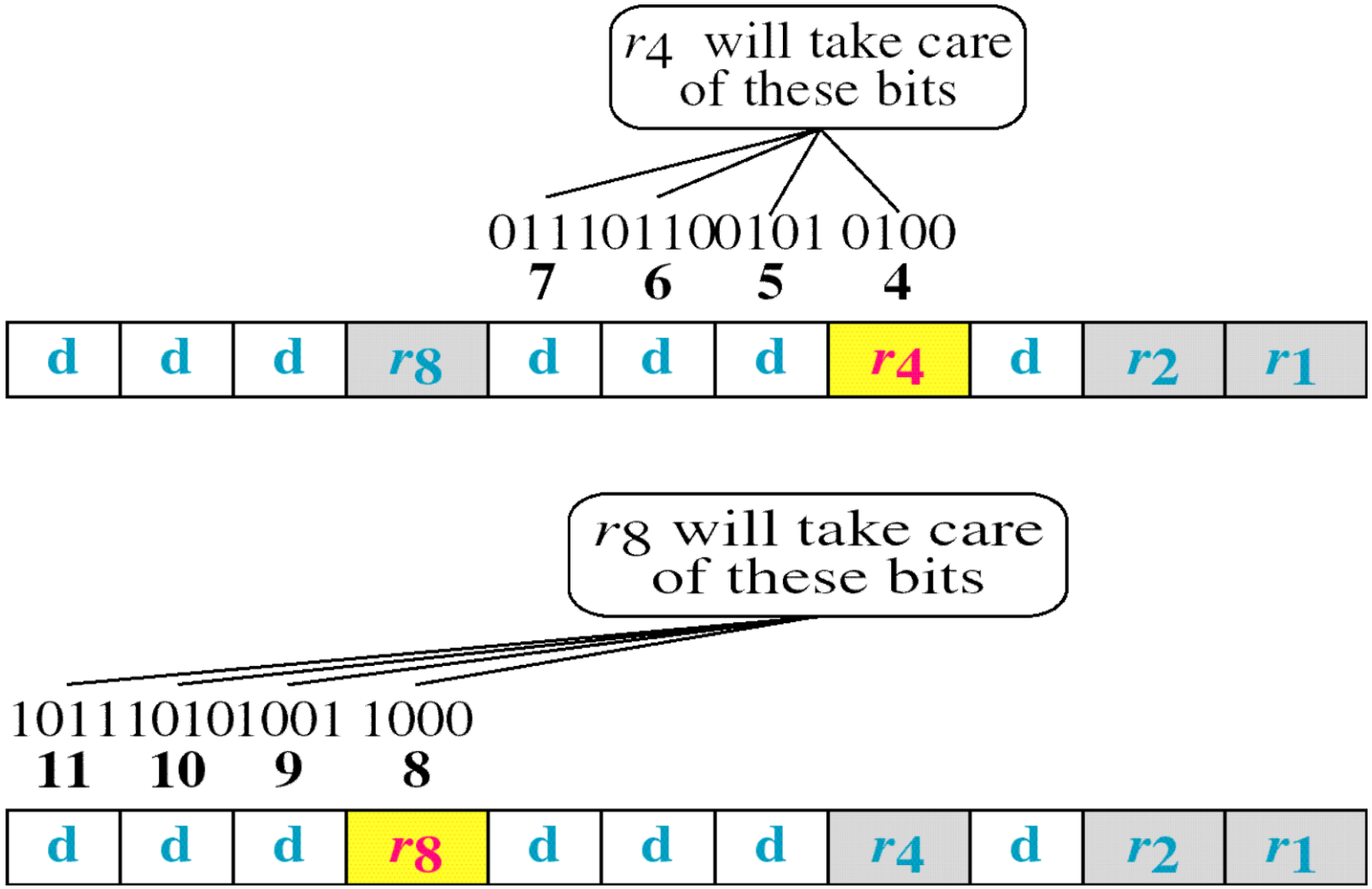
  1=1, 2=2, 3= 1+2, 4=4, 5= 1+4, 6= 2+4, 7= 1+2+4, 8=8, 9= 1+8, 10= 2+8, 11= 1+2+8

so now r_1= 1,3, 5, 7, 9, 11; r_2= 2,3,6,7,10,11; r_4= 4,5, 6,7; r_8= 8,9,10,11

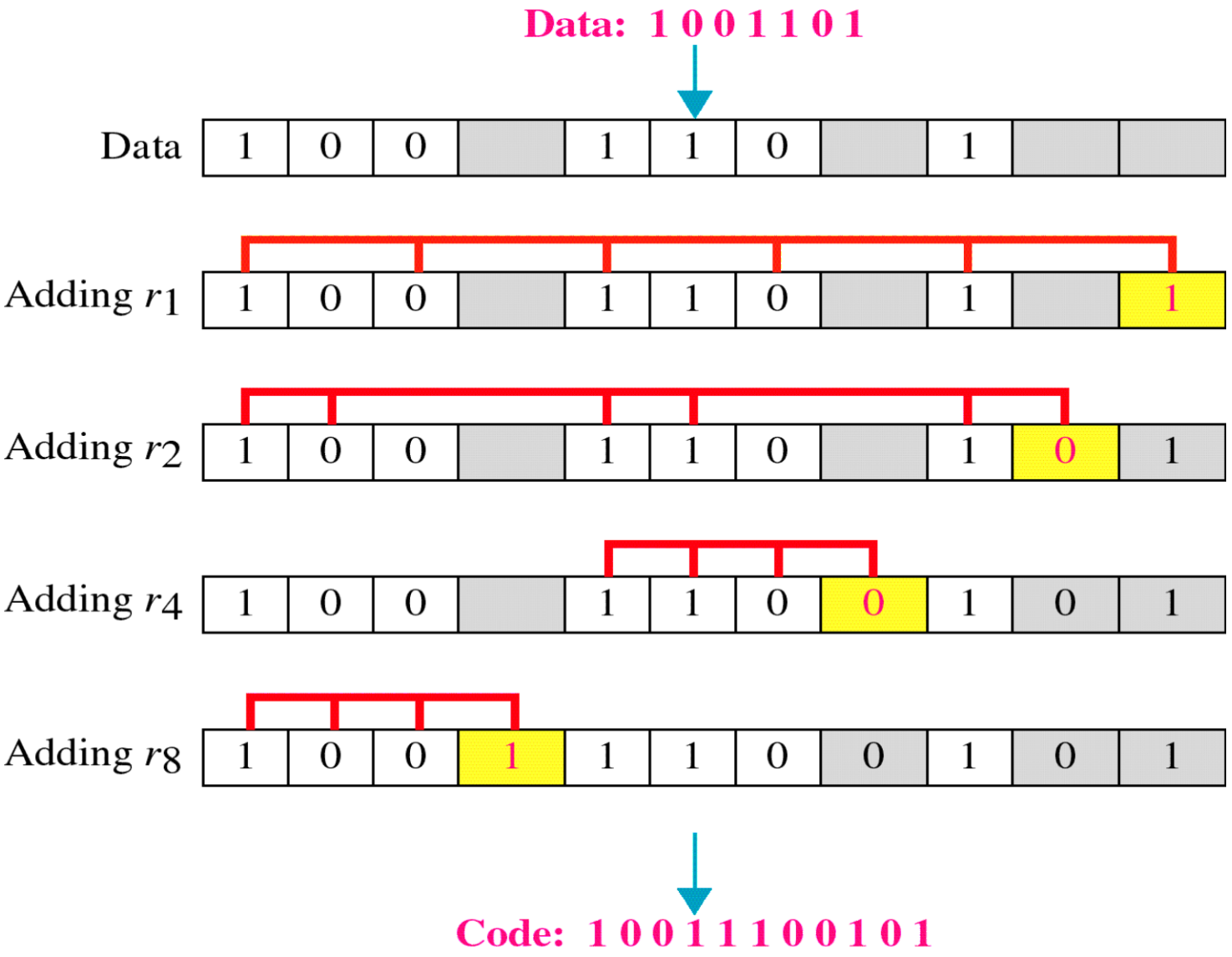
-


r1 will take care of these bits
1011
11
1001
9
0111
7
0101
5
0011
3
0001
1
d
d
d
r8
d
d
d
r4
d
r2
r1


r2 will take care of these bits
10111010
11 10
01110110
7 6
0011 0010
3 2
d
d
d
r8
d
d
d
r4
d
r2
r1


r4 will take care of these bits
0111011001010100
7 6 5 4
d d d r8 d d d r4 d r2 r1
r8 will take care of these bits
1011101010011000
11 10 9 8
d d d r8 d d d r4 d r2 r1

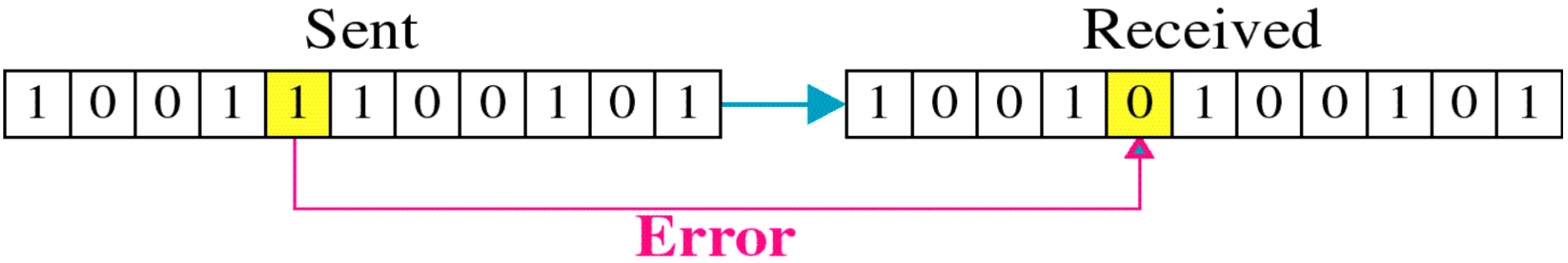
Example


Data: 1 0 0 1 1 0 1
Data
1 0 0 1 1 0 1
Adding r1
1 0 0 1 1 0 1 1
Adding r2
1 0 0 1 1 0 1 0 1
Adding r4
1 0 0 1 1 0 0 1 0 1
Adding r8
1 0 0 1 1 1 0 0 1 0 1
Code: 1 0 0 1 1 1 0 0 1 0 1

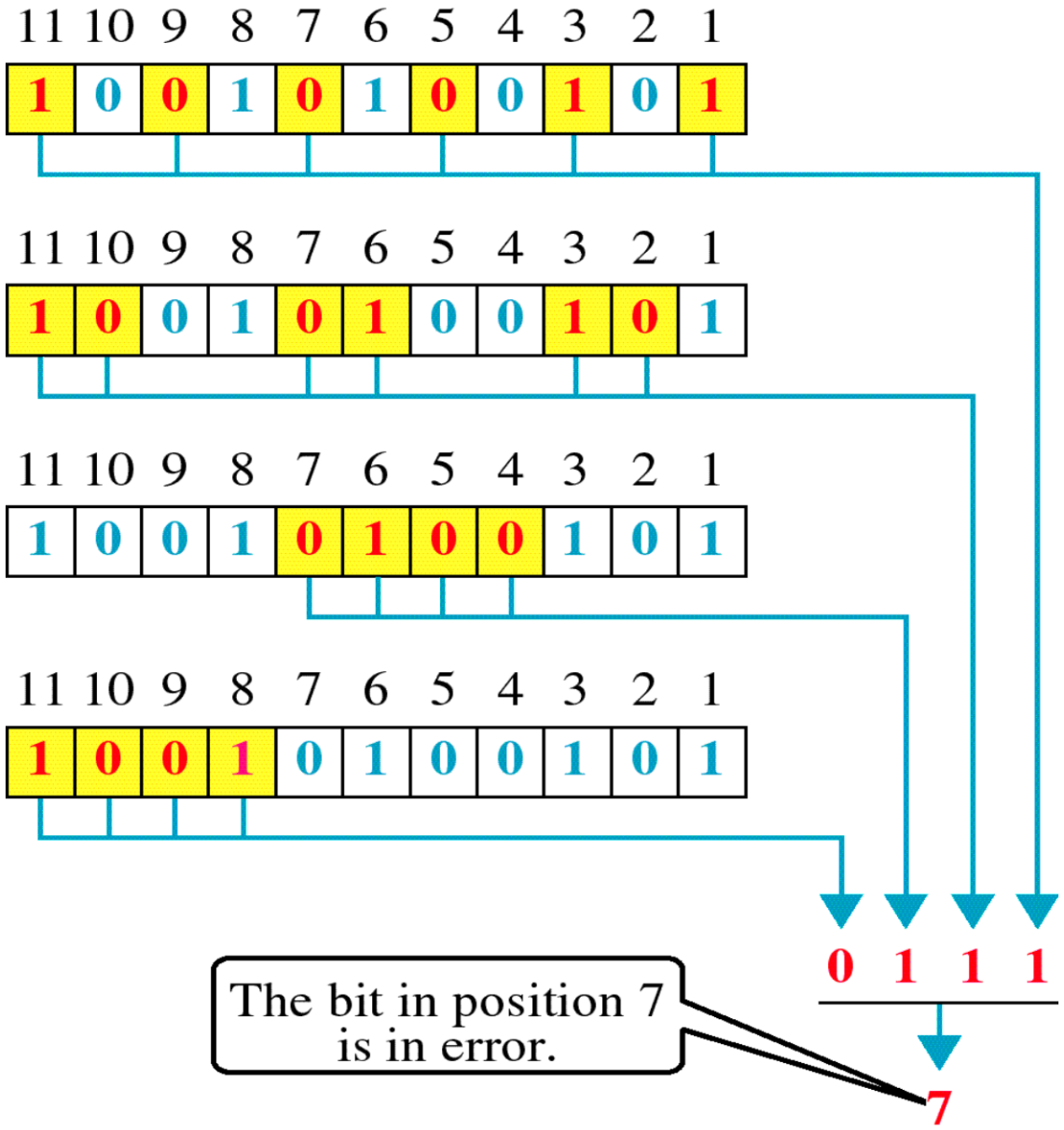
Hamming Code

- Now we write the parity bit for each of the r value . For example parity bit of r1 is calculated to provide even parity of combination 3,5,7,9,11 which sees odd number of 1's and we add 1 to r1. Similarly we perform for r_2, r_4 and r_8 ending in the final code as 10011100101
- Now the code is sent to the receiver say 10010100101and receiver calculates the four new VRC's using the same set of bits used by sender plus relevant parity bits (r1,r2,r4, r8) for each set
- Then receiver reassembles new parity values into a binary number in order of r position (r8, r4, r2, r1) which results in 0111.
- That is bit 7 is the error and is corrected to give 10010100101

Single-bit error



Error Detection



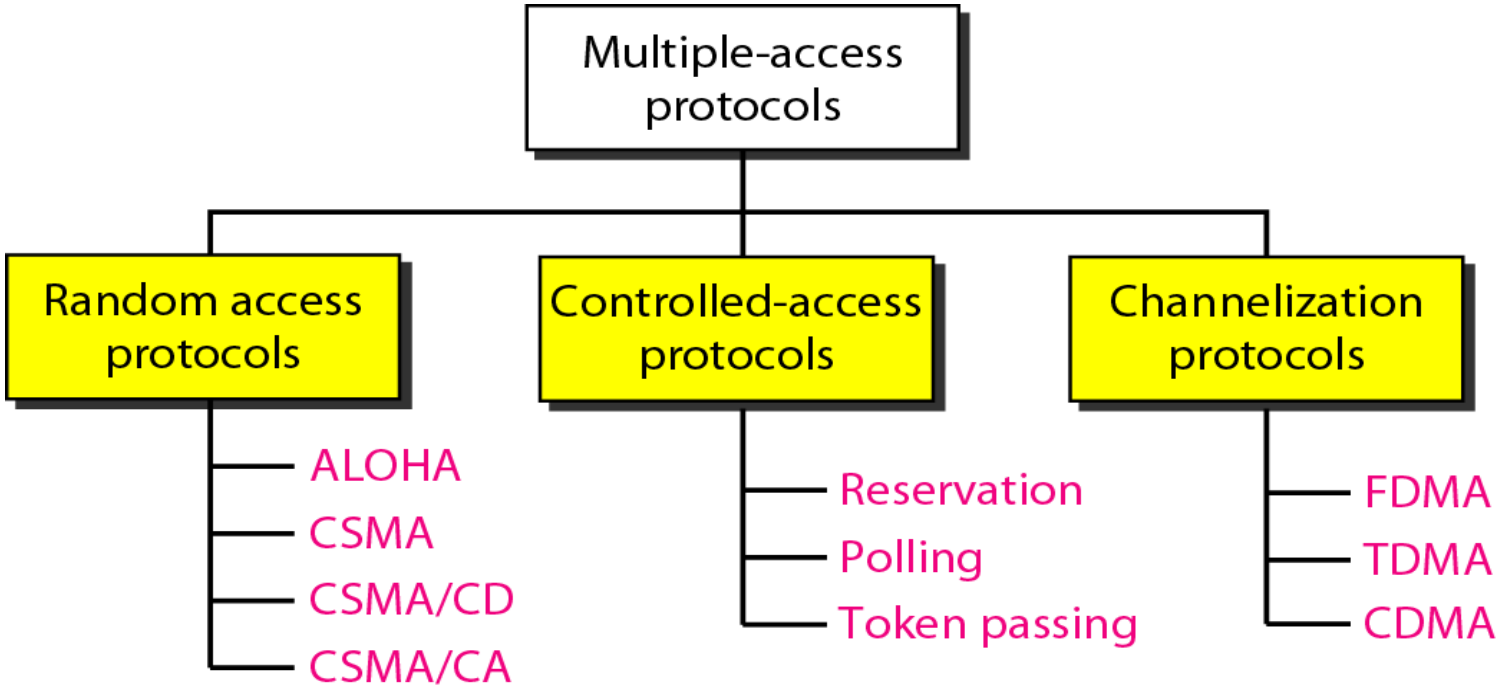
SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Medium Access control Methods –CSMA, CSMA/CA & /CD

MULTIPLE ACCESS PROTOCOLS

- **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.**
- **The problem of controlling the access to the medium is similar to the rules of speaking in an assembly.**
- **The procedures guarantee that the right to speak is upheld and ensure that**
  - **Two people do not speak at the same time,**
  - **Do not interrupt each other,**
  - **Do not monopolize the discussion, and so on.**

Taxonomy of multiple-access protocols discussed in this chapter



Random Access Methods

- In **random access or contention methods**, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.
- This procedure depends on the state of the medium whether it is idle or busy.

Reason for Random Access or Contention

Two features give this methods its name

- No scheduled time for a station to transmit and Transmission is random among the stations. So these methods are called ***random access*****.**
- No specific rules as which station should send next . Stations compete with one another to access the medium. So called ***Contention methods***

Procedure followed by Station for Random Access

- Each station has the right to the medium without being controlled by another station
- If more than one station tries to send, there is an access conflict-collision and frames will be **either destroyed or modified**
- To avoid access conflict or to resolve it when it happens, each station follows a procedure which answers the following queries:

- *When can station access the medium*
- *What can station do if medium is busy*
- *How can the station determine the success or failure of the transmission*
- *What can station do if there is an access conflict*

- Random access methods we would be studying have evolved from a very interesting protocol known as ***ALOHA*** which uses a very simple procedure called ***Multiple Access (MA)***

- Method was later improved with the addition of procedure that **forces the station to sense the medium before transmitting**. This was called Carrier Sense Multiple Access

- This later evolved into two parallel methods

  - *Carrier Sense Multiple Access (CSMA)*

  - *Carrier Sense Multiple Access with Collision Detection and Avoidance (CSMA/CD) & (CSMA/CA)*

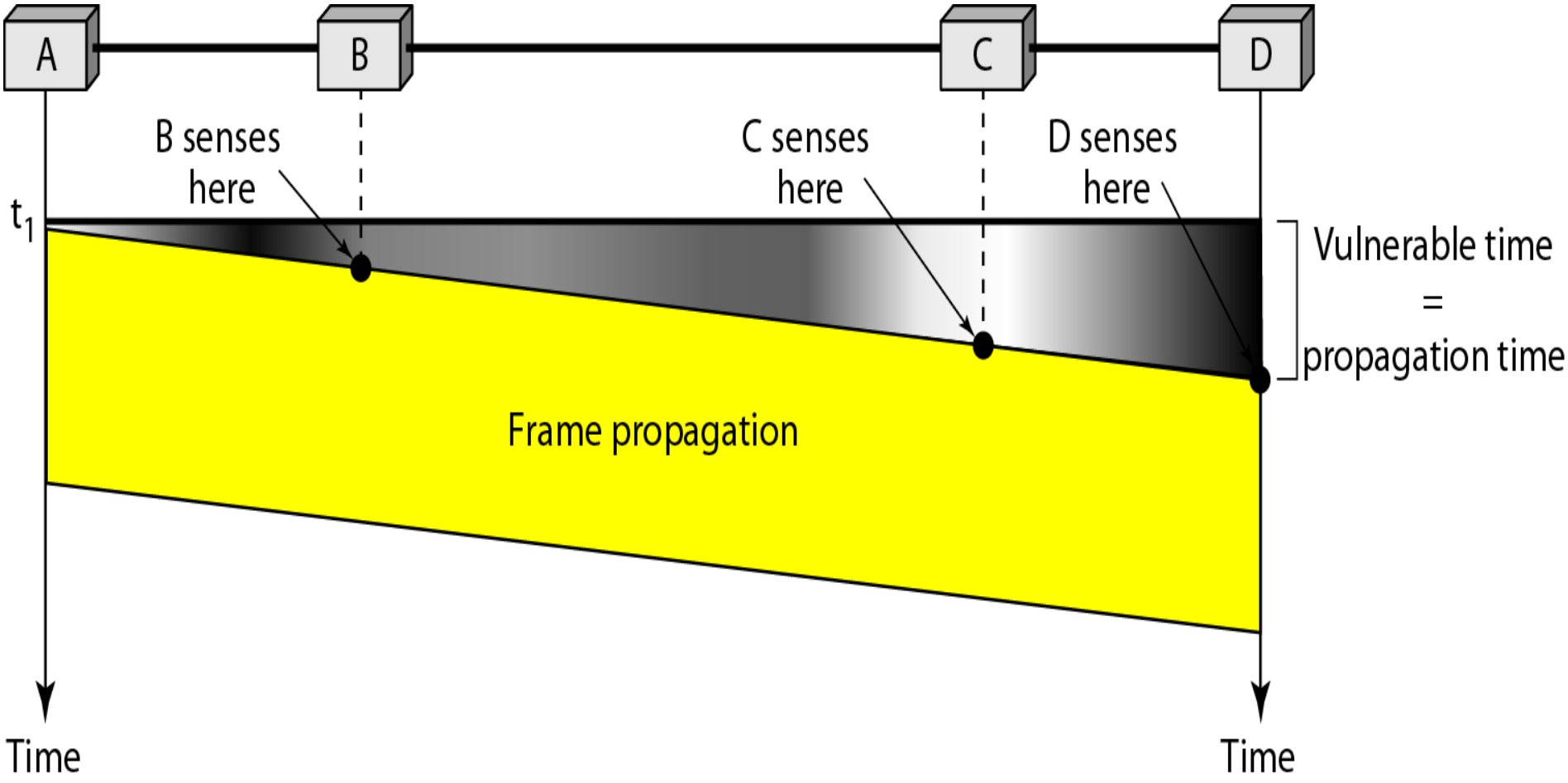
CSMA protocol

- To minimize the chance of collisions and increase the performance, the CSMA (Carrier Sense Multiple Access) method was developed
- CSMA requires that each station first listen to the medium before sending
- CSMA can reduce the possibility of collision but cannot eliminate it.
- Possibility of collisions still exists due to propagation delay
- Two CSMA protocols developed were: Persistent and non-persistent

Vulnerable time in CSMA

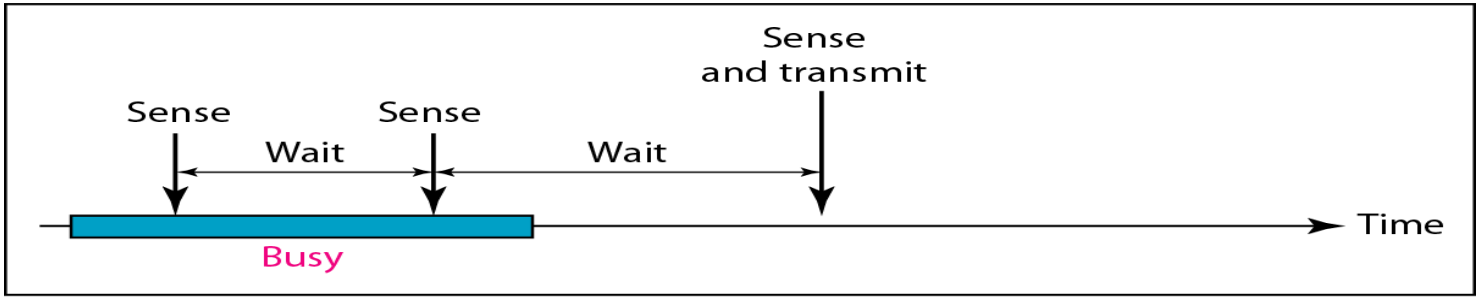
- Vulnerable time in CSMA is the propagation time which is T_p i.e. time needed for a signal to propagated from one end to other.
- When a station sends a frame and any other station sends a frame during this time, a collision will result.
- But if the first bit of frame reaches the end of medium, every station will have heard the bit and will refrain from sending.
- Figure in next slide shows the worst case where a frame sent by station A at time t_1 reaches the rightmost station D at time $t_1 + T_p$

Vulnerable Time in CSMA

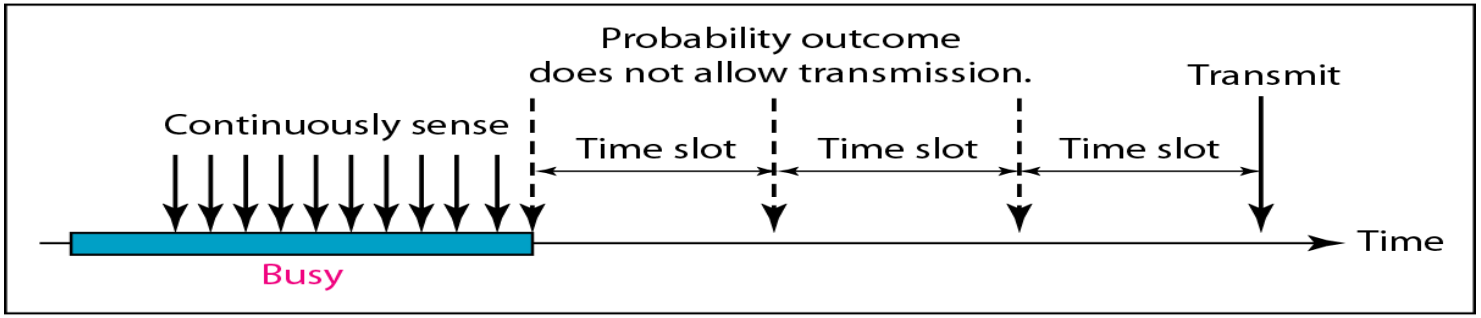


Behavior of three persistence methods

a. 1-persistent



b. Nonpersistent



c. p-persistent

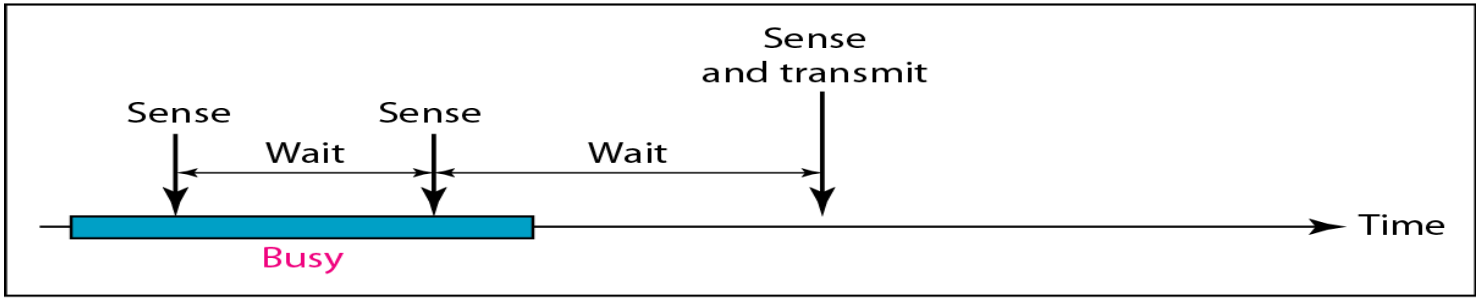
1-Persistent CSMA protocol

- When station finds the medium is idle, it sends its frame immediately with a probability of 1.
- If the medium is busy it waits until it becomes idle and sends its frame with a probability of 1.
- Method has highest chance of collisions because two or more stations may find the line idle and send their frames immediately.

a. 1-persistent

Non-persistent CSMA protocol

- Station senses a channel
- If channel is idle, station begins transmitting
- If channel is busy, station does not continually wait for accessing the channel
- Instead it waits a random period of time and then repeats algorithm again- Exponential Back off
- This method reduces the collision as it is unlikely two or more stations will wait the same amount of time and retry to send simultaneously



b. Nonpersistent

p-persistent CSMA protocol

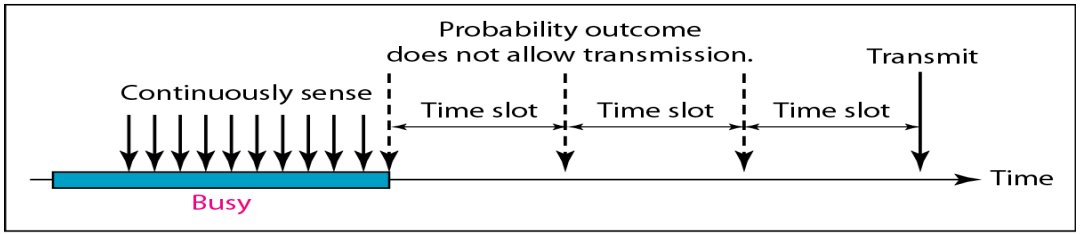
- This method is used if channel has time slots with slot duration equal to or greater than maximum propagation time
- p-persistence approach combines the advantages of other two methods.
- Reduces the chances of collision and improves efficiency
- Here once the station finds the line is idle, it follows these steps:

i With probability p, station sends its frame

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

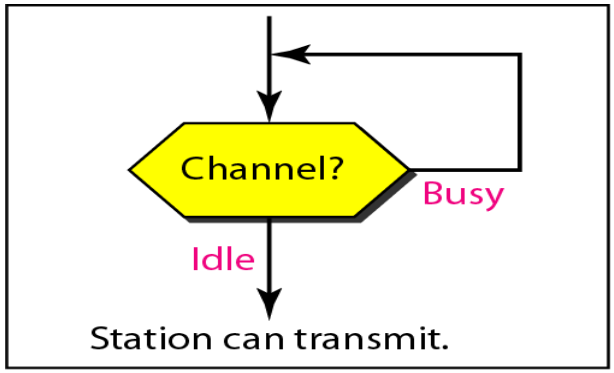
a. If line is idle, it goes to step i

b. If line is busy, it acts as collision has occurred and uses back off procedure.

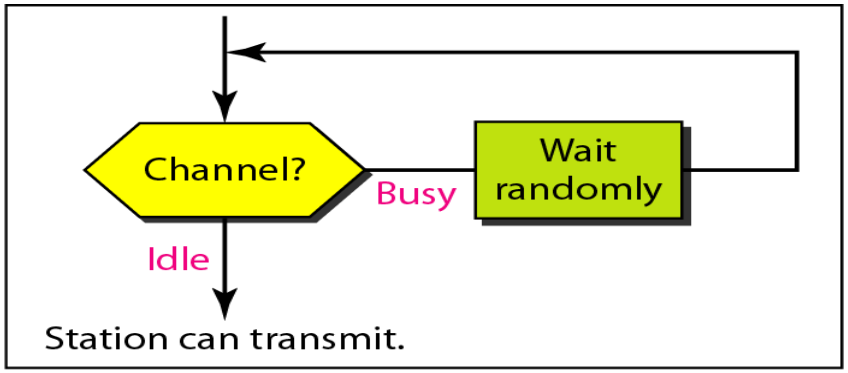


c. p-persistent

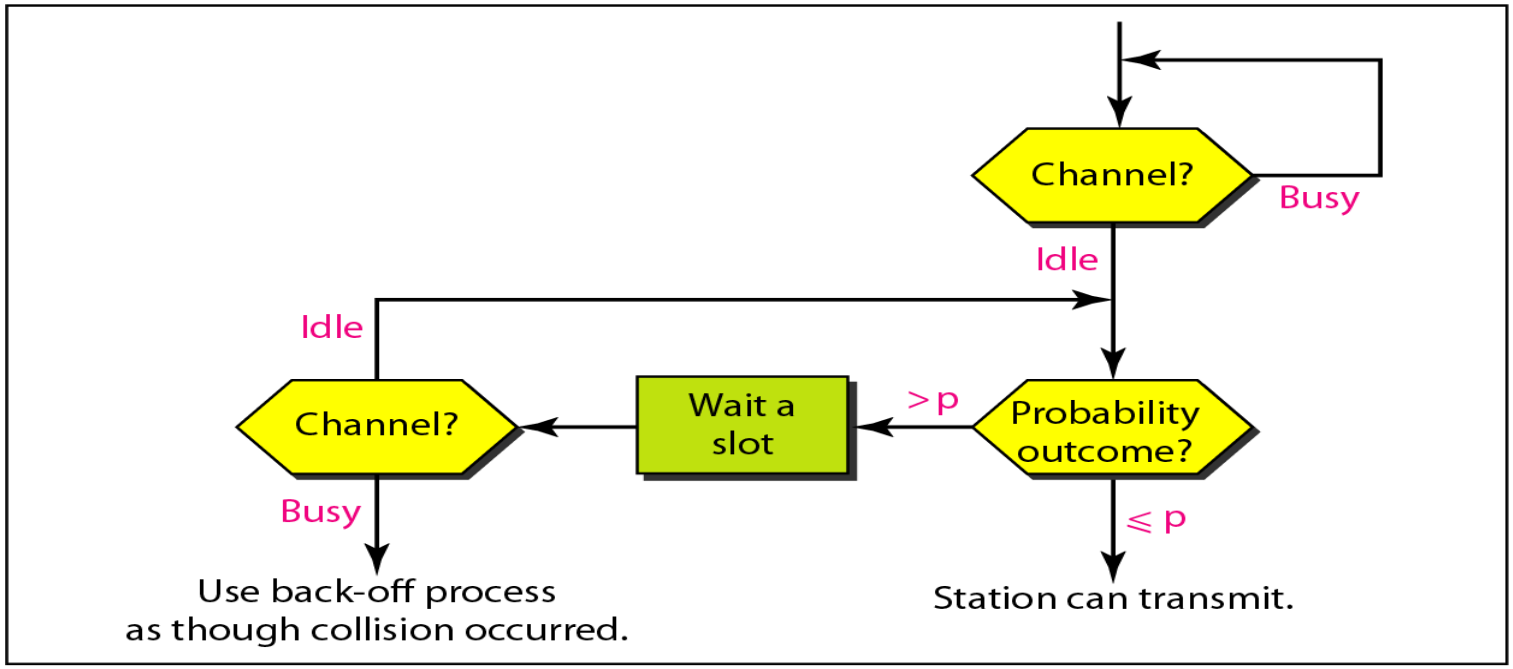
Flow Diagram of three persistence methods



a. 1-persistent



b. Nonpersistent

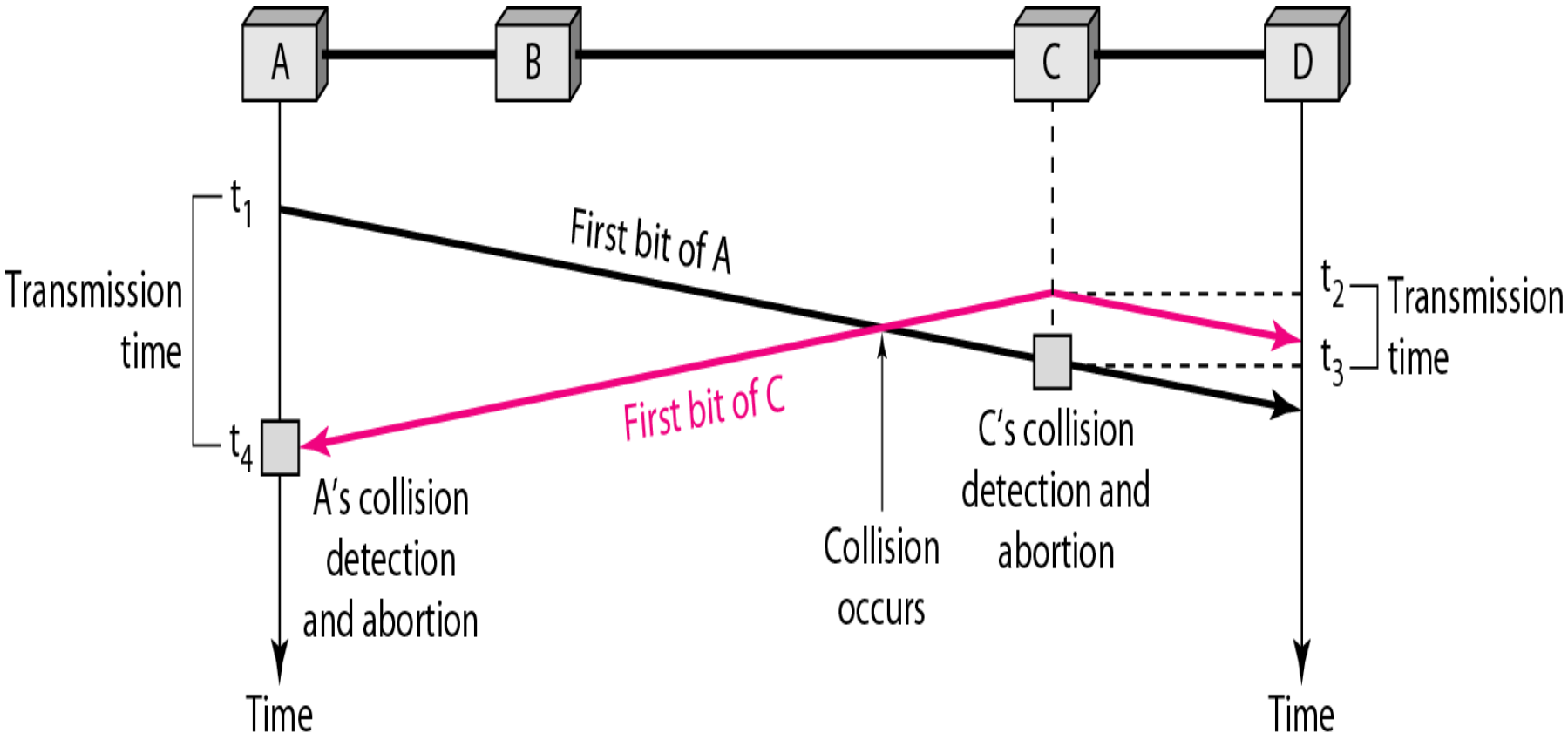


c. p-persistent

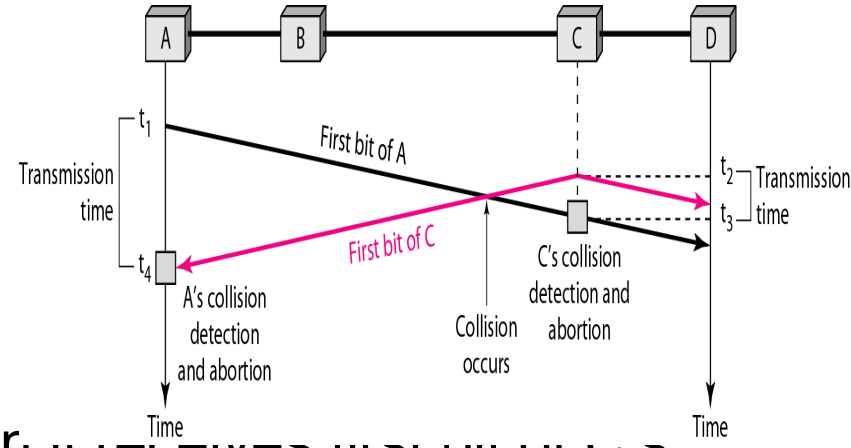
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- CSMA method does not specify the procedure following a collision
- CSMA/CD augments the algorithm to handle collision
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful
- If successful, the station is finished
- If not, frame is sent again.
- We can better understand CSMA/CD with the diagram in next slide.

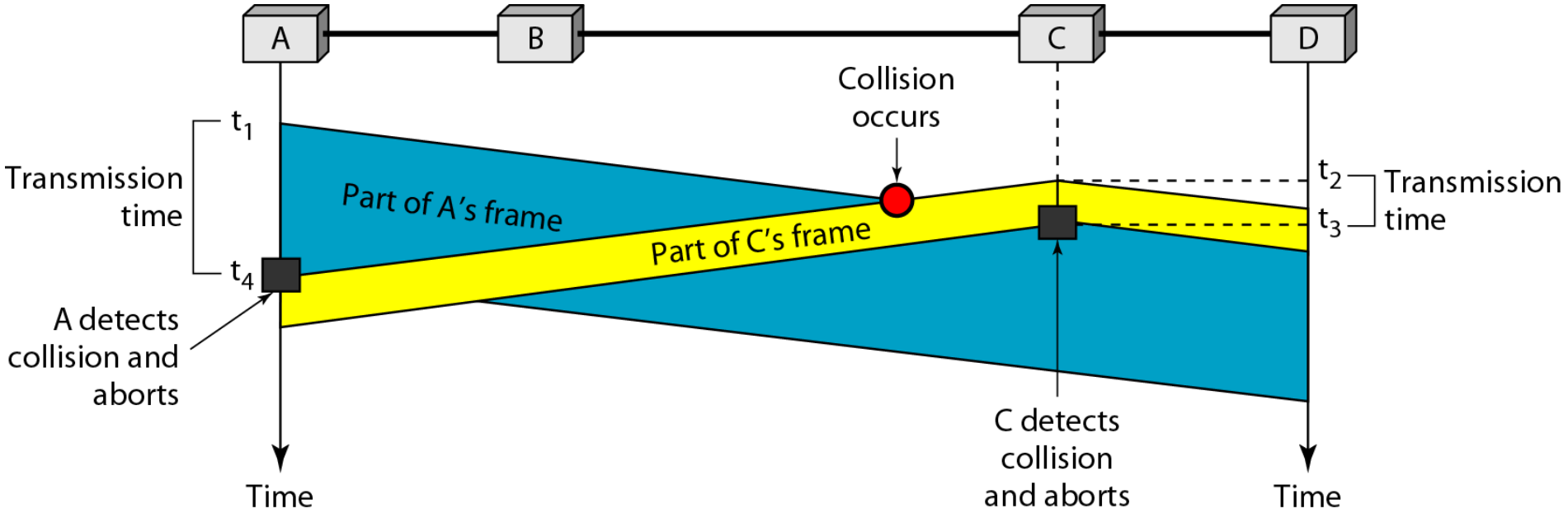
Collision of first bit in CSMA/CD



- At time t1, Station A has executed the 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 bits in frame which propagates to both left and right
- Collision occurs after time t2.
- Station C detects a collision at time t3 when it receives first bit of A's frame.
- Station C aborts its transmission
- Station A detects collision at time t4 when it receives first bit of C's frame; it also aborts its transmission immediately.
- We see that A transmits for a duration of t_4-t_1; C transmits for duration of t_3-t_2.
- At time t_4 transmission of A's frame though incomplete is aborted; time t_3 transmission of C's frame though incomplete is aborted



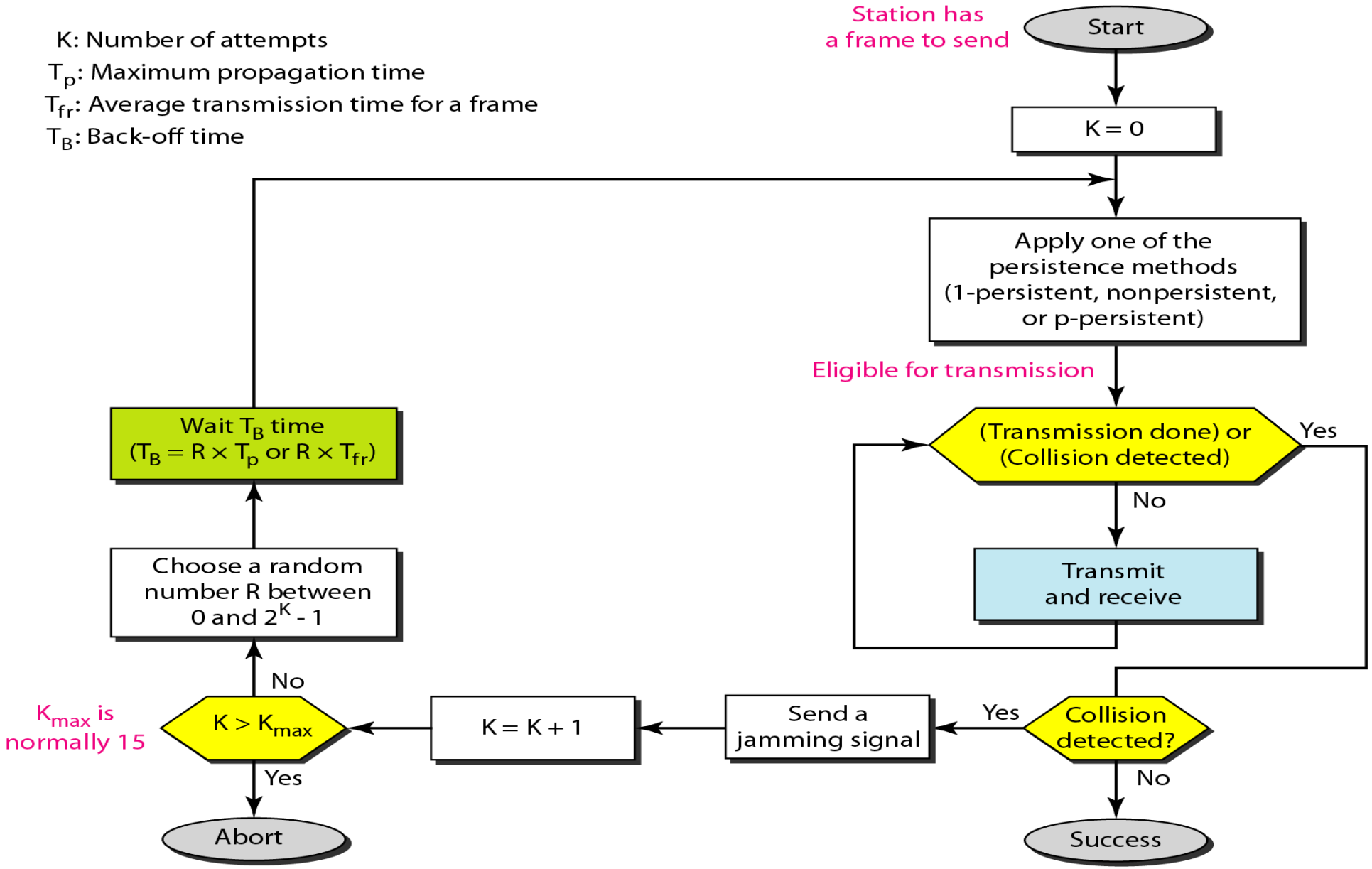
Collision and abortion in CSMA/CD



Minimum Frame size for CSMA/CD

- For CSMA/CD we need restriction of the frame size
- Before sending the last bit of frame, sending station must detect collision , if any must abort the transmission
- Reason for this is a station once sent the entire frame does not monitor the line for collision detection
- So, Frame Transmission time $T_{fr} = 2 * T_p$
- If two stations involved in collision are maximum distance apart, signals from first takes time T_p to reach the second and effect of collision takes another time T_p to reach the first.
- Requirement is first station should still be transmitting after 2 T_p

Flow Diagram for CSMA/CD



Example

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

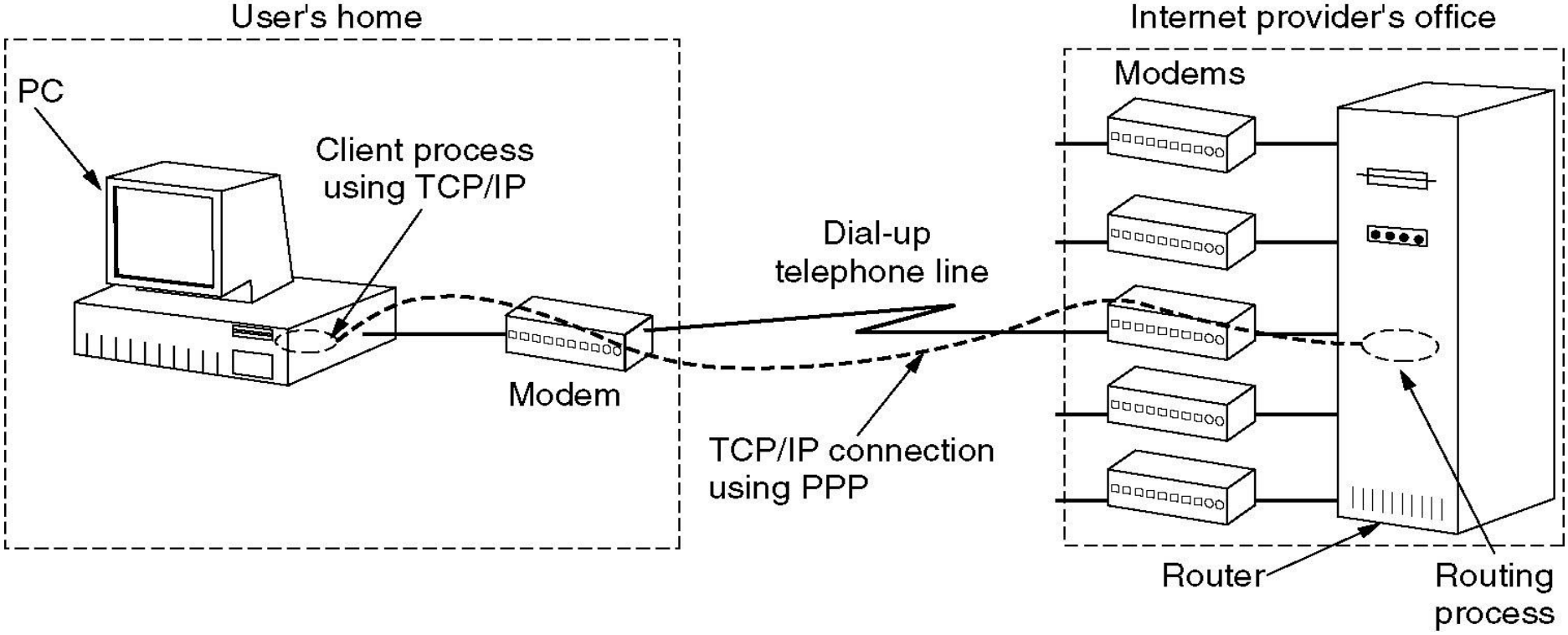
Solution

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

HDLC and PPP

The Data Link Layer in the Internet

A home personal computer acting as an internet host.



Technology like Ethernet cannot provide "high-level" functionality like connection management and

Point to Point Data Link Control

- One sender, one receiver, one link: easier than broadcast link:
  - No Media Access Control
  - No need for explicit MAC addressing
  - E.g., dialup link, ISDN line
- Popular point-to-point and high-level DLC protocols:
  - PPP (point-to-point protocol)
  - HDLC: High level data link control (Data link used to be considered "high layer" in protocol stack). HDLC is also used in multi-point links (one station many receivers)
- These protocols can often be run over other data link technologies providing best of both worlds
  - E.g., PPPoE, HDLC encapsulation by Ethernet

PPP Design Requirements [RFC 1557]

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Functionality : (similar to link layer services + extra management functions)

- **Packet framing - encapsulation of network-layer datagram in data link frame**
- **Multi-protocol - carry network layer data of any network layer protocol (not just IP) *at same time* ability to demultiplex upwards**
- **Bit transparency - must carry any bit pattern in the data field (even if underlying channel can't)**
- **Error detection - not correction**

PPP Design Requirements (cont.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

The extra stuff:

- **Connection liveness:** detect, signal link failure to network layer
- **Network layer address negotiation:** endpoint can learn/configure each other's network address and other characteristics.
- **Authentication:** who are you (or at least whose account do I bill for your dial-in time?)
  - This information is used by traffic management software to control bandwidth to individual subscribers
- **Management features:** loopback detection

PPP non-requirements

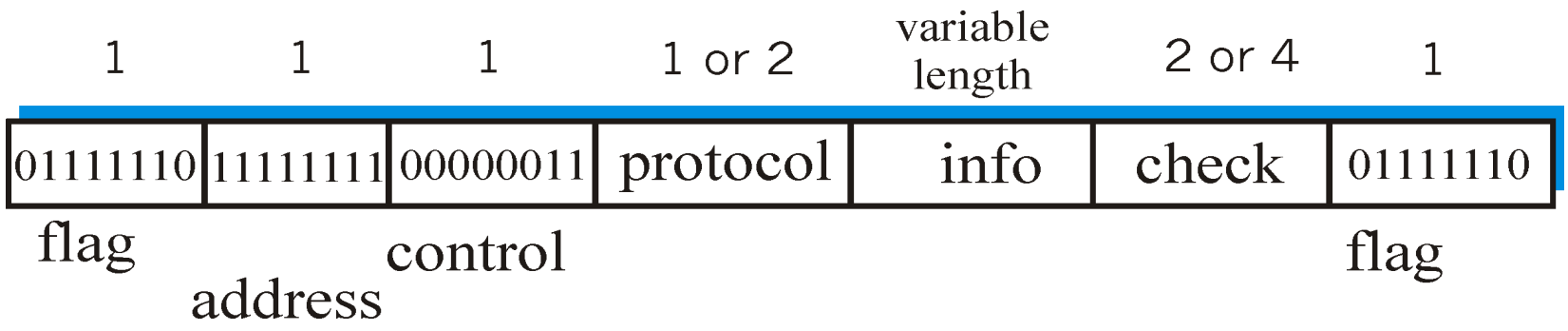
- **No error correction/recovery**

  (modems do one layer FEC, one layer packetization + retransmission "under the covers" anyway; other technologies are pretty reliable)
- **No flow control**
- **Out of order delivery OK**

Error recovery, flow control, data re-ordering all relegated to higher layers!

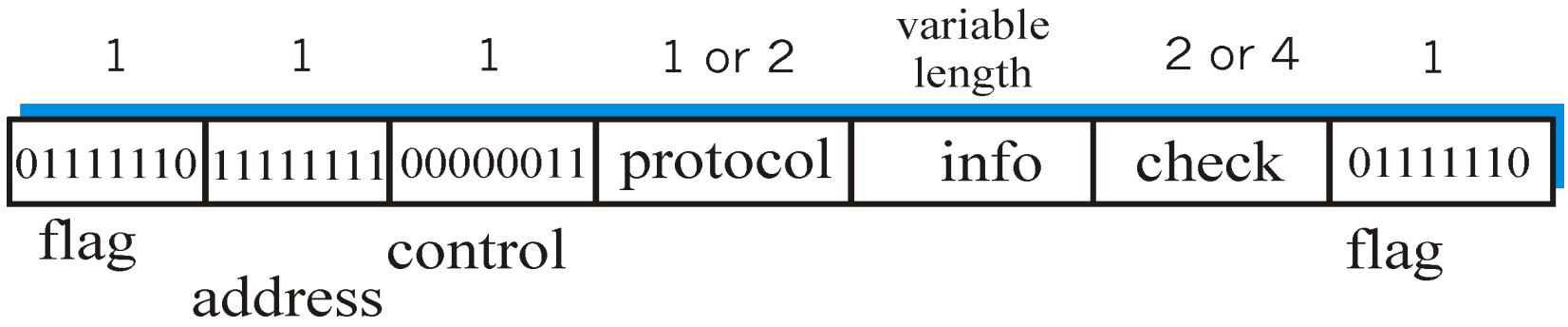
PPP Data Frame

- **Flag:** delimiter (framing)
- **Address:** ignored. (historical)
- **Control:** ignored. (historical)
- **Protocol:** upper layer protocol to which frame delivered (e.g., PPP-LCP, IP, IPCP, etc)

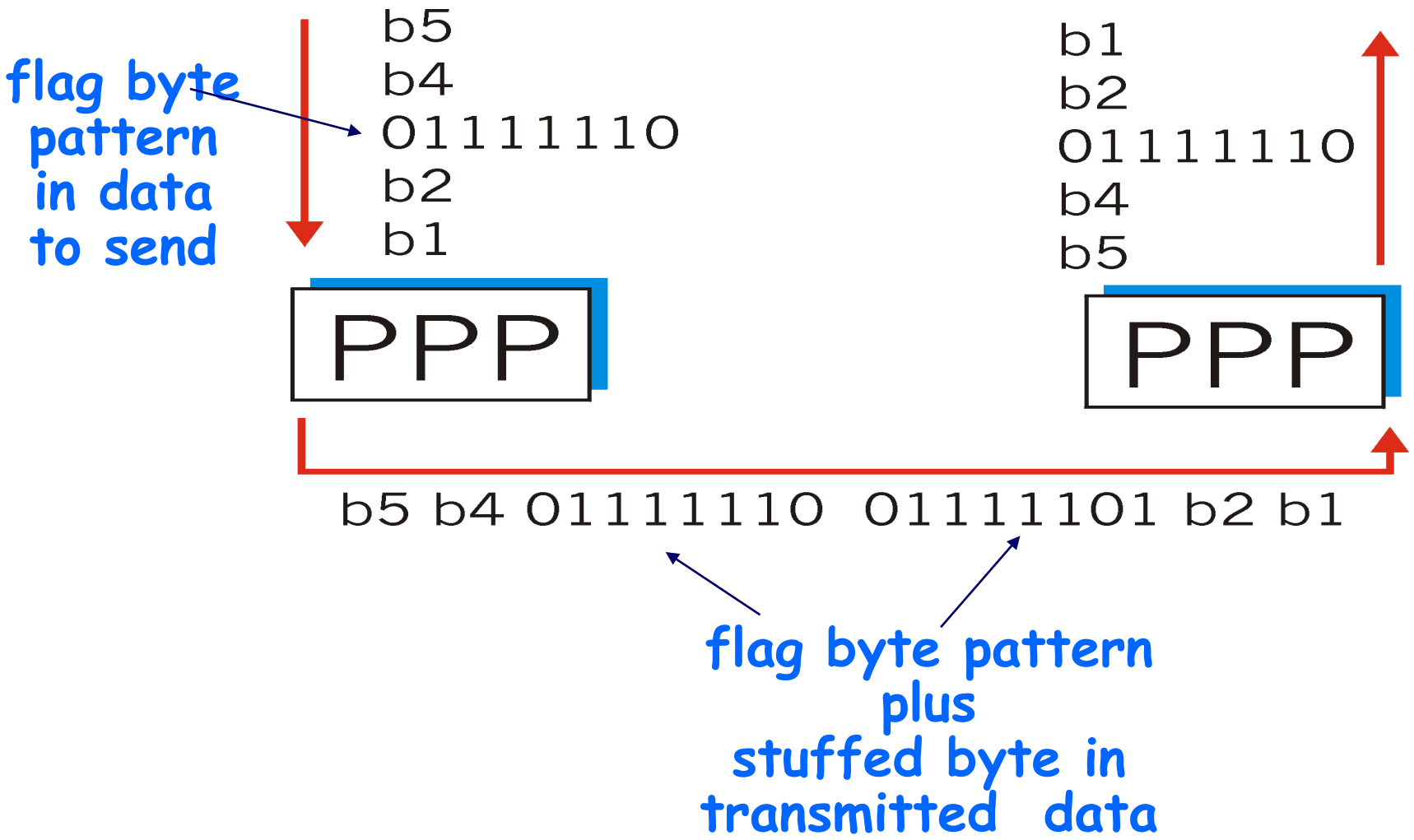


PPP Data Frame

- **info: upper layer data being carried**
- **check: cyclic redundancy check for error detection**



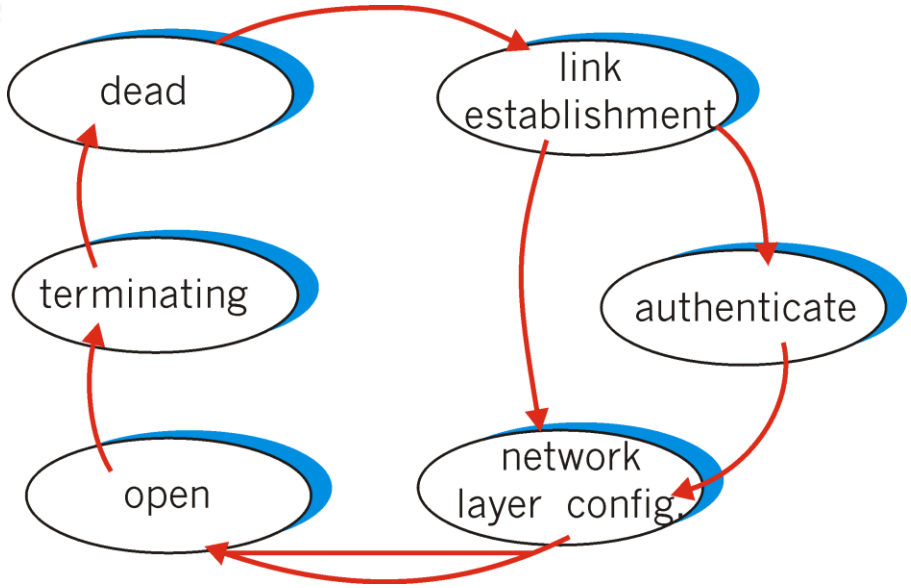
Byte Stuffing



PPP Data Control Protocol

Before exchanging network-layer data, data link peers must

- **Configure PPP link (max. frame length, authentication)**
- **Learn/configure network layer information**
  - **for IP: carry IP Control Protocol (IPCP) msgs (protocol field: 8021) to configure/learn IP address**



Where does PPP get used?

- Dial-up – PPP over async serial, over modem
- ADSL – PPP over Ethernet
- Backbone – Packet over SONET (POS)
- Why?
  - Framing (dialup, POS)
  - Efficiency (POS)
  - Authentication, address negotiation (PPPoE)

High-Level Data Link Control (HDLC)

- **HDLC was defined by ISO for use on both point-to-point and multipoint data links.**
- **It supports full-duplex communication**
- **Other similar protocols are**
  - **Synchronous Data Link Control (SDLC) by IBM**
  - **Advanced Data Communication Control Procedure (ADCCP) by ANSI**
  - **Link Access Procedure, Balanced (LAP-B) by CCITT, as part of its X.25 packet-switched network standard**

HDLC Overview

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Broadly HDLC features are as follows:

- **Reliable protocol**
  - **selective repeat or go-back-N**
- **Full-duplex communication**
  - **receive and transmit at the same time**
- **Bit-oriented protocol**
  - **use bits to stuff flags occurring in data**
- **Flow control**
  - **adjust window size based on receiver capability**
- **Uses physical layer clocking and synchronization to send and receive frames**

HDLC Overview

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- **Defines three types of stations**
  - **Primary**
  - **Secondary**
  - **Combined**
- **Defines three types of data transfer mode**
  - **Normal Response mode**
  - **Asynchronous Response mode**
  - **Asynchronous Balanced mode**
- **Three types of frames**
  - **Unnumbered**
  - **information**
  - **Supervisory**

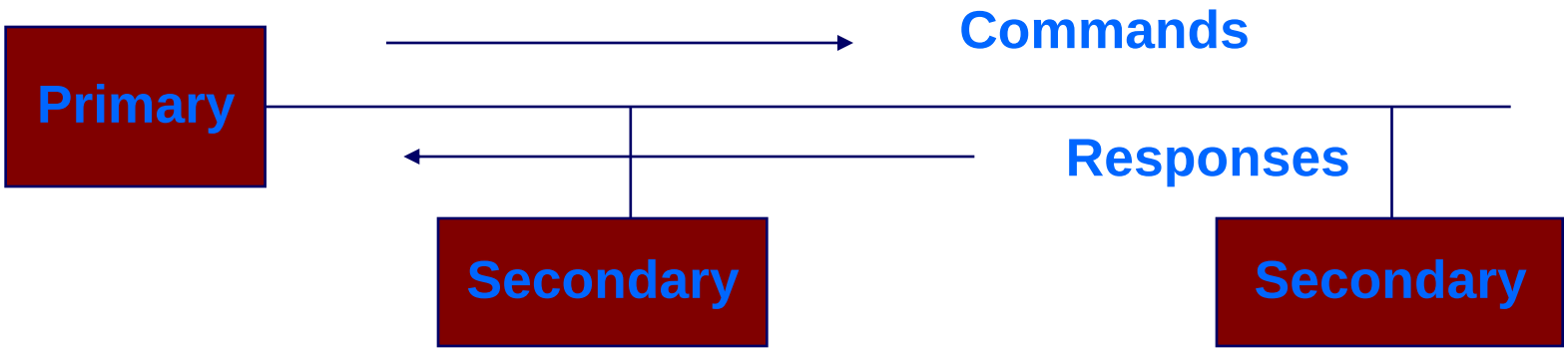
HDLC

- **The three stations are :**
  - **Primary station**
    - **Has the responsibility of controlling the operation of data flow the link.**
    - **Handles error recovery**
    - **Frames issued by the primary station are called *commands*.**
  - **Secondary station,**
    - **Operates under the control of the primary station.**
    - **Frames issued by a secondary station are called *responses*.**
    - **The primary station maintains a separate logical link with each secondary station.**
  - **Combined station,**
    - **Acts as both as primary and secondary station.**
    - **Does not rely on other for sending data**

HDLC

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

Unbalanced Mode



Balanced mode

HDLC

- **The three modes of data transfer operations are**
  - **Normal Response Mode (NRM)**
    - **Mainly used in terminal-mainframe networks. In this case,**
    - **Secondaries (terminals) can only transmit when specifically instructed by the primary station in response to a polling**
    - **Unbalanced configuration, good for multi-point links**
  - **Asynchronous Response Mode (ARM)**
    - **Same as NRM except that the secondaries can initiate transmissions without direct polling from the primary station**
    - **Reduces overhead as no frames need to be sent to allow secondary nodes to transmit**
    - **Transmission proceeds when channel is detected idle , used mostly in point-to-point-links**
  - **Asynchronous Balanced Mode (ABM)**
    - **Mainly used in point-to-point links, for communication between combined stations**

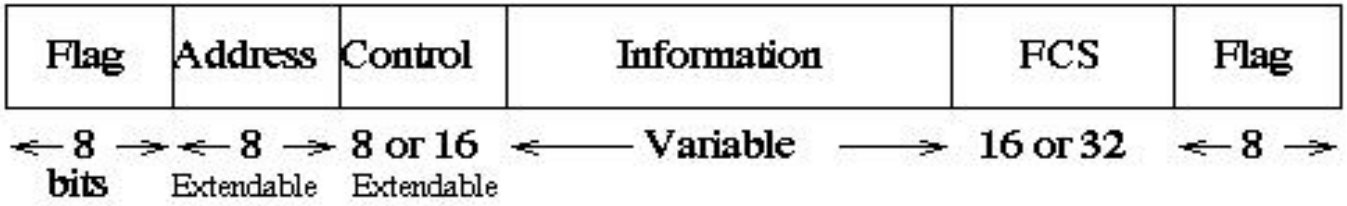
Non-operational Modes

- **Normal Disconnected Mode**
- **Asynchronous Disconnected Mode**

Both the above modes mean that the secondary node is logically disconnected from the primary node

- **Initialization Mode**
  - **A node negotiates transmission parameters with the other node E.g., flow control information**
  - **Parameters negotiated in this mode are used during any of the data transfer modes**

Data Link Control HDLC frame structure



(a) Frame format

(a) Frame Format

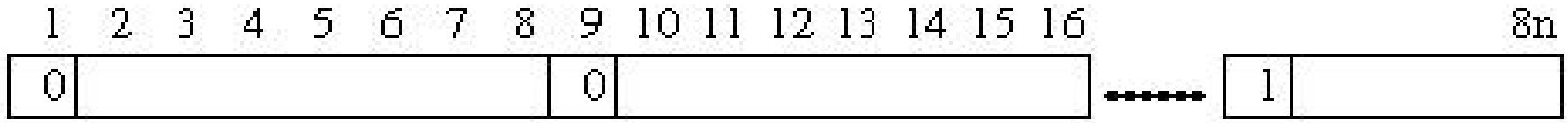
	1	2	3	4	5	6	7	8
I: Information	0	N(S)			P/F	N(R)		
S: Supervisory	1	0	S		P/F	N(R)		
U: Unnumbered	1	1	M		P/F	M		

N(S) = Send sequence number
N(R) = Receive sequence number
S = Supervisory function bits
M = Unnumbered function bits
P/F = Poll/final bit

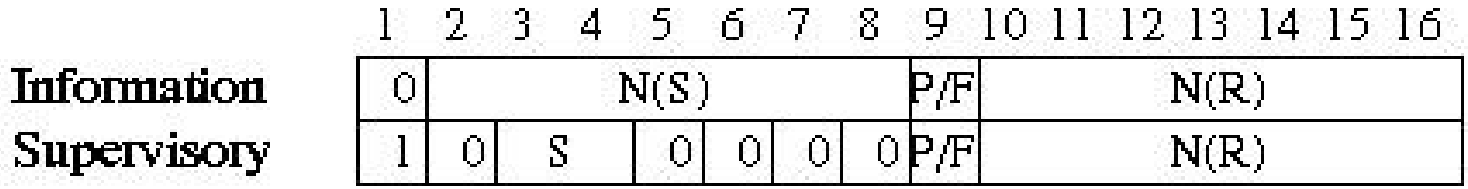
(b) Control field format

(b) Control field format

Data Link Control
HDLC frame structure



(c) Extended address field



(d) Extend control fields

(c) Extended address field **(d) Extended control field**

HDLC

- **Flag: 01111110- start and ending delimiter. Bits are stuffed for flags in data frames**
- **FCS: 16-bit CRC using generating polynomial**

$$G(x) = x^{16} + x^{12} + x^5 + 1$$

- **Address field:**
  - **mainly used in multidrop link configuration, and not used in point-to-point**
  - **In unbalanced configuration, every secondary is assigned a unique address. Contains address of secondary station in both command and response frames**
  - **In balanced mode, command frame has destination address and response frame has sending node's address**
  - **Group addresses are also possible. E.g., One command sent to all the secondaries**
- **In I-frames, N(s) is the sequence number of the frame being sent, and R(s) is the sequence number of the frame being expected.**
- **The P/F bit, known as the poll/final bit, is used with different meaning in different contexts.**
  - **It is used to indicate polling, to indicate the final I-frame, etc**

HDLC

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- **There are three different classes of frames used in HDLC**
  - **Unnumbered frames, used in link setup and disconnection, and hence do not contain ACK.**
  - **Information frames, which carry actual information. Such frames can piggyback ACK in case of ABM**
  - **Supervisory frames, which are used for error and flow control purposes and hence contain send and receive sequence numbers**

HDLC

- **There are four different supervisory frames**
  - **SS=00, Receiver Ready (RR), and N(R) ACKs all frames received up to and including the one with sequence number N(R) - 1**
  - **SS=10, Receiver Not Ready (RNR), and N(R) has the same meaning as above**
  - **SS=01, Reject; all frames with sequence number N(R) or higher are rejected, which in turns ACKs frames with sequence number N(R) -1 or lower.**
  - **SS=11, Selective Reject; the receive rejects the frame with sequence number N(R)**

HDLC

- **The unnumbered frames can be grouped into the following categories:**
  - **Mode-setting commands and responses**
  - **Recovery commends and responses**
  - **Miscellaneous commands and responses**

Review of Link Layer

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- **Services**
  - Framing
  - Error control
  - Reliability
  - Connection management
  - Medium access control
  - Switching
- **Protocols, Standards**
  - Ethernet
  - Token Ring
  - FDDI
  - Wireless
  - PPP
  - HDLC