The best and most beautiful things in the world cannot be seen or even touched – they must be felt with the heart.

Helen Keller

3

Data Link Layer

3.1 Introduction

- The data link layer is second layer of OSI reference model and located between physical layer and network layer.
- The data link layer uses the services of the physical layer to send and receive bit over communication channels and provides an interface for the network layer to send information from one machine to another.
- The data link layer takes the packets in gets from the network layer and encapsulates them into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer as show in figure 3.1.
- The frames are then transmitted to the physical layer.
- The data link layer has three specific functions:

1. Provide a well-defined service interface to the network layer.
2. Dealing with transmission erors.
3. Regulating the flow of data so that slow receivers are not swamped by fast sender.

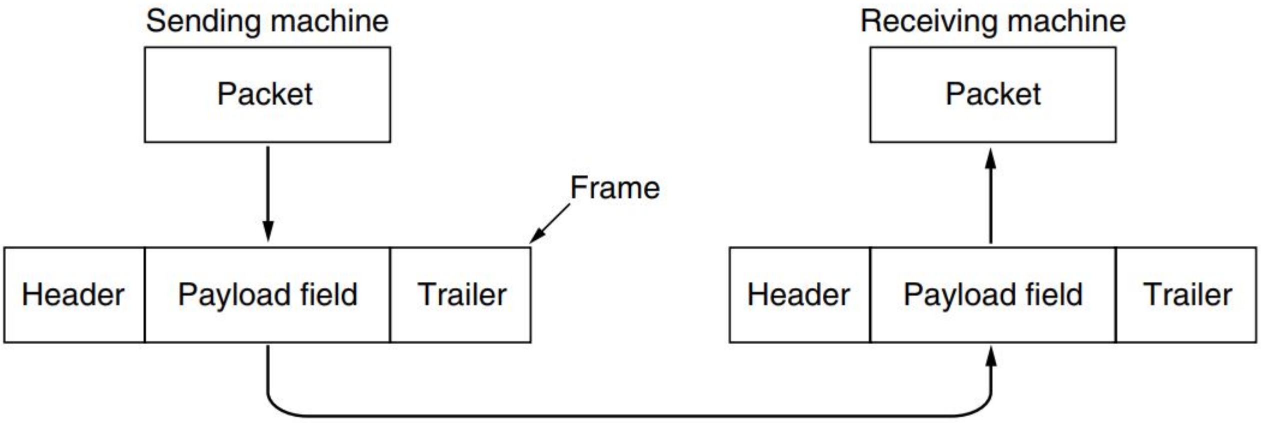


Figure 3.1: Relationship between packets and frames.

3.2 Functions of Data Link Layer

3.2.1 Services Provided to the Network Layer

- The data link layer provides services to its upper layer, network layer. It transport data from the network layer on the source machine to the network layer on the destination machine.

- The actual transmission follows the path as shown in figure 3.2(b); however, the data link layer communicates using data link protocol through virtual link as shown in 3.2(a).

- The data link layer can be designed to offer various services. The actual services that are offered vary from protocol to protocol. There are three common services:

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection oriented service.

Unacknowledged Connectionless Service

- In this type of service source machine sends independent frames to destination machine but the destination machine does not send any acknowledgement of these frames back to the source. Hence it is called unacknowledged service.

- There is no connection establishment between source and destination machine before data transfer or release after data transfer. Therefore it is known as connectionless service.

- There is no error control i.e. if any frame is lost due to noise on the line, no attempt is made to recover it. - This type of service is used when error rate is low, so recovery is left to higher layer.

- It is suitable for real time traffic such as voice.

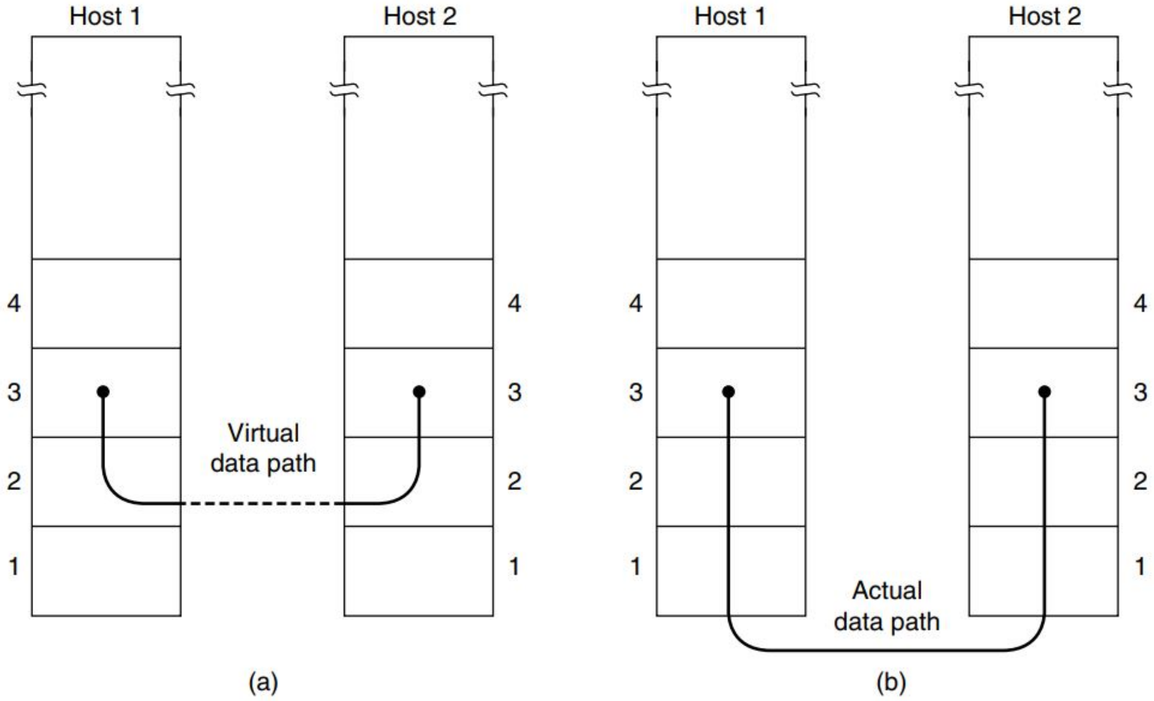


Figure 3.2: Data flow. (a) Virtual Communication (b) Actual communication.

- Ethernet is a good example of a data link layer that provides this class of service.

Acknowledged Connectionless Service

- In this class of service, there is still no logical connection used between source and destination, but each frame sent is individually acknowledged.
- Thus, the sender knows whether a frame has arrived correctly or been lost. Also, the sender can resend the frame, if the frame is not delivered within the specified time.
- This type of service is useful over unreliable channels, such as wireless system. 802.11 (WiFi) is a good example of this class of service.

Acknowledged Connection Oriented Service

- This service is the most sophisticated service provided by data link layer to network layer.
- It is connection-oriented. It means that logical connection is establishment between source & destination before any data is transferred.
- In this service, data transfer has three distinct phases: *connection establishment, data transfer, and connection release*.
- Here, each frame being transmitted from source to destination is given a specific number and is acknowledged by the destination machine.
- All the frames are received by destination in the same order in which they are send by

the source.
- This type of service is suitable for appropriate over long, unreliable links such as a satellite channel or a long-distance telephone circuit.

3.2.2 Framing

- In the sender side, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission over physical layer. The process is known as *framing*. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer. (Figure 3.1)
- The trailer consists of redundant bits such as checksum for each frame for computing errors. - When the frame arrives at the destination, the checksum is recomputed.
- If the newly-computed checksum is different from the original checksum, the data link knows that error has occurred and takes steps to deal with it.

3.2.2.1 Types of Framing

1. **Fixed Size Framing**
   - Fixed size frame.
   - No need for defining the boundaries of frames; the size of the frame itself acts as a delimiter.
   - Example: ATM WAN frame s(56 bytes)
2. **Variable Size Framing**
   - Not fixed size.
   - Need to define the end of frame and beginning of the next frame
   - Prevalent in LAN.
   - Four methods for variable framing:

   (i) Byte count.
   (ii) Flag bytes with byte stuffing.
   (iii) Flag bits with bit stuffing.
   (iv) Physical layer code violations.

Byte Count/Character Count

- In this method, a field in header is used to specify the number of bytes in the frame.
- The destination sees the byte count, it knowns how many bytes follow and hence where the end of the frame is.
- This method can cause problem if the count is garbled in the transit; in that case, the receiver will not know where to pick up and the sender will not know how much frame to resend.
- So, this method is rarely used any more.

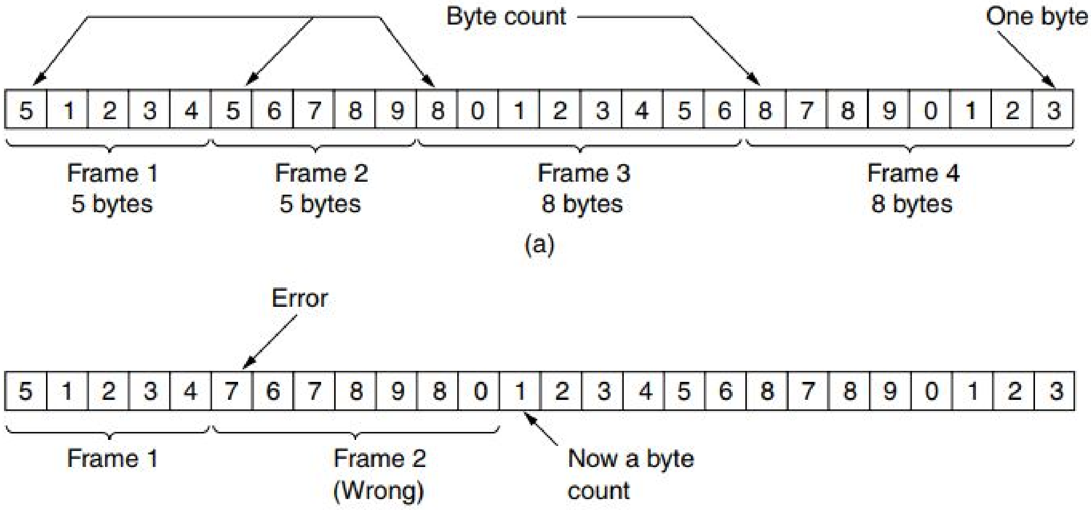


Figure 3.3: A byte stream; (a) Without error (b) With error.

Flag Bytes With Byte Stuffing

- In this method, frame is begins and ends with a special byte, called **FLAG**.
- Two consecutive flag bytes indicate the end of one frame and the start of the next frame. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.

Problem with this method:

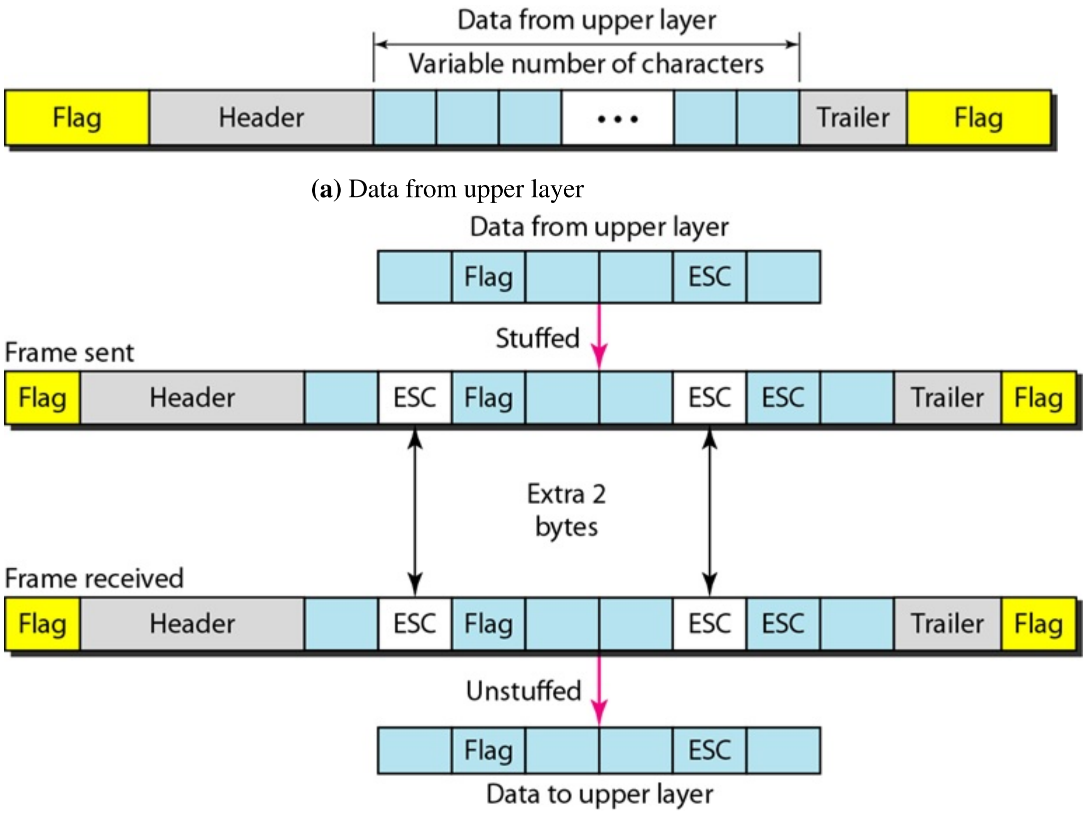
- Still this method has a problem when "flag" byte occurs in the data, especially when binary data such as images, videos, or audio are transmitted.
- If this happens, the receiver could interpret this as the end of frame.
- Solution is **byte stuffing or character stuffing**.
- Byte stuffing is the process of inserting one extra escape byte(ESC) just before the each "accidental" flag byte in the data. Here, if an escape byte occurs in the data, then it too is stuffed with an escape byte. (Figure 3.4)
- Figure 3.4 shows an example of byte stuffing process used in **PPP (Point-to-Point Protocol)**.

Disadvantage of Byte Stuffing

- Use of 8-bit byte which can cause overhead bits in the frame.
- Also, not suitable if two machines communicating where one uses 8-bit characters and one uses 16-bit characters.

Bit Stuffing

- Bit stuffing was developed for once very popular **HDLC (High-level Data Link Control)** protocol.



(a) Data from upper layer

(b) Byte stuffing and unstuffing.

Figure 3.4: Byte stuffing

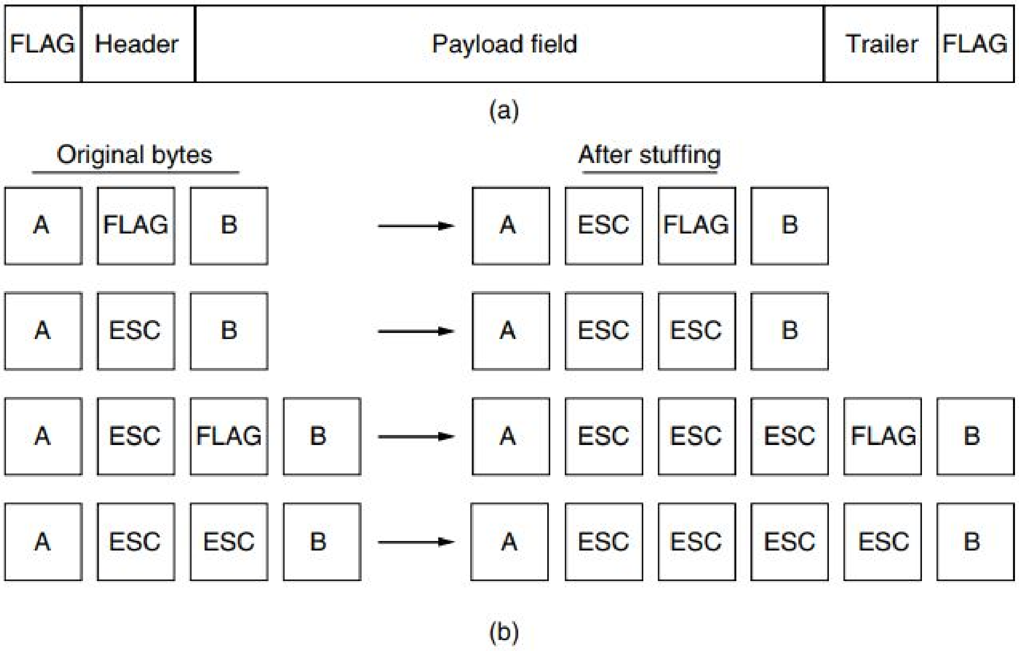


Figure 3.5: (a) A frame delimited by flag bytes. (b) Four examples of byte sequences before and after byte stuffing.

- Each frame begins and ends with a special bit pattern, **01111110 or 0x7E** in hexadecimal (in fact, a flat byte).
- Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e. deletes) the 0 bit.
- With bit stuffing, the boundary between two frames can be determined by the flag pattern. So, if the receiver losses the synchronization, it has to do is scan for flag sequences, since they can only occur at frame boundaries and never within the data.

- Bit stuffing ensures a minimum density of transitions that help the physical layer maintain synchronization. **USB (Universal Serial Bus)** uses bit stuffing for this reason.

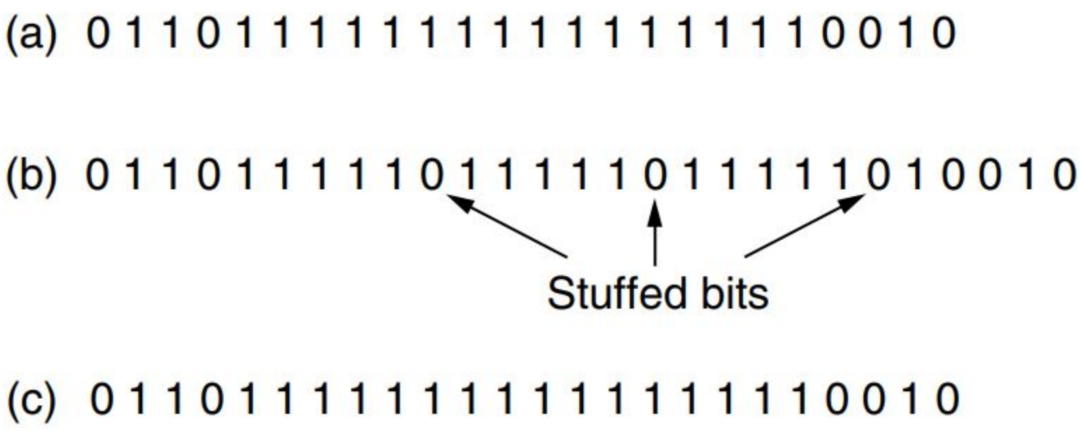

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0
(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0
Stuffed bits
(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Figure 3.6: Bit sutffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they stored in the receiver's memory after destuffing.

Physical Layer Coding Violations Framing

- Some reserved signals are used to indicate the start and end of frames.

Many data link protocols use a combination of these methods for safety. A common pattern used for Ethernet and 802.11 is to have a frame begin with a well-defined pattern called a **preamble**. This pattern might be quite long (72 bits is typical for 802.11) to allow the receiver to prepare for an incoming packet. The preamble is then followed by a length (i.e., count) field in the header that is used to locate the end of the frame.

3.2.3 Error Detection and Control

Error

- During data transmission, when the receiver does not receive the exact bits sent by the sender, then **error** is said to be occurred.

- Error is corruption of bit(s)during transmission because of noise, distortion or attenuation in the media.

- Due to error, some bits value in transmitted data change from 0 to 1 or 1 to 0.

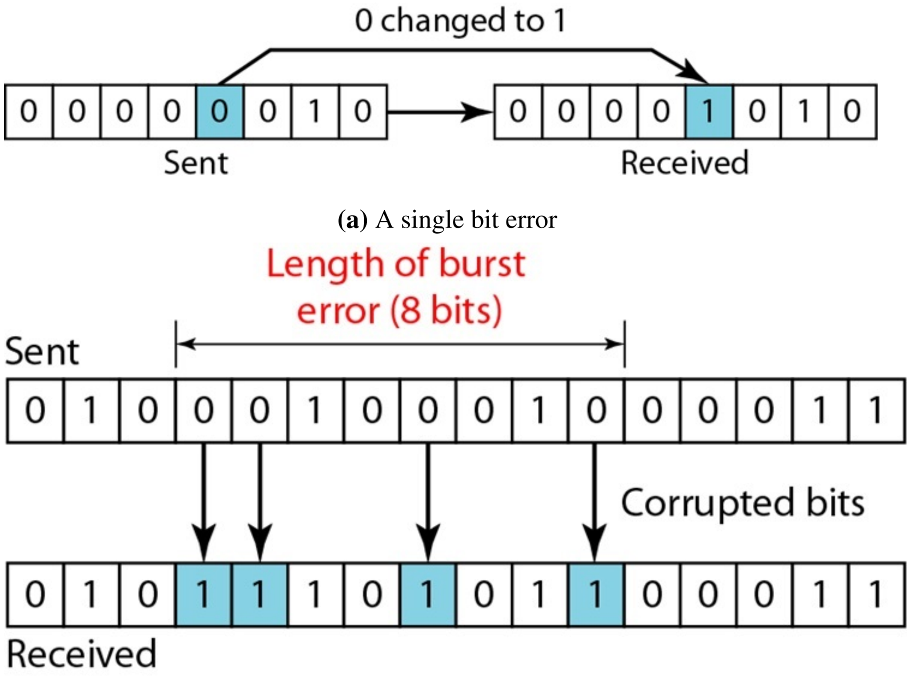
- There are two types of error:

1. **Single Bit Error**

   If a single bit error, only 1 bit in the data has changed from 1 to 0 or 0 to 1. It is easy to detect and correct the single bit error.

2. **Burst Error**

   Burst error means that two or more bits in the data have changed form 0 to 1 or 1 to 0. It is easy to detect but much harder to correct the burst error when do occur.



(a) A single bit error

(b) A burst error.

Figure 3.7: Types of error

- Error control allows the receiver to inform the sender of any frames lost or duplicated or damaged in transmission and coordinates the retransmission of those frames by the sender.

- Error control is divided into two main categories:

1. **Error detection**

   - It allows a receiver to check whether received data has been corrupted during transmission.

- If corrupted, it coordinates for retransmission.
- Example: Parity checking, CRC, checkum.

2. **Error Correction**
   - It allows the receiver check error and to reconstruct the original information when it has been corrupted during transmission.
   - Example: Hamming code

There are two ways to correct found errors:

1. **Forward Error Correction (FEC**)
   - FEC is accomplished by adding redundancy to the transmitted information using a predetermined algorithm.
   - Each redundant bit is invariably a complex function of many original information bit.
2. **Automatic Repeat reQuest (ARQ)**
   - Receiver detects transmissions errors in a message and automatically requests a retransmission of the frame from the sender.
   - When the sender receives the ARQ, the sender retransmits the message until it is either correctly received or the error persists beyond a predetermined number of retransmission.
   - A few types of ARQ protocols are Stop-and-wait ARQ, Go-Back and Selective Repeat ARQ.

Redundancy

- In order to detect and correct error, extra bits (i.e. redundant) are added to the original data by the sender and removed by the receiver. - Their presence allows the receiver to detect and correct corrupted bits.
- This technique is called **redundancy**.

Block Coding

- In block coding, we divide the message into blocks, each k bits, called **datawords**.
- We add r redundant bits to each block to make the length $n = k + r$.
- The resulting n-bit blocks are called **codewords**.
- With k kits, we can create a combination of 2^k datawords and , with n bits, we can create a combination of 2^n datawords.
- Invalid or illegal codeword = $2^n - 2^k$.

Conditions for error detection using block coding

- The receiver has (or can find) a list of valid code words.
- The original codewords has changed to an invalid one.

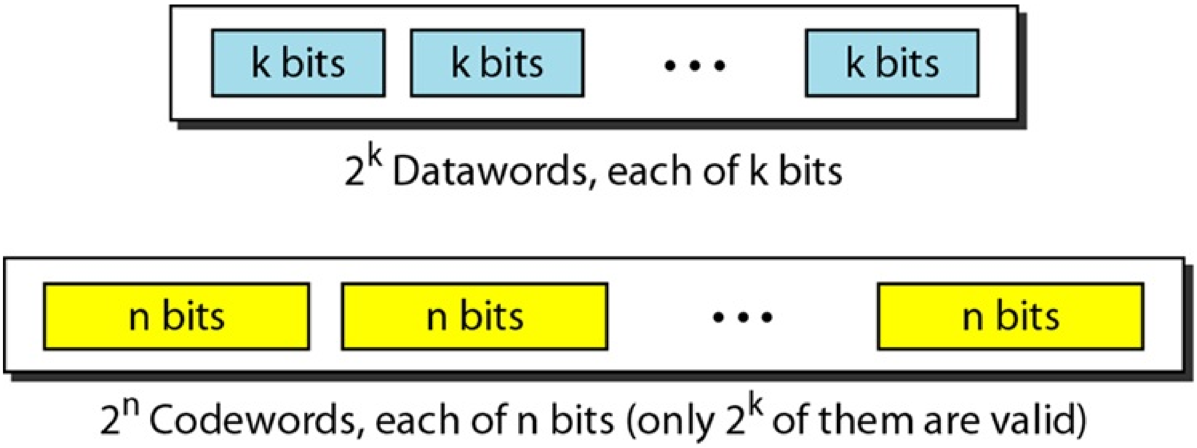

k bits
k bits
• • •
k bits
2^k Datawords, each of k bits
n bits
n bits
• • •
n bits
2^n Codewords, each of n bits (only 2^k of them are valid)

Figure 3.8: Datawords and codewords in block-coding.

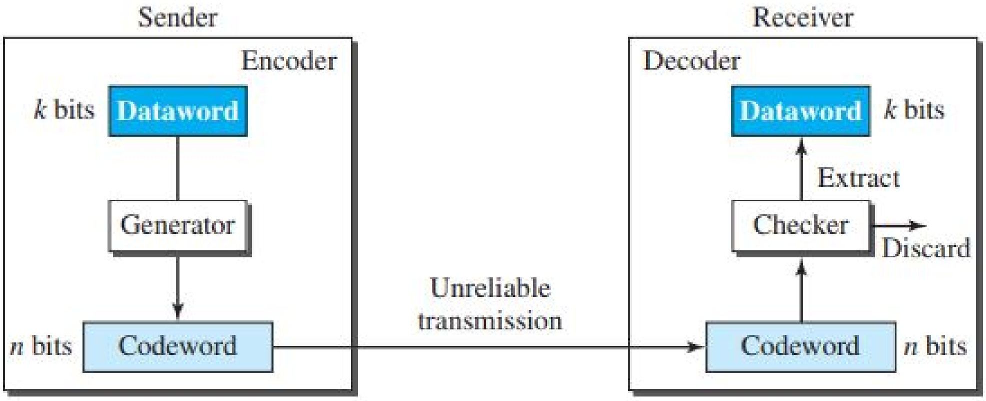


Figure 3.9: Process of error detection in block coding.

Hamming Distance

- The hamming distance between two words (of same size) is the number of differences between corresponding bits.

- The hamming distance between two words x and y is $d(x,y)$.

- We find the hamming distance by XORing operation on the two words.

Minimum Hamming Distance

- The minimum hamming distance is the smallest hamming distance between all possible pairs in a set of words.

- We use d_{min} to define the minimum hamming distance in the coding scheme.

- Example:

i. The hamming distance between d(000,011) is 2 since (000 $\oplus$ 011) is 011 (two 1's)

2. The hamming distance between d(10101, 11110) is 3 because (010101 $\oplus$ 11110) = 01011 (three 1's)

Minimum Hamming Distance for Error Detection

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

Example:

- For coding scheme with $d_{min} = 2$, only a single bit error can be detected.
- For coding scheme with $d_{min} = 3$, only two bit errors can be detected.

Minimum Hamming Distance for Error Correction

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

Linear Block Code

- Linear block code is used for error detection and error correction.
- In a linear block code, the exclusive OR (XOR) of any two valid codewords creates another valid code word.

Cyclic Codes

- Special linear block codes in which in a codeword is cyclically shifted (rotated), the result is another codeword.

3.2.3.1 Error Detection Methods

- Error detection method uses the concept of redundancy.
- Redundancy bits are generated by making some relation with data bits.
- Examples: Parity, CRC, Checksum.

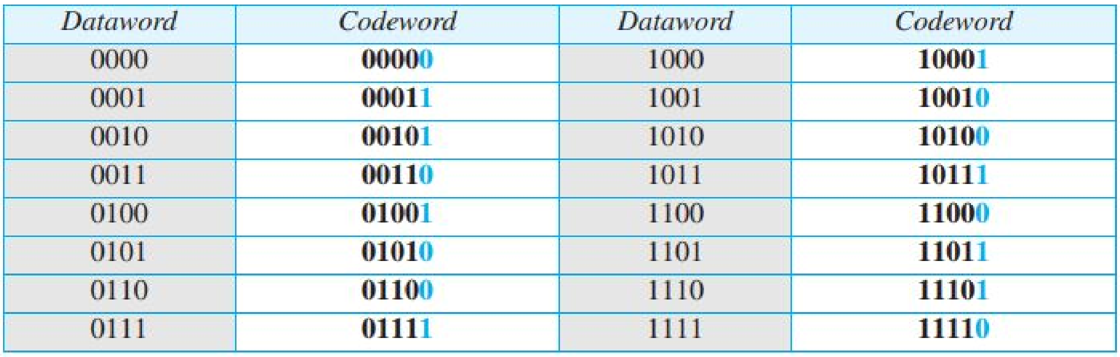
Parity Checking

- It is the simplest form of error detection method.
- A parity is a single bit added to data so as to make the number of 1's either odd or even.
- It is one bit redundant bit method.
- It is of two types:
  - Odd parity
  - Even parity

Parity bit r_0 is calculated as modulo-2 operation:

$$r_0 = a_3 \oplus a_2 \oplus a_1 \oplus a_0 \quad (modulo - 2)$$

$r_0 = 0$, if the number of 1's even in dataword
else,



Dataword	Codeword	Dataword	Codeword
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

Figure 3.10: Simple parity check code for *C(5,4)*.

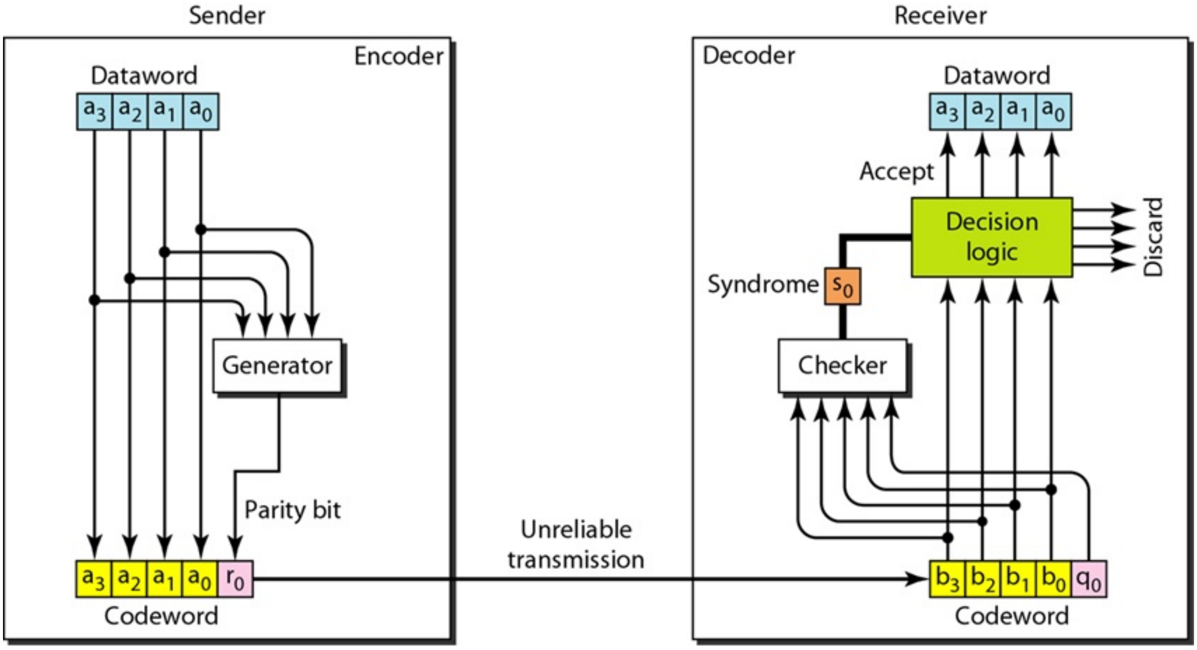


Figure 3.11: Encoder and decoder for simple parity check code.

$= 1$

At receiver side, syndrome is calculated as

$$s_0 = b_3 \oplus b_2 \oplus b_1 \oplus \oplus b_0 \oplus r_0 \quad (modulo-2)$$

And,

$s_0 = 0$, if received code has even number of 1's. i.e Data is accepted.

If, $s_0 = 1$, dataword is rejected; i.e. error occured.

Note:

A simple parity check method can only detect an odd number of errors.

Two Dimensional Parity Check

- One of the way to overcome the problem of simply parity is to use two dimensional

parity check.
- In this technique, the parity bits are produced for each row and columns on block of data.
- When large number of binary words are begin transmitted or received in succession, the resulting collection of bits is considered as block of data.
- The two set of parity bits so generated are known as:

1. Longitudinal redundancy checks (LRC) bit
   The LRC indicate the parity of rows. The LRC bits are parity bit associated with the rows of data blocks. Here a block of bits is organized in the form of a list of rows. If we want to send 32 bits then we arrange them in list of four rows each of 8 bits. Then parity for each columns is calculated and a new row of eight bits is created. These become the parity of bits for the whole block.

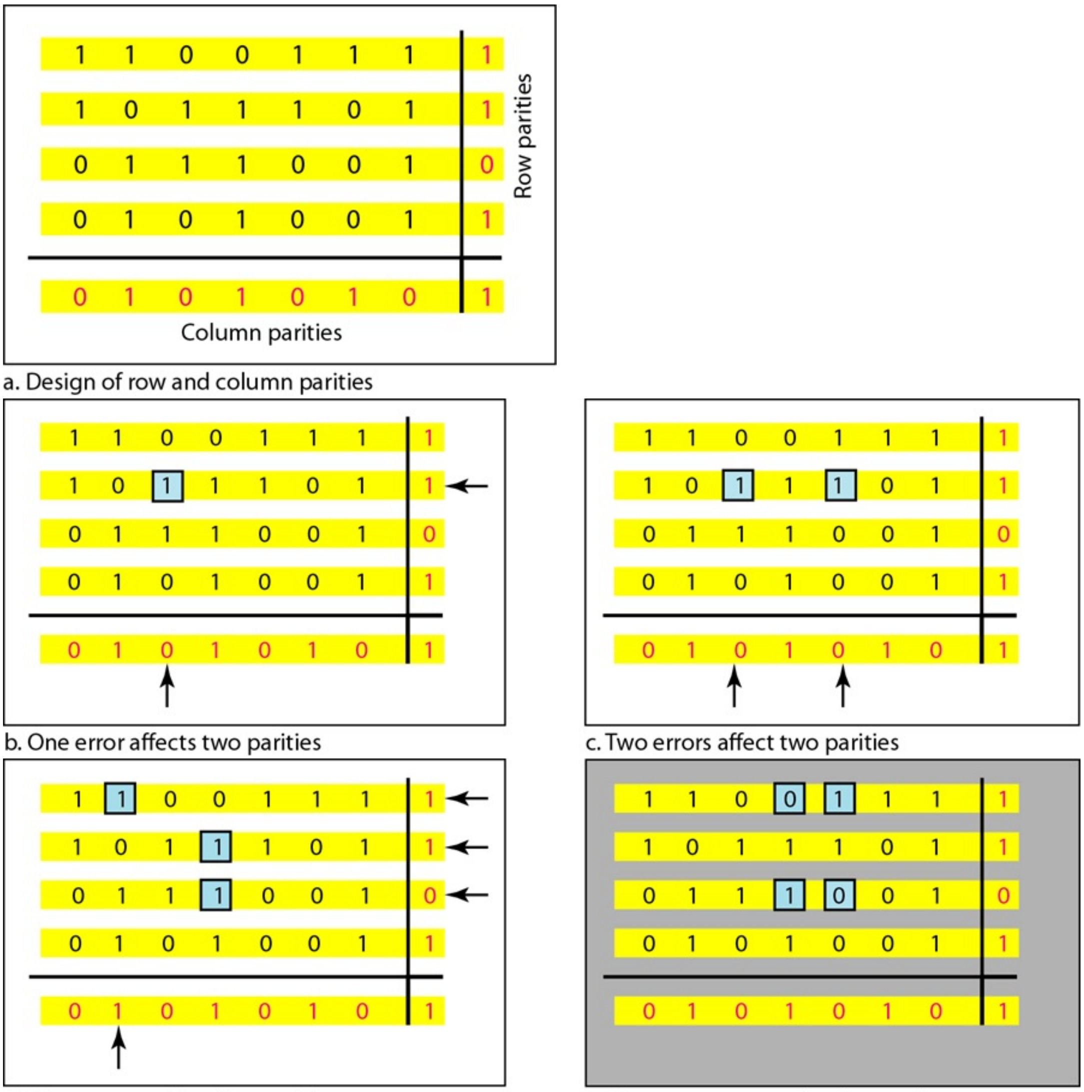
2. Vertical redundancy checks (VRC) bit
   A VRC also known as parity check is a simple technique which consists of adding a single bit called parity bit to the ned of each word before transmitting. The VRC indicate the parity of columns. The VRC bits are parity bit associated with columns of data block. Each VCR bit will make the parity of corresponding column, an even parity. It can detect all single bit error as well as burst error if the total number of bits changed is odd.

Cyclic Redundancy Check (CRC)
- It is a error detecting method based on binary division in which the desired sequence of redundant bits (*r bits*)) are generated and is appended to the end of data unit (*k-bits*), so that the resulting frame is of (*n* = *k*+*r bits*) - It is also called as *CRC reminder*, so that the resulting data unit becomes exactly divisible by a predetermined binary number.
- It is used in LANs and WANs.

Example: Figure 3.13.

At encoder side:
- Dataword = k-bits(here 4) and codeword = n-bits(here 7).
- $n-k$ (here 3) 0's are added to right-hand side of dataword and then fed to generator. Generator uses $n-k+1$ (here 4) bit divisor, which is predefined.
- Generator divides the augmented dataword. Quotient is discarded while remainder is appended to the dataword to create the codeword.

At decoder side:
- Receives the possible corrupted codeword, and fed to checker.
- Uses the division by the same divisor and produce the remainder (syndrome) of $n-k$



a. Design of row and column parities

b. One error affects two parities

c. Two errors affect two parities

d. Three errors affect four parities

e. Four errors cannot be detected

Figure 3.12: Two dimensional parity check

(here 3 bit) bits, which is fed to decision logic analyzer.

- If the analyzer finds all the syndrome 0's, the leftmost k (here 4) bits of codeword is accepted, else it is rejected (i.e. error has been occurred).

Polynomials

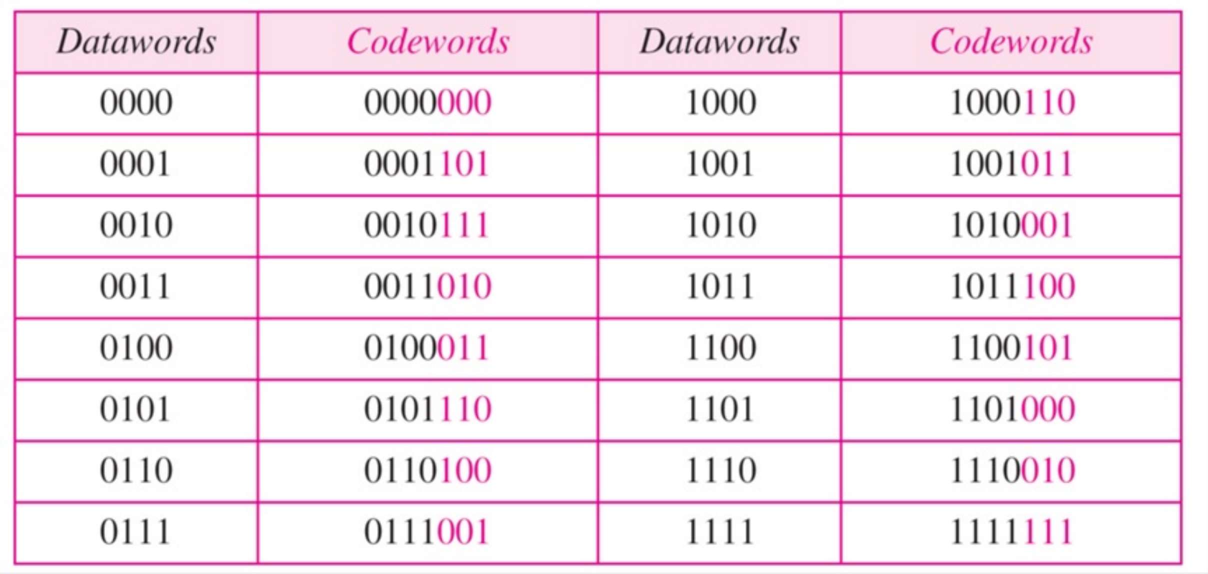
- Better way to understand and analyze the cyclic code.

- A pattern of 1's and 0's can be represented as a polynomial with coefficients of 0 and 1.

- The **power** of each term shows the position of the bit; the **coefficient** show the value of the bit.

Degree of polynomials

- The **degree of polynomial** is the highest power in the polynomials. For example: in $x^6 + x + 1$, the degree is equal to 6.



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

Figure 3.13: A CRC code with *C(7,4)*.

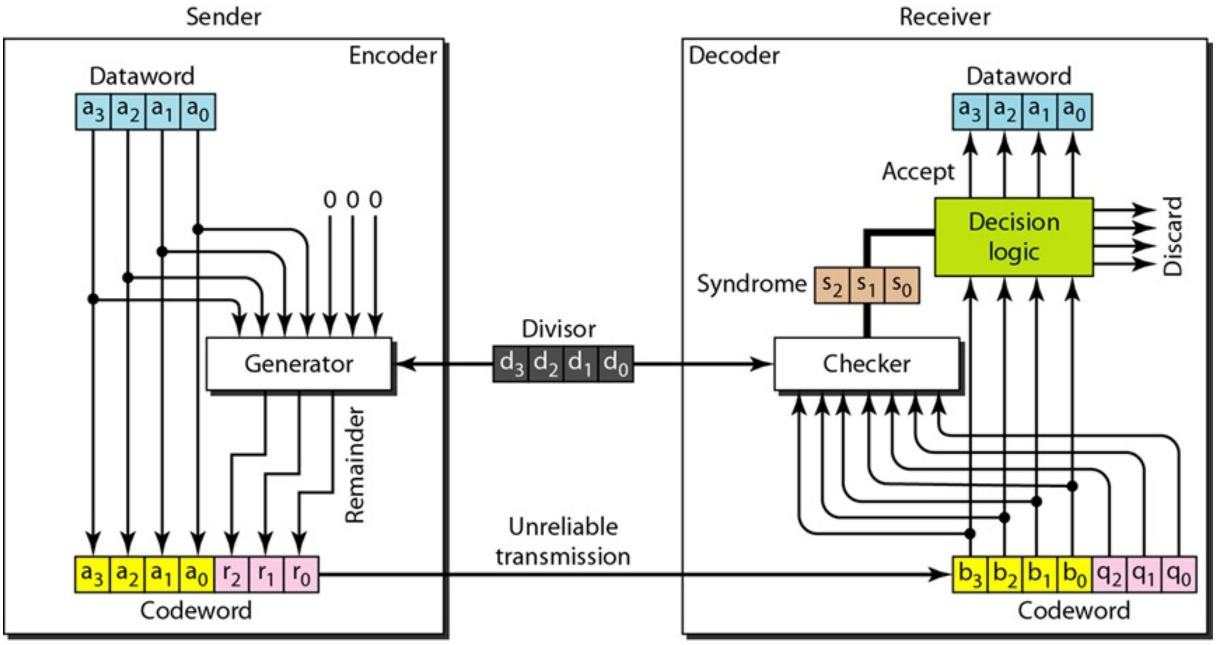


Figure 3.14: A CRC encoder and encoder.

- Degree of polynomial is always 1 less then the total bit pattern.

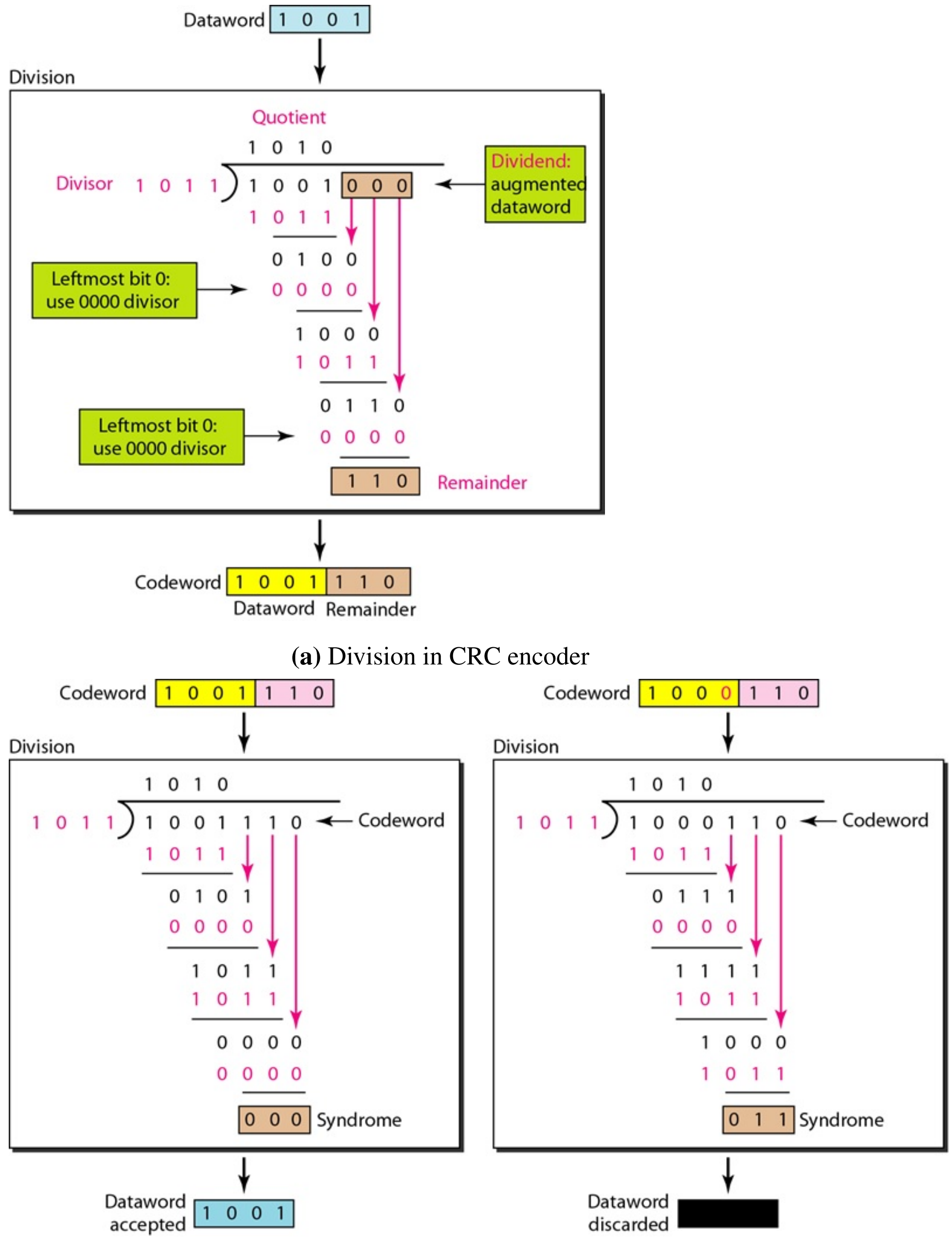
Adding and subtracting polynomials

- The coefficients of terms with same power is added or subtracted.

- The coefficients are 1 and 0. So, adding and subtracting are same, done with modulo-2 operation.

- Adding and subtracting is done by combining term and deleting the identical terms.

- Example: adding $x^5 + x^4 + x^2$ and $x^6 + x^4 + x^2$ gives just $x^6 + x^5$.



(a) Division in CRC encoder

(b) Division in the CRC decoder for two cases

Figure 3.15: An example of CRC.

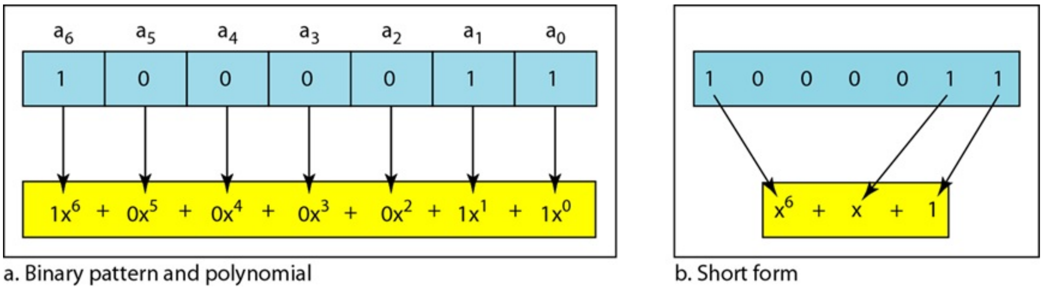

a_6 a_5 a_4 a_3 a_2 a_1 a_0
1 0 0 0 0 1 1
$1x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$
1 0 0 0 0 1 1
$x^6 + x + 1$
a. Binary pattern and polynomial
b. Short form

Figure 3.16: An polynomial to represent a binary example.

Multiplying Two Polynomials

- Multiplying a polynomials by another is done term by term.
- Pairs of equal terms are deleted.

Shifting of polynomial

Shifting to the left

- Adding 0's as rightmost bits.
- Accomplished by multiplying each the polynomial by x^m, where m is number of shifted bits.

Shifting to right

- Deleting by some rightmost bits
- Accomplished by dividing each term of the polynomial by x^m.

Shifting left 3 bits: 10011 becomes 10011000 x^4+x+1 becomes $x^7+x^4+x^3$

Shifting right 3 bits: 10011 becomes 10 x^4+x+1 becomes x

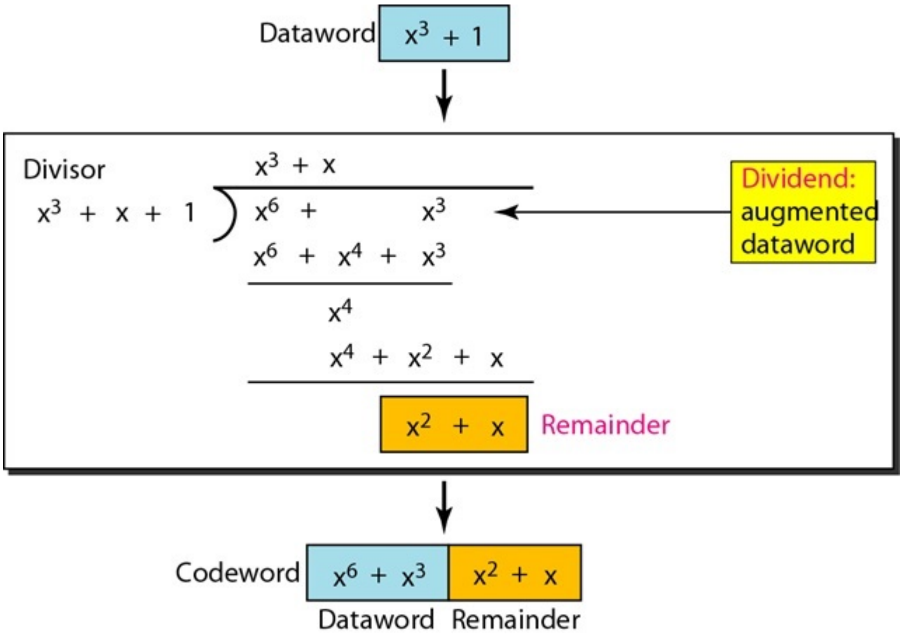


Figure 3.17: A CRC division using polynomials.

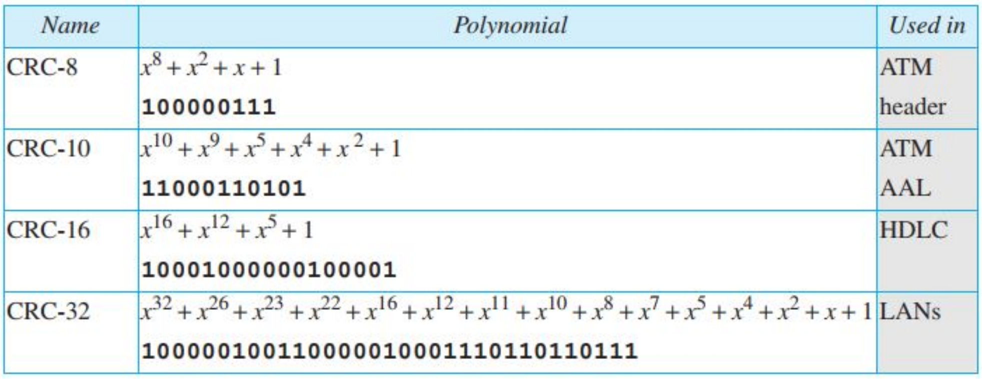
Standard Polynomials

- Some standard polynomials used by popular protocols for CRC generation.

Checksum

- Checksum is an error-detecting technique that can be applied to a message of any length.

In the internet, the checksum technique is mostly used at the network and transport layer rather than the data-link layer.



Name	*Polynomial*	*Used in*
CRC-8	x^8+x^2+x+1 100000111	ATM header
CRC-10	$x^{10}+x^9+x^5+x^4+x^2+1$ 11000110101	ATM AAL
CRC-16	$x^{16}+x^{12}+x^5+1$ 10001000000100001	HDLC
CRC-32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$ 100000100110000010001110110110111	LANs

Figure 3.18: Standard polynomials.

- It is based on the concept of redundancy. However, we briefly discuss it here to complete our discussion on error checking.

Principle of checksum

- At the source, the message is first divided into m-bits units.

- The generator then creates an extra m-bits unit called the checksum, which is sent with the message.

- At the destination the checker creates a new checksum from the combination of the message and sent checksum. If the new checksum is all 0s, the message is accepted; otherwise,the message is discarded.

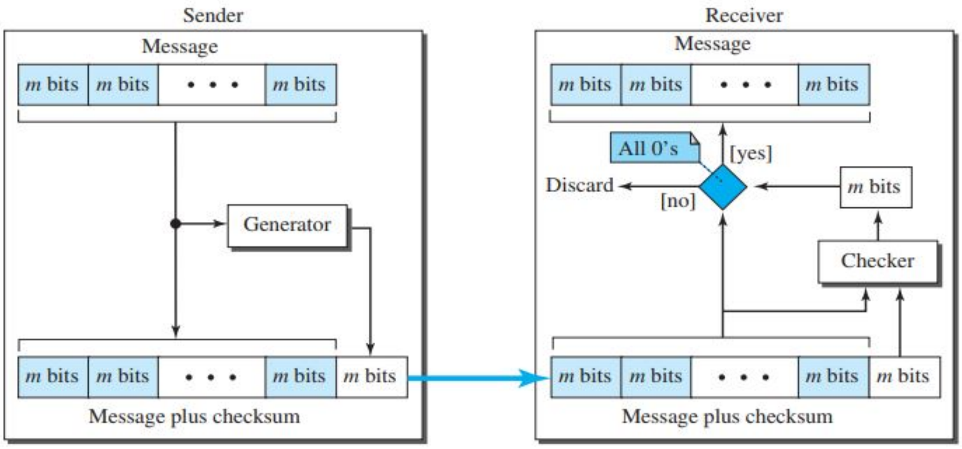


Figure 3.19: Checksum.

One's Complement Addition

- In this arithmetic, we can represent unsigned numbers between 0 and 2m-1 using only m bits. If the number has more than m-bits, the extra bits need to be added to the m-

rightmost bits (wrapping).
Example:
- 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. - In one's complement arithmetic, the negative or complement of a number is found by inverting all bits. For example, one's complement arithmetic of -6 is 1001, as Positive 6 is 0110 and its one's complement is 1001 i.e. 9.

Checksum Calculation Example:
Suppose the sender is sending a list of five 4-bit numbers (7, 11, 12, 0, 6). Figure 3.20 shows the checksum calculation.

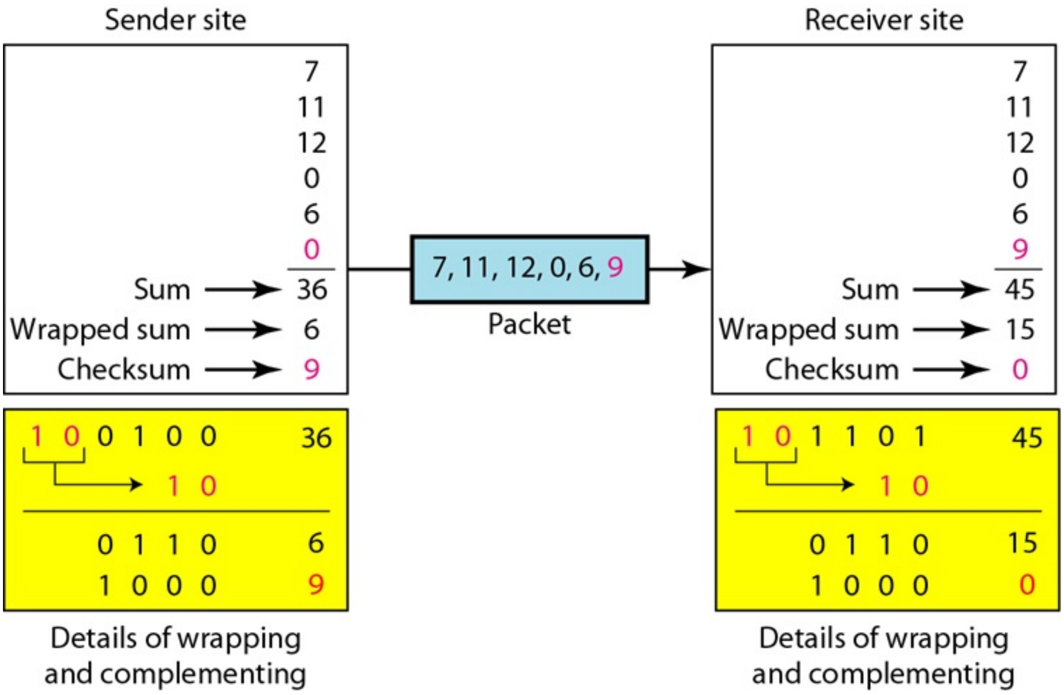


Figure 3.20: An example of checksum calculation.

Procedure to calculate the traditional checksum at sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Procedure to calculate the traditional checksum at receiver site:

1. The message (including checksum is divided into 16-bit words.

2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

3.2.3.2 Error Correction Codes

- Error correction codes allows a receiver check for error and to reconstruct the original information when it has been corrupted during transmission.
- It is also called Forward Error Correction (FEC).
- An example of error correction codes are:

- Hamming Codes.
- Binary Convolution Codes.
- Reed-Solomon Codes.
- Low-Density Parity Check Codes

Hamming Code

- Hamming code is the block code that is used to check and correct error.
- It was developed by R.W. Hamming for error correction.
- Hamming code is based on minimum hamming distance (d_{min}).
- consider Hamming code(n,k)

- n: no. of code bits
- k: no. of data bits
- r: no. of redundant bit
- n: k+r

- With the help of below equation we can calculate the number of redundant bit for given data bit

$$2^r \geq k+r+1$$

Example:

- Consider an example of hamming code (7 ,4)
- No. of data bits (k) = 4 - Calculate the redundant bits with help of formula $2^r \geq k+r+1$

- Consider r = 1 $\rightarrow$ 2 $\geq$ 4 + 1 + 1 (*Not Feasible*)
- Consider r = 2 $\rightarrow$ 4 $\geq$ 4 + 2 + 1 (*Not Feasible*)
- Consider r = 3 $\rightarrow$ 8 $\geq$ 4 + 3 +1 (*Feasible*)

- For data (k) bits = 3, we need 3 redundant bits.
- So, total number of bits in code word (n) = 4 + 3 = (k+r) = 7.
- In this example, Minimum hamming distance is d_{min} = 3.

Steps for Hamming code

- An information of 'k' bit are added to the redundant bits 'r' to form k+r.
- The location of each of the (k+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 2^0, 2^1, ... 2^{n-1}.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determined the position of an error.

Position of Redundant bits

- For example, a seven bit message data requires four redundant bits. Here, m =7, r= 4, n = m + r = 11.

- The redundant bits are placed in the positions 1,2,4 and 8. We refer these bits as r_1, r_2, r_3 and r_4.

- The r_1 is calculated using all the bit positions whose binary representation include a 1 in the *right most* position.

- The r_2 is calculated using all the bit positions whose binary representation include a 1 in the *second* position.

- The r_3 is calculated using all the bit positions whose binary representation include a 1 in the *third* position.

- The r_4 is calculated using all the bit positions whose binary representation include a 1 in the *forth* position.

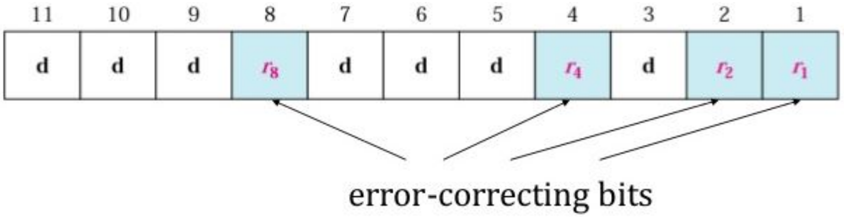


Figure 3.21: Position of Redundancy Bits.

Example: Consider the original message data 1001101 which is to be sent.

Then

At sender side

Total no. of data bits, $k = 7$

Number of redundant bits,r: $2^r \geq m + r + 1$ –> $2^4 \geq 7 + 4 + 1 = 12$ (*Satisfied*)

Therefore, the value of r is 4 that satisfied the above relation.

Total number of bits = m + r = 7 + 4 = 11

The value of r_1 is calculated as even parity of the bit position values at 1,3,5,7,9 and 11. The similar process is followed for $r_2.r_3$ and r_4. we get:

$r_1 = 1$, $r_2 = 0$, $r_3 = 0$, $r_4 = 1$

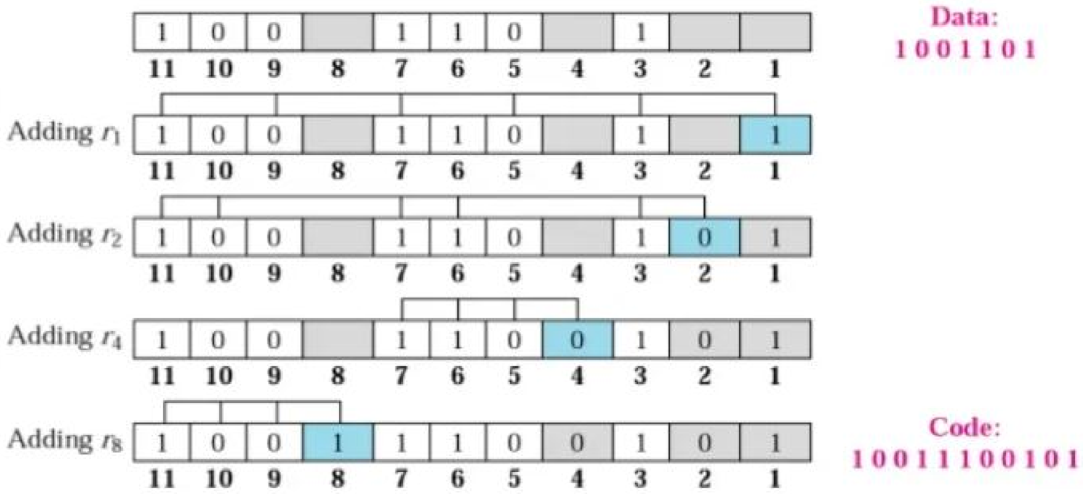


Figure 3.22: Example of redundacy bit calculation.

∴ Data transferred is 10011100101.

At Receiver Side:

- When a codeword arrives, the receiver redoes the check bit computations including the values of the received check bits. We call these the check results. If the check bits are correct then, for even parity sums, each check result should be zero. In this case the codeword is accepted as valid.

- If the check results are not all zero, however, an error has been detected. The set of check results forms the **error syndrome** that is used to pinpoint and correct the error.

- Suppose the 7^{th} bit is changed from 1 to 0 at the receiving end, then parity bit are recalculated as shown in figure 3.23.

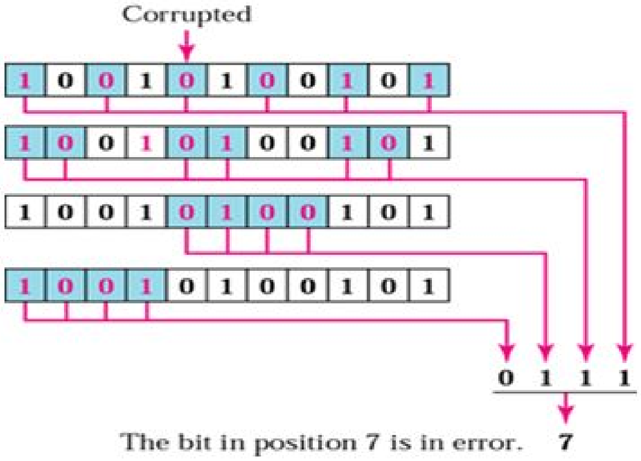


Figure 3.23: Error detection.

The corresponding decimal value of redundant bits 0111 is 7. Therefore, error is detected in 7^{th} bit position .i.e.
Received data = 10010100101
Errot bit = 7^{th}
Corrected bit: 1001**1**100101
Original message bit (removing redundant bit) = 1001101

Question: Check if error is detected if sender sends the message that is ASCII letter "A".

3.2.4 Flow Control

- Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data.
- The receiving entity buffers the received data before passing the data to the higher-level layer, and it has limited speed for processing.
- Therefore, when the receiving device's buffer tends to get full, it has to inform the sender to temporarily stop sending the data.
- In the absence of flow control, the receiver's buffer may fill up and overflow while it is processing old data.

- Two methods has been developed to control flow of data:

- Stop-and-Wait Flow Control
- Sliding Window Flow Control

3.2.4.1 Stop-and-Wait Flow Control

- It is the simplest form of flow control.
- In this protocol, the sender sends one frame, stops until it receives confirmation (**Acknowledgement Frame**) from the receiver, and then sends the next frame.
- Need half duplex link.

- Though this protocol is simple, it has a disadvantage of sending only one frame and has to wait for acknowledgement before sending next frame. There is no good use of transmission media.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.

3.2.4.2 Sliding Window Flow Control

- This protocol improves the efficiency of stop and wait protocol by allowing multiple frames to be transmitted before receiving an acknowledgement.

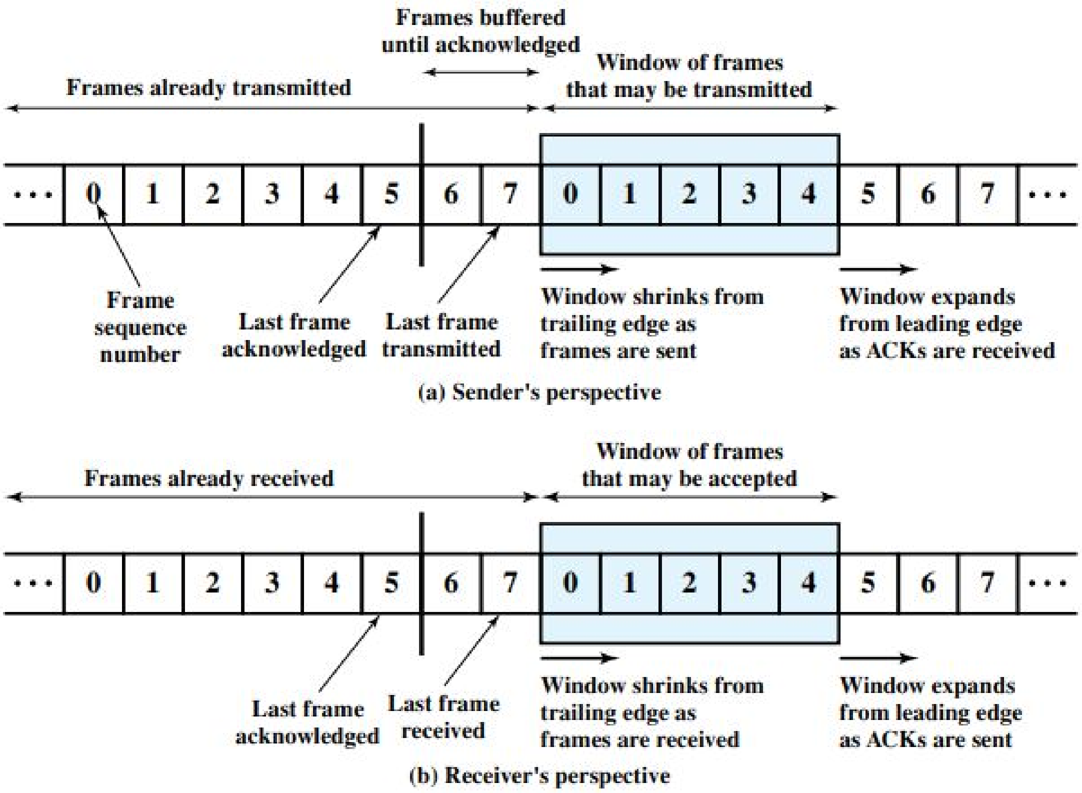

Frames buffered until acknowledged
Frames already transmitted
Window of frames that may be transmitted
... 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 ...
Frame sequence number
Last frame acknowledged
Last frame transmitted
Window shrinks from trailing edge as frames are sent
Window expands from leading edge as ACKs are received
(a) Sender's perspective
Frames already received
Window of frames that may be accepted
... 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 ...
Last frame acknowledged
Last frame received
Window shrinks from trailing edge as frames are received
Window expands from leading edge as ACKs are sent
(b) Receiver's perspective

Figure 3.24: Sliding Window Depiction.

- Figure 3.24 is an illustration of sliding window process. It assumes the use of a 3-bit sequence number, and window size of 5.

3.2.5 Error Control:ARQ

- Protocol in which the sender waits for a positive acknowledgement before advancing to the next frame are often called **ARQ (Automatic Repeat reQuest)** or **PAR (Positive Acknowledgement with Retransmission)**.
- It is an error-correction protocol that automatically initiates a call to retransmit any data frame after receiving flawed or incorrect data.
- When the transmitting device(sender) fails to receive an acknowledgement signal from receiver to confirm the data has been received, it usually retransmits the data after a predefined timeout and repeats the process a predetermined number of times until the transmitting device receives the acknowledgement.
- ARQs are often used to assure reliable transmissions over an unreliable service.
- Three version of ARQ have been standardized:

1. Stop and Wait ARQ
2. Go-Back-N-ARQ
3. Selective Repeat ARQ

3.2.5.1 Stop and Wait ARQ

- A stop-and-wait ARQ sender sends one frame at a time; it is a special case of the general sliding window protocol with both transmit and receive window sizes equal to 1.
- After sending each frame, the sender doesn't send any further frames until it receives an acknowledgement (ACK) signal. After receiving a good frame, the receiver sends an ACK. If the ACK does not reach the sender before a certain time, known as the timeout, the sender sends the same frame again.

- In stop-and-wait ARQ protocol, error correction is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.
- Data link layer adds the a field to the data frame to hold the sequence number of that frame.
- Also, when the frame is received by the receiver it need to send an acknowledgement frame to the sender. The acknowledgement number specifies the sequence number to be expected at the receiver.
- Sequence number and acknowledgement number are based on modulo-2 arithmetic. i.e. 1 bit is used either 0 and 1.

- Two sorts of errors could occur:
i. Error in Data Frame
ii. Error in Acknowledgement

Error in Data Frame

- First, the frame that arrives at the destination could be damaged.
- The receiver detects this by using the error-detection technique referred to earlier and simply discards the frame.
- To account for this possibility, the source station is equipped with a timer.

  - After a frame is transmitted, the source station waits for an acknowledgment.
  - If no acknowledgment is received by the time that the timer expires, then the same frame is sent again.

Error in Acknowledgement

- When acknowledgement frame send by receiver get lost, the sending device after timeout, resends the frame again.
- To avoid the receiving of duplicate frames, frames are number with sequence number of 1 bit i.e. 0 or 1.

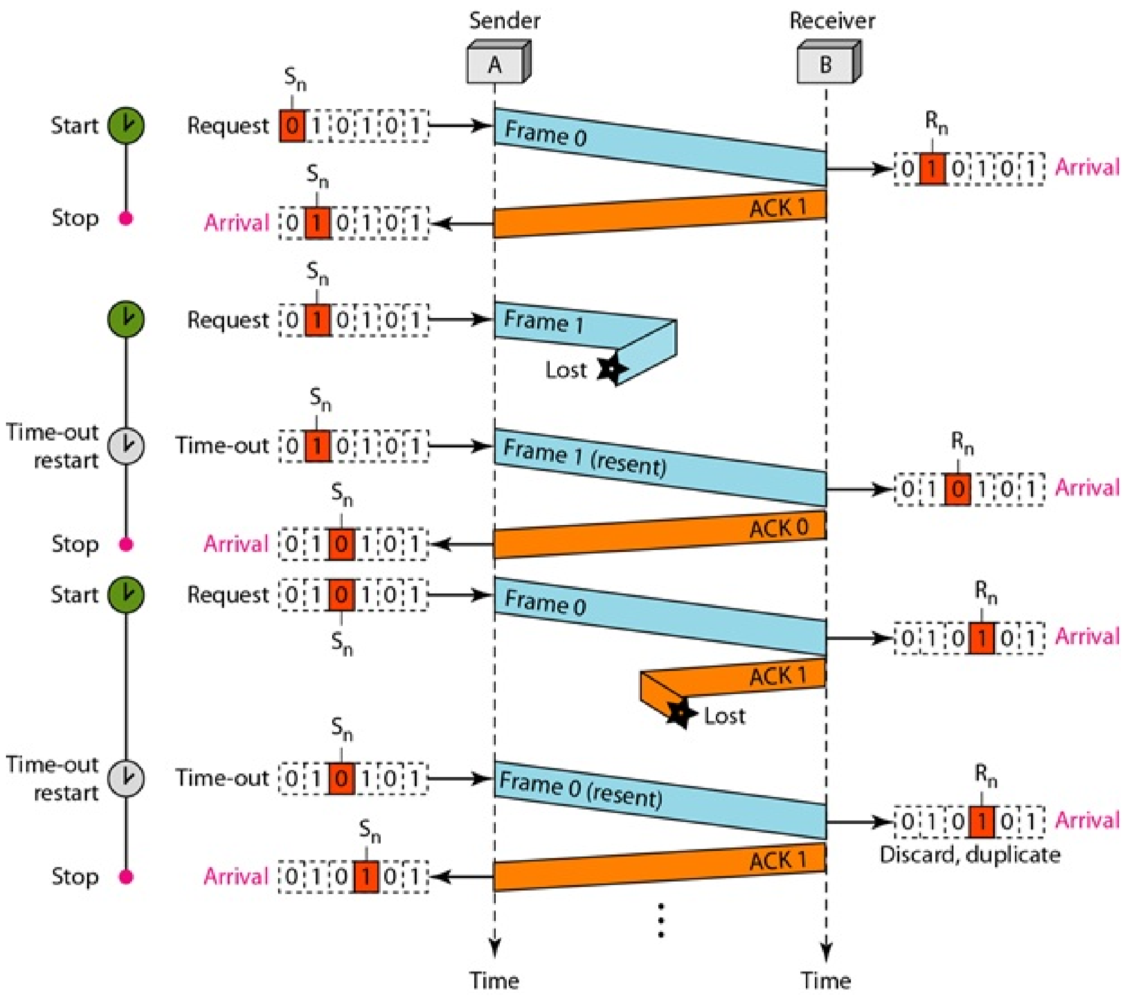


Figure 3.25: Stop-and-wait ARQ.

Piggybacking:- It is a method to combine a data frame with an acknowledgement.

The principal advantage of stop-and-wait ARQ is its simplicity. Its principal disadvantage is bandwidth wastage. The sliding-window flow control technique can be adapted to provide more efficient line use; in this context, it is sometimes referred to as *continuous ARQ*.

Sliding window

- Sliding window ARQ is a technique used for multiple transmission of frames for efficient use of line.

- It is an abstract concept that defines the range of sequence number that is concern of the sender and receiver.

- The range which is the concern of the sender is called the **send sliding window**.

- The range that is concern of the receiver is called the **receive sliding window**.

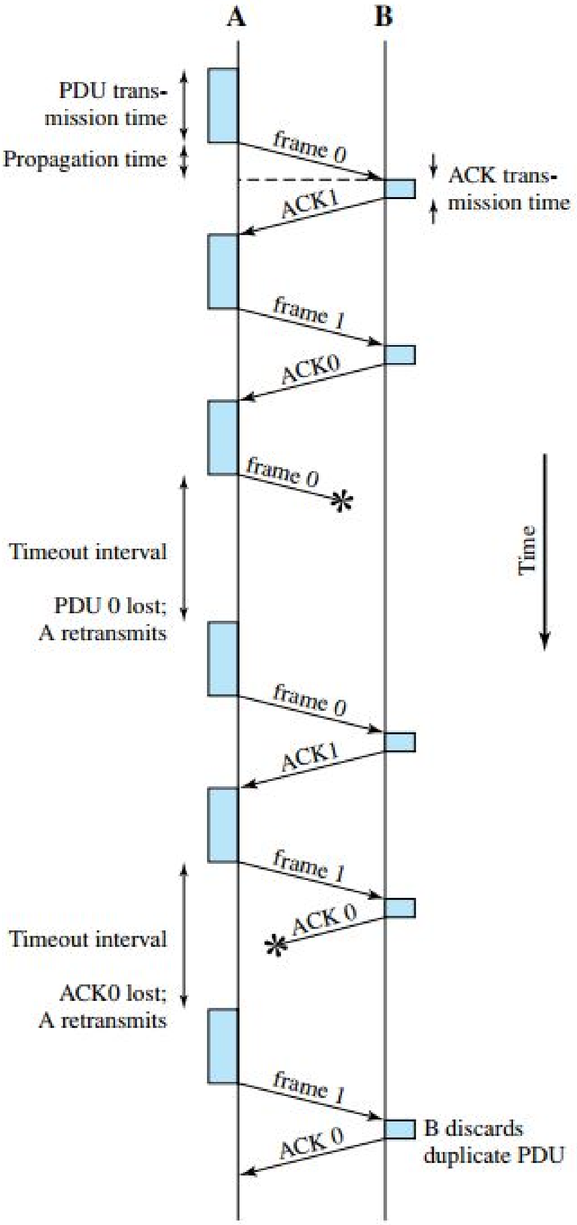


Figure 3.26: Stop-and-wait ARQ.

3.2.5.2 Go-Back-N ARQ

- Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) frame from the receiver.

- It is a special case of the general sliding window protocol with the transmit window size of *N* and receive window size of *1*.

Sequence Number

- If the data link layer adds *m* bit sequence number to each frame then, the sequence number range from 0 to $2^m - 1$.

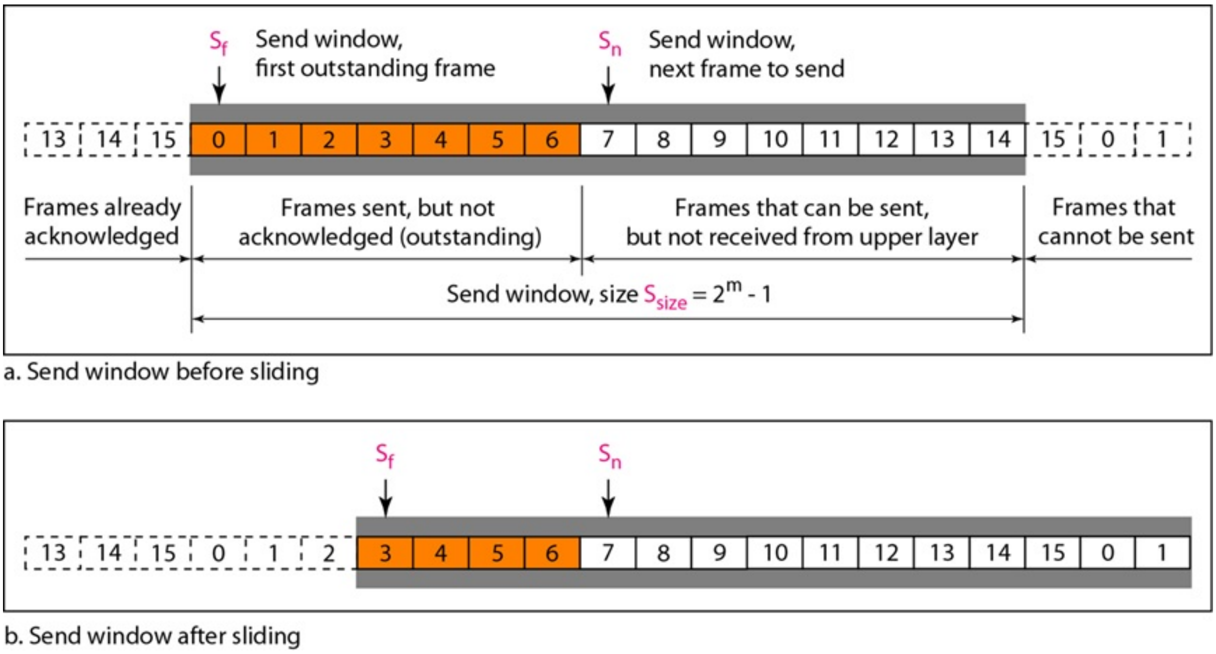

S_f
Send window, first outstanding frame
S_n
Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size S_size = 2^m - 1
a. Send window before sliding
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
b. Send window after sliding

Figure 3.27: Send window for Go-Back-N ARQ.

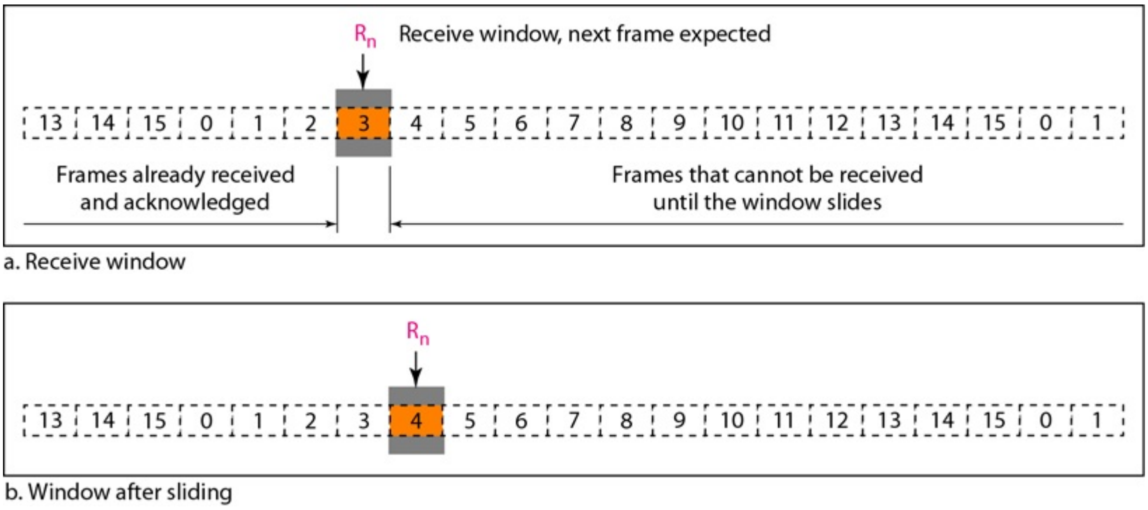
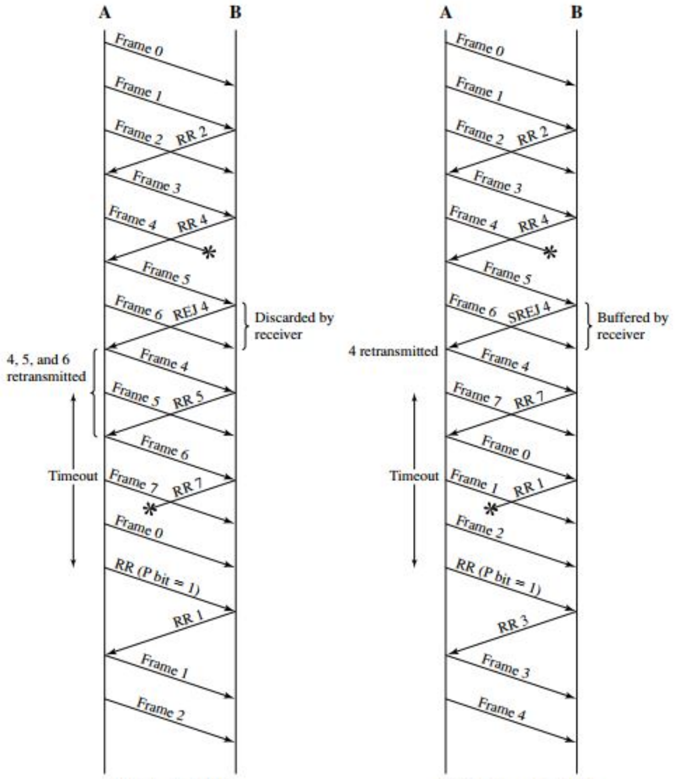


Figure 3.28: Receive window for Go-Back-N ARQ.

- For example: if m=4, the only sequence numbers are 0 to 15 inclusive.

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

- The sequence number are modulo-2^m.
- It has two types of acknowledgement frames in the scenario:
i. RR (Received Ready)
- It like the positive acknowledgement.
- When all frames upto i^{th} frame is received, receiver with send RR i+1, and after that sender will receive RR i+1 frame, then it sends i+2 frame.



(a) Go-back-N ARQ

(b) Selective-reject ARQ

Figure 3.29: Sliding window ARQ protocols.

ii. REJ(Reject)

- It is like negative acknowledgement.
- REJ i is send and sender will resend the frames starting from i.

3.2.5.3 Selective Request

- Also called selective Reject ARQ (SREJ)
- SREJ used as negative ACK.
- With selective-reject ARQ, the only frames retransmitted are those that receive a negative acknowledgment, in this case called SREJ, or those that time out.
- It appears to be more efficient than go-back-N, because it minimizes the amount of retransmission.
- The receiver must maintain a buffer large enough to hold damaged frames until the frame in error is retransmitted and must contain logic for reinserting that frame in the proper sequence.

- The transmitter, too, requires more complex logic to be able to send a frame out of sequence. Because of such complications, select-reject ARQ is much less widely used than go-back-N ARQ. Selective reject is a useful choice for a satellite link because of

the long propagation delay involved.
- It's send window and receive window are of same size; however the size of the sender and receiver window must be at most one-half of 2^m.

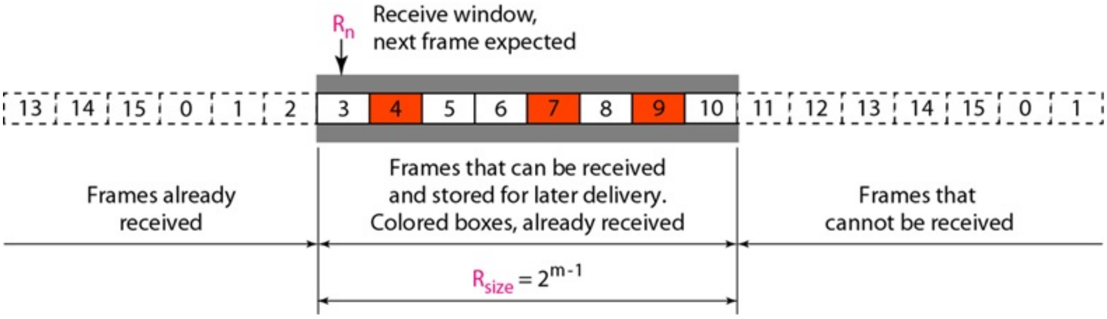

R_n
Receive window, next frame expected
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already received
Frames that can be received and stored for later delivery. Colored boxes, already received
Frames that cannot be received
$R_{size} = 2^{m-1}$

Figure 3.30: Receive window for selective repeat ARQ.

Overlapping windows

- We have to make sure that there is no overlap between the two windows that may cause error.
- Error can occur when retransmitted frames can look like new frame. - To ensure there is no overlap, the number of frames should be, at most, 1/2 of the range of sequence numbers,

3.3 Example Data Link Protocol

3.3.0.1 HDLC

- HDLC stands for High-Level Link Control. - It is mostly used in data link control protocol. - It is a bit oriented protocol for communication over point-to-point and multipoint links.
- HDLC is a synchronous Data Link bit oriented protocol developed by International Organization for Standardization (ISO).
- HDLC provides both connection-oriented and connectionless service.
- HDLC provides synchronous serial transmission to provide error free communication between two points.
- HDLC defines layer 2 framing structure that allows flow control and error-control through use of acknowledgement.
- HDLC defines:

- Three types of stations,
- Two link configurations, and
- Three data transfer modes

Station Types: i. Primary Station

- Responsible to control the operation of link
- Frames issued by primary are called commands.

ii. Secondary Station
- Operates under the control of the primary station.
- Frames issued by a secondary are called responses.

ii . Combined Station
- Combines the features of primary and secondary.
- A combined station may issue both commands and responses.

Link Configuration

i. Unbalanced configuration
- Consists of one primary and one or more secondary stations and supports both full-duplex and half-duplex transmission.

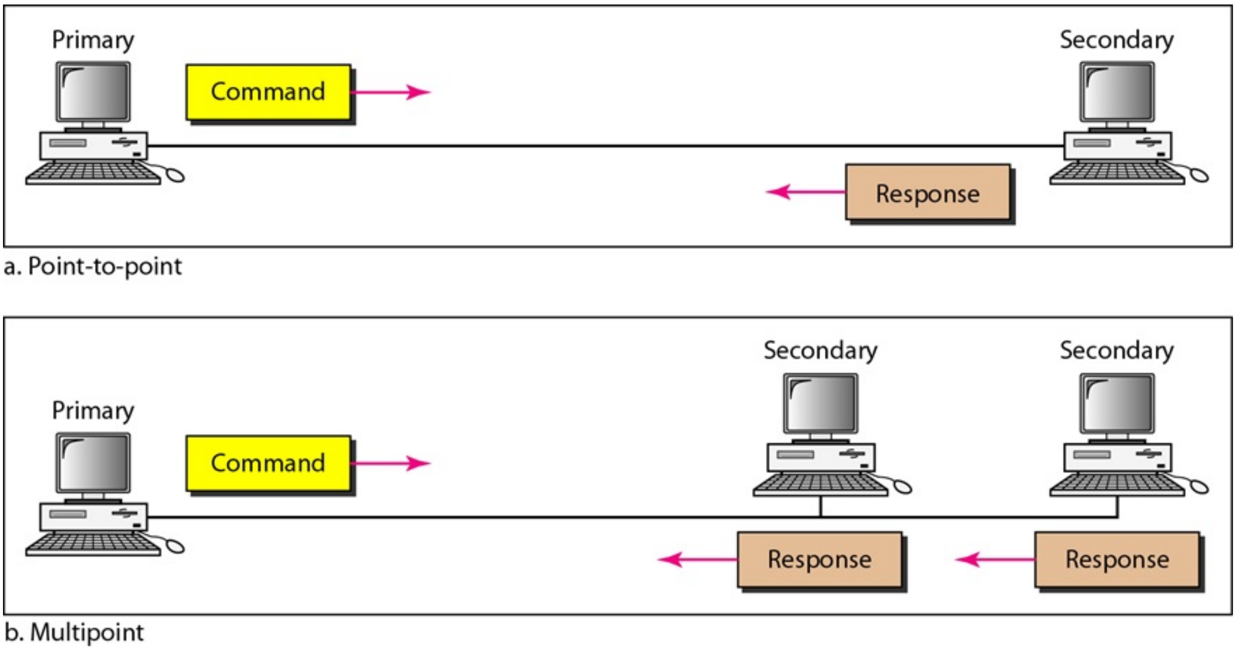
ii. Balanced configuration
- Consists of two combined stations and supports both full-duplex and half-duplex transmission.

Data Mode

i. Normal Response Mode (NRM)
- Used with an unbalanced configuration.
- The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary.

ii. Asynchronous Balanced Mode (ABM)
- Used with a balanced configuration.
- Either combined station may initiate transmission without receiving permission from the other combined station.
- Mostly used.

iii. Asynchronous Response Mode (ARM)
- Used with an unbalanced configuration.
- The secondary may initiate transmission without explicit permission of the primary.
- The primary still retains responsibility for the line, including initialization, error recovery, and logical disconnection.
- Rarely used.



a. Point-to-point

b. Multipoint

Figure 3.31: Normal response mode.

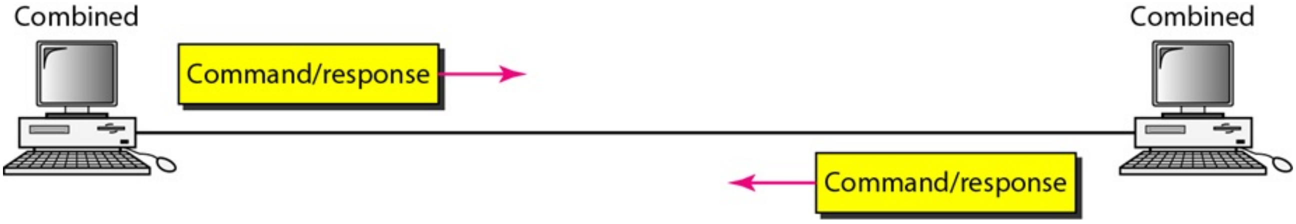
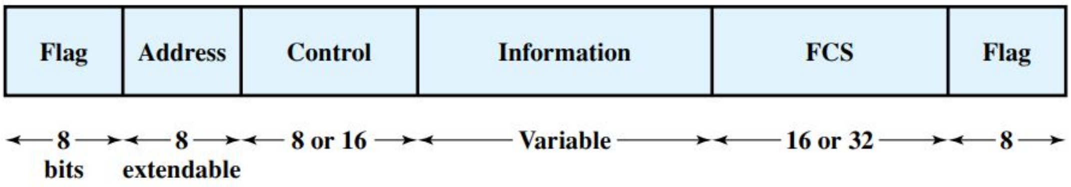


Figure 3.32: Asynchronous balanced mode.

HDLC frame format



Flag	Address	Control	Information	FCS	Flag
8 bits	8 extendable	8 or 16	Variable	16 or 32	8

Figure 3.33: HDCL frame format.

Figure 3.33 shows the frame format of HDLC. The flag, address, and control fields that precede the information field are known as a **header**. The FCS and flag fields following the data field are referred to as a **trailer**.

There are three types of HDLC frame format. They are:

1. Information frames (I-frames)
   - used to transmit user data and control information (piggybacking).

2. Supervisory frames (S-frames)

   - Used to transmit only control information

3. Unnumbered frames (U-frames)

   - Reserved for system maintenance (link management).

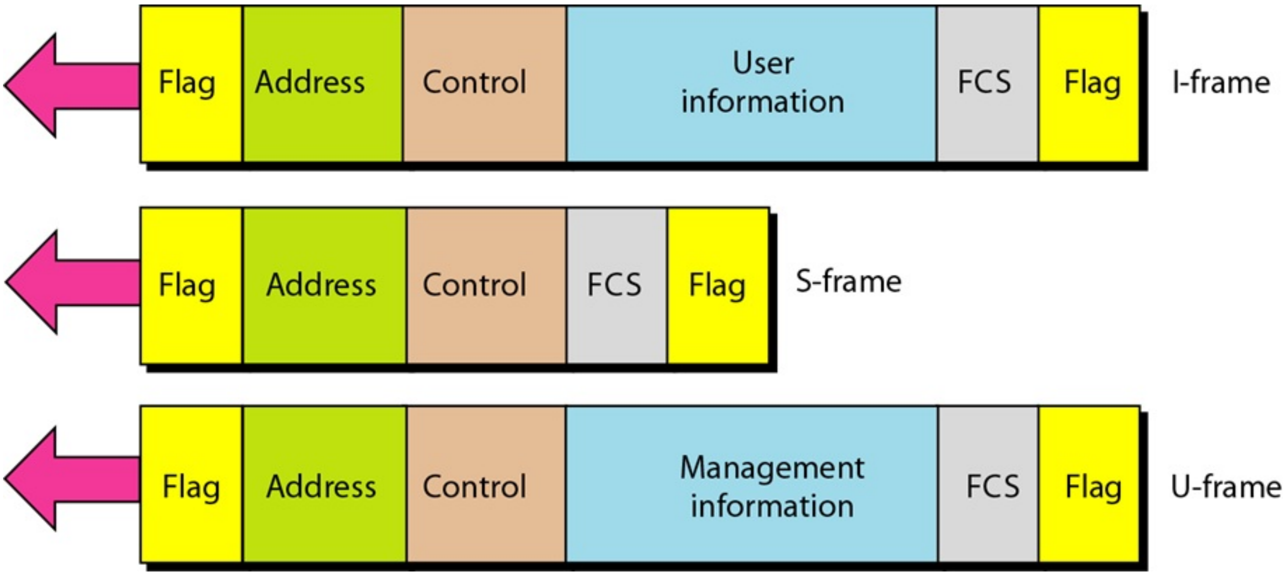


Figure 3.34: HDCL frame types.

3.3.1 Point-to-Point Protocol

- Although HDLC is a general protocol that can be used for both point-to-point and multipoint configurations, one of the most common protocols for point-to-point access is the **Point-to-Point Protocol (PPP)**.

- PPP is a byte-oriented protocol.

- PP uses set of protocols to establish the link, authenticate the parties involved, and carry the network-layer data. Three sets of protocols are defined to make PPP powerful: the Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs).

- It is used to connect the home PC to the ISP server.

- It provides error detection.

PPP provides several services:

- PPP defines the format of the frame to be exchanged between devices.
- PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP defines how network layer data are encapsulated in the data link frame.
- PPP defines how two devices can authenticate each other.

- PPP provides multiple network layer services supporting a variety of network layer protocols.
- PPP provides connections over multiple links.
- PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

PPP does not provide following service:

1. PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
2. PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.
3. PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration

Framing

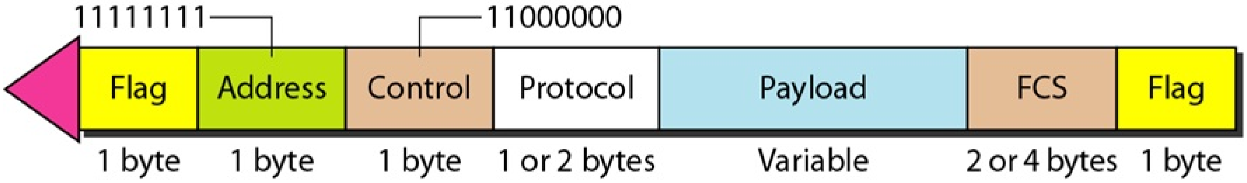


Figure 3.35: PPP frame format.

Figure 3.35 shows the frame format of PPP.

- **Flag**: It indicates the start and end of frame. Flag byte is 01111110. Although this patter is same as that of HDCL, HDLC is bit-oriented while PPP is byte oriented.

- **Address**: It contains the constant value of 11111111, which means all the station can accept the frame.

- **Control**: It is set to constant value of 11000000. This shows that the frame doesnot contain any sequence number and there is no flow control or error control.

- **Protocol**: It defines what is being carried in the data field : either user data or other information.

- **Payload field**: It length is variable. It carries user data or other information.

- **FCS**: It stands for frame check sequence. It contains checksum. It is either 2 bytes or 4 bytes.

PPP stack
- PPP uses several other protocols to establish the link, authenticate the parties involved, and carry the network layer data.
- Three protocols are used. They are:

- **Link Control Protocol**
  - It is responsible for establishing, maintaining, configuring, and terminating links.
  - All LCP packets are carried in the payload field of the PPP frame with the protocol field set to C021 in hexadecimal.
- **Authenticate Protocol**
  - Authentication plays a very important role in PPP because PPP is designed for use over dial-up links where verification of user identity is necessary.
  - Authentication means validating the identity of a user who needs to access a set of resources.
  - PPP has created two protocols for authentication: Password Authentication Protocol and Challenge Handshake Authentication Protocol
- **Network Control Protocol**
  - After establishing the link and authenticating the user, PPP connects to the network layer.
  - This connection is established by NCP.
  - Therefore, NCP is a set of control protocols that allow the encapsulation of the data coming from the network layer.
  - After the network layer configuration is done by one of the NCP, the user can exchange data from the network layer.

3.4 The Medium Access Control Sub-Layer

- The data link layer is divided into two sub-layer:

1. Logic Link Control (LLC) Layer
   - Defined by IEEE 802.2 Standard
   - LLC provides framing, flow control, acknowledgement and error control
2. Media Access Control (MAC) Layer
   - It provides physical addressing and channel access control mechanism

3.5 The Channel Allocation Problem

- In broadcast channel (i.e. also called multiaccess channel or random access channel), a single channel is shared by several stations.
- This channel can be allocated to only one transmitting user at a time. So, a mechanism is need to allocate a single broadcast channel among competing users.
- There are two different methods of channel allocations:

- Static Channel Allocation
- Dynamic Channel Allocation

3.5.0.1 Static Channel Allocation

- In this method, a single channel is divided among various users either on the basis of frequency or on the basis of time.
- It either use FDM or TDM.
- A static channel allocation is poor fit to the computer system, in which data traffic is extremely bursty.

3.5.0.2 Dynamic Channel Allocation

- In this method, no user is assigned fixed frequency of fixed time slot.
- All users are dynamically assigned frequency or time slots, depending upon the requirements of the user.

Assumptions for Dynamic Channel Allocation

1. **Independent Traffic**
   - The model consists of N independent stations (e.g., computers, telephones), each with a program or user that generates frames for transmission.
2. **Single Channel**
   - A single channel is available for all communication. All stations can transmit on it and all can receive from it. The stations are assumed to be equally capable, though protocols may assign them different roles (e.g., priorities).
3. **Observable Collisions**
   - All stations can detect that a **collision** has occurred.
4. **Continuous or Slotted Time**
   - Time may be assumed continuous, in which case frame transmission can begin at any instant. Alternatively, time may be slotted or divided into discrete intervals (called slots).
5. **Carrier Sense or No carrier Sense**
   - With the carrier sense assumption, stations can tell if the channel is in use before

trying to use it. No station will attempt to use the channel while it is sensed as busy.

3.6 Multiple Access Protocol

- MAC protocols are distribute algorithms that determine how nodes can access the shared channel to transmit the data.
- It is classified into four categories as shown in figure 3.36.

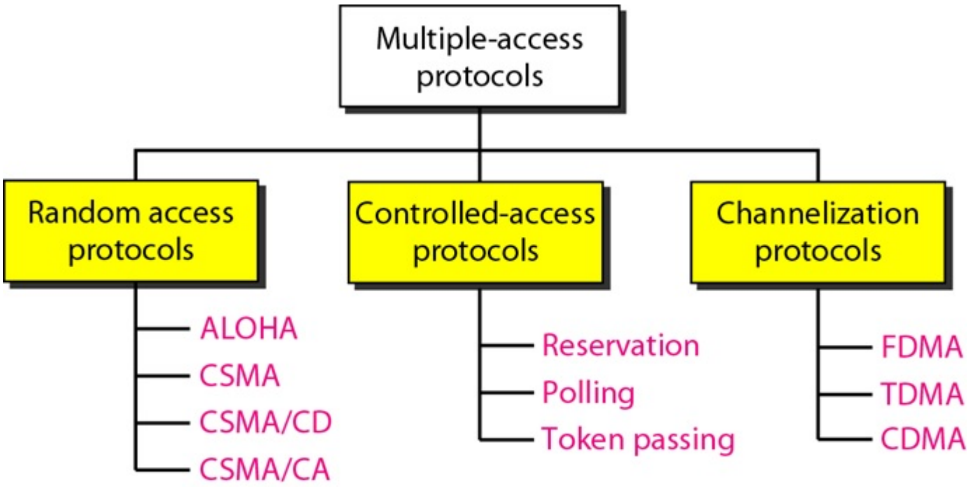


Figure 3.36: Media access protocols.

3.6.1 Random Access Method

- It is also called contention method.
- In this method, all stations have equal priority to send frame over the channel and no stations have control over another stations.
- At each instance, a stations that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. The decision is based on the state of medium, *busy* or *idle*.

Two features of this protocol

- There is no schedule time for a station to transmit. Transmission is random among the stations. Hence, named **random access**.
- No rules specify which station should send next. Stations compete with each another to access the medium. Hence, the name **contention method**.

- The various random access method are:

1. ALOHA

   (a) Pure ALOHA

   (b) Slotted ALOHA

2. Carrier Sense Multiple Access
3. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
4. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

3.6.1.1 ALOHA

- In the ALOHA system, a node transmits whenever data is available to send.
- If packet is received correctly, the base station transmit an acknowledgement.
- If no acknowledgement is receive:

- It assumes the packet to be lost
- It retransmit the packet packet after waiting a *random time*.

- If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost.
- There are two versions of ALOHA:

1. ALOHA
2. Slotted ALOHA

Pure ALOHA
- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost.
- Collision is said to be occurred when the first bit of the new frame overlaps with the last bit of another frame.
- If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

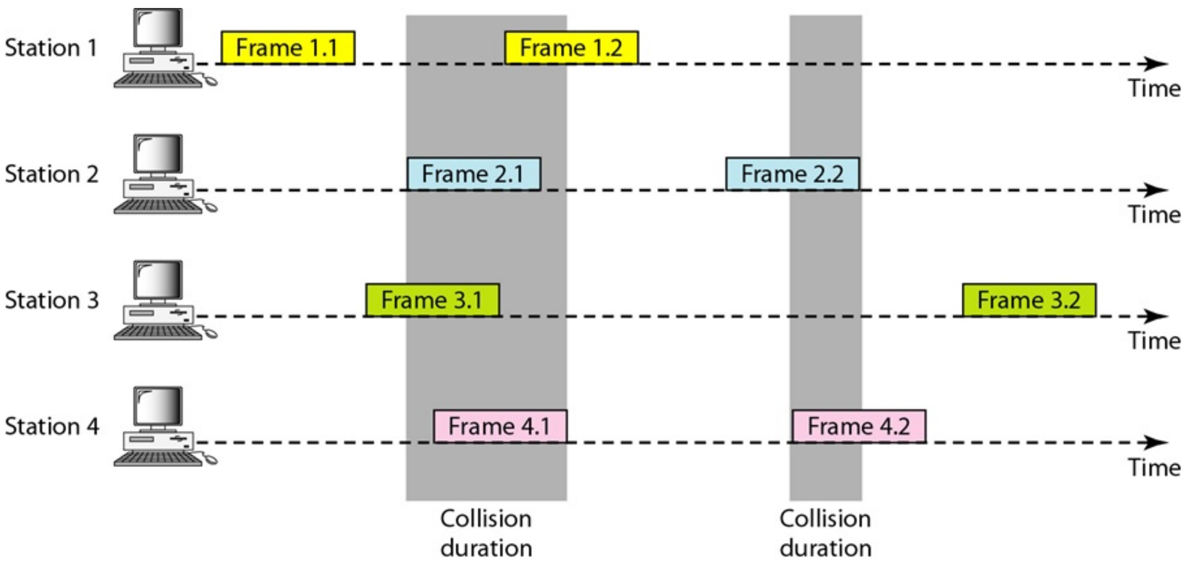


Figure 3.37: Collision in pure ALOHA network.

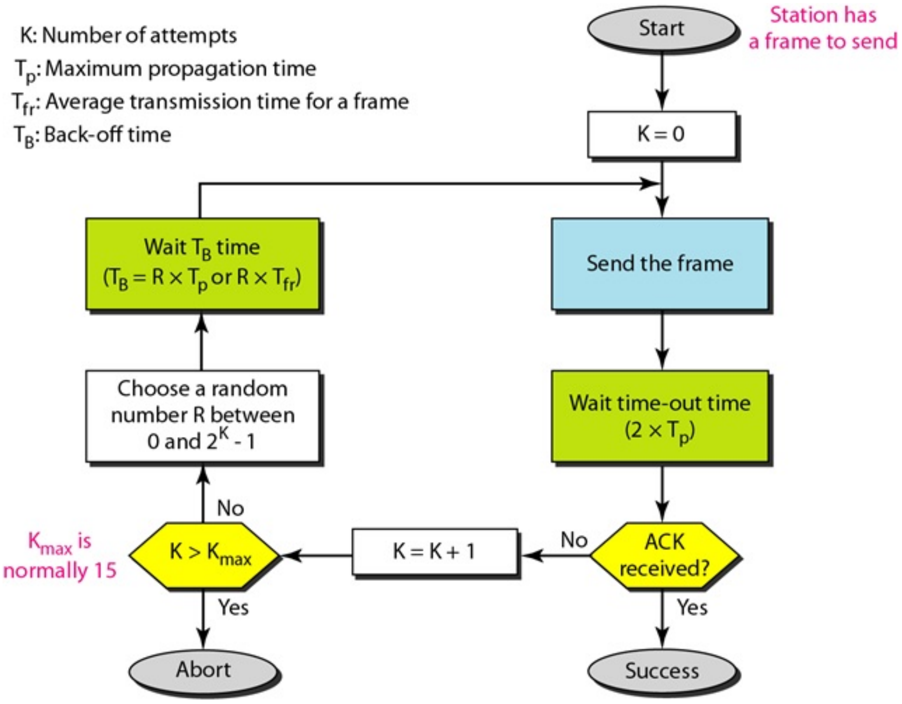

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Start
Station has a frame to send
K = 0
Send the frame
Wait time-out time ($2 \times T_p$)
ACK received?
No
Yes
Success
K = K + 1
$K > K_{max}$
K_{max} is normally 15
No
Yes
Abort
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)

Figure 3.38: Procedure for pure ALOHA protocol.

Vulnerable Time:

- It is the length of time, in which there is possibilty of collision.

- Vulnerable time of pure ALOHA = $2 \times T_{fr}$.

where,

T_{fr} = time to send a fixed-length frame by a station.

Throughput for pure ALOHA = $G \times e^{-2G}$

where,

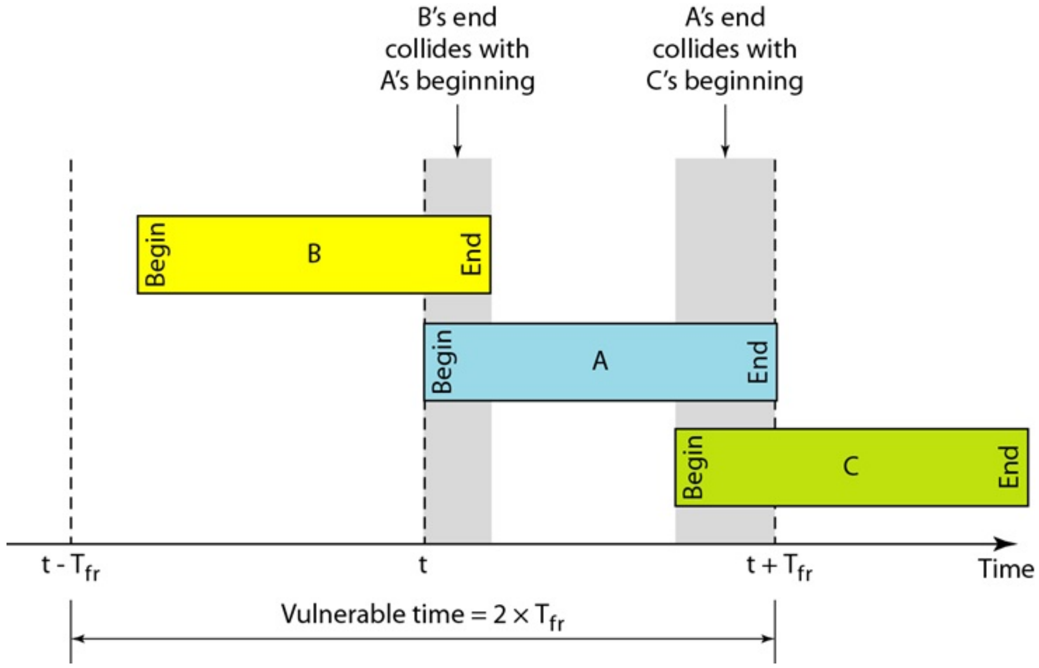


Figure 3.39: Vulnerable time for pure ALOHA protocol.

G = average no. of frames generated by the station in one frame transmission time.

- Maximum S = 0.184 when $G = 1/2$
- That is if one-half frame is generated in one frame transmission time (in other word, one frame in two transmission time) then, 18.4 percent of these frame can reach the destination successfully.

Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots. Figure 3.40.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in figure above.
- Vulnerable time for slotted ALOHA = T_{fr}.
- Throughput, $S = G \times e^{-2G}$, S_{max} = .368 when G = 1.

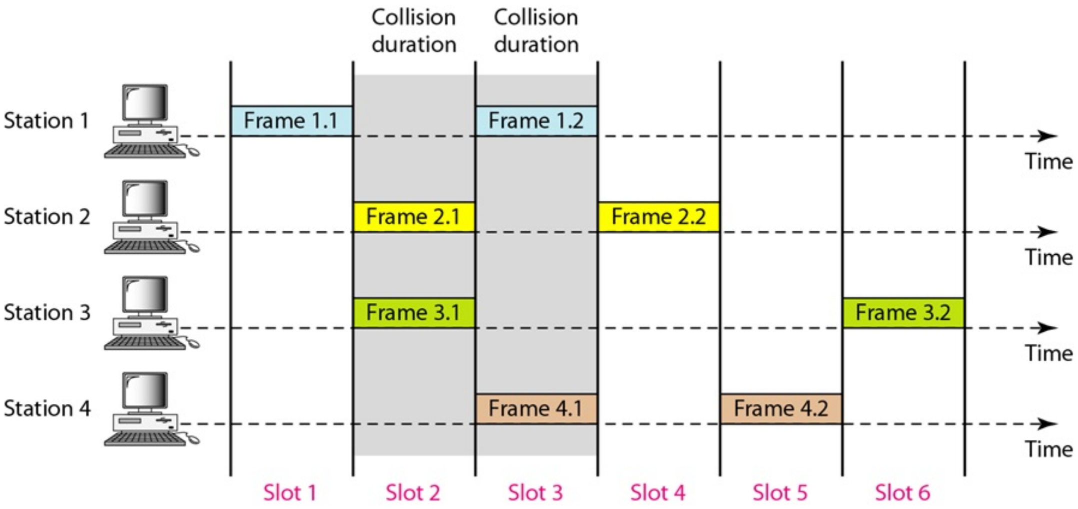


Figure 3.40: Frames in a slotted ALOHA network.

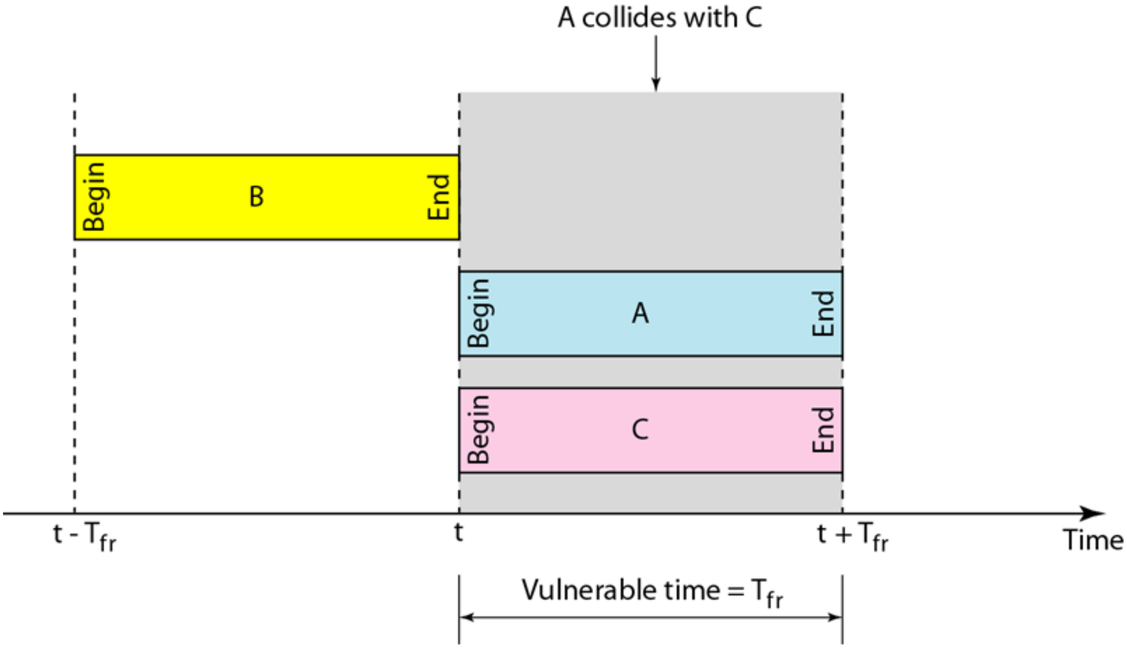


Figure 3.41: Vulnerable time for slotted ALOHA protocol.

That is, if one frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination success.

3.6.1.2 CSMA

- CSMA protocol was developed to overcome the problem found in ALOHA i.e. to minimize the chances of collision, so as to improve the performance.
- CSMA protocol is based on the principle of 'carrier sense'. The station senses the carrier or channel before transmitting a frame. It means the station checks the state of channel, whether it is idle or busy.
- Even though devices attempt to sense whether the network is in use, there is a good chance that two stations will attempt to access it at the same time.

- The chances of collision still exist because of propagation delay. The frame transmitted by one station takes some time to reach other stations. In the meantime, other stations may sense the channel to be idle and transmit their frames. This results in the collision.
- There are three different types of CSMA protocols:

- 1-persistent CSMA
- Non-persistent CSMA
- P-persistent CSMA

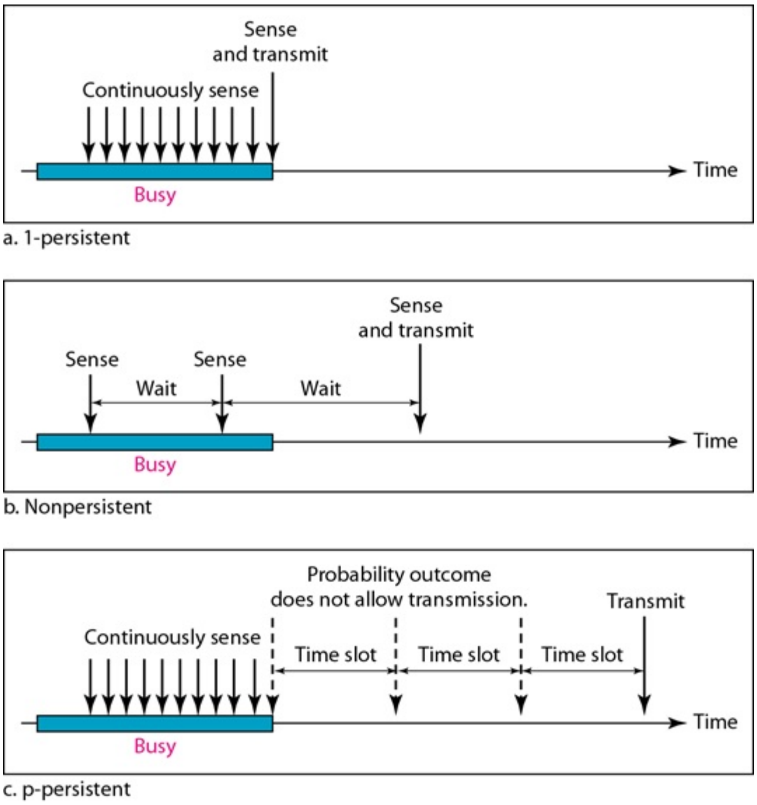


Figure 3.42: Behavior of three persistence methods.

1-Persistent CSMA

- In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, the station waits until it becomes idle.
- When the station detects an idle-channel, it immediately transmits the frame with probability 1. Hence it is called 1-persistent CSMA.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
- When the collision occurs, the stations wait a random amount of time and start all over

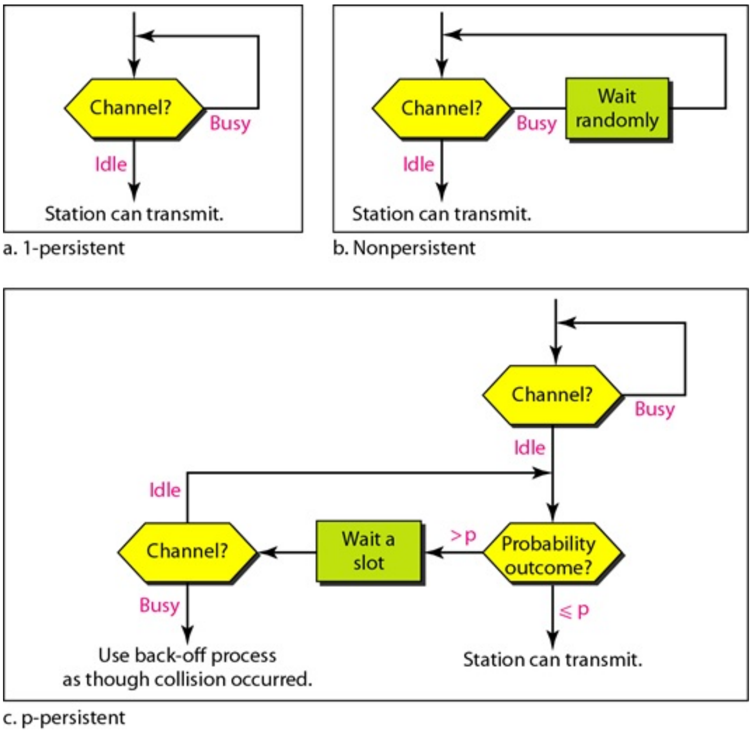


Figure 3.43: Flow diagram of three persistence method.

again.

Non-Persistent CSMA

In this method: - A station that has a frame to send senses the channel.

- If the channel is idle, it sends immediately.

- If the channel is busy, it waits a random amount of time and then senses the channel again. This waiting of random amount of time reduces the chances of collision.

- It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

P-Persistent Method

- This method is used when channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.

- Whenever a station becomes ready to send, it senses the channel.

- If channel is busy, station waits until next slot.

- If channel is idle, it transmits with a probability p.

-With the probability q=1-p, the station then waits for the beginning of the next time slot.

- If the next slot is also idle, it either transmits or waits again with probabilities p and q.

- This process is repeated till either frame has been transmitted or another station has begun transmitting.

- In case of the transmission by another station, the station acts as though a collision has occurred and it waits a random amount of time and starts again.

3.6.1.3 CSMA/CD

- Carrier Sense Multiple Access with Collision Detection - It is the modification of pure CSMA.
- It is MAC protocol that defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The CSMA/CD rules define how long the device should wait if a collision occurs.

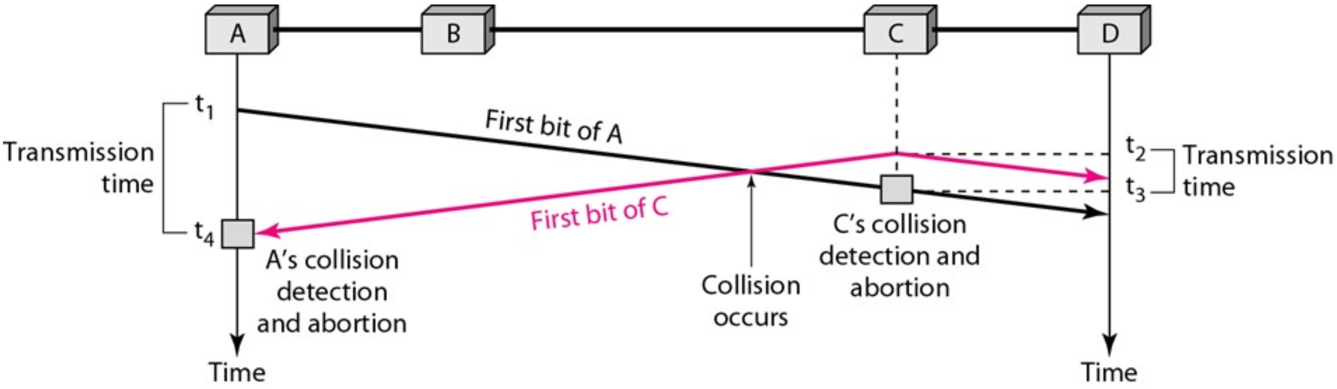


Figure 3.44: Collision Detection and abortion.

Main Procedure

The following procedure is used to initiate a transmission. The procedure is complete when the frame is transmitted successfully or a collision is detected during transmission.

1. Is my frame ready for transmission? If yes, it goes on to the next point.
2. Is medium idle? If not, wait until it becomes ready.
3. Start transmitting and monitor for collision during transmission.
4. Did a collision occur? If so, go to collision detected procedure.
5. Reset retransmission counters and end frame transmission.

Collision Detection Procedure

The following procedure is used to resolve a detected collision. The procedure is complete when retransmission is initiated or the retransmission is aborted due to numerous collisions.

1. Continue transmission (with a jam signal instead of frame header/data/CRC) until minimum packet time is reached to ensure that all receivers detect the collision
2. Increment retransmission counter
3. Was the maximum number of transmission attempts reached? If so, abort transmission.

4. Calculate and wait random backoff period based on number of collisions.
5. Re-enter main procedure at stage 1.

Jam Signal

The jam signal or jamming signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations of the collision and that they must not transmit.

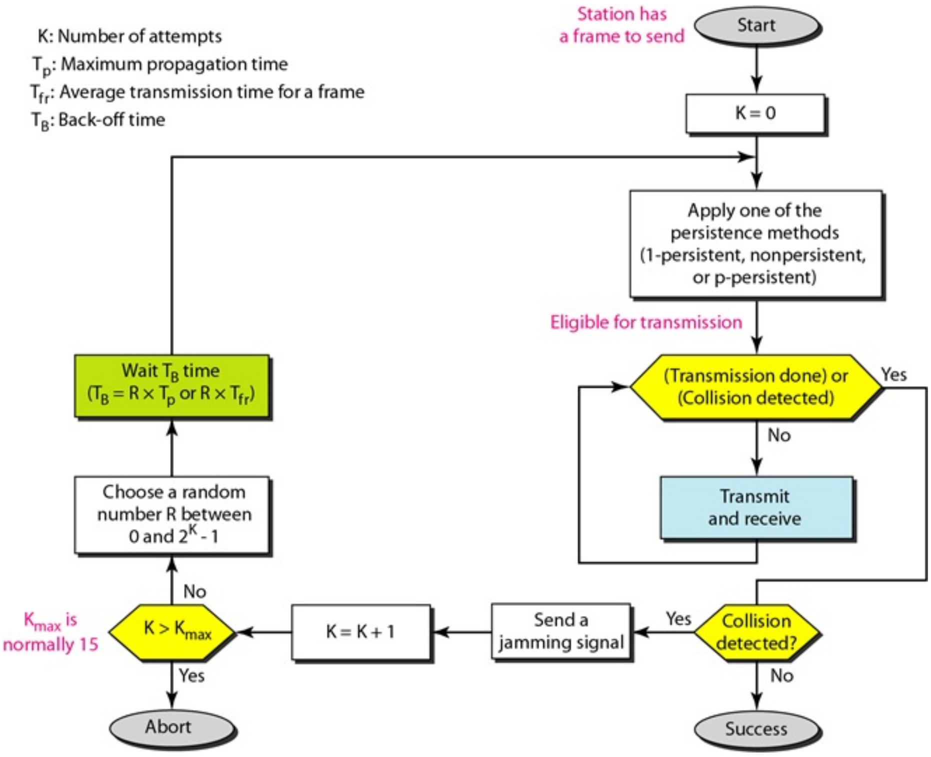

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Choose a random number R between 0 and $2^K - 1$
No
K_{max} is normally 15
$K > K_{max}$
Yes
Abort
K = K + 1
Send a jamming signal
Yes
Collision detected?
No
Success

Figure 3.45: Flow diagram for the CSMA/CD.

Energy Level

Energy level in a channel can have three levels: zero, normal and abnormal.

- At the zero level, the channel is idle.

- At the normal level, the station has successfully captured the channel and is sending its frame.

- At the abnormal level, there is a collision and the level of energy is twice the normal level.

A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy or in collision mode.

3.6.1.4 CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance.

- CSMA/CA is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle“.

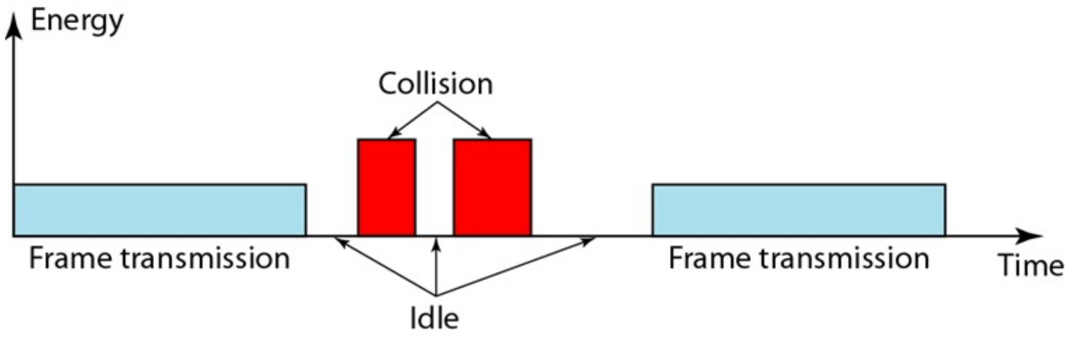


Figure 3.46: Energy level during transmission, idleness, or collision.

- CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.
- CSMA/CA avoids the collisions using three basic techniques.

i. Inter-frame space
ii. Contention Window
iii. Acknowledgements

Inter-frame Space

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that some distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.
- If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.
- IFS variable can also be used to define the priority of a station or a frame.

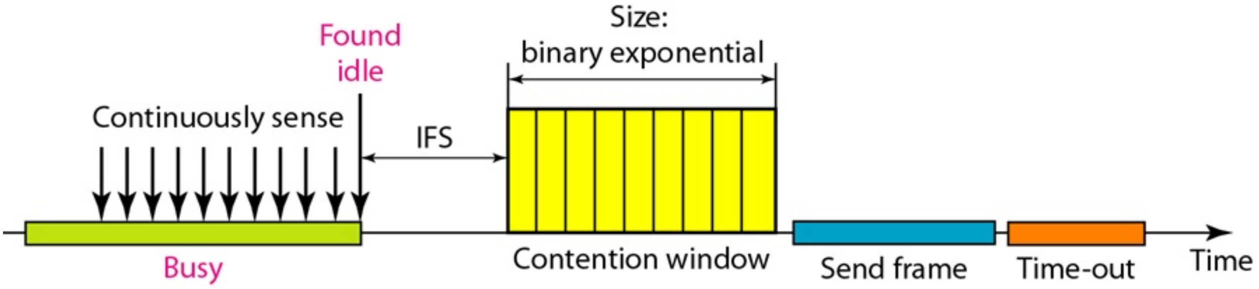


Figure 3.47: Timing in CSMa/CA.

Contention Window

- Contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential backoff strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.
- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- In contention window the station needs to sense the channel after each time slot.
- If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

Acknowledgement

- Despite all the precautions, collisions may occur and destroy the data.
- The positive acknowledgement and the time-out timer can help guarantee that receiver has received the frame.

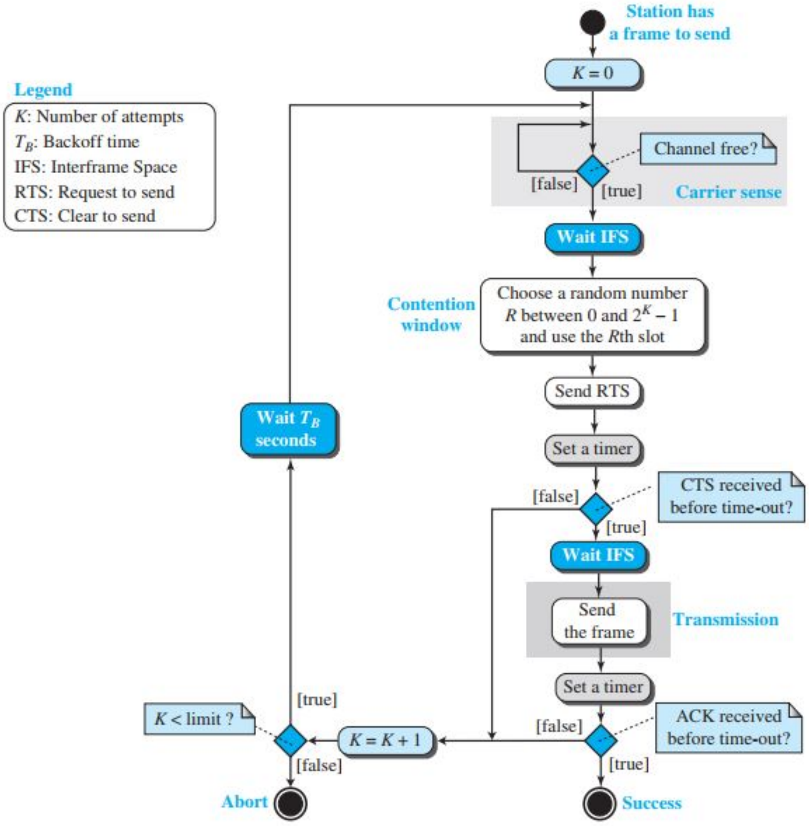


Figure 3.48: Flow diagram for the CSMA/CA.

Figure 3.49 shows the exchange of data and control frames in time.

1. Before sending a frame, the source station senses the medium by checking the

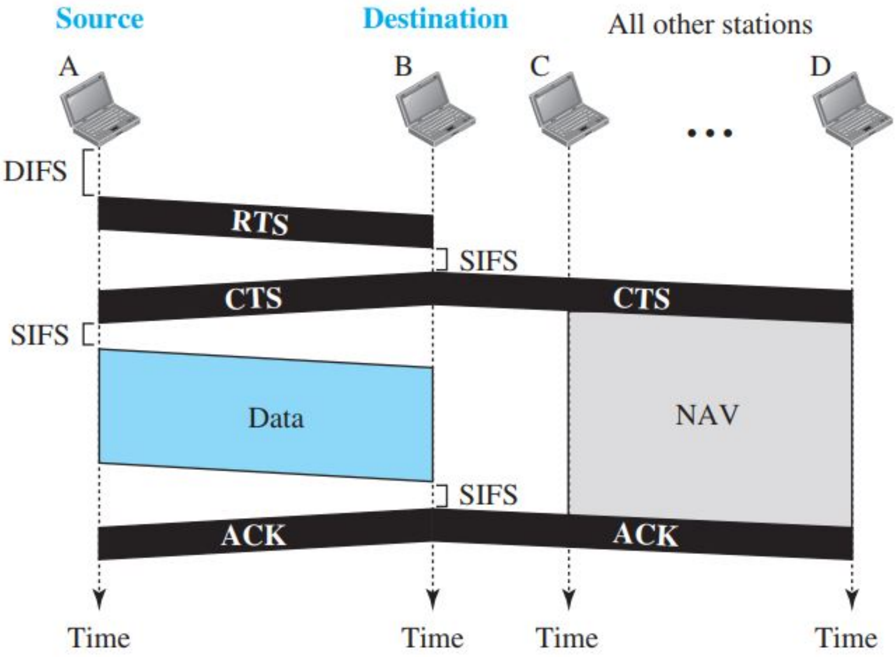


Figure 3.49: CSMA/CA and NVA.

energy level at the carrier frequency.

(a) The channel uses a persistence strategy with backoff until the channel is idle.

(b) After the station is found to be idle, the station waits for a period of time called the DCF interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived.

Network Vector Allocation (NVA)

How do other stations defer sending their data if one station acquires access? In other words, how is the collision avoidance aspect of this protocol accomplished? The key isa feature called **NAV**.

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired. Figure 3.49 shows the idea of NAV.

3.6.2 Contention Method

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

1. Reservation
2. Polling
3. Token Passing

Reservation

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

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

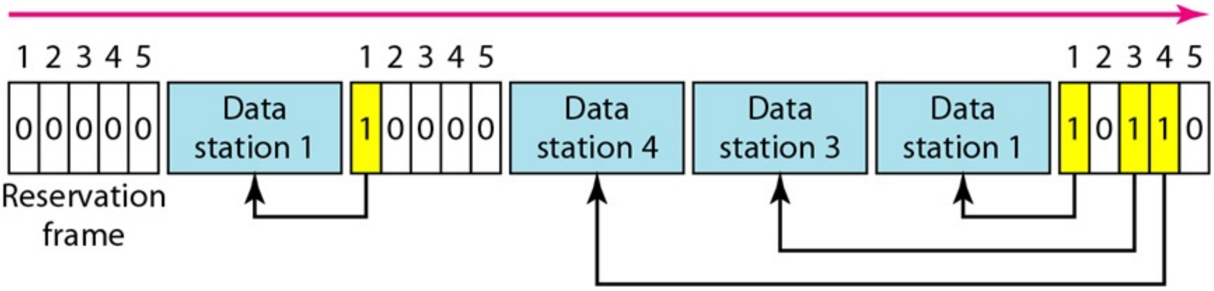


Figure 3.50: Figure showing a situation with five stations and a minislots reservation frame.

Polling

- Polling works with topologies in which one device is designated as a primary station

and the other devices are secondary stations.
- All the data exchange is done through primary station. - The primary device controls the link; the secondary devices follow its instruction.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.
- The primary device is always the initiator of a session.
- This method uses *poll* and *select* functions to prevent collisions.
- The drawback of this method is that the system goes down if the primary station fails.

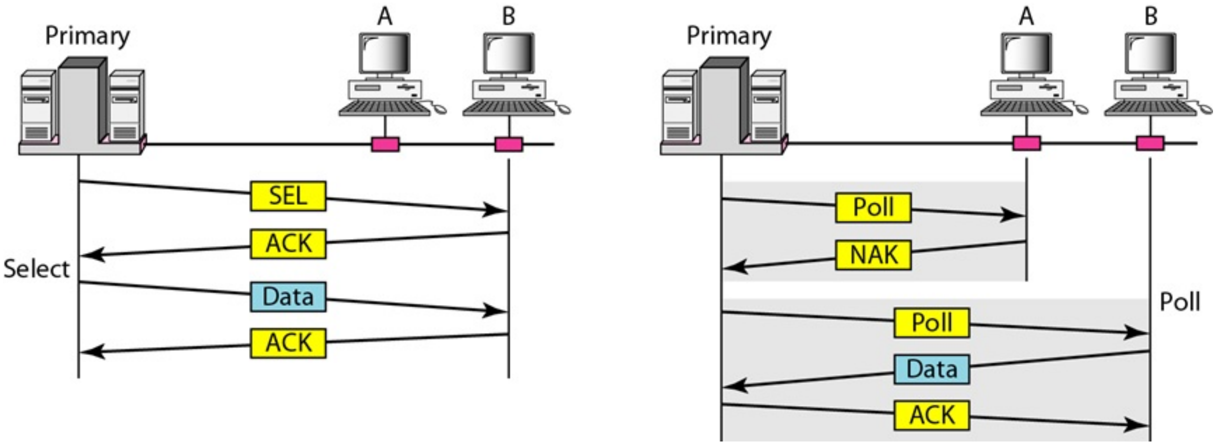


Figure 3.51: Select and poll functions in polling-access method.

Token Passing

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

- In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token, and sends the data. When the station has no more data to send, it released the token, passing it to the next logical station in the ring.

Token Management

Token management is needed for this method.
- Stations must be limited to time they can have possession of the token.
- The token must be ensured that it is not lost or destroyed.
- Assign the priorities to the stations and to the types of data being sent.

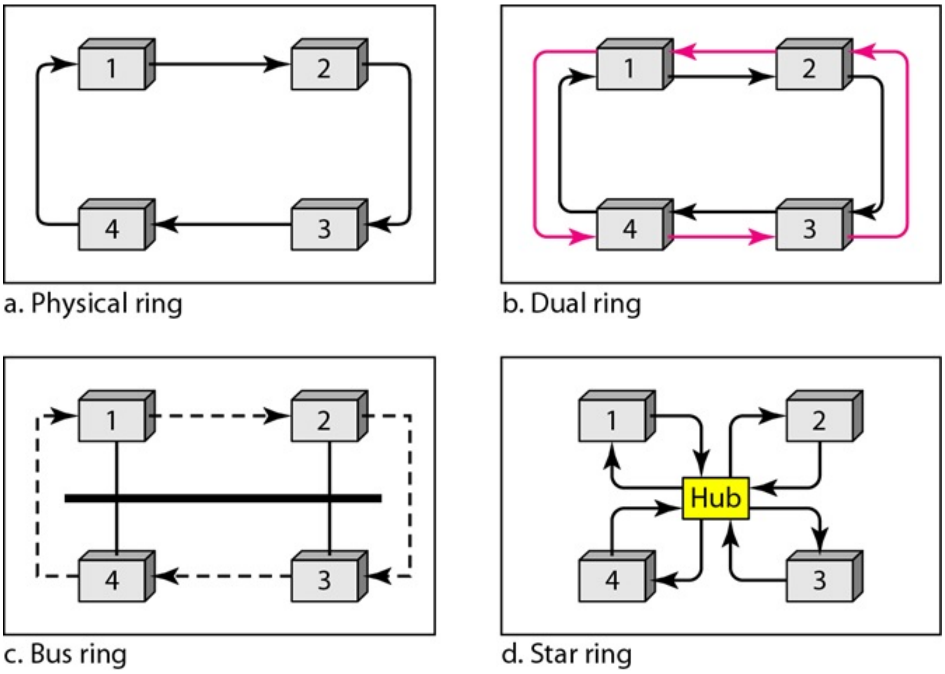


Figure 3.52: Logical ring and physical topology in token-passing-access method.

- Make low priority stations release token to the high priority stations.

3.6.2.1 Channelization

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

- Three channelizations methods:

i. Frequency Division Multiple Access (FDMA)
ii. Time-Division Multiple Access (TDMA)
iii. Code-Division Multiple Access (CDMA)

3.7 FDDI

- FDDI stands for Fiber Distributed Data Interface.
- It is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables.
- It is applicable in large LANs that can extend up to 200 Km in diameter.
- A total of 500 stations can be connected with a maximum separation of 2 Km.
- FDDI uses dual counter-rotating rings (called the primary and secondary). Data normally travels on the primary ring.
- Stations can be attached to the primary ring as **single attachment stations (SAS)** or both rings as **dual attachment stations**.

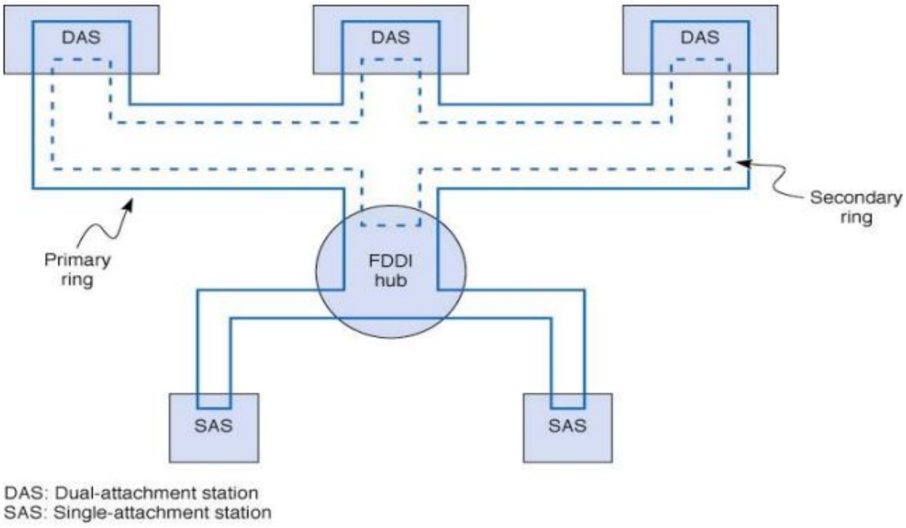


Figure 3.53: Optical cable topology for an FDDI local area network.

3.7.0.1 FDDI's Self Healing Rings

- An important feature of FDDI is ability to handle a breaks in the network by forming a single temporary ring out of the pieces of the primary and secondary rings.
- Once the stations detect the break, traffic is rerouted through a new ring formed out of the parts of the primary and secondary rings not affected by the break.
- The network then operates over this temporary ring until the break can be repaired.

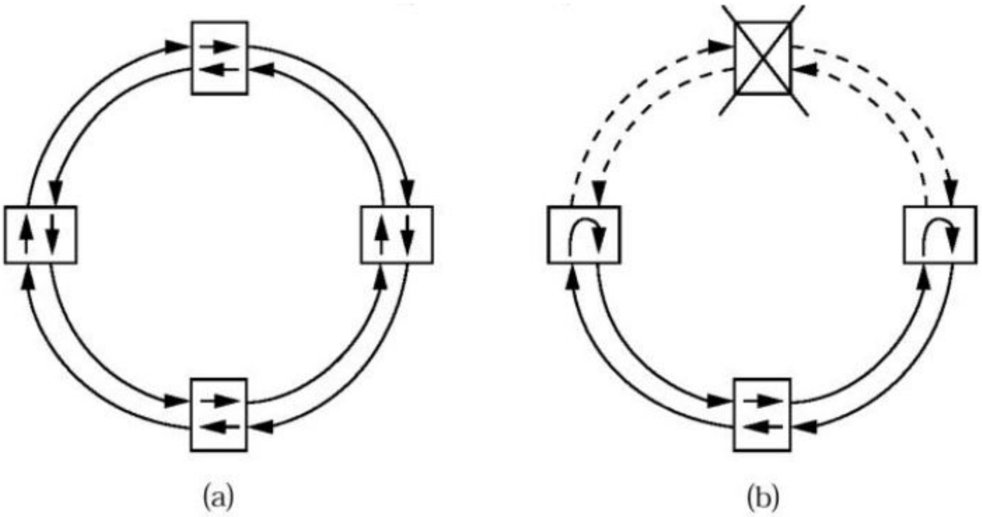


Figure 3.54: Managing a broken circuit in FDDI.

3.7.0.2 FDDI Frame

Figure 3.55shows a FDDI frame. It control fields are as below:

- **Preamble**: 1 byte for synchronization.

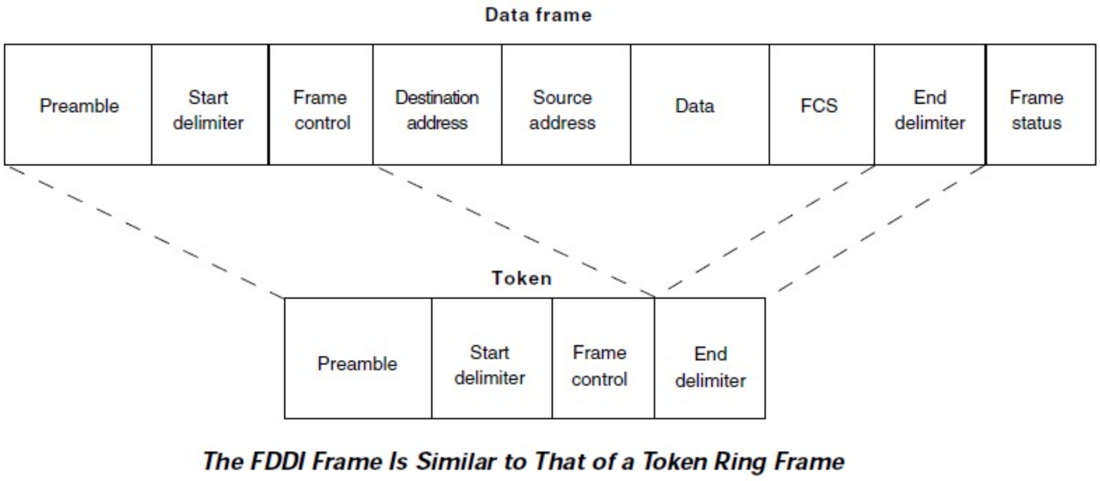


Figure 3.55: FDDI frame.

- **Start Delimiter**: 1 byte that marks the beginning of the frame.
- **Frame Control**: 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address**: 2-6 bytes that specifies address of destination station.
- **Source Address**: 2-6 bytes that specifies address of source station.
- **Payload**: A variable length field that carries the data from the network layer.
- **Checksum**: 4 bytes frame check sequence for error detection.
- **End Delimiter**: 1 byte that marks the end of the frame.

3.8 IEEE Data Link Layer Protocols/Standards

- **IEEE 802** refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.
- The services and protocols of IEEE 802 map to the lower two layer, Data Link Layer and Physical Layer, of OSI reference model.
- That is IEEE 802 standards define the specifications for NICs, networking components, and media for the data-link and physical layers of the OSI reference model.
- Examples:

- 802.3 defines the Ethernet specifications.
- 802.4 defines the Token Bus specifications.
- 802.5 defines the Token Ring LAN specifications.
- 802.11 defines the wireless LAN (Wi-Fi)

3.8.1 IEEE 802.3

- The IEEE standard for Ethernet is 802.3.
- Ethernet has been a relatively inexpensive, reasonably fast and very popular LAN technology for several decades.

- Ethernet operates in two areas of the OSI model, the lower half of the data link layer, which is known as the MAC sub layer, and the physical layer.
- Ethernet uses CSMA/CD as media access control.
- Two kinds of Ethernet exits:

- Classic Ethernet
- Switched Ethernet

3.8.1.1 Classic Ethernet

Classic Ethernet is the original form and ran at rates from 3 to 10 Mps. Repeaters are used at each 2.5 km apart. Manchester encoding is used to encode information over the cable.

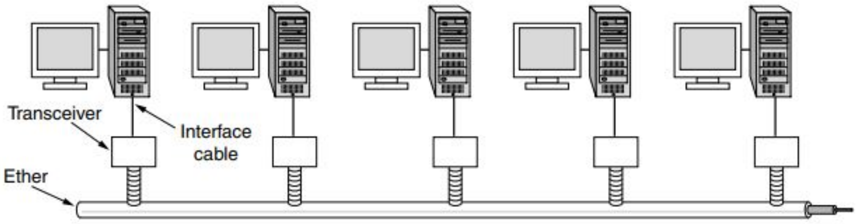


Figure 3.56: Architecture of classic Ethernet.

IEEE 802.3 Ethernet Frame (802.3 MAC frame)

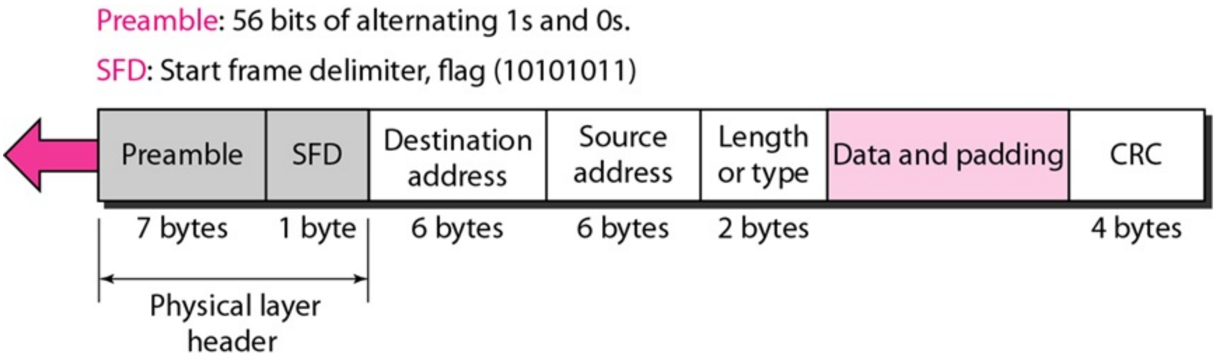


Figure 3.57: Ethernet frame (IEEE 802.3 MAC frame).

Figure 3.57 shows IEEE 802.3 Ethernet frame. It consists of following fields:

Preamble

- First field, consists of alternate 1's and 0's - Alerts the receiver of incoming frame and enables it for synchronize its input timing. - Actually added at physical layer and not(formally) part of the frame.

Start Frame Delimiter (SFD)

- 1 byte : 10101011.
- Signals the beginning of the frame. - The last 2 bit, 11, alerts next field is the destination address.
- This is actually a flag that defines the beginning of the frame.

Destination Address (DA)

- Six bytes (48 bits).
- Contains the link layer address of the destination station or stations to receive the packet.

Source Address (SA)

- Six bytes (48 bits)
- Contains the link-layer address of the sender of the packet

Type

- Defines the upper layer protocol whose packet is encapsulated in the frame.
- It specifies which process to know which one to hand the frame to. For example, a type code of 0x0800 means that the data contains an IPv4 packet.
- Protocol can be IP, ARF, OSPF, and so on.
- Used for multiplexing and de-multiplexing.

Data

- Contains the encapsulated data from upper layer.
- Minimum length : 46 bytes
- Maximum length : 1500 bytes
- If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame.
- If it is less than 46 bytes, it needs to be padded with extra 0s.

CRC

- Contains error detection information

Link Layer Addressing

- A link-layer addressing is variously called LAN address, a physical address, or a MAC address.
- Each station on an Ethernet network(PC, printer, etc.) has its own network interface card (NIC).
- 6-byte physical address imprinted on its NIC.

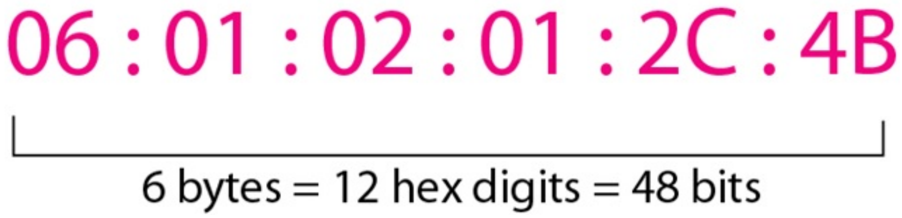

06 : 01 : 02 : 01 : 2C : 4B
6 bytes = 12 hex digits = 48 bits

Figure 3.58: Example of an Ethernet address in hexadecimal notation.

- The first 3 bytes of the address field are used for an **OUI (Organizationally unique Identifier)**.
- Values for this field are assigned by IEEE and indicate a manufacturer.Manufacturers are assigned blocks of 224 addresses.
- The manufactures assigns the last 3 bytes of the address and program the complete address into the NIC before it is sold.

Unicast, Multicast, and Broadcast Address

Source Address - Always unicast address, - frames come from only one station.

Destination address - can be unicast, multicast or broadcast.

Unicast destination address
- Defines only one recipient
- Relationship between sender and receiver is one-to-one.

Multicast destination address.

Defines a group of address.

Relationship between sender and receiver is one-to-many.

How can we differentiate?
- The least significant bit of the first byte defines the type of address.
- If the bit is 0, the address is unicast; otherwise it is multicast.

- Broadcast address is special case of multicast in which all bits are 1s.

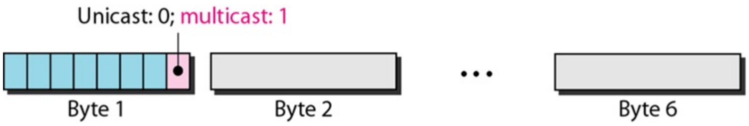


Figure 3.59: Unicast and multicast address.

3.8.1.2 Switched Ethernet

- A networking device called, switches, are used to connect different computers.
- Switch contains a high-speed backplane that connects all of the ports.
- It contains 4 to 48 ports, each with a standard RJ-45 connector for a twisted-pair cable.
- It differs from hub; in a hub, all stations are in the same collision domain while in switch, each port is its own independent collision domain.
- Mostly cable switch are full duplex, so both the station and the port can send a frame on the cable at the same time, without worrying about other ports and stations.
- Collisions are now impossible and CSMA/CD is not needed.
- However, if the cable is half duplex, the station and the port must contend for transmission with CSMA/CD in the usual way.

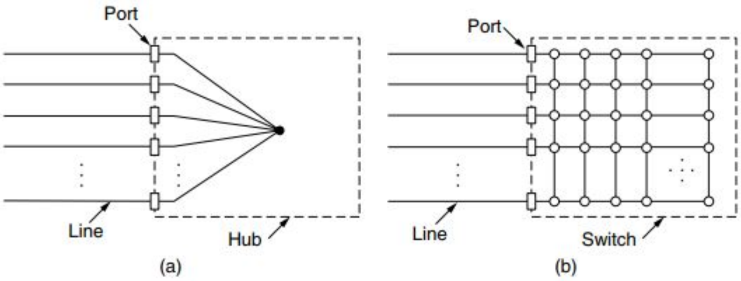


Figure 3.60: a.Hub b. Switch

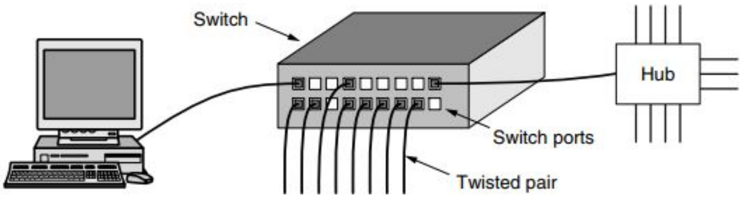


Figure 3.61: An Ethernet switch

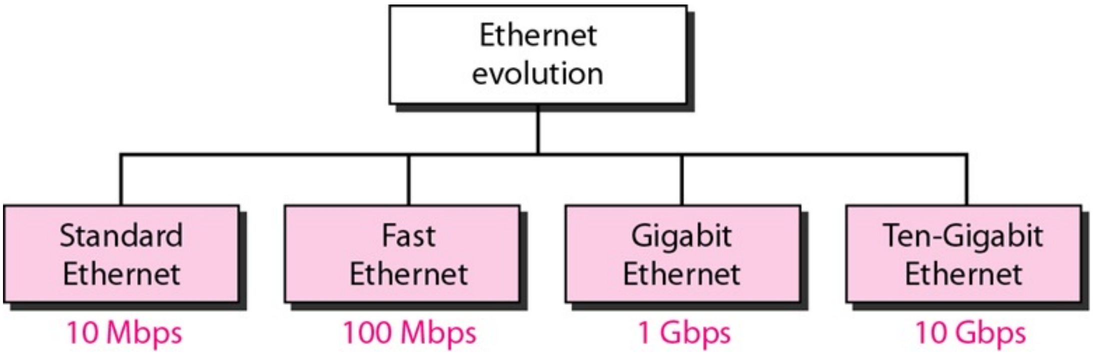


Figure 3.62: An Ethernet evolution

3.8.1.3 Ethernet Evolution

3.9 IEEE 802.4 Token Bus

3.9.1 Evolution of 802.4

- 802.3 suffer from the difficulty of large delay in getting the access.
- Poor performance under heavy load.
- There are also no priorities in 802.3, making then unsuited for real time systems.
- Token passing protocols were proposed and were found to be very attractive for situation with heavy load.

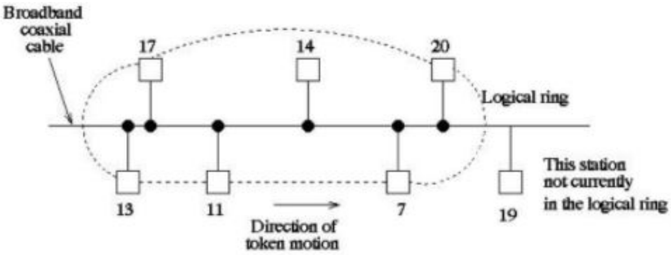

Broadband coaxial cable
17
14
20
Logical ring
13
11
7
19
This station not currently in the logical ring
Direction of token motion

Figure 3.63: Token bus structure

- The 802.4 IEEE standard defines the Token Bus protocol for a token-passing access method on a bus topology.
- A special packet called a token is passed from station to station and only the token holder is permitted to transmit packets onto the LAN.
- No collision can occur with this protocol as only one station can transfer.
When a station is done transmitting its packets, it passes the token to the “next” station.
- The next station does not need to be physically closest to this one on the bus, just the next logical station.
- Normally a token can be held by a user for a prescribed time only after which it has to be passed to the next station.

IEEE 802.4 Token Bus Frame Format

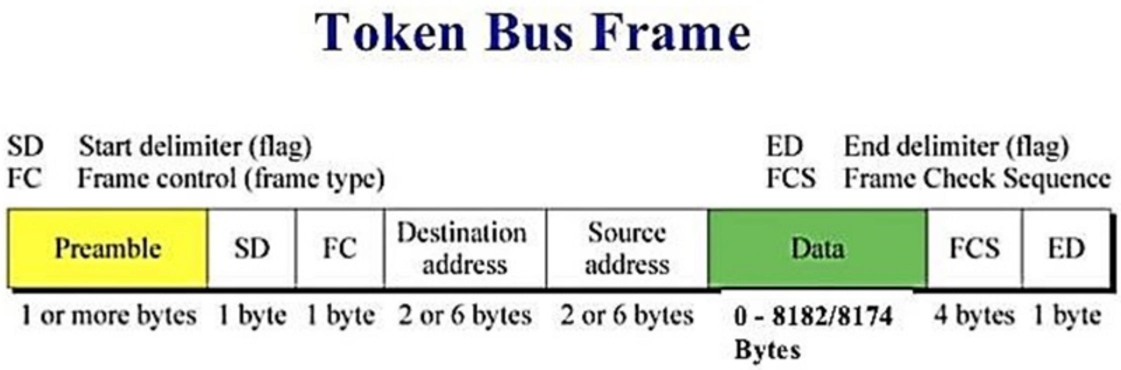


Figure 3.64: IEEE 802.4 Token Bus frame format

Figure 3.65 shows the IEEE token bus frame format whose fields are as below:

- **Preamble** – It is used for bit synchronization. It is 1 byte field.
- **Start Delimiter** – These bits marks the beginning of frame. It is 1 byte field.
- **Frame Control** – This field specifies the type of frame – data frame and control frames. It is 1 byte field.
- **Destination Address** – This field contains the destination address. It is 2 to 6 bytes field.
- **Source Address** – This field contains the source address. It is 2 to 6 bytes field.
- **Data** – If 2 byte addresses are used than the field may be upto 8182 bytes and 8174 bytes in case of 6 byte addresses.
- **FCS** – This field contains the checksum bits which is used to detect errors in the transmitted data. It is 4 bytes field.
- **End Delimiter** – This field marks the end of frame. It is 1 byte field.

3.10 IEEE 802.5 Token Ring

- The IEEE 802.5 standard defines the Token Ring protocol which, like, Token Bus, is another token-passing access control, but for a ring topology.

- A ring topology consists of a series of individual point-to-point links that forms a circle. These point-to-point links can be created with twisted pair, coaxial cable or fiber optics.

- A token is passed from station to station in one direction around the ring, and only the station holding the token can transmit packets onto the ring.

- A token is a special bit pattern (3 bytes long). There is only one token in the network. It get circulates in the ring.
- A station wishing to transmit must wait until it detect a free token passing by.
- It then seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.
- A station can hold a token for a specific duration of time. During this time, it has to complete its transmission and regenerates the token in ring. Whenever a station finishes its transmissions, the other station grabs the token and starts its own transmission.

Use of wire centres

- If the cable breaks, the entire ring network goes down. This can completely stop the propagation of token in the ring.

- This problem can be solved by using wire centre.

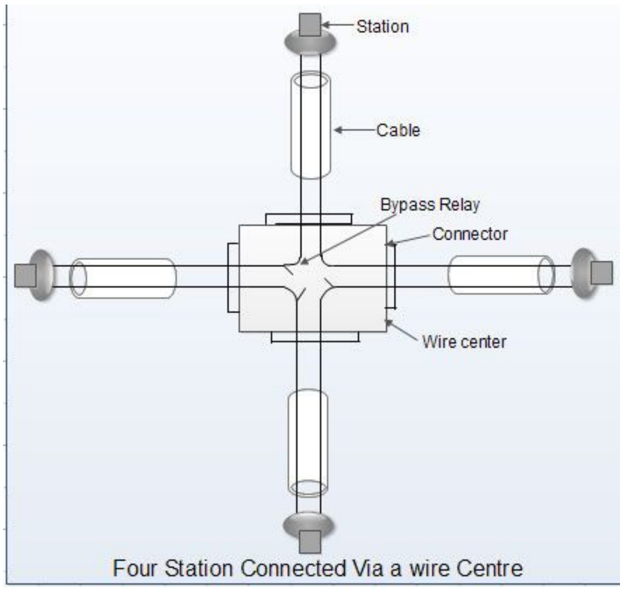


Figure 3.65: Four stations connected via a wire centre

- A wire centre has bypass relays which draws current from the station.

- If a station is powered down the relays close thereby removing the station from the ring an maintaining the ring.

- Relays can be operate by software for network management.

- Wire centres make the ring a star-shaped ring.

3.11 IEEE 802.11: Wireless LAN

- IEEE 802.11 defines the standard for wireless LAN.

- Also referred to Radio LAN (WLAN).

- Operates both in data link layer and physical layer.

- It uses CSMA/CA as media access protocol.

3.11.0.1 IEEE 802.11 Services

IEEE 802.11 standard defines two type of services. They are

1. Basis Set Service(BSS)
2. Extended Set Service (ESS)

Basic Service Set

- IEEE 802.11 defines the BSS as the building blocks of a wireless LAN.

- The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).

- The use of access point is optional.

- If the access point is not present, it is known as stand-alone network. Such a BSS cannot send data to other BSSs.

This type of architecture is known as ad hoc architecture. - The BSS in which an access point is present is known as an infrastructure network.

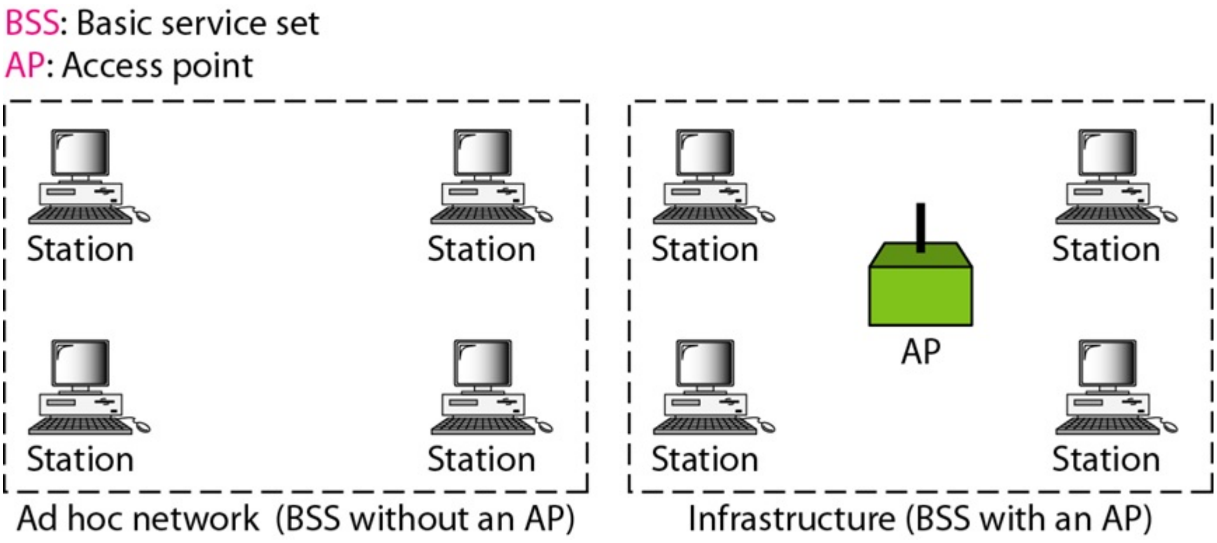


Figure 3.66: Basic Service Set

Extended Service Set (ESS)

- An extended service set is created by joining two or more basic service sets (BSS) having access points (APs). - These extended networks are created by joining the access points of basic services sets through a wired of wireless - LAN known as distribution system (DS). The DS connects the APs in the BSSs. - The distribution system can be any IEEE LAN such as Ethernet.

- There are two types of stations in ESS:

i. **Mobile stations**:
   - These are normal stations inside a BSS.
   A mobile station can belong to more than one BSS at the same time

ii. **Stationary stations**:
   These are AP stations that are part of a wired LAN.

- Communication between two stations in two different BSS usually occurs via two APs.

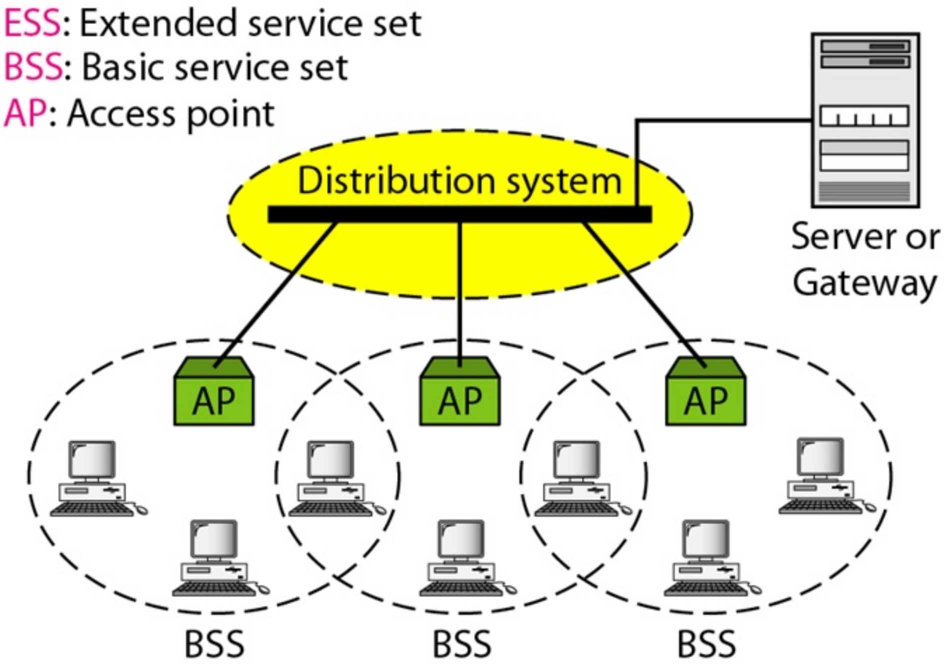


Figure 3.67: Extended Service Set

3.11.0.2 IEEE 802.11b Standard

- Operates at 2.4 GHz range
- Maximum data rate = 11 Mbps
- Uses CSMA/CA media access protocol
- Use DSSS modulation techniques

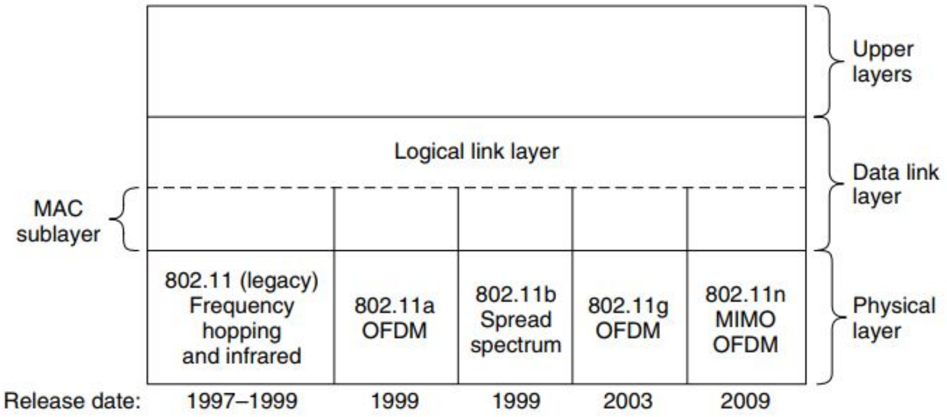


Figure 3.68: Part of the 802.11 protocol stack.

Drawback:

802.11b devices experience interference form other products operating in the 2.4 GHz band. Device operating in the 2.4 GHz range include microwave ovens, Bluetooth devices, cordless telephones, and some amateur radio equipment's.

3.11.0.3 IEEE 802.11g Standard

- Extension of 802.11b
- Extended throughput up to 54 Mbit/s.
- Use the same 2.4 GHz band as 802.11b.

802.11g hardware is fully backwards compatible with 802.11b hardware.

- Modulation scheme use is OFDM.

3.11.0.4 IEEE 802.11a Standard

- Completely different from 802.11b and 80.11g.
- Shorter range than 11b and 11g.
- Runs in the 5 GH range, so less interference from other devices.
- Has 12 channels, 8 non-overlapping, and supports rates from to Mbps, but realistically about 27bps max.
- Uses FDM.

3.11.0.5 IEEE 802.11n Standard

- Wireless networking standard.
- Uses multiple antennas to increase data rates.
- Maximum data rate from 54 Mbps to 600 Mbps.
- Use OFDM and MIMO technologies.
- Use sRF band of 2.4 GHz or 5 GHz.

3.11.0.6 IEEE802.11ac and 802.11ad Standard

- IEEE 802.11ac will deliver its throughput over the 5 GHz band, affording easy migration from IEEE 802.11n, which also uses 5 GHz band.
- IEEE 802.11ad, targeting shorter range transmission, will use the unlicensed 60 GHz band.
- Through range improvements and faster wireless transmissions, IEEE 802.11ac and ad will:

- Improve the performance of HDTV and digital video streams in the home an advances application in enterprise networks.
- Help business reduce capital expenditure by freeing them from the cost of laying and maintaining Ethernet cabling.
- Increase the reach and performance of hotspots.
- Allow connection to handle more clients
- Improve overall user experience where and wherever people are connected.

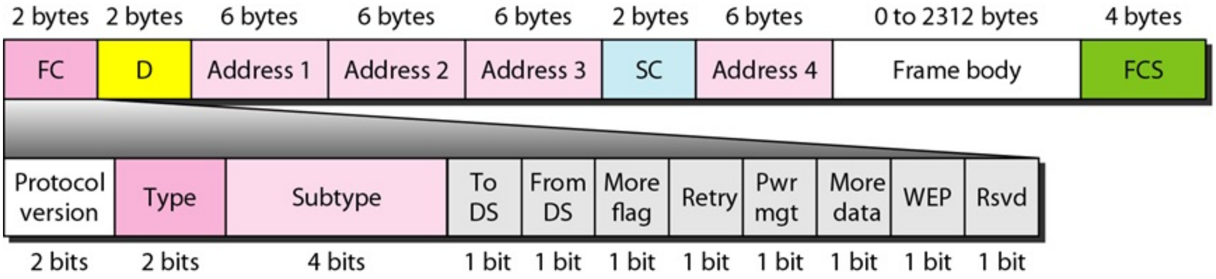


Figure 3.69: IEEE 802.11 frame format.

3.12 Virtual LANs

- A virtual LAN (VLAN) is logical subgroup within a LAN that is created by software.
- It combines use stations an network devices into a singe broadcast domain regardless of the physical LAN segment they are attached to.
- VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch.
- The VLAN logic is implemented in LAN switches and functions at the MAC layer.
- A router is required to link one VLAN to another VLAN.
- VLAN have been standarized as IEEE 802.1q and IEEE 802.1p.

- Computer can be assigned to VLANs in three ways:

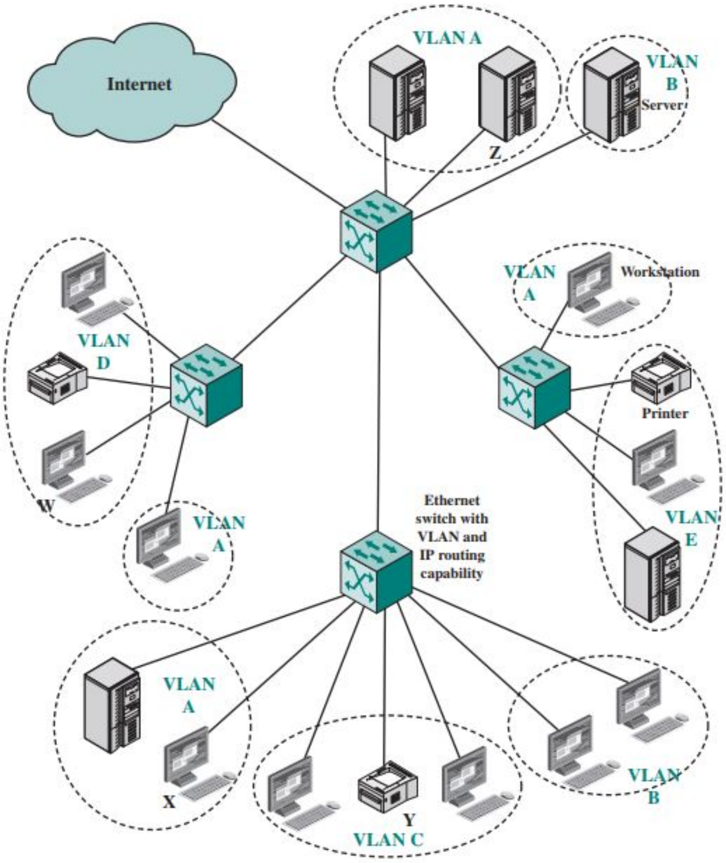


Figure 3.70: An example of VLAN configuration.

1. Port-based VLANs assign computers according to the VLAN switch end port to which they are attached.
2. MAC-based VLANs assign computer according to each computer's data link layer address.
3. protocol-based VLANs assign computer based on IP address, transport protocol information, or even higher level protocol.

- Figure 3.70 shows an example of five VLANs defined LAN.
- A transmission from workstation X to server Z is within the same VALN, so it is efficiently switched to the MAC level.
- A broadcast MAC frame from X is transmitted to all devices in all portions of the same VLAN.
- But a transmission from X to printer Y goes from one VLAN to another. Accordingly, router logic at the IP level is required to move the IP packet from X to Y.

A VLAN acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch. Here are the main reasons why VLANs are used:

- **Performance** –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations.e.g-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain therefore all will receive the traffic i.e wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups** – As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- **Security** – In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility** – VLAN provide flexibility to add, remove the number of host we want.
- **Cost reduction** – VLANs can be used to create broadcast domains which eliminate the need for expensive routers.

VLAN Ranges

- **VLAN 0**, 4095:These are reserved VLAN which cannot be seen or used.
- **VLAN 1**:It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001**: This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005**: These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094**: This is the extended range of Vlan.