Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

Unit 2: Data Link Layer

School of Computer Engineering and Technology (SCET)

Data Link Layer

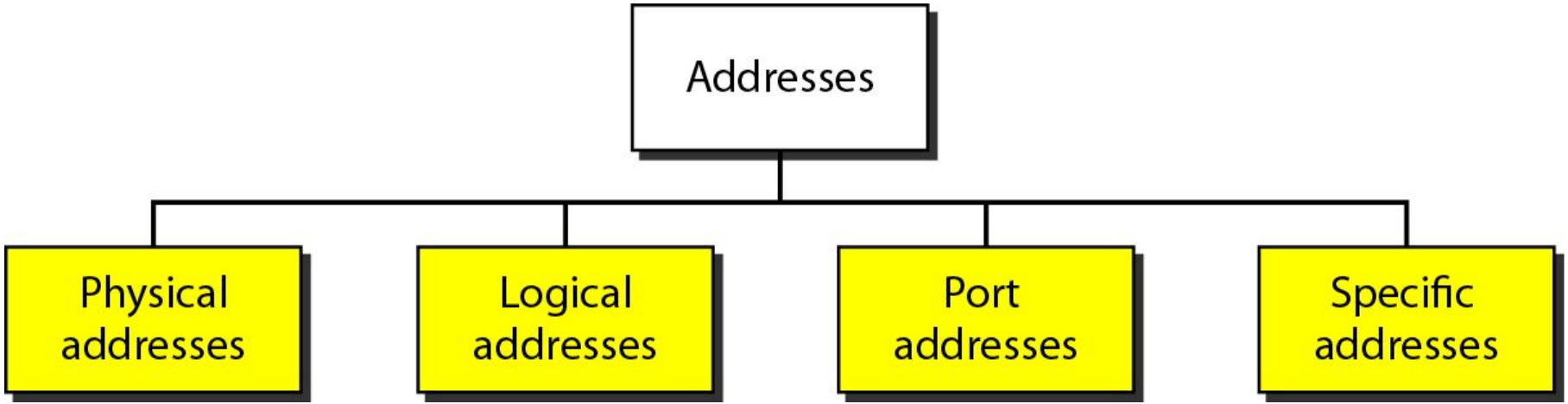
Services

- Provide service interface to the network layer
- Dealing with transmission errors
- Regulating data flow
  - Slow receivers not swamped by fast senders

Frame

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Addresses in TCP/IP Network

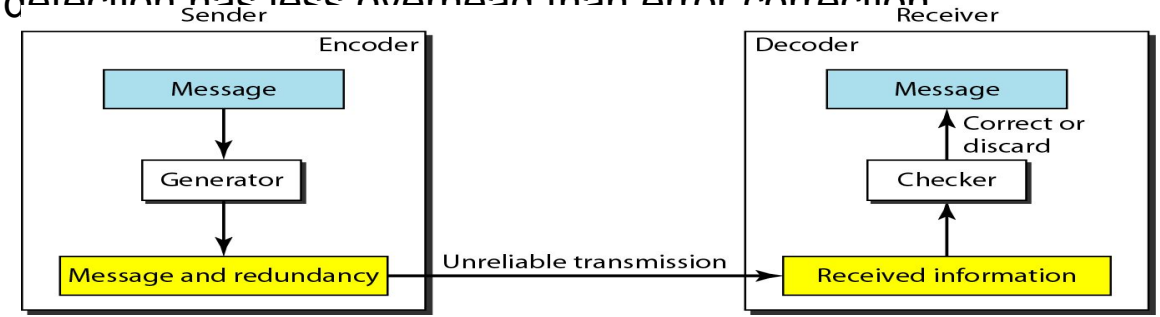


Link Layer Address

- Six bytes = 48 bits
- Flat address not hierarchical
- Burned into the NIC ROM
- First three bytes from left specify the vendor. Cisco 00-00-0C, 3 Com 02-60-8C and the last 24 bit should be created uniquely by the company
- Destination Address can be:
  - Unicast: second digit from left is even (one recipient)
  - Multicast: Second digit from left is odd (group of stations to receive the frame – conferencing applications)
  - Broadcast (ALL ones) (all stations receive the frame)
- Source address is always Unicast

Error Control

- To detect or correct errors, we need to send extra (redundant) bits with data.
- Enough redundancy is added to detect an error.
- In error detection, the receiver knows an error occurred but does not know which bit(s) is(are) in error.
- Error detection has less overhead than error correction



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

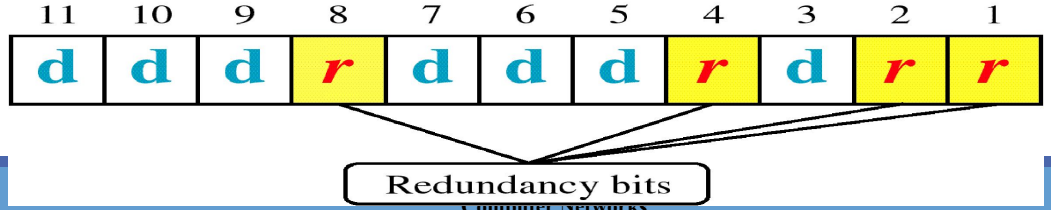
Hamming Code

- Hamming Codes are the family of linear error correcting codes invented by Richard hamming in 1950.
- Hamming code can detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors.
- Easy to implement
- Commonly 7/8 bit hamming code is used. (But we can use hamming code greater than this).

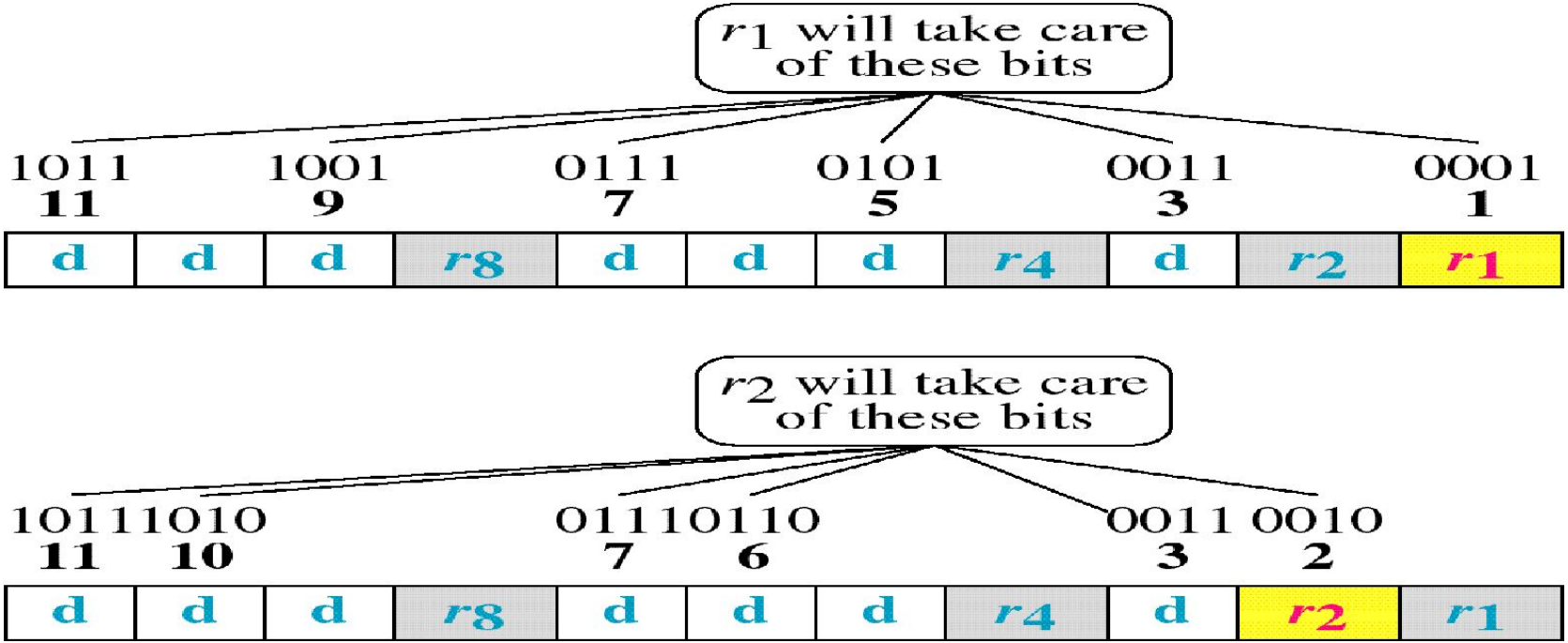
Hamming Code

- In hamming code the bits of the code word are numbered consecutively starting with bit 1, and bit 2, & so on
- The bits that are power of '2' are 'r' – Check bits (parity bits) (e.g. 1, 2, 4, 8, ..).
- The rest (e.g. 3, 5, 6, 7, 9, 10, 11, …..) are filled with 'm' – Data bits.
- The pattern is shown for an (n, m) here (11,7) where

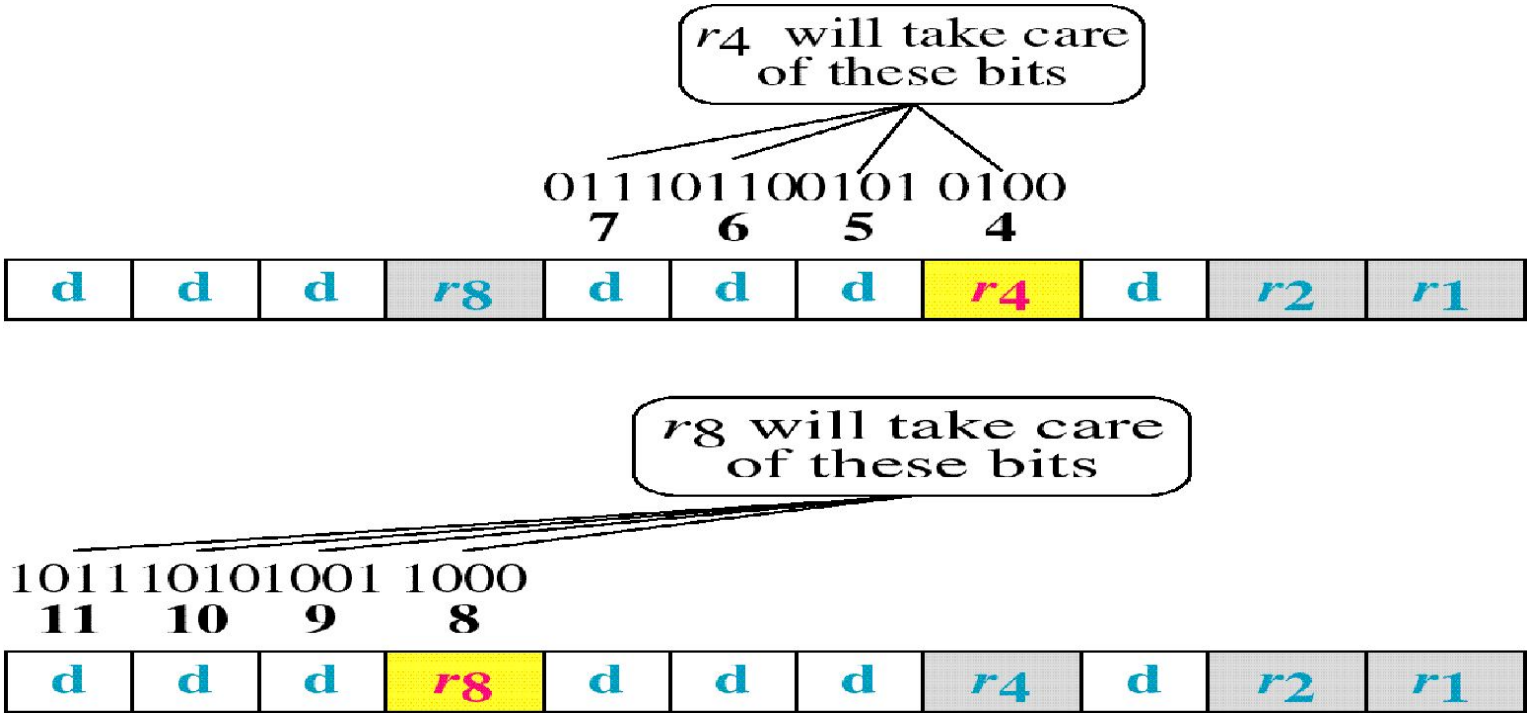
  'm' = data bits = 7, 'r' = check bits = 4, 'n' = code word = 11
- *The value of r must satisfy the following relation*: $2^r \geq m+r+1$.



Hamming Code



Hamming Code



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Hamming Code

- That is
- R1 = M3, M5, M7, M9, M11 => (Alternate 1 Bit including r1 itself).
- R2 = M3, M6, M7, M10, M11 => (Alternate 2 Bit including r2 itself).
- R4 = M5, M6, M7 => (Alternate 4 Bit including r4 itself).
- R8 = M9, M10, M11 => (Alternate 8 Bit including r8 itself).
- And so on……..

Hamming Code

- Consider another Example where we send data stream **1000001 [ASCII 'A']**
- Now we will encode the message
- Use modulo - 2 to calculate parity bits

R1 = M3, M5, M7, M9, M11 => 1+0+0+0+1 => 0.
R2 = M3, M6, M7, M10, M11 => 1+0+0+0+1 => 0.
R4 = M5, M6, M7 => 0+0+0 => 0.
R8 = M9, M10, M11 => 0+0+1 => 1.

Data stream to be sent on transmission line from sender

1	0	0	1	0	0	0	0	1	0	0
11	10	9	**8**	7	6	5	**4**	3	**2**	**1**

Hamming Code

- when this stream is received at receiver same process will be followed for decoding if we are getting same values for parity bits as we got at sender side then we say that transmission was error free
- Consider an erroneous stream where 5th bit is flipped.

1	0	0	1	0	0	1	0	1	0	0
11	10	9	**8**	7	6	5	**4**	3	**2**	**1**

Data stream received on transmission line from sender

Now getting corrupted bit position

= (R8, R4, R2, R1)

$= (0, 1, 0, 1)_2$

$= (5)_{10}$

R1 = R1, M3, M5, M7, M9, M11 => 0+1+1+0+0+1 => 1.

R2 = R2, M3, M6, M7, M10, M11 => 0+1+0+0+0+1 => 0.

R4 = R4, M5, M6, M7 => 0+1+0+0 => 1.

R8 = R8, M9, M10, M11 => 1+0+0+1 => 0.

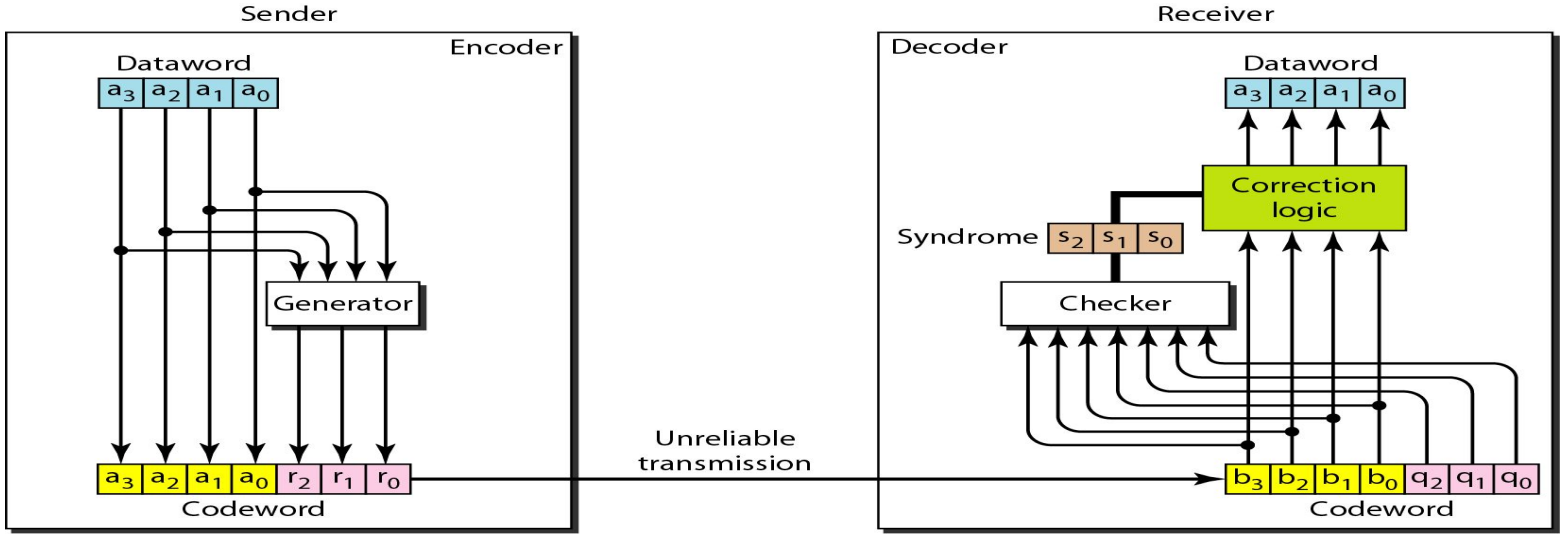
Hamming Code

Table: Hamming code C(7, 4) - n=7, k = 4

Datawords	*Codewords*	*Datawords*	*Codewords*
0000	0000000	1000	1000110
0001	0001101	1001	1001011
0010	0010111	1010	1010001
0011	0011010	1011	1011100
0100	0100011	1100	1100101
0101	0101110	1101	1101000
0110	0110100	1110	1110010
0111	0111001	1111	1111111

Hamming Code

Encoder and decoder for a Hamming code



Hamming Code

Calculating the parity bits at the transmitter:

Modulo 2 arithmetic:

$r_0 = a_2 + a_1 + a_0$

$r_1 = a_3 + a_2 + a_1$

$r_2 = a_1 + a_0 + a_3$

Calculating the syndrome at the receiver:

$s_0 = b_2 + b_1 + b_0$

$s_1 = b_3 + b_2 + b_1$

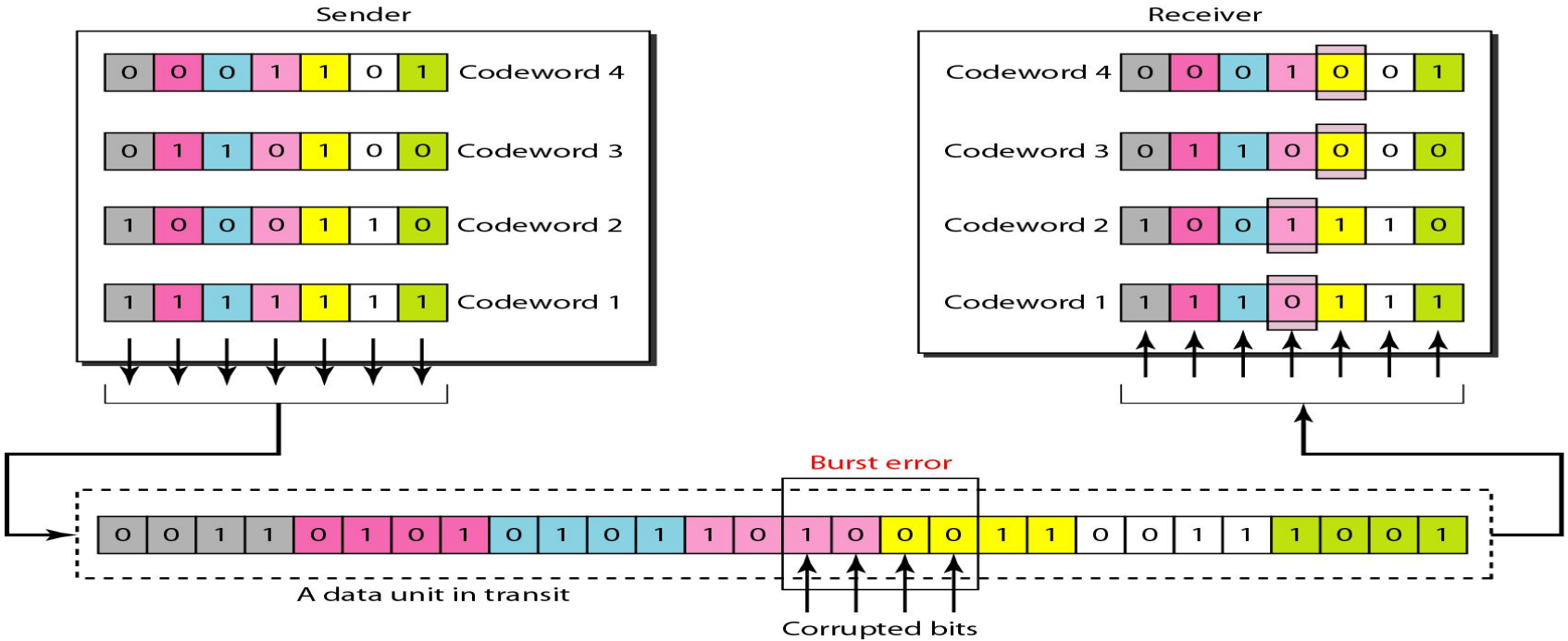
$s_2 = b_1 + b_0 + b_3$

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

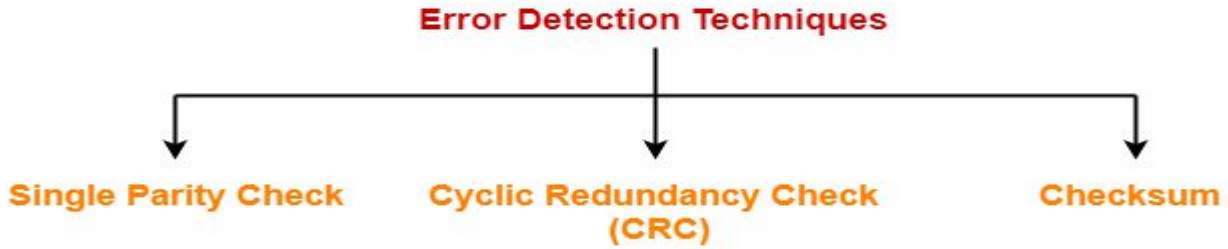
Hamming Code for Detecting Burst Errors

- Burst errors are very common, in particular in wireless environments where a fade will affect a group of bits in transit. The length of the burst is dependent on the duration of the fade.
- One way to counter burst errors, is to break up a transmission into shorter words and create a block (one word per row), then have a parity check per word.
- The words are then sent column by column. When a burst error occurs, it will affect 1 bit in several words as the transmission is read back into the block format and each word is checked individually.

Hamming Code for Burst Errors



Cyclic Redundancy Check (CRC)



- Cyclic Redundancy Check (CRC) is an error detection method.
- It is based on binary division

Cyclic Redundancy Check (CRC)

- Widely used error detection technique is CRC.
- CRC codes are also known as polynomial code since it is possible to view the bit string to be sent as a polynomial whose coefficients are the '0' and '1' values in bit stream.
- A 'k' – bits frame is regarded as the coefficient list for polynomial with 'k' terms ranging from Xk-1 to X0 such polynomial is said to be degree of 'k-1'.
- The high order (left most) bit is the coefficient of Xk-1 the next bit is coefficient of Xk-2 and so on.
- For example 110001 has 6 bits thus represent 6 term polynomial with coefficient 1, 1, 0, 0, 0, and 1 (i.e. 1X5 + 1X4 + 0X3 + 0X2 + 0X1 +1X0).
- Polynomial arithmetic is done in modulo - 2, according to the rules of algebraic field theory.
- It does not have carries in addition and borrows in subtraction.
- Addition and subtraction both are identical to XOR (⊕)

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

CRC

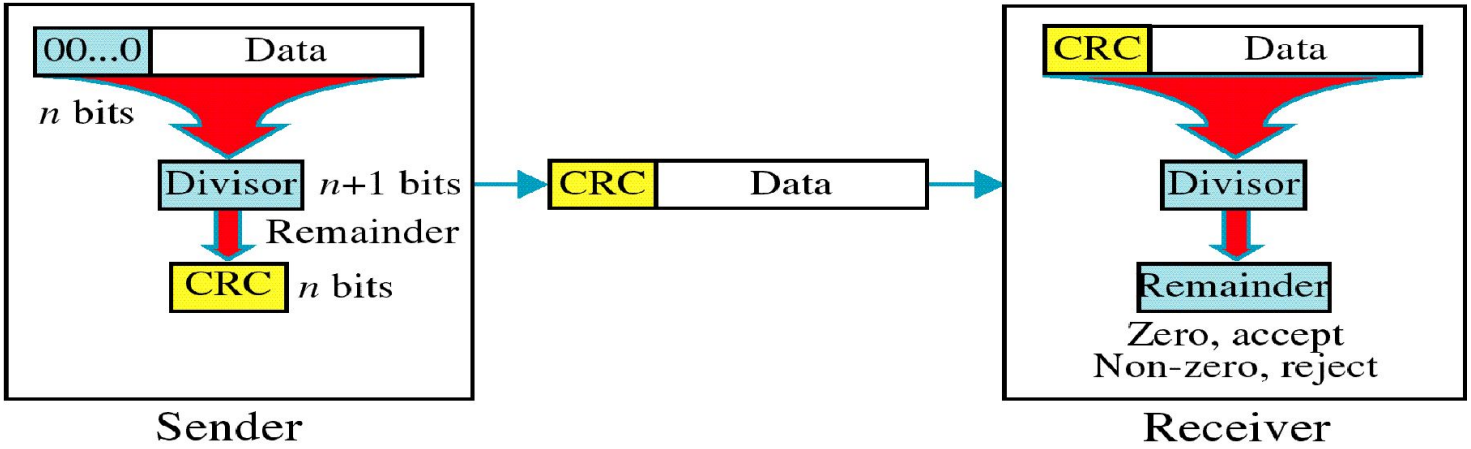
Given a k-bit frame or message, the transmitter generates an n-bit sequence, known as a *frame check sequence (FCS)*,

The resulting frame, consisting of (k+n) bits, is exactly divisible by some predetermined number.

The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

CRC

A cyclic redundancy check (CRC) is **an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data**



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

CRC

How to apply the CRC (step-by-step)

1. Determine the degree r of G(x) and write down G(x) and M(x) as bit sequences.
2. Determine $x^r M(x)$ by appending r zeros (or 'the length of G(x) -1' => same) to M(x).
3. Determine the remainder by dividing $x^r M(x)$ by G(x) from the front until $x^r M(x)$ can't be divided anymore.
   -> If there is a '1' at the front during the processing steps, divide by G(x)
   -> If there is a '0', divide by a bit sequence of zeros with the same length as G(x) (or shift to the first 1 => same)
4. Determine the message to be send (T(x)) by adding the remainder to $x^r M(x)$.

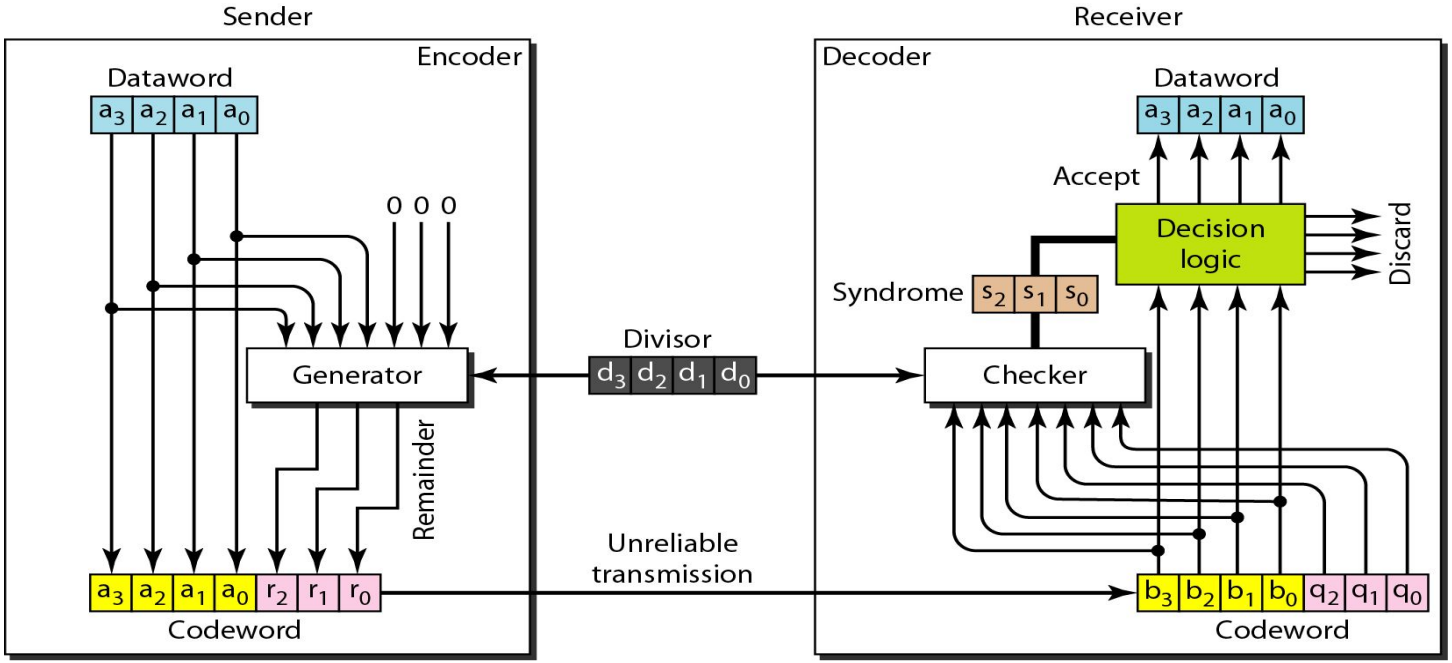
CRC

- 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.

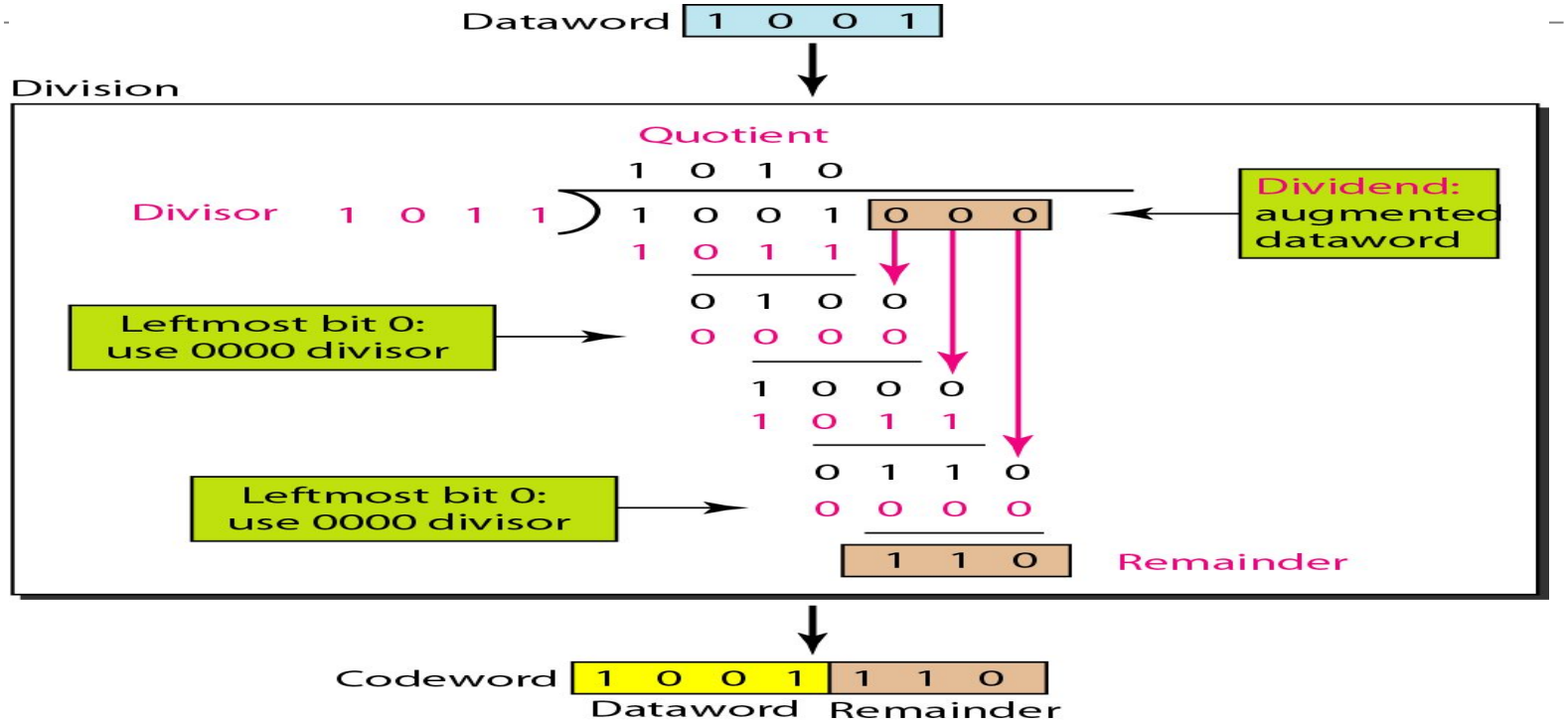
Table: A CRC code with C(7, 4)

Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

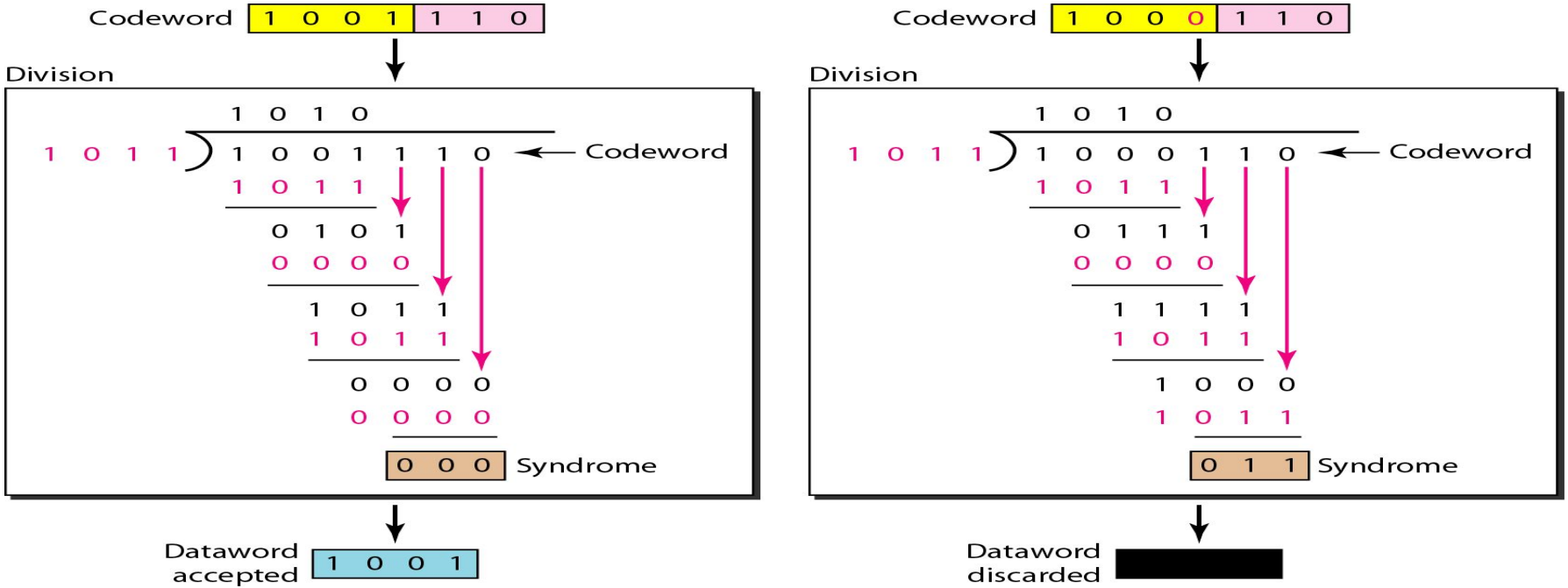
CRC


Sender
Encoder
Dataword
a_3 a_2 a_1 a_0
0 0 0
Generator
Remainder
a_3 a_2 a_1 a_0 r_2 r_1 r_0
Codeword
Divisor
d_3 d_2 d_1 d_0
Unreliable transmission
Receiver
Decoder
Dataword
a_3 a_2 a_1 a_0
Accept
Decision logic
Discard
Syndrome
s_2 s_1 s_0
Checker
b_3 b_2 b_1 b_0 q_2 q_1 q_0
Codeword

Division in CRC Encoder



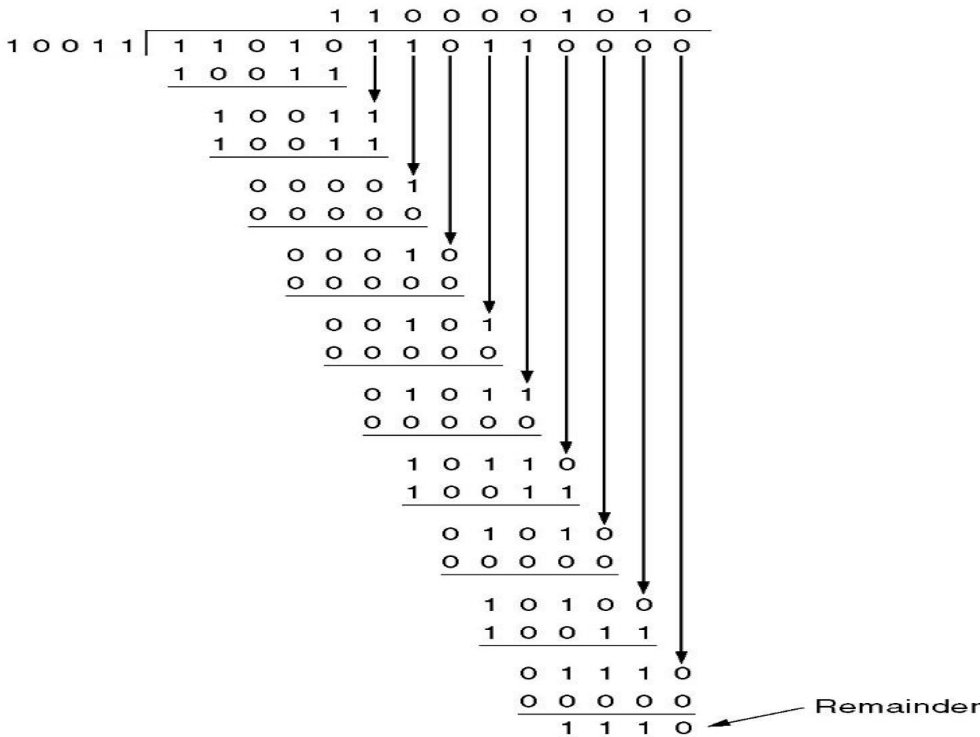
Division in CRC Decoder for two cases



CRC Example

- Solve 1101011011

Frame : 1 1 0 1 0 1 1 0 1 1
Generator: 1 0 0 1 1
Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0

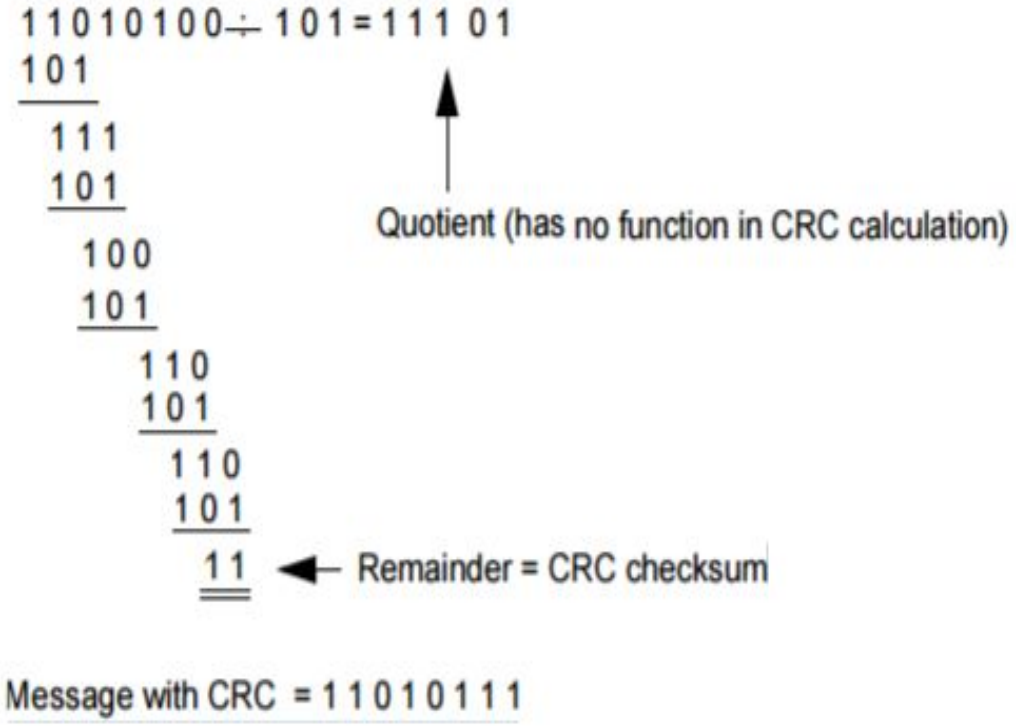


Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0

CRC

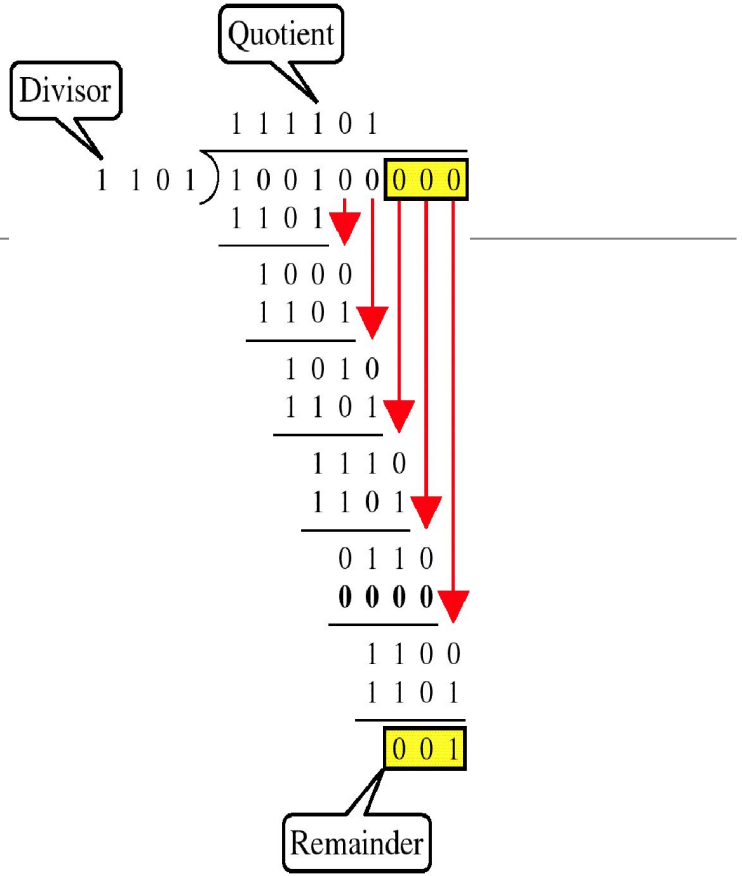
Message = 110101
Polynomial = 101
FIND CRC?

Message = 110101
Polynomial = 101



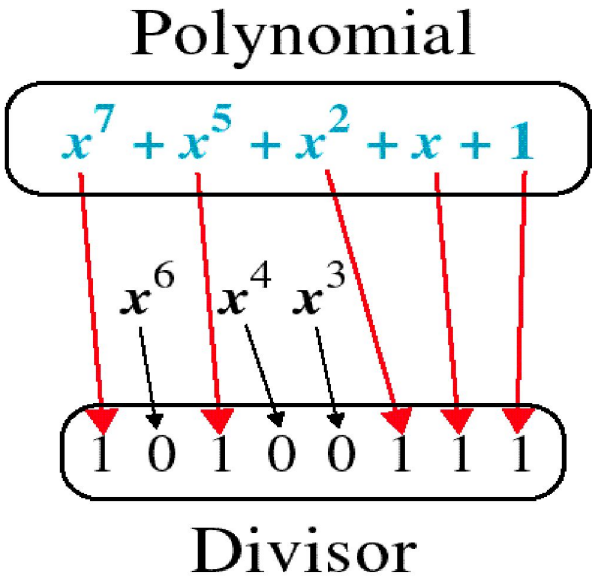
Message with CRC = 1 1 0 1 0 1 1 1

Binary Division



Polynomial

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



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Standard Polynomials

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

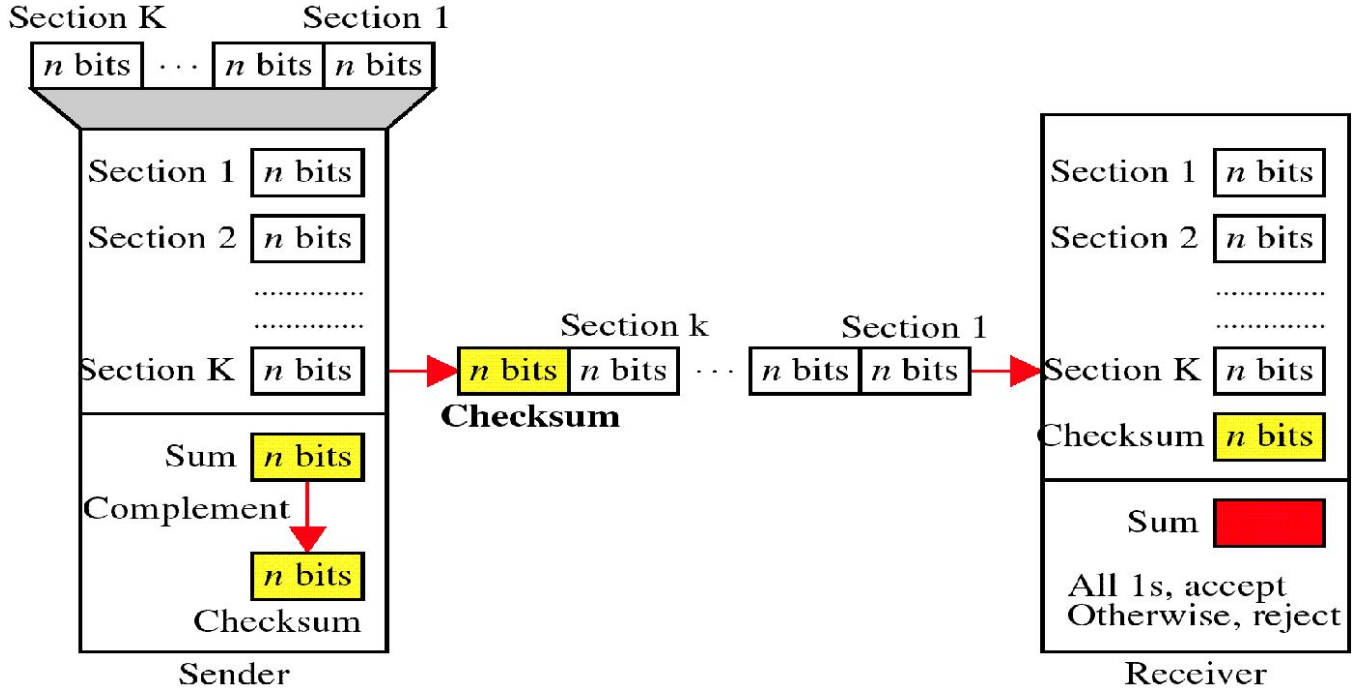
$$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$$

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Checksum

- The checksum is used in the Internet by several protocols although not at the data link layer. However, we briefly discuss it here to complete our discussion on error checking.

Checksum


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

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Checksum Example

- 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

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Checksum Example

- We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum.
- In this case, we send (7, 11, 12, 0, 6, −36). The receiver can add all the numbers received (including the checksum).
- If the result is 0, it assumes no error;
- otherwise, there is an error.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Checksum Example

How can we represent the number 21 in one's complement arithmetic using only four bits?

Solution :

The number 21 in binary is 10101 (it needs five bits). We can wrap the leftmost bit and add it to the four rightmost bits. We have (0101 + 1) = 0110 or 6.

Checksum Example

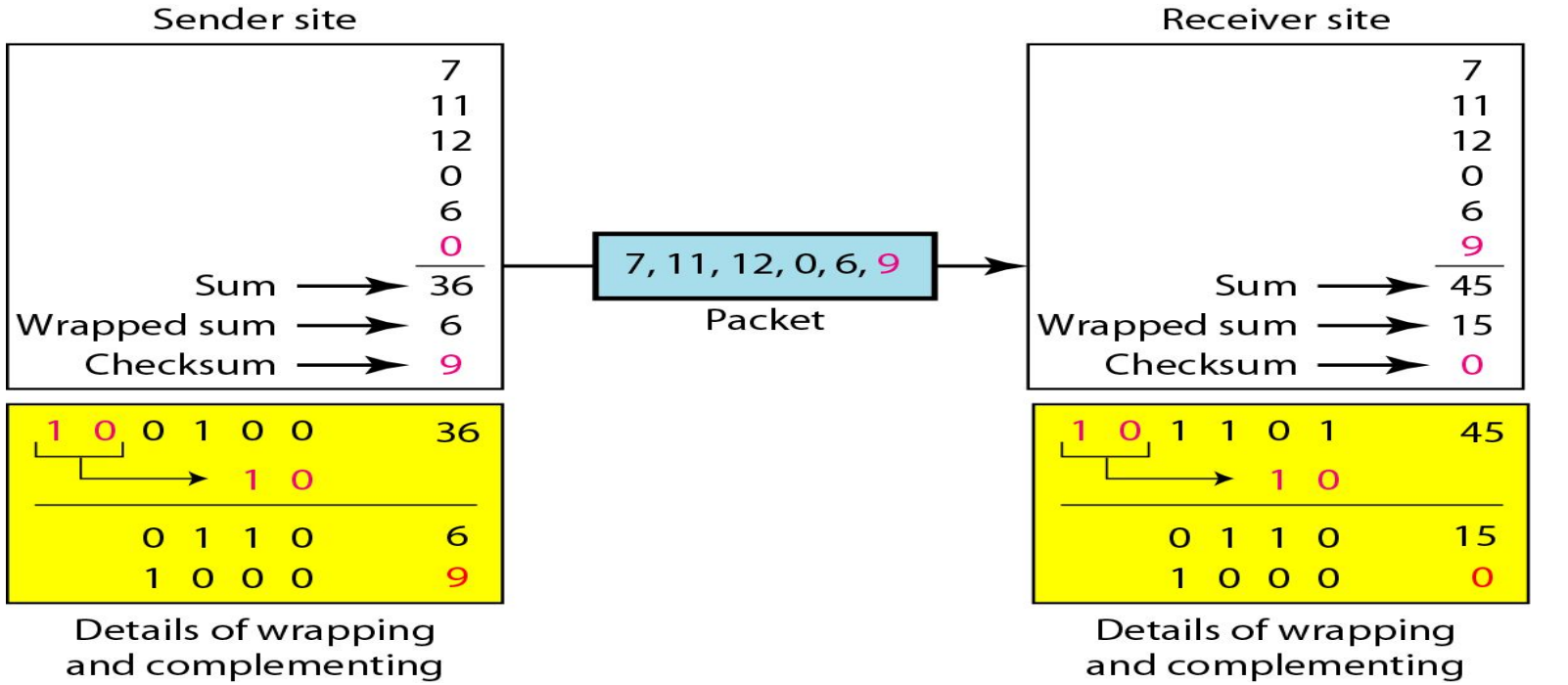
- Let us redo Exercise using one's complement arithmetic. **Figure a.** shows the process at the sender and at the receiver.
- The sender initializes the checksum to 0 and adds all data items and the checksum (the checksum is considered as one data item and is shown in color).
- The result is 36. However, 36 cannot be expressed in 4 bits. The extra two bits are wrapped and added with the sum to create the wrapped sum value 6.
- In the figure, we have shown the details in binary. The sum is then complemented, resulting in the checksum value 9 (15 − 6 = 9). The sender now sends six data items to the receiver including the checksum 9.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Checksum Example

- The receiver follows the same procedure as the sender.
- It adds all data items (including the checksum); the result is 45. The sum is wrapped and becomes 15.
- The wrapped sum is complemented and becomes 0.
- Since the value of the checksum is 0, this means that the data is not corrupted. The receiver drops the checksum and keeps the other data items.
- If the checksum is not zero, the entire packet is dropped.

Checksum Example



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Steps

On Sender Side

- 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

On Receiver Side

- The message (including checksum) 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.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Flow Control and Error control

The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

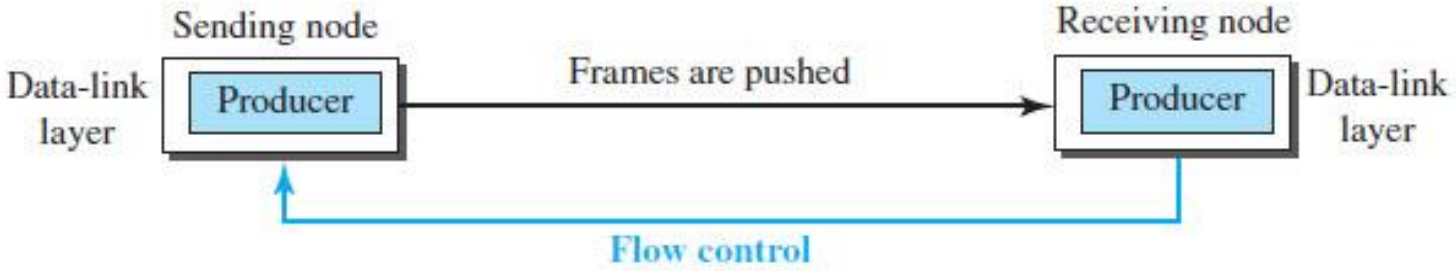
Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

Flow Control

- The sending data-link layer at the end of a link is a producer of frames; the receiving data-link layer at the other end of a link is a consumer.
- If the **rate of produced frames is higher than the rate of consumed frames**, frames at the receiving end **need to be buffered** while waiting to be consumed (processed).
- As an unlimited buffer size at the receiving side is not possible, any one of the following steps are followed
  - **receiving data-link layer drop the frames if its buffer is full**.
  - **to let the receiving data-link layer send a feedback to the sending data-link layer to ask it to stop or slow down**.
- Different data-link-layer protocols use different strategies for flow control

Flow Control



- data-link layer at the sending node tries to push frames toward the data-link layer at the receiving node.
- **If the receiving node cannot process and deliver the packet to its network at the same rate that the frames arrive, it becomes overwhelmed with frames.**
- Flow control in this case can be feedback from the receiving node to the sending node to stop or slow down pushing frames.

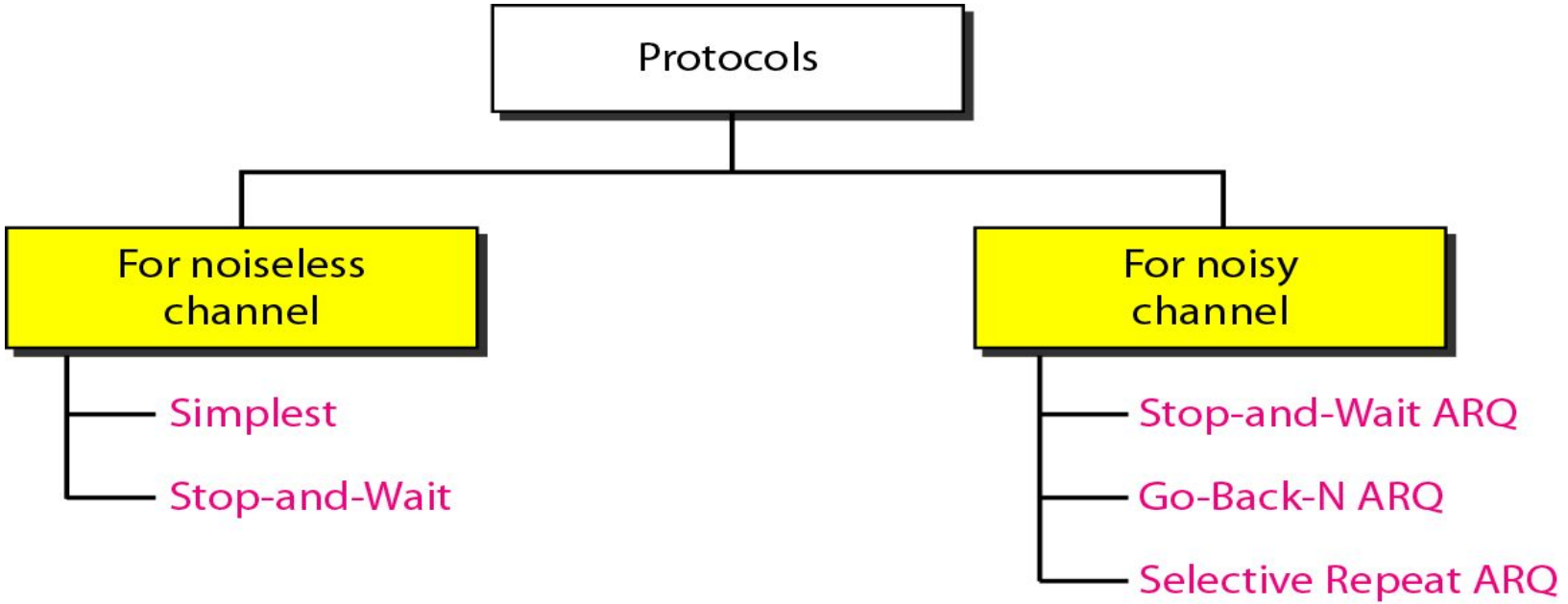
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Flow Control

- **Flow and error control can be combined**. In a simple situation, the acknowledgment that is sent for flow control can also be used for error control to tell the sender the packet has arrived uncorrupted.
- The lack of acknowledgment means that there is a problem in the sent frame.
- A frame that carries an acknowledgment is normally called an ACK to distinguish it from the data frame.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Taxonomy of protocols



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

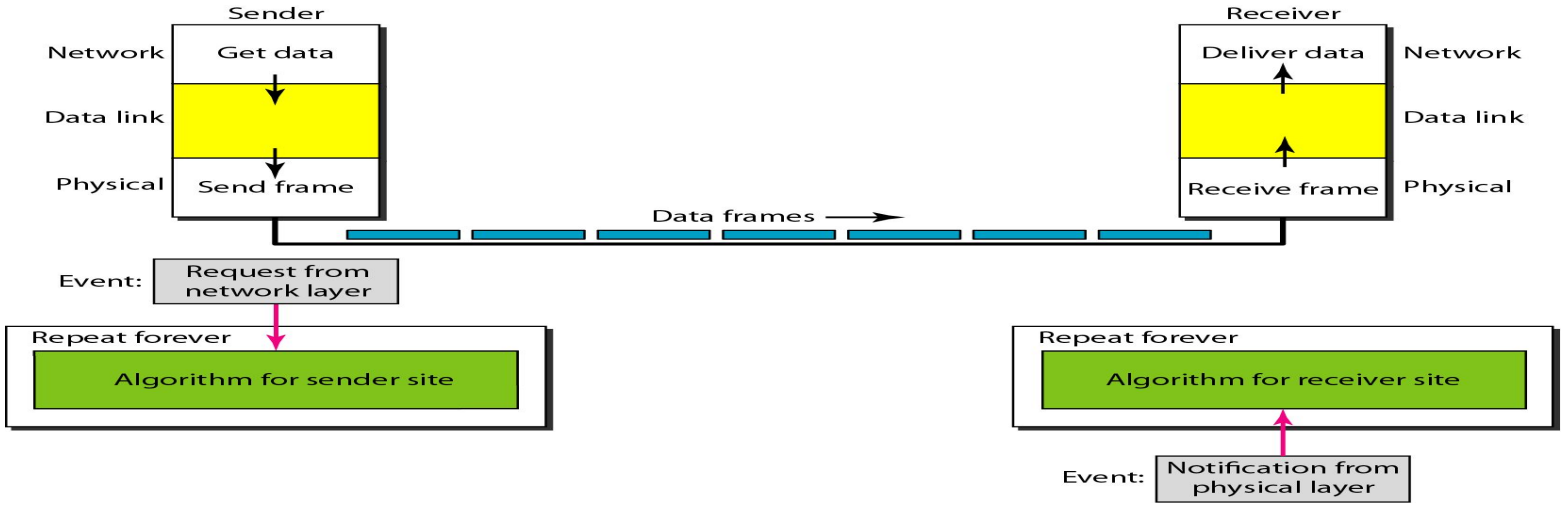
Noiseless Channels

Two protocols are used for ideal cases having noiseless channels

- **Simplest Protocol**
- **Stop-and-Wait Protocol**

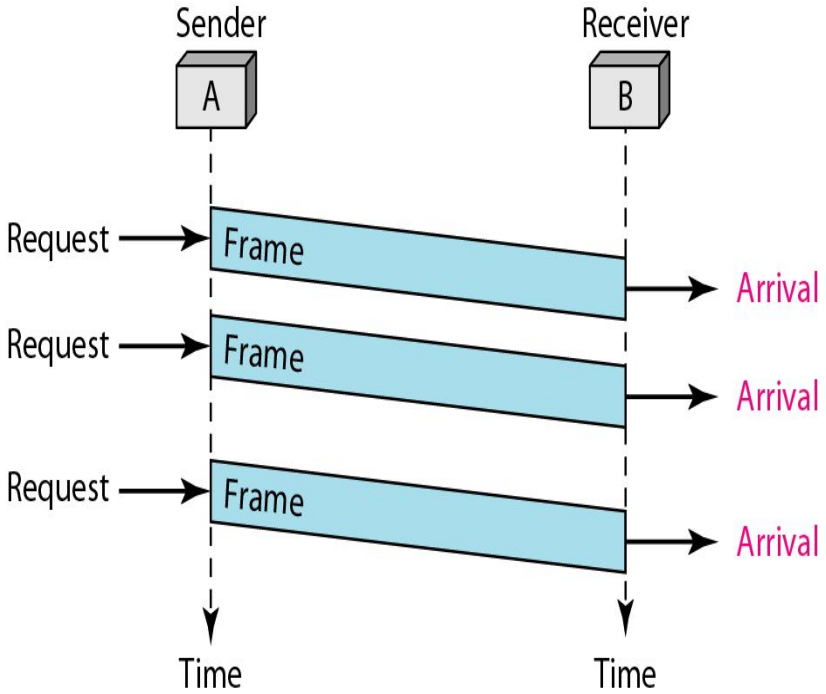
Simple Protocol

Let us first assume we have an ideal channel in which no frames are lost, duplicated, or corrupted. We introduce two protocols for this type of channel.



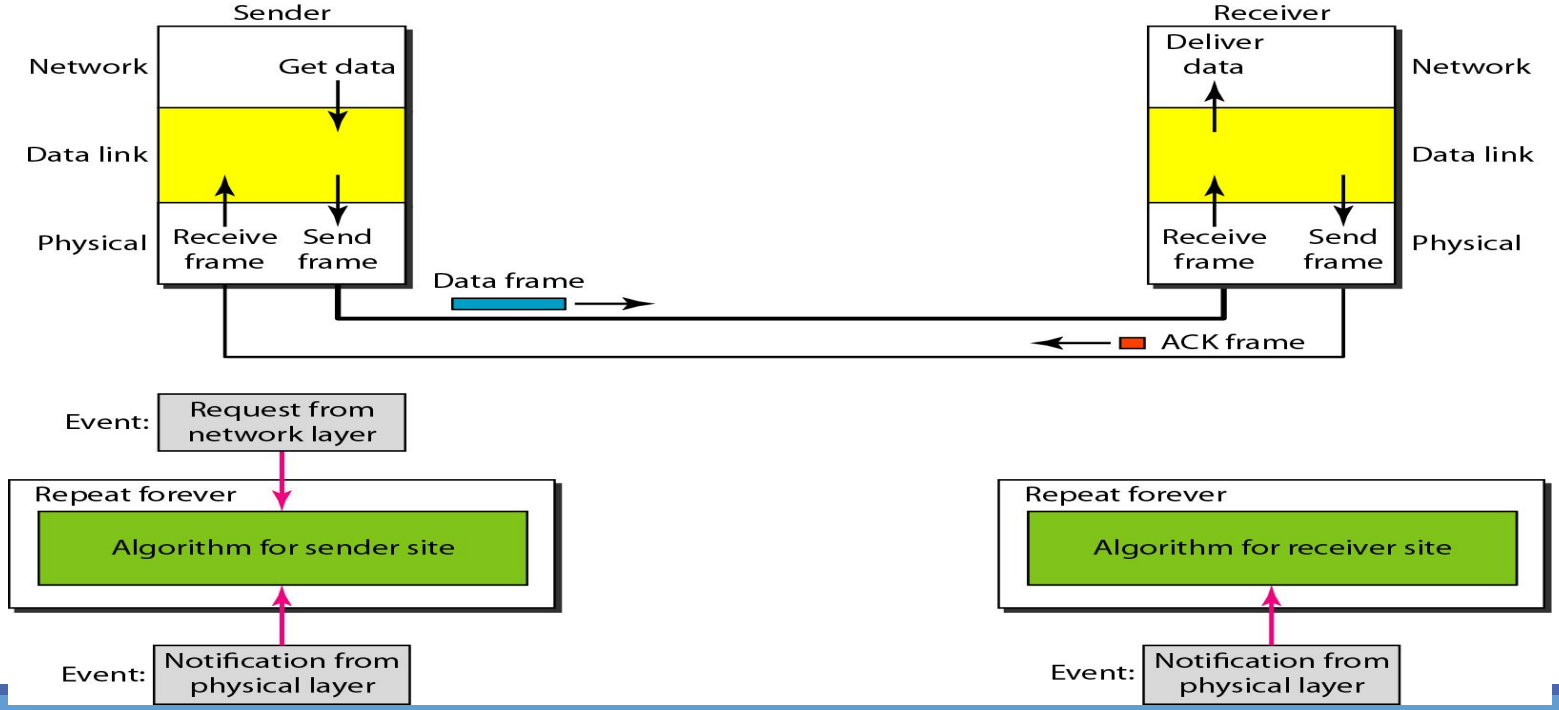
Simple Protocol

- The sender sends a sequence of frames without even thinking about the receiver.
- To send three frames, three events occur at the sender side and three events at the receiver side.
- The data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.



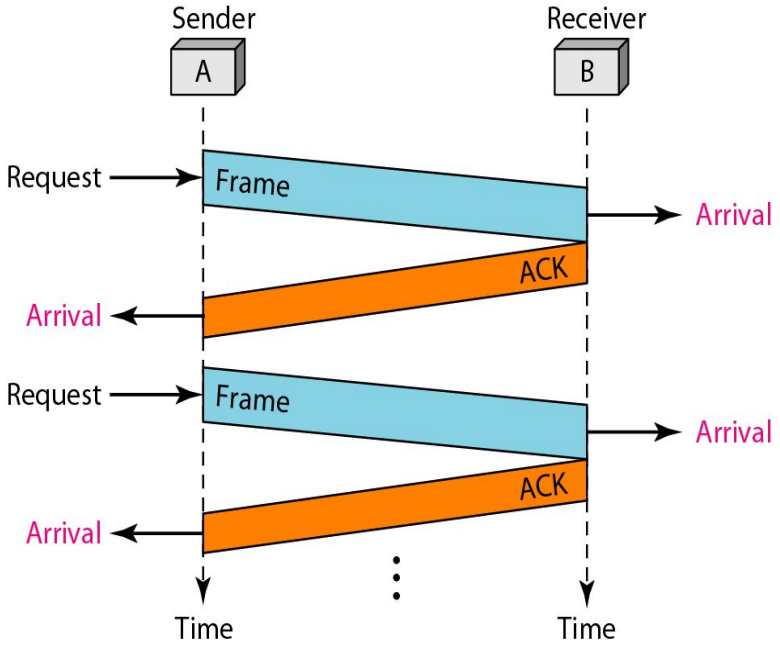
Stop & Wait Protocol

- In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one.



Stop & Wait Protocol

- The sender sends one frame and waits for feedback from the receiver.
- When the ACK arrives, the sender sends the next frame.
- Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.



Noisy Channel

Noiseless channels are nonexistent.

For noisy channels, following protocols are used for flow and error control

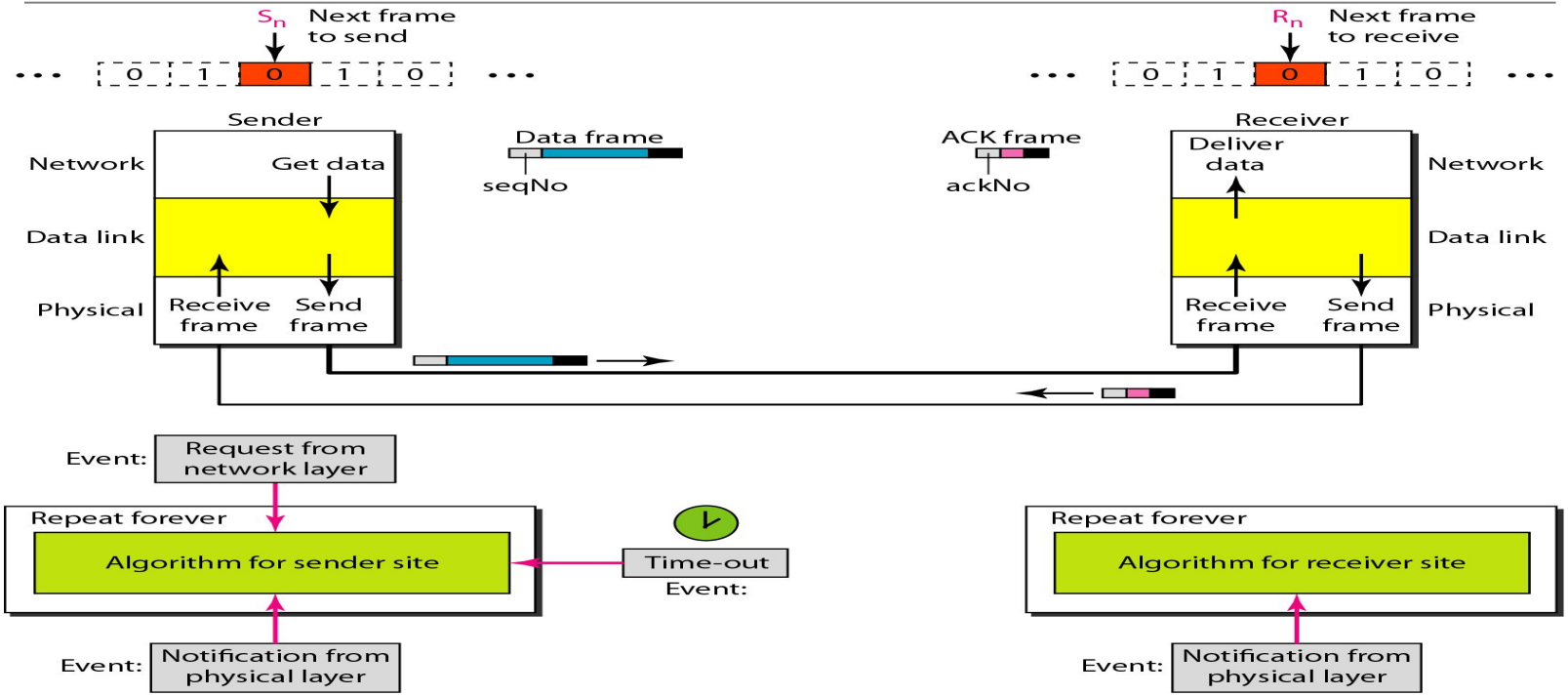
- **Stop-and-Wait Automatic Repeat Request**
- **Go-Back-N Automatic Repeat Request**
- **Selective Repeat Automatic Repeat Request**

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

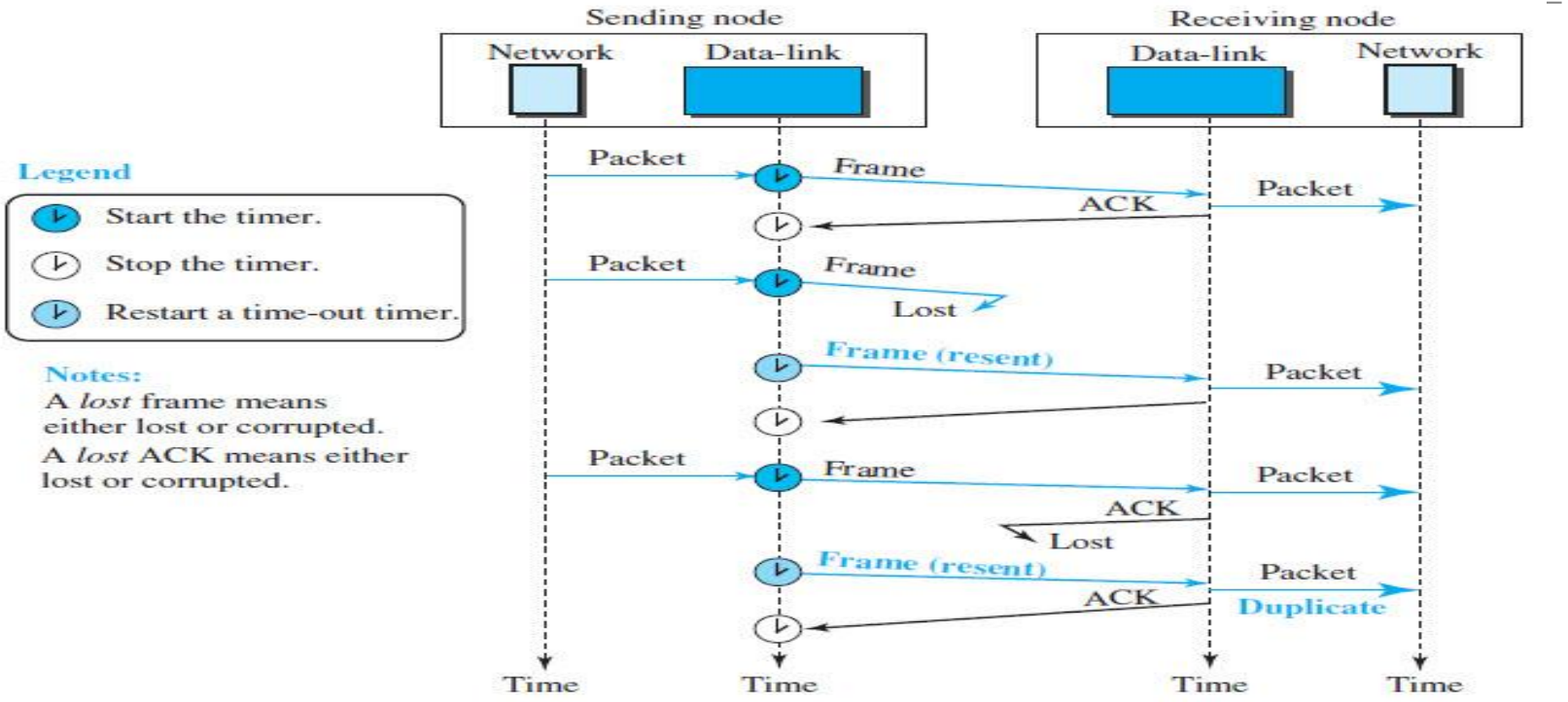
Stop-and-Wait Automatic Repeat Request

- **To detect corrupted frames, we need to add a CRC to each data frame**. When a frame arrives at the receiver site, it is checked. If its CRC is incorrect, the frame is corrupted and silently discarded.
- **Every time the sender sends a frame, it starts a timer**. If an acknowledgment arrives before the timer expires, the timer is stopped and the sender sends the next frame (if it has one to send).
- If the timer expires, the sender resends the previous frame, assuming that the frame was either lost or corrupted.
- Sender needs to keep a copy of the frame until its acknowledgment arrives. When the corresponding acknowledgment arrives, the sender discards the copy and sends the next frame if it is ready.
- Note that only one frame and one acknowledgment can be in the channels at any time.

Stop-and-Wait Automatic Repeat Request



Stop-and-Wait [without sequence number]

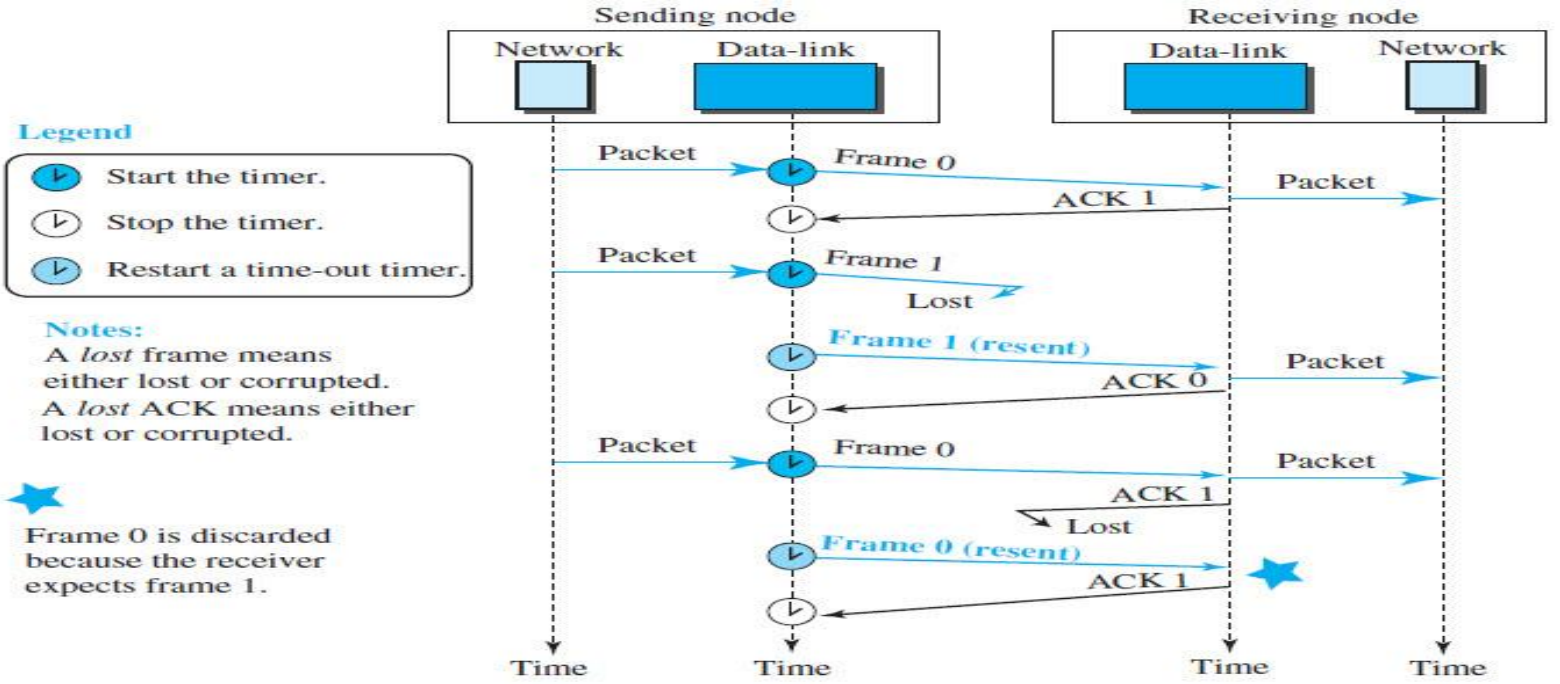


MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Stop-and-Wait [without sequence number]

- **Duplicate packets, as much as corrupted packets, need to be avoided**.
- To correct the problem, we need to add **sequence numbers** to the data frames and **acknowledgment numbers** to the ACK frames.
- A 1-bit sequence number/acknowledgement number (0 or 1) is therefore sufficient.

Stop-and-Wait [with sequence number]



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Stop-and-Wait Automatic Repeat Request

- Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.
- In Stop-and-Wait ARQ, we use sequence numbers to number the frames. The sequence numbers are based on modulo-2 arithmetic.
- In Stop-and-Wait ARQ, the acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.

✓ **Aim of stop & wait protocol is to turn unreliable data link into reliable one**

✓ **Therefore Stop & Wait protocol is suitable for large sizes of packets.**

✓ **Similarly Stop & Wait protocol is suitable for small size networks(i.e. LAN)**

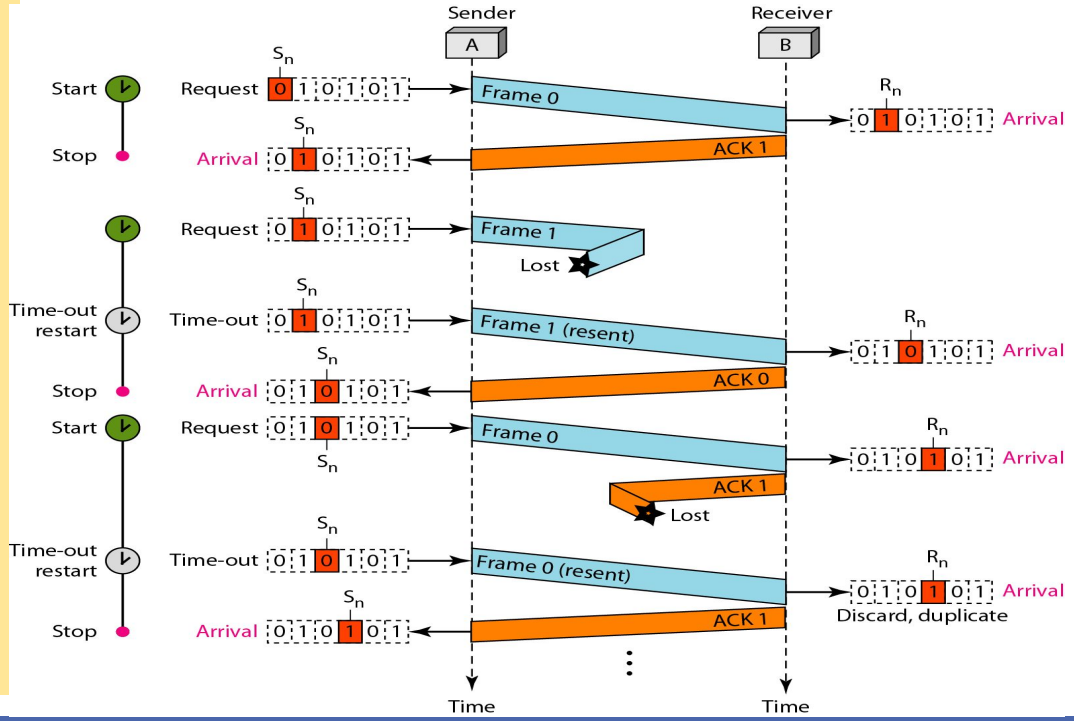
Stop-and-Wait Automatic Repeat Request: Example

Frame 0 is sent and acknowledged. Frame 1 is lost and resent after the time-out.

The resent frame 1 is acknowledged and the timer stops.

Frame 0 is sent and acknowledged, but the acknowledgment is lost.

The sender has no idea if the frame or the acknowledgment is lost, so after the time-out, it resends frame 0, which is acknowledged.



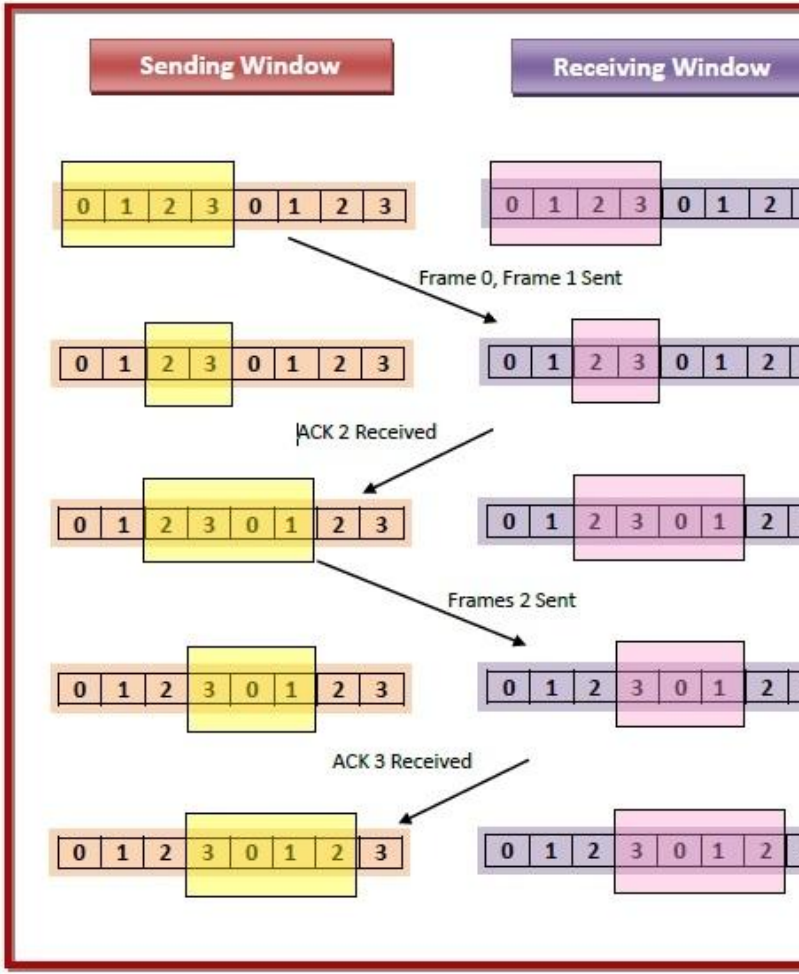
MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Sliding Window Protocol

- The sliding window is a technique for sending multiple frames at a time.
- It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed
- In this technique, each frame has sent from the sequence number.
- The sequence numbers are used to find the missing data in the receiver end.
- The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Sliding Window Protocol

- Suppose that we have sender window and receiver window each of size 4.
- So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on.
- The diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Types of Sliding Window Protocol

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Go-Back-N ARQ

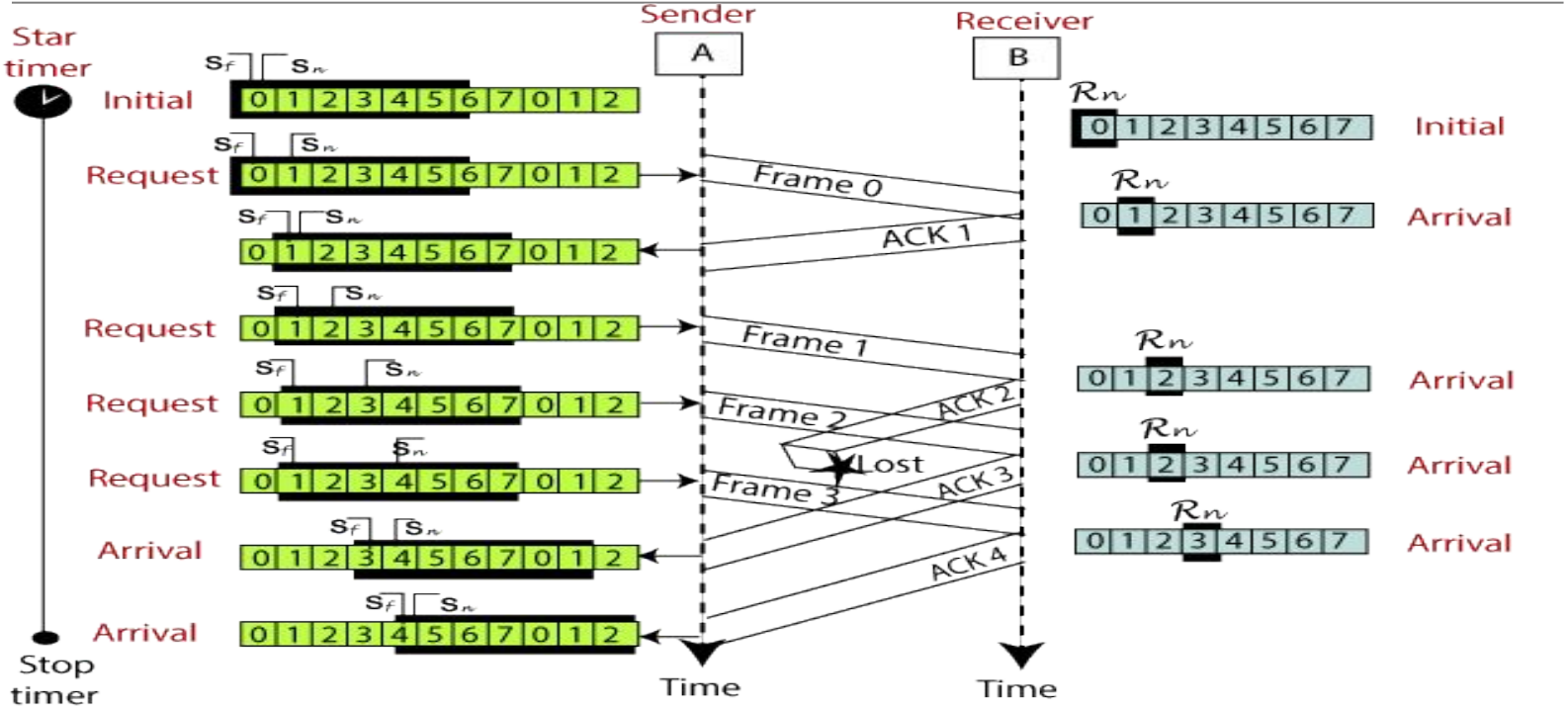
- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The frames are sequentially numbered and a finite number of frames are sent.
- If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Go-Back-N ARQ

- In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
- The size of the sending window determines the sequence number of the outbound frames.
- If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1.
- Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.
- The sequence numbers are numbered as modulo-n.
- For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.
- The size of the receiving window is the maximum number of frames that the receiver can accept at a time.
- It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Go-Back-N ARQ

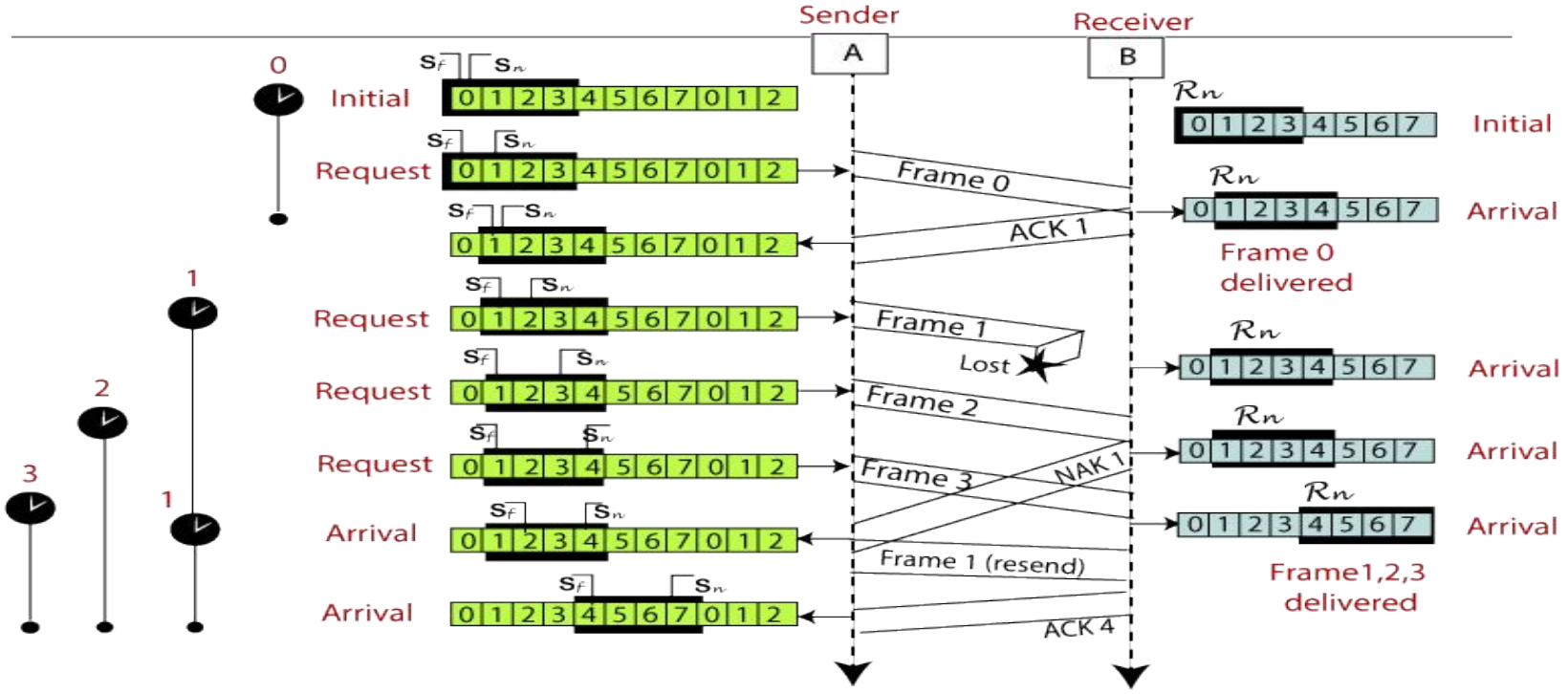

Sender
Receiver
A
B
Star timer
Initial
Request
Request
Request
Request
Arrival
Arrival
Stop timer
Frame 0
ACK 1
Frame 1
Frame 2
ACK 2
Lost
Frame 3
ACK 3
ACK 4
Initial
Arrival
Arrival
Arrival
Arrival
Time
Time

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Selective Repeat ARQ

- The Go-back-N ARQ protocol works well if it has fewer errors.
- But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again.
- In the Selective Repeat ARQ protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.
- If the receiver receives a corrupt frame, it does not directly discard it.
- It sends a negative acknowledgment to the sender.
- The sender sends that frame again as soon as on the receiving negative acknowledgment.
- There is no waiting for any time-out to send that frame.

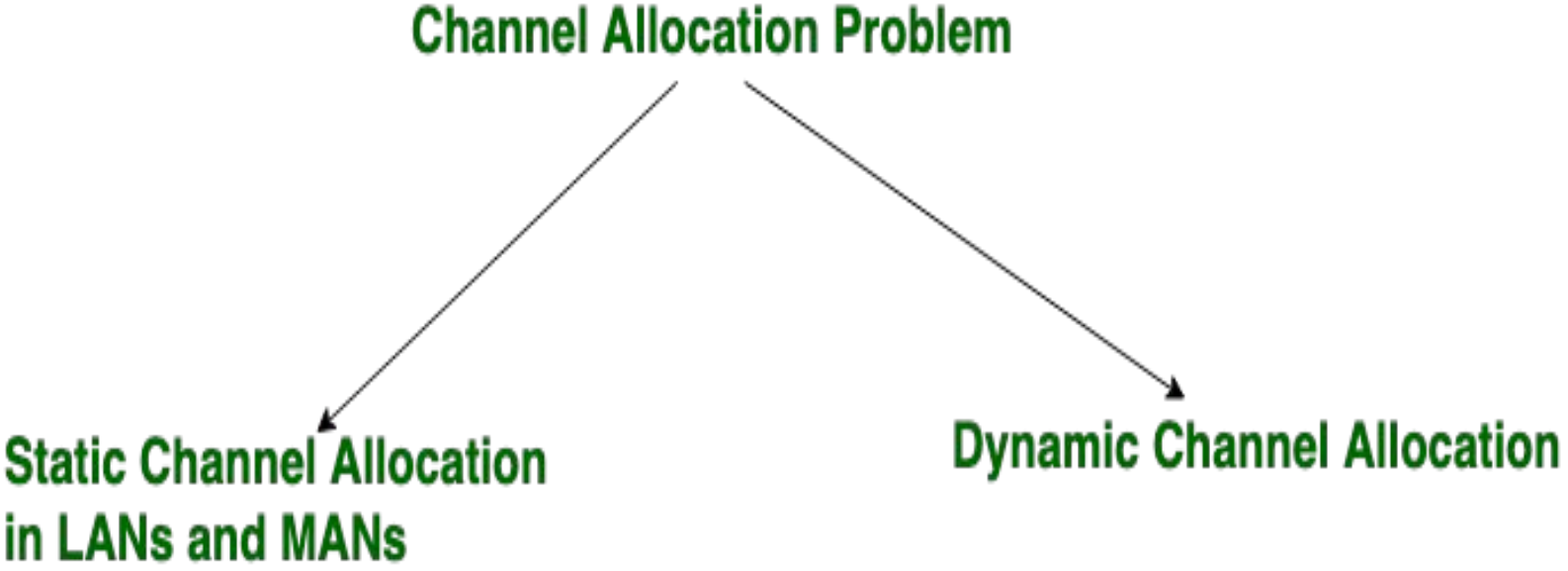
Selective Repeat ARQ



Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Channel Allocation



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel.
- However, it is not suitable in case of a large number of users with variable bandwidth requirements

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Dynamic Channel Allocation

- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users.
- Instead channels are allotted to users dynamically as needed, from a central pool.
- The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimizes bandwidth usage and results is faster transmissions.
- Dynamic channel allocation is further divided into centralized and distributed allocation.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Dynamic Channel Allocation Assumptions

Station Model:
Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.

Single Channel Assumption:
In this allocation all stations are equivalent and can send and receive on that channel.

Collision Assumption:
If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re transmitted. Collisions are only possible error.

Time can be divided into Slotted or Continuous.

Stations can sense a channel is busy before they try it.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

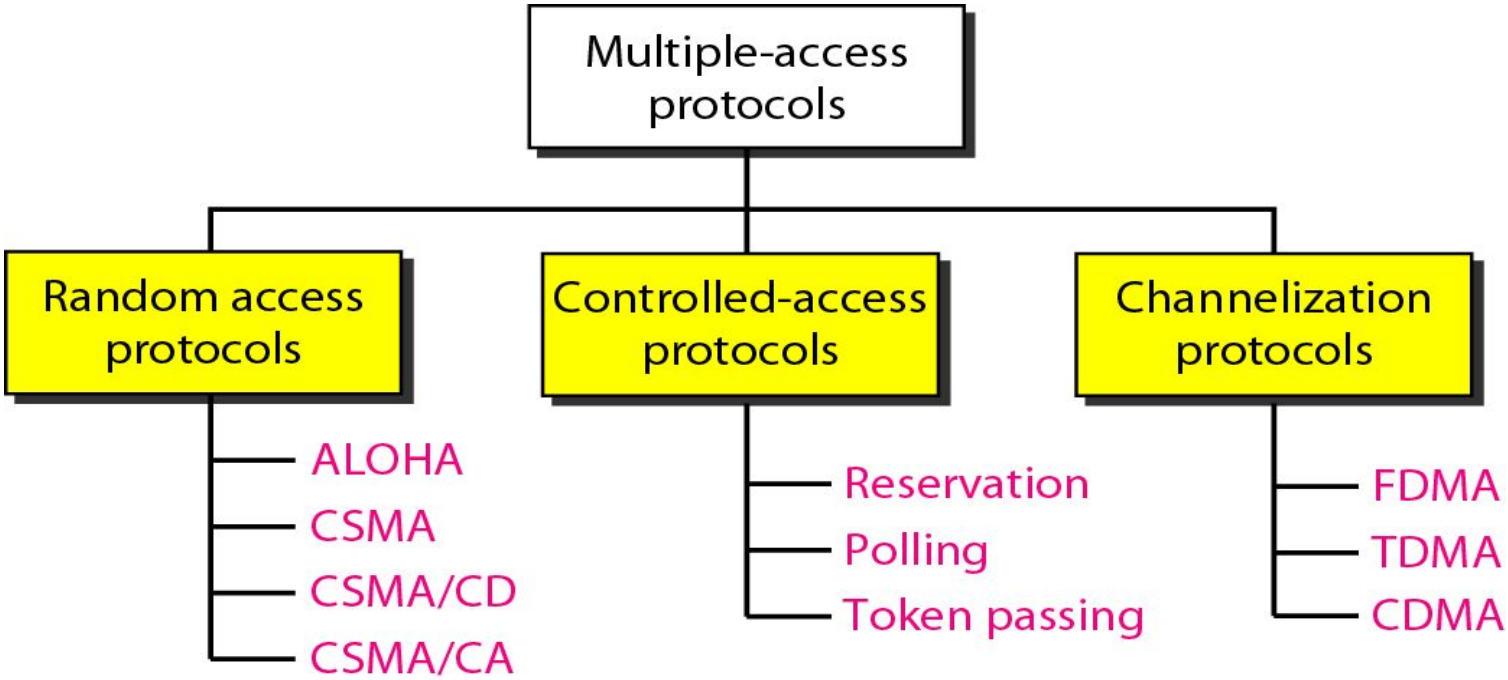
Multiple Access Protocol

- The data link layer is used in a computer network to transmit the data between two devices or nodes.
- It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**.
- The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**.
- Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel.
- Hence it is termed as **media access control** or the multiple access resolutions.

Multiple Access Protocol

- A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.
- When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel.
- Suppose there is no dedicated path to communicate or transfer the data between two devices, then multiple stations access the channel and simultaneously transmit the data over the channel.
- It may create collision and cross talk.
- Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

Multiple Access Protocols



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Random Access Protocol

- 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.
- Protocols
  - ALOHA (Pure and Slotted ALOHA)
  - CSMA
  - CSMA/CD
  - CSMA/CA

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

ALOHA

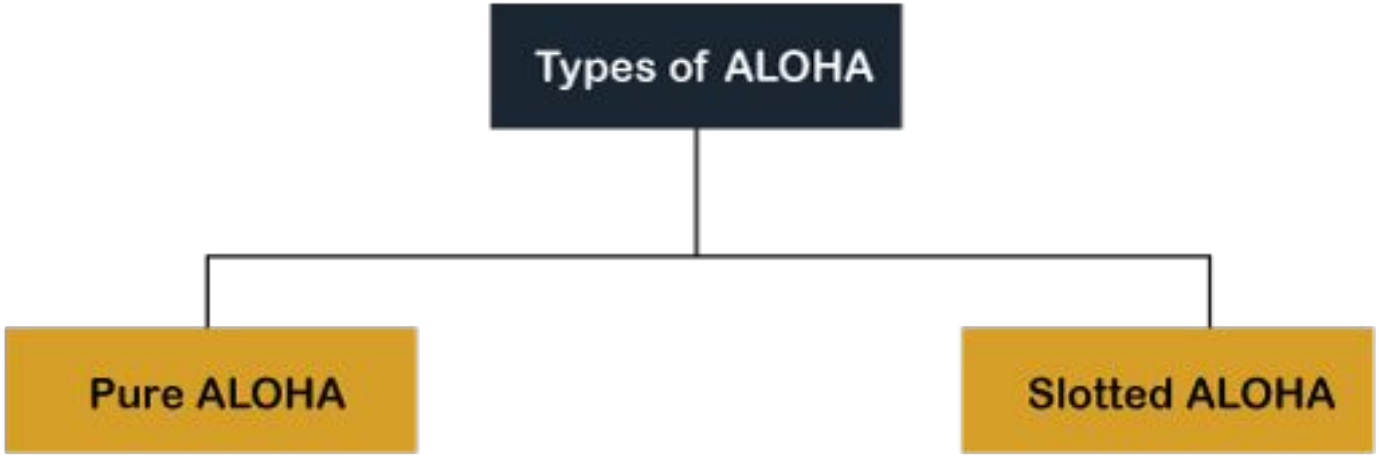
It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data.
Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

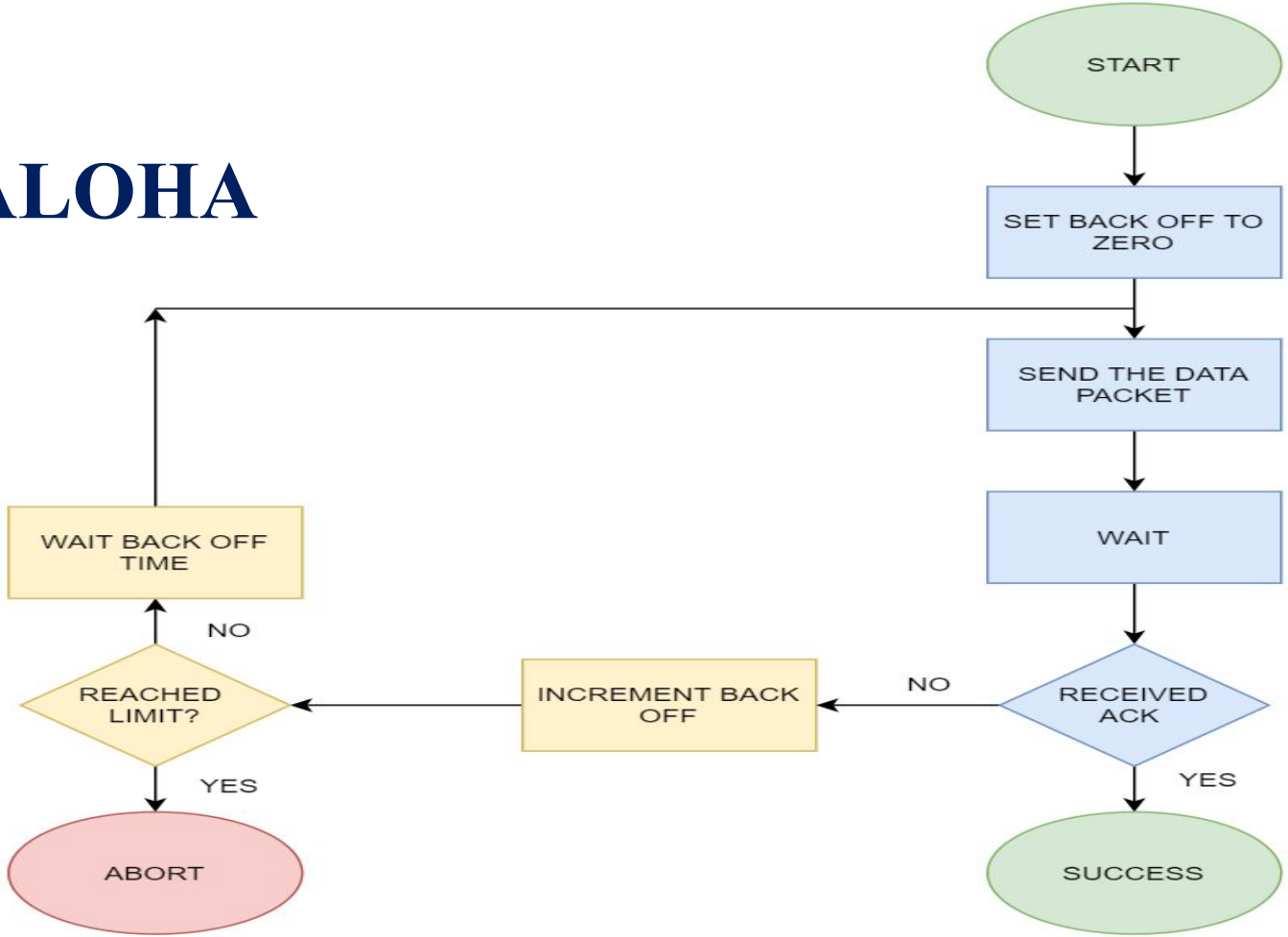
ALOHA



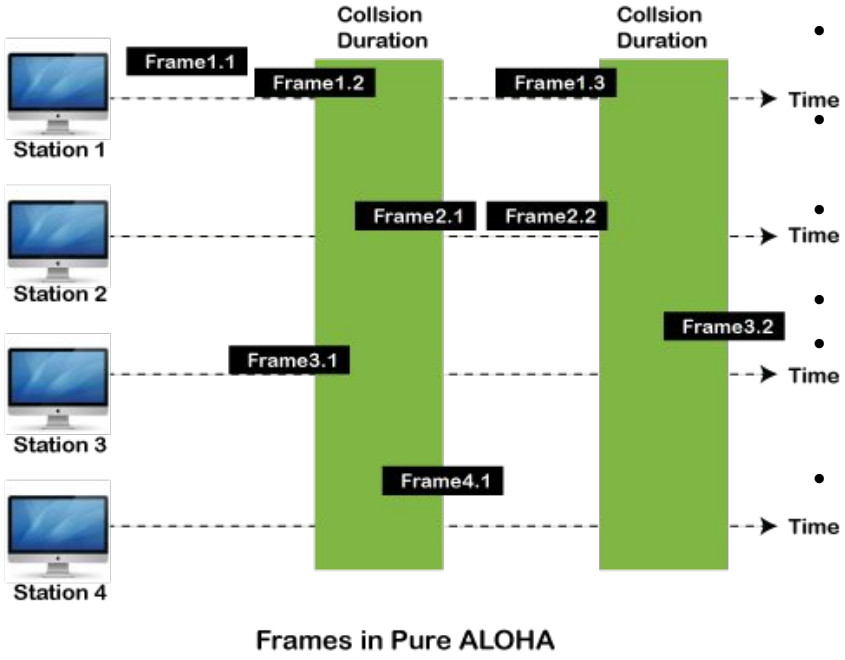
Pure ALOHA

- Whenever data is available for sending over a channel at stations, we use Pure Aloha.
- In pure Aloha each station transmits data to a channel without checking whether the channel is idle or not
- the chances of collision may occur, and the data frame can be lost.
- When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment.
- If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb).
- And the station may assume the frame has been lost or destroyed.
- Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

Pure ALOHA


START
SET BACK OFF TO ZERO
SEND THE DATA PACKET
WAIT
RECEIVED ACK
NO
INCREMENT BACK OFF
REACHED LIMIT?
NO
WAIT BACK OFF TIME
YES
ABORT
YES
SUCCESS

Pure ALOHA



Frames in Pure ALOHA

- There are four stations for accessing a shared channel and transmitting data frames.
- Some frames collide because most stations send their frames at the same time.
- Only two frames, frame 1.1 is successfully transmitted to the receiver end.
- At the same time, other frames are lost or destroyed.
- Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage.
- If the new frame's first bit enters the channel before finishing the last bit of the second frame.

Pure ALOHA

Efficiency-

Efficiency of Pure Aloha (η) = $G \times e^{-2G}$

where G = Number of stations willing to transmit data

Maximum Efficiency-

For maximum efficiency,

- We put $d\eta / dG = 0$
- Maximum value of η occurs at G = 1/2
- Substituting G = 1/2 in the above expression, we get-

Maximum efficiency of Pure Aloha

$= 1/2 \times e^{-2 \times 1/2}$

$= 1 / 2e$

$= 0.184$

$= 18.4\%$

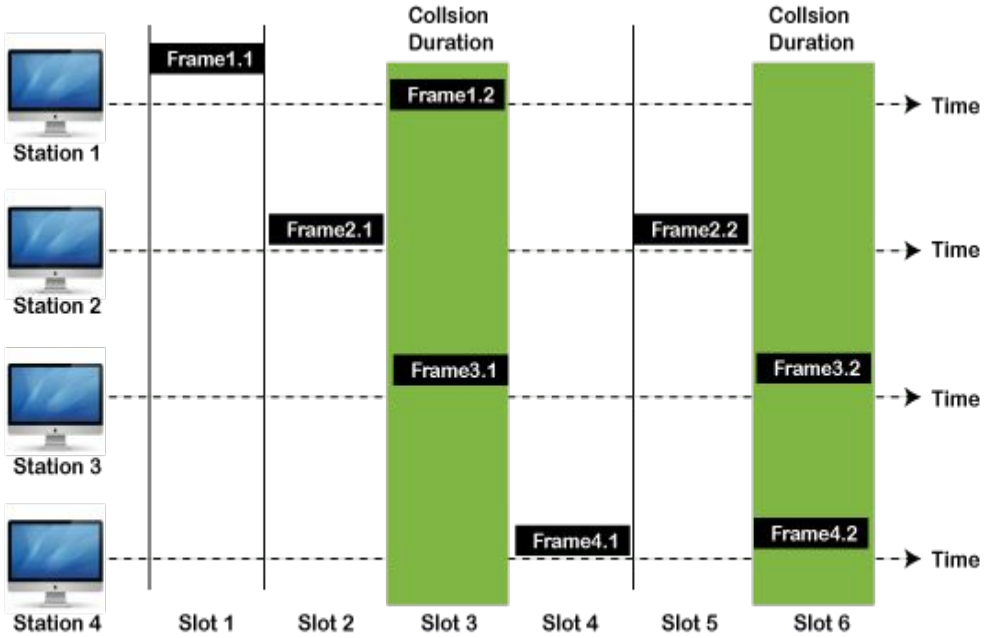
1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Slotted ALOHA

- The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting.
- In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**.
- if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot.
- if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time.
- However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

Slotted ALOHA



Frames in Slotted ALOHA

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.

Slotted ALOHA

Efficiency-

Efficiency of Slotted Aloha (η) = $G \times e^{-G}$

where G = Number of stations willing to transmit data at the beginning of the same time slot

Maximum Efficiency-

For maximum efficiency,

We put $d\eta / dG = 0$

Maximum value of η occurs at G = 1

Substituting G = 1 in the above expression, we get-

Maximum efficiency of Slotted Aloha

$= 1 \times e^{-1}$

$= 1 / e$

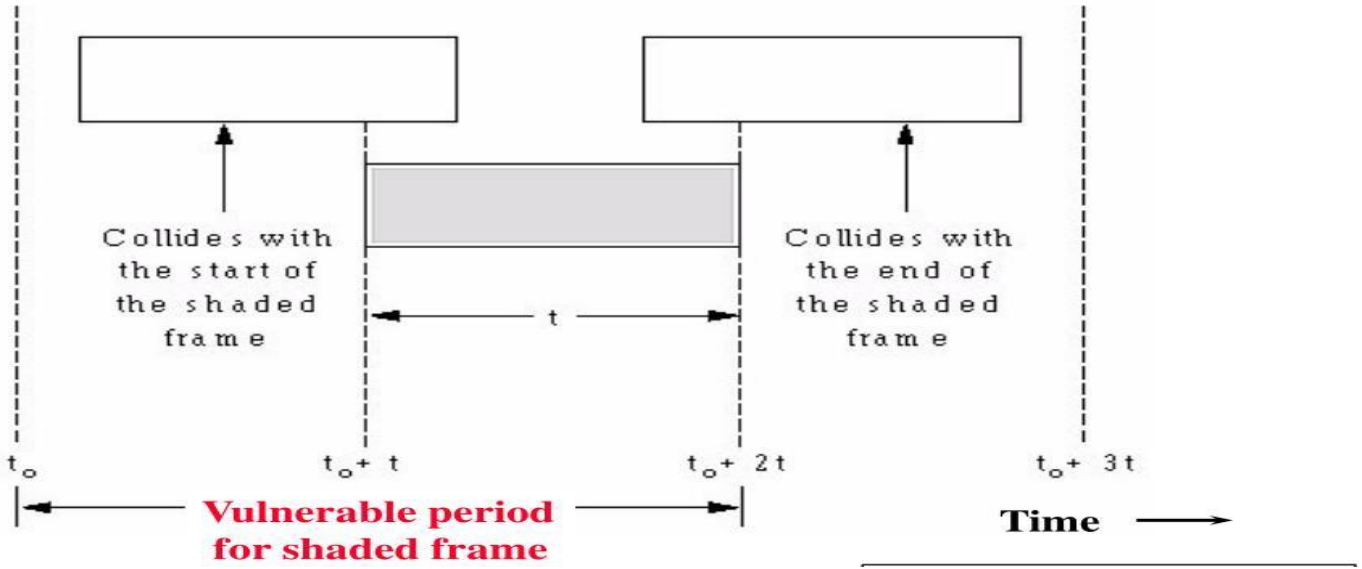
$= 0.368$

$= 36.8\%$

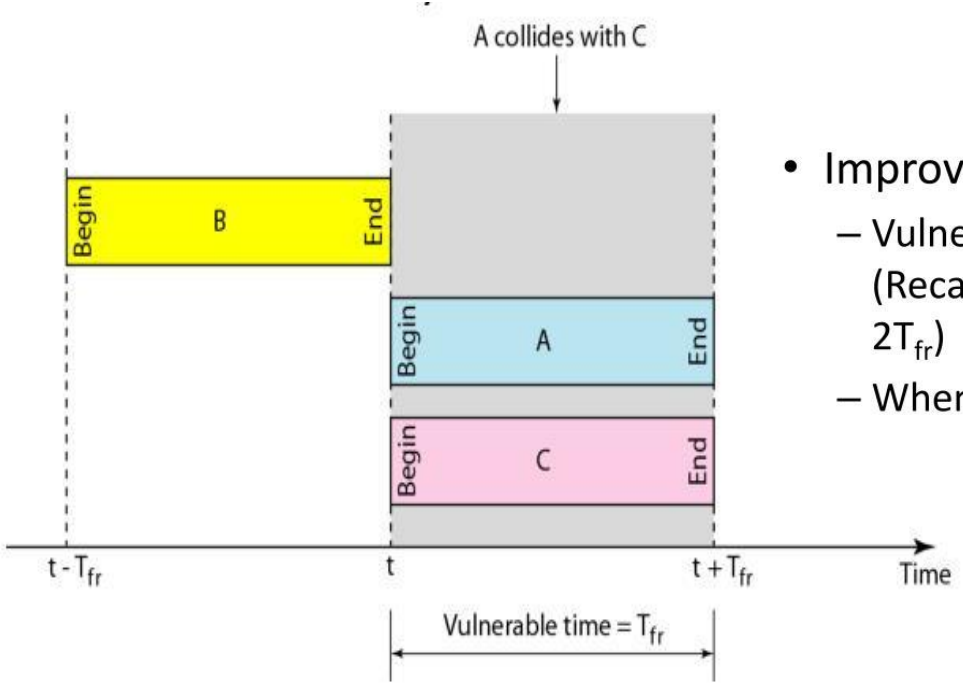
Vulnerable period for Pure ALOHA

For successful frame transmission:

No other frame should be on the channel for vulnerable period equal to twice the time to transmit one frame = $2t$



Vulnerable period for Slotted ALOHA



- Improves the efficiency
  - Vulnerable time is T_{fr} (Recall that pure ALOHA has vulnerable time of $2T_{fr}$)
  - When a data arrives, it waits until the next slot

Pure Aloha	Slotted Aloha
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur $= 2 \times T_t$	Vulnerable time in which collision may occur $= T_t$
Probability of successful transmission of data packet $= G \times e^{-2G}$	Probability of successful transmission of data packet $= G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)
The main advantage of pure aloha is its simplicity in implementation.	The main advantage of slotted aloha is that it reduces the number of collisions to half and doubles the efficiency of pure aloha.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Answer the following question

A group of N stations share 100 Kbps slotted ALOHA channel. Each station output a 500 bits frame on an average of 5000 ms even if previous one has not been sent. What is the required value of N?

Answer

Throughput Of One Station-

Throughput of each station
= Number of bits sent per second
= 500 bits / 5000 ms
= 500 bits / (5000 x 10^{-3} sec)
= 100 bits/sec

Throughput Of Slotted Aloha-

Throughput of slotted aloha
= Efficiency x Bandwidth
= 0.368 x 100 Kbps
= 36.8 Kbps

Total Number Of Stations-

Throughput of slotted aloha = Total number of stations x Throughput of each station
Substituting the values, we get-
36.8 Kbps = N x 100 bits/sec
$\therefore$ N = 368

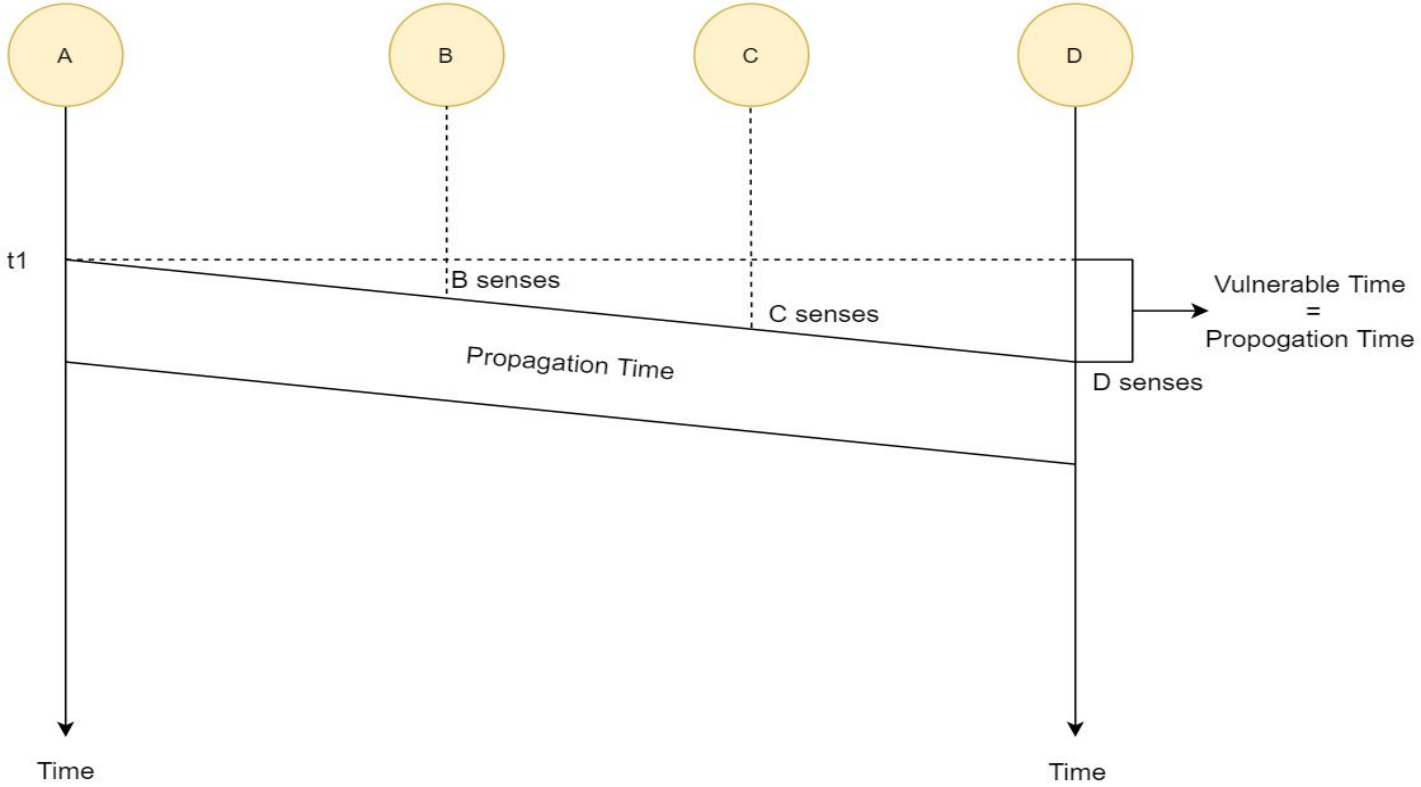
Thus, required value of N = 368.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Carrier Sense MA protocols

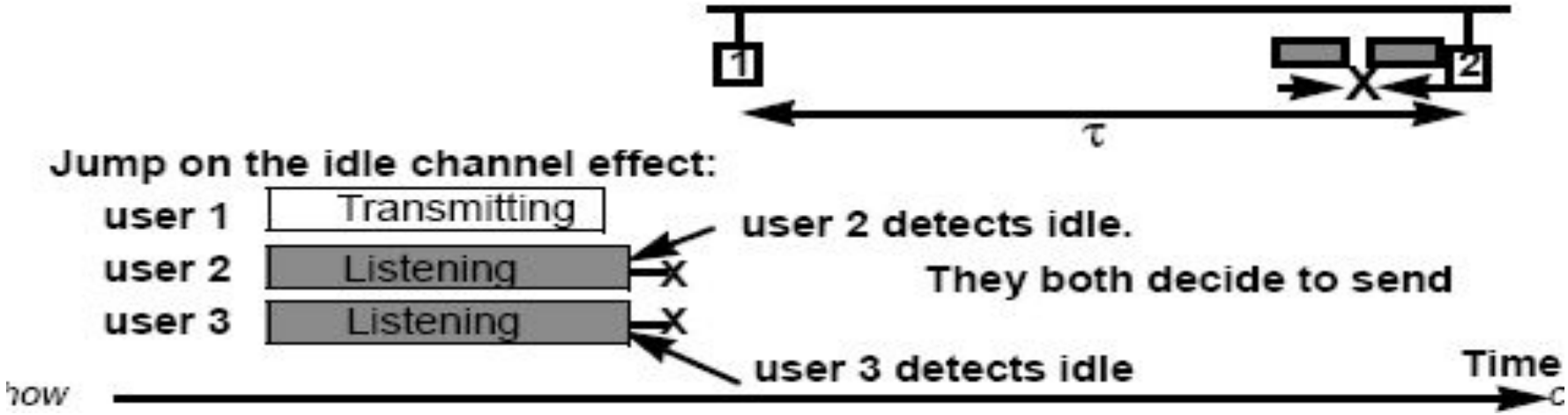
- It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data.
- It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle.
- Hence, it reduces the chances of a collision on a transmission medium.
- CSMA method was developed to decrease the chances of collisions when 2 or more stations start sending their signals over the data link layer

Carrier Sense MA protocols



Carrier Sense MA protocols

But, what to do if the channels are busy? Now, here the persistence methods can be applied to help the station act when the channel is busy or idle.



Carrier Sense MA protocols

The CSMA has 4 access modes:

- **1-persistent mode**: In this, first the node checks the channel, if the channel is idle then the node or station transmits data, otherwise it keeps on waiting and whenever the channel is idle, the stations transmit the data-frame.

- **Non-persistent mode**: In this, the station checks the channel similarly as 1-persistent mode, but the only difference is that when the channel is busy it checks it again after a random amount of time, unlike the 1-persistent where the stations keep on checking continuously.

Carrier Sense MA protocols

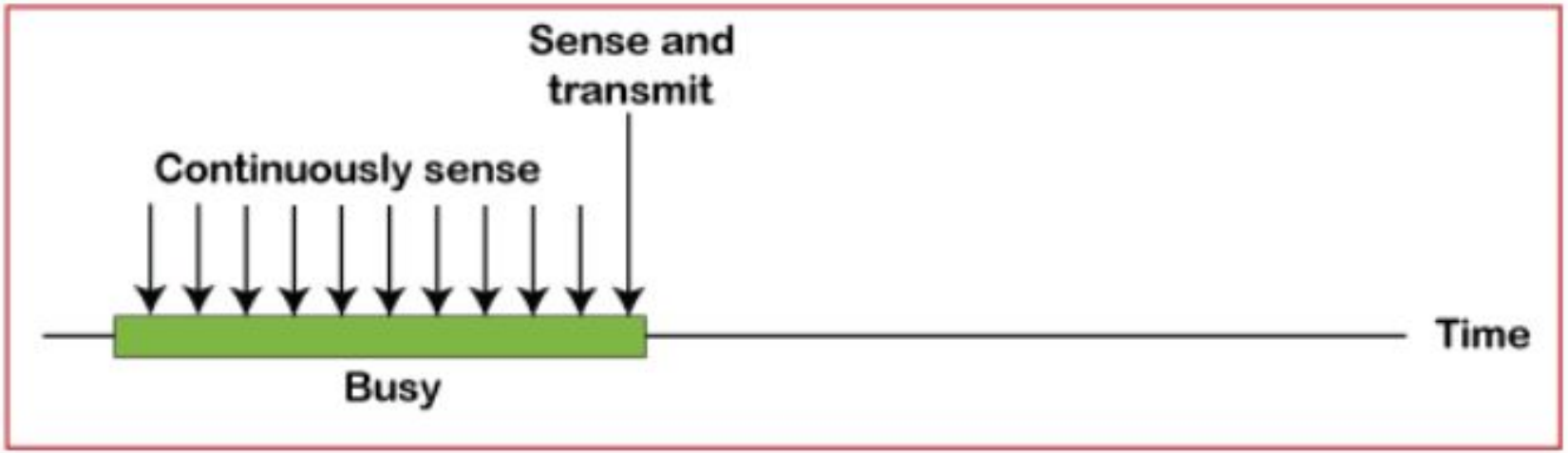
The CSMA has 4 access modes:

- **P-persistent mode**: In this, the station checks the channel and if found idle then it transmits the data frame with the probability of P and if the data is not transmitted (1-P) then the station waits for a random amount of time and again transmits the data with the probability P and this cycle goes on continuously until the data-frame is successfully sent.

- **O-persistent:** In this, the transmission occurs based on the superiority of stations which is decided beforehand and transmission occurs in that order. If the channel is idle, then the station waits for its turn to send the data-frame.

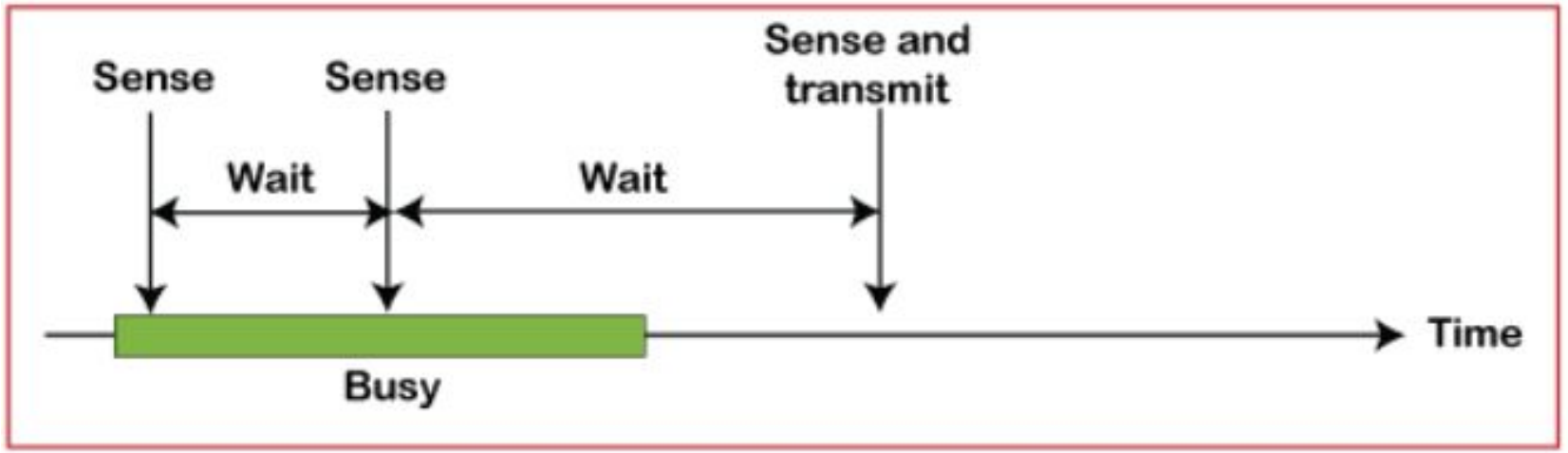
Carrier Sense Multiple Access (CSMA)

1-persistent mode



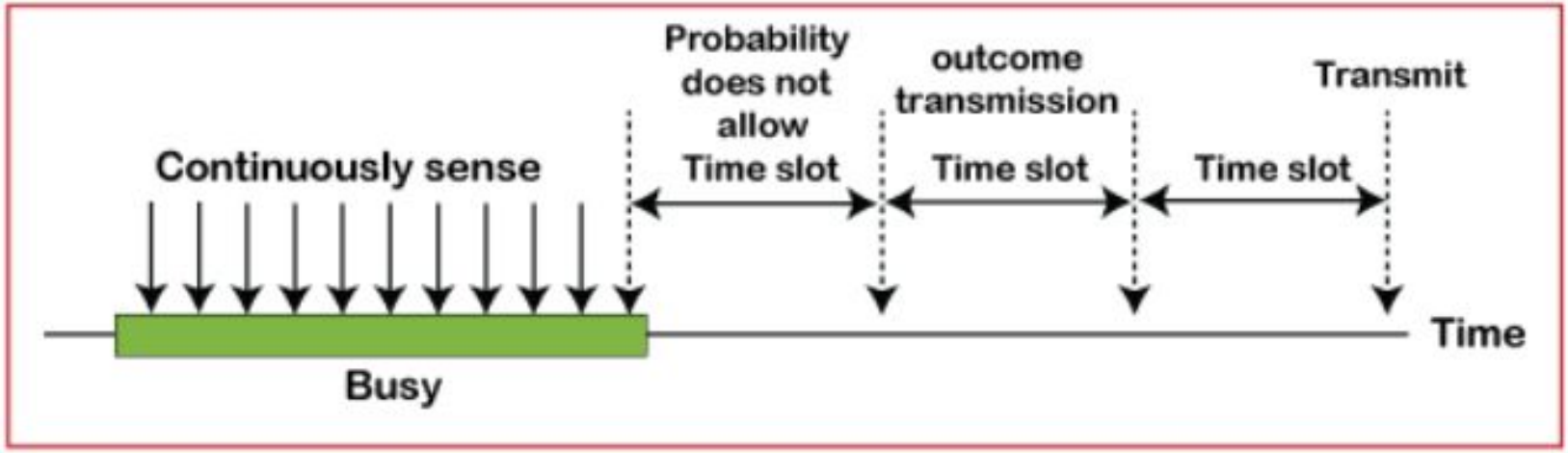
Carrier Sense Multiple Access (CSMA)

Non-persistent mode



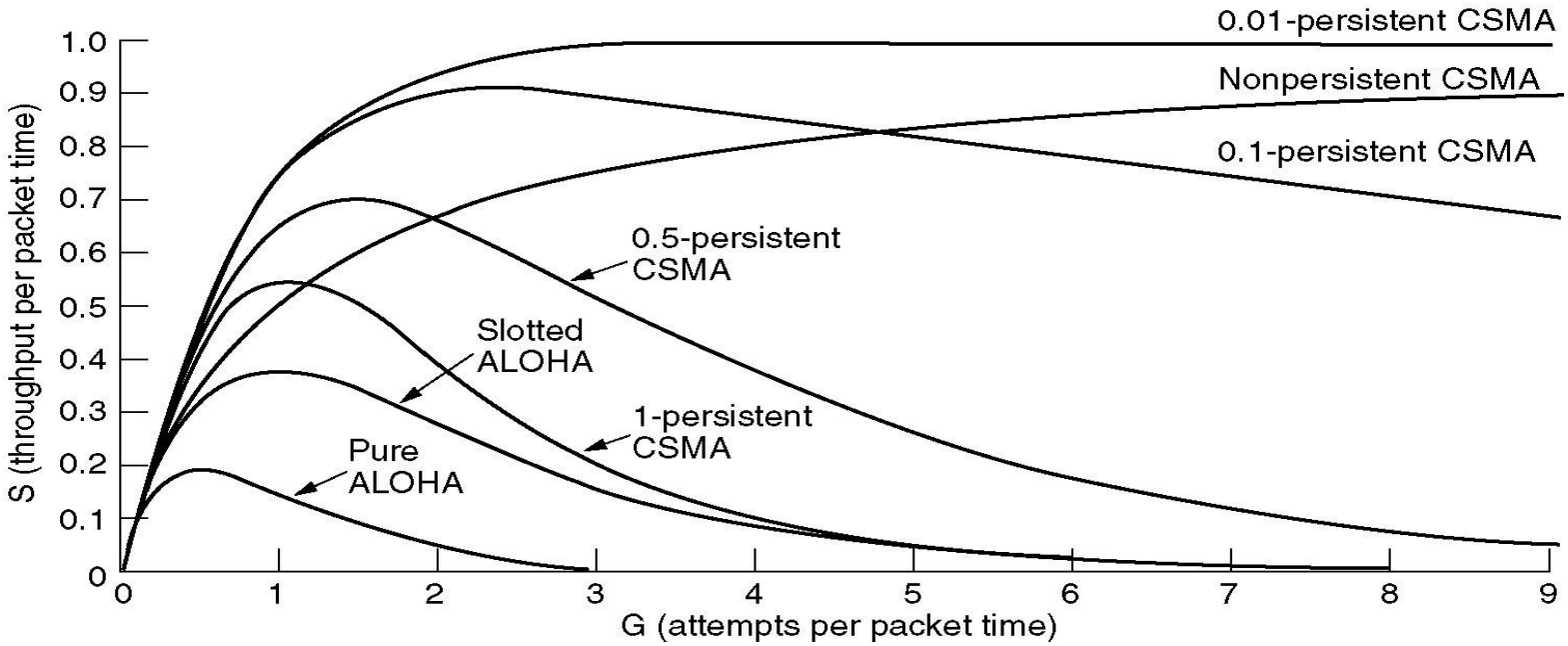
Carrier Sense Multiple Access (CSMA)

P-persistent mode



Persistent and Non-persistent CSMA

Comparison of the channel utilization versus load for various random access protocols.



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

CSMA with Collision Detection

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames.

The CSMA/CD protocol works with a medium access control layer.

Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful.

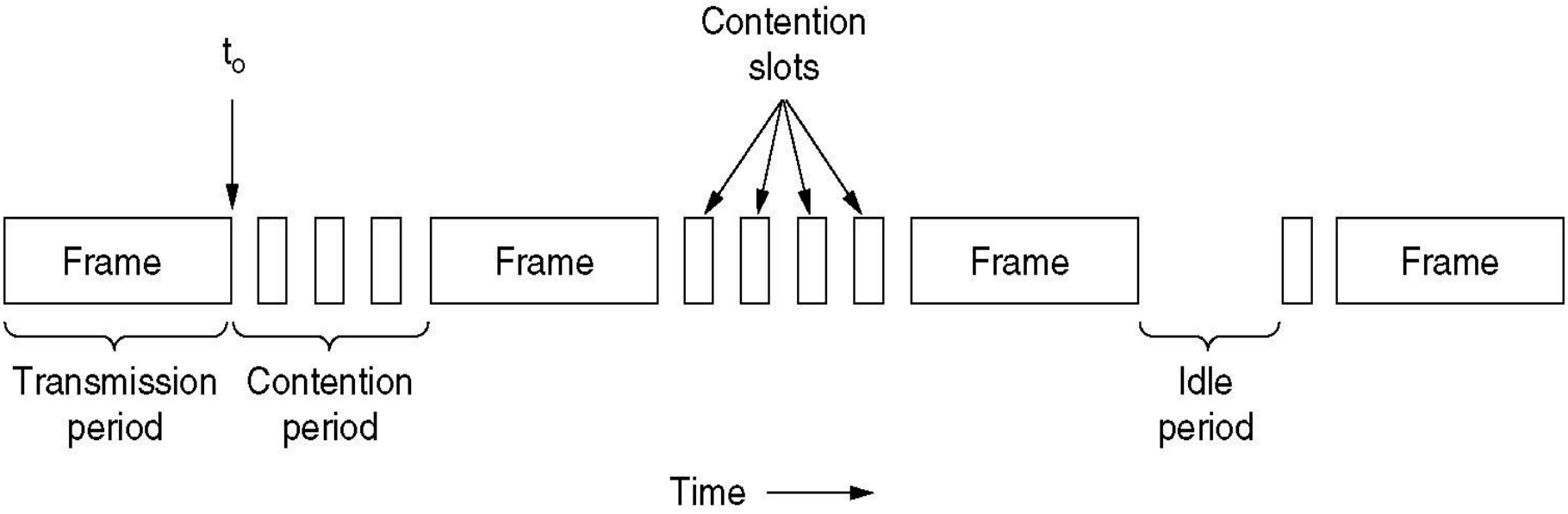
If the frame is successfully received, the station sends another frame.

If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission.

After that, it waits for a random time before sending a frame to a channel.

CSMA with Collision Detection

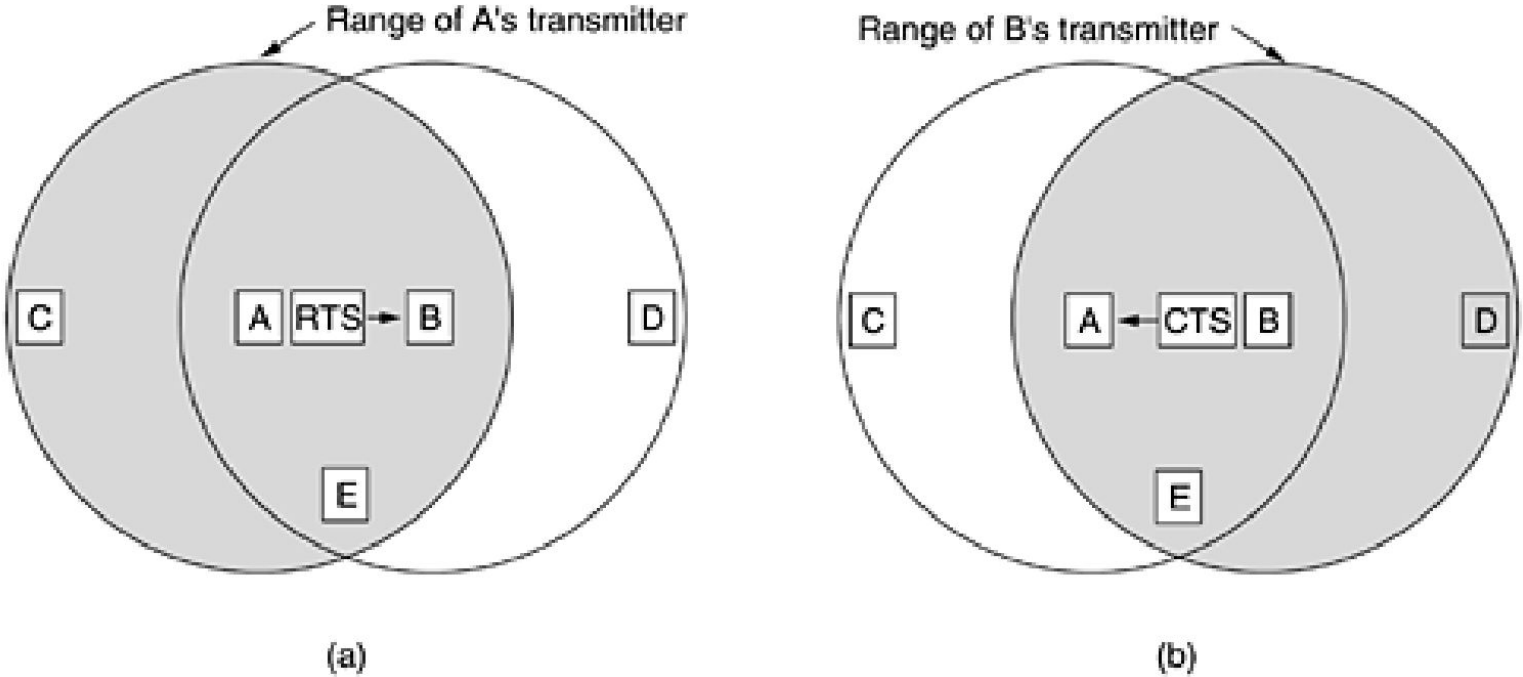
States of CSMA/CD: contention, transmission or idle



CSMA/CA (MACA) (Multiple Access with Collision Avoidance)

- It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames.
- It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear.
- If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver.
- But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.
- Following are the methods used in the CSMA/ CA to avoid the collision:

CSMA/CA (MACA)
(Multiple Access with Collision Avoidance)



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

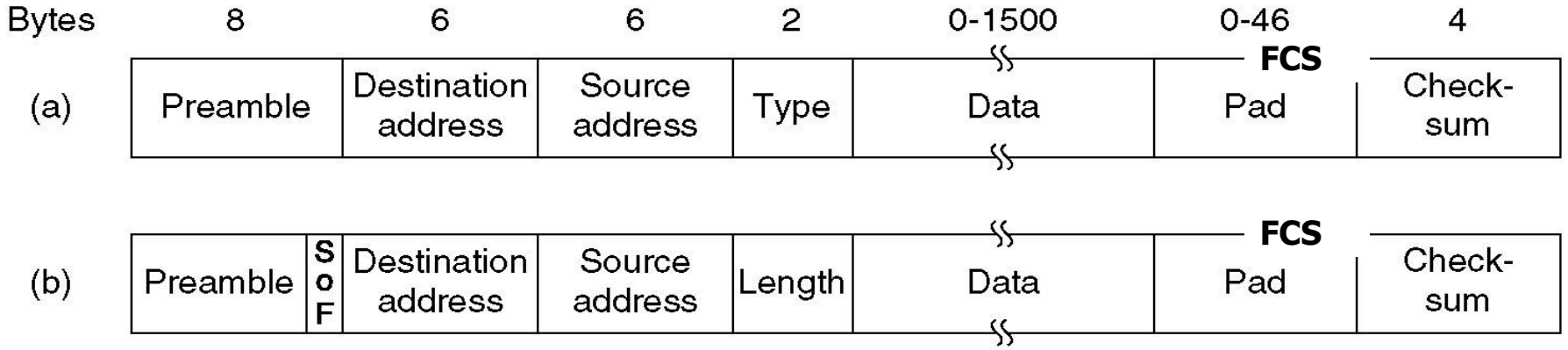
Ethernet Frame format

IEEE Standards

1. **Ethernet:** It is a LAN protocol that is used in Bus and Star topologies and implements CSMA/CD as the medium access method
2. **DIX:** Original (traditional) Ethernet developed in 1980 by three companies: Digital, Intel, Xerox (DIX).
3. **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.

   Current version is called IEEE Ethernet

Ethernet Frame format

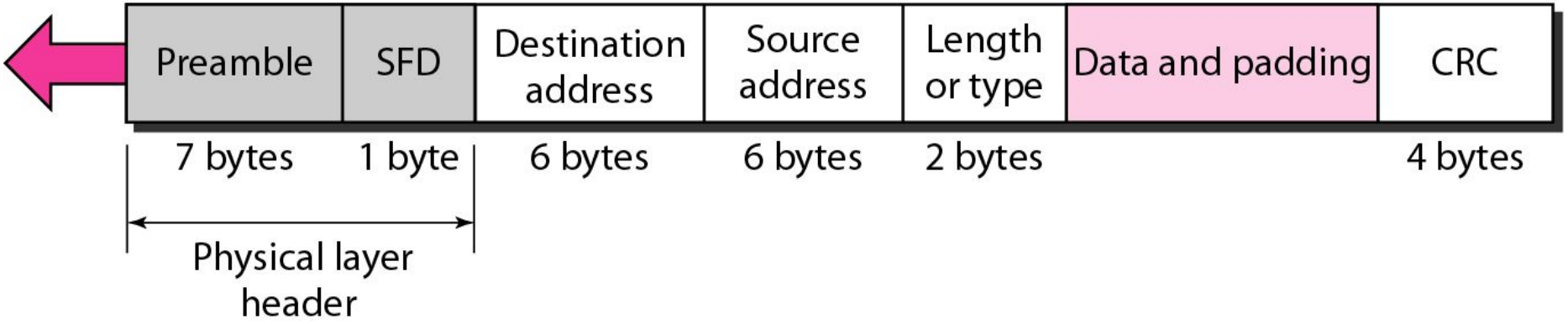


Frame formats. (a) DIX Ethernet , (b) IEEE 802.3.

IEEE 802.3 MAC frame

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Content

In IEEE 802.3 Ethernet Data link layer is split into two sublayers:

- Bottom part: MAC
  - The frame is called **IEEE 802.3**
  - Handles framing, MAC addressing, Medium Access control
  - **Specific implementation for each LAN p**rotocol
    - Defines **CSMA/CD** as the access method for Ethernet LANs and **Token passing** method for Token Ring.
  - Implemented in **hardware**
- Top part: LLC (Logical Link Control)
  - The subframe is called **IEEE 802.2**
  - Provides **error and flow control** if needed
  - It makes the MAC sublayer transparent
    - Allows interconnectivity between different LANs data link layers
  - Used to multiplex multiple network layer protocols in the data link layer frame
  - Implemented in **software**

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

IEEE 802.3 Cable Types

Name / Topology	Cable Max.	Max Cable Segment Length	Nodes / Segment
10Base5 / Bus	Thick coax	500 meters	100
10Base2 / Bus	Thin coax	185 meters	30
10BaseT / Star	Twisted pair	100 meters	1
10BaseF / Star	Fiber Optic	2Km	1

Frequently Asked Questions

1. Explain what might happen if two stations are accidentally assigned the same hardware address?
2. Why wireless LAN can not use the same CSMA/CD mechanism that Ethernet uses?
3. Complete given table and answer yes or no-

Characteristic	CSMA/CD	CSMA/CA	Token Ring
Multiple access			
Carrier Sense			
Collision checking			
Acknowledgement			

References

Text Books:

1. Behrouz A. Forouzan, ‘Data Communications and Networking’, 5th Edition, McGraw-Hill Publishing Company, ISBN 978-0-07-337622-6
2. Tanenbaum A. S., ‘Computer Networks’, Pearson Education , 5th Edition, ISBN-978-0-13-212695-3

Reference Books:

1. James F. Kurose and Keith W Ross ‘Computer Networking, A Top-Down Approach’, 5th Edition, Pearson Education, ISBN-978-81-317-9054-0
2. W. Richard Stevens, Unix Network Programming, The Sockets Networking API, Vol 1, 3rd Edition, PHI Learning Pvt. Ltd.

Supplementary Reading:

1. William Stallings, ‘Data and Computer Communications’, 6th Edition, Prentice Hall of India Pvt.

Web Resources:

1. https://nptel.ac.in/courses/106/105/106105080/
2. https://nptel.ac.in/courses/106/106/106106091/

Web links:

1. https://nptel.ac.in/courses/106/105/106105081/
2. https://nptel.ac.in/courses/106/105/106105183/
3. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-829-computer-networks-fall-2002/index.htm

MOOCs:

1. https://www.coursera.org/learn/computer-networking
2. https://www.edx.org/course/introduction-to-networking?index=product&queryID=0befdc538866babf2facfdc2dce06204&position=1

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Thank You

Any Questions