Q.2 *State and explain the basic service primitives used in client-server model.* **(Refer section 1.5)** [6]

Q.3 *Draw the neat diagram of OSI model and explain in brief the function of each layer in it.* **(Refer section 1.6)** [10]

Q.4 *Explain UTP cable with reference to following :*
i) Categories ii) Connectors iii) Performance iv) Applications
(Refer section 1.10) [8]

Dec. 2012

Q.5 *Explain TCP - IP for its relationship of layers and their addresses with an example.* **(Refer section 1.7)** [8]

May 2013

Q.6 *Draw OSI-reference model and explain any three layers.* **(Refer section 1.6)** [9]

Q.7 *Differentiate OSI reference model and TCP/IP.* **(Refer section 1.7)** [9]

Dec. 2013

Q.8 *Explain the terms interfaces, services and protocols.* **(Refer section 1.5)** [6]

Q.9 *Explain the TCP / IP model with protocols at each layer.* **(Refer section 1.7)** [8]

May 2014

Q.10 *Compare OSI and TCP / IP network reference models.* **(Refer section 1.7)** [4]

Q.11 *What are the different types of address exists ?* **(Refer section 1.8)** [4]

Q.12 *Compare guided and unguided transmission media.* **(Refer section 1.9)** [4]

Dec. 2014

Q.13 *Explain TCP / IP reference model with suitable diagram. Compare OSI reference model with TCP / IP.* **(Refer section 1.7)** [10]

Q.14 *Give classification of transmission media. Explain any two guided transmission media.* **(Refer section 1.10)** [8]

❑❑❑

2 Data Link Layer

Syllabus

Introduction to data link layer, DLC services, DLL protocols, HDLC, PPP, Media access control : Random access, Controlled access, Channelization, Wired LAN : Ethernet protocol, Standard ethernet, Fast ethernet, Gigabit ethernet, 10 gigabit ethernet.

Contents

2.1 Introduction to Data Link Layer

SPPU : May-12, 14, Dec.-14

- Some important functions of data link layer include well defined service interface to the network layer, framing, flow control, error detection and error control, frame formatting and sequencing. All these are very important functions for reliable communication and plays a vital role in designing data link layer.

2.1.1 Services Provided to the Network Layer

- The primary responsibility of data link layer is to provide services to the network layer. The principle service is transferring data from the network layer on the source machine to the network layer on the destination machine.
- The two data link layer communicates with each other by data link control protocol.
- Following are the important services provided by data link layer to the network layer.
  1) Unacknowledged connectionless service.
  2) Acknowledged connectionless service.
  3) Acknowledged connection-oriented service.

1) Unacknowledged connectionless service : As the name suggests, it is unacknowledged form of transmission. Here the source machine sends the data to the destination machine without any acknowledgement. For this, no connection is either established or released. If the data is lost due to noise or interference, the lost data is not even recovered by the layer.

2) Acknowledged connectionless service : In acknowledged connectionless service each data frame is acknowledged by the destination machine. If any data frame is lost or not arrived in time the same can be transmitted again. In this service no connection are used.

3) Acknowledged connection service : Acknowledged connection service establishes a connection prior to data transmission. Each frame is numbered before transmission and corresponding acknowledgement is also received. The transmission is carried out in distinct phases.

2.1.2 Framing

- Framing in the data link layer separates a message from one source to a destination or from other messages to other destinations by adding a sender address and a destination address.

- To service the network layer, data link layer uses the service provided to it by the physical layer.
- Physical layer accepts the raw bit stream and delivers it to the destination. This bit stream may contain error i.e. number of bits received may not be equal to number of bits transmitted.
- The data link layer breaks the stream into discrete frames and computes the checksum for each frame.
- At the destination the checksum is recomputed.
- The breaking of bit stream by inserting spaces or time gaps is called framing. Since it is difficult and risky to count on timing and mark the start and end of each frame.

Fixed-size framing

- Frames can be of fixed or variable size. In fixed size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
- ATM is the example of fixed size framing.

2.1.2.1 Variable Size Framing

- In variable size framing, end of the frame and the beginning of the next frame is defined.
- Two methods are used for this purposes.
  1. Character oriented 2. Bit oriented

2.1.2.2 Character Oriented Protocol

- In this type, data to be carried are 8-bit characters from a coding system such as ASCII. Header contains source and destination address and other control information are also multiple of 8 bits. Trailer contains error detection or error correction redundant bits are also multiples of 8 bits.
- Fig. 2.1.1 shows character oriented protocol frame.

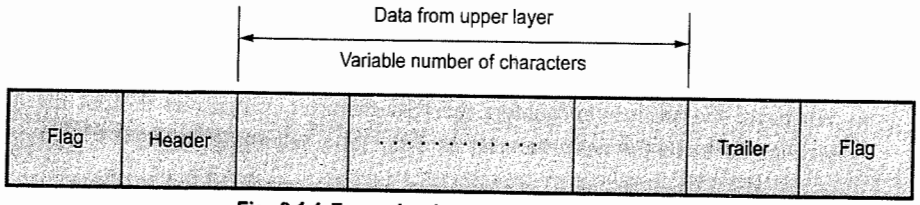


Fig. 2.1.1 Frame in character oriented protocol

- To separate one frame from the next, an 8-bit flag is added at the beginning and the end of a frame. The flag consists of protocol dependent special characters, signals the start or end of a frame.

- Character oriented framing was suitable only for text data transmission. The flag could be selected to be any character not used for text communication.
- When we send other types of information such as graphs, audio and video, the flag could also be part of the information. So it creates problem for receiver. When receiver encounters this pattern in the middle of the data, thinks it has reached the end of the frame.
- To solve this problem, a **byte stuffing** was used.

Byte stuffing

- A special byte is added to the data section of the frame. When there is a character with the same pattern as flag. The data section is stuffed with an extra byte. This byte is usually called the **Escape Character (ESC)**; which has a predefined bit pattern.
- Fig. 2.1.2 shows byte stuffing.

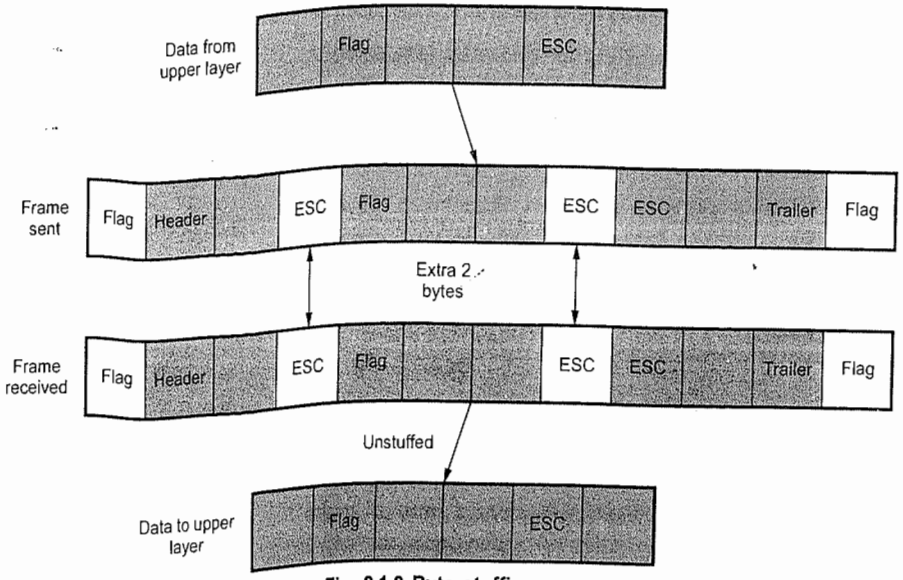


Fig. 2.1.2 Byte stuffing

- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.
- If the escape character is part of the text an extra one is added to show that the second one is part of the text.

2.1.3 Bit Oriented Protocols

- In this protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio and video. Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame.
- In bit stuffing a specific bit is stuffed into the outgoing character stream. The format is as follows :

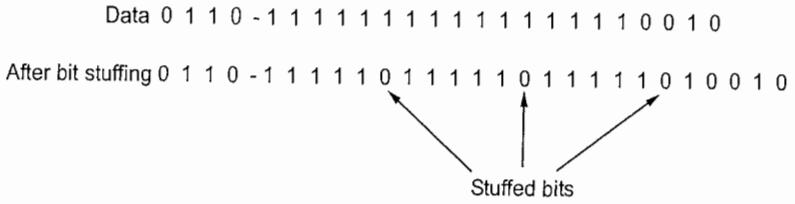


Fig. 2.1.3 Bit stuffing

- Each frame begins and ends with a special bit pattern, 01111110 called a flag byte. When five consecutive 1's are encountered in the data, it automatically stuffs a '0' bit into outgoing bit stream.

2.1.4 Error Control

- To ensure the proper sequencing and safe delivery of frames at the destination, an acknowledgement should be sent by the destination network. The receiver sends back special control frames bearing positive or negative acknowledgements about the incoming frames.
- If the sender receives a positive acknowledgement it means the frame has arrived safely.
- If a negative acknowledgement arrives that means, something has gone wrong and the frame is to be retransmitted.
- A timer at sender's and receiver's end is introduced. Also sequence numbers to the outgoing frames are maintained so that the receiver can distinguish retransmissions from originals. This is one of the most important part of data link layer duties.

2.1.5 Flow Control

- When the sender is running on fast machine or lightly loaded machine and receiver is on slow or heavily loaded machine. Then the transmitter will transmit frames faster than the receiver can accept them.

- Even if the transmission is error free at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some.
- To prevent this, flow control mechanism is incorporated which includes a feedback mechanism requesting transmitter a retransmission of incorrect message block.
- The most common retransmission technique is known as Automatic-Repeat -Request.
- Error control in Data Link Layer (DLL) is based on Automatic Repeat Request (ARQ) i.e. retransmission of data in three cases.
  1. Damaged frames 2. Lost frames 3. Lost acknowledgements.

Example 2.1.1 *If the bit string 0110111110111011111010 is subjected to bit stuffing, what output string will be transmitted ?*

Solution : The output is 011110011111001111100

University Questions

1. *State and explain in brief the functions associated with data link layers in OSI model.* **SPPU : May-12, Marks 8**
2. *Explain any framing technique in detail.* **SPPU : May-14, Marks 6**
3. *What are the functions of data link layer protocol ?* **SPPU : May-14, Marks 3**
4. *What are the different functions of data link layer ? Explain different types of framing techniques in detail.* **SPPU : Dec.-14, Marks 8**

2.2 Error Detection and Correction

- Data transmission from one device to another device with complete accuracy is possible through network. An unavoidable noise and interference is added to the communication channel. Error is reduced using the digital transmission system but complete control of error is not possible. Error bit rate for copper wires is 10^{-6}. Modem optical fiber cable have the error bit rate 10^{-9}, which is less than copper wires.
- It is more likely that some part of a message will be changed in transmission. Many factors like noise, electromagnetic interference can alter the given data unit. In this topic we discuss parity check codes, the Internet checksum and polynomial codes that are used in error detection. Data link layer or transport layer of the OSI model support the error detection and error correction method.
- **Reasons for error :**
  1) If the power supply in the system is not exactly at the specified voltage component may not operate perfectly.
  2) System may be operating at its low or high temperature limit.

  3) Crosstalk from adjacent signals can corrupt the signal.
  4) Because of resistance, inductance and capacitance, the data signal in the wire becomes weak.
  5) Voltage level is not proper after crash the system or trip through the wire.
  6) Errors occur in modern system by the laws of probability, specially with computer memory circuit.
- To ensure the proper sequencing and safe delivery of frames at the destination, an acknowledgement should be sent by the destination network. The receiver sends back special control frames bearing positive or negative acknowledgements about the incoming frames.
- If the sender receives a positive acknowledgement it means the frame has arrived safely.
- If a negative acknowledgement arrives that means, something has gone wrong and the frame is to be retransmitted.
- A timer at sender's and receiver's end is introduced. Also sequence numbers to the outgoing frames are maintained so that the receiver can distinguish retransmissions from originals. This is one of the most important part of data link layer duties.

2.2.1 Types of Errors

- Two general types of errors can occur
  1) Single bit error 2) Burst error

1) Single bit error

- It means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1. A single bit error is an isolated error condition that alters one bit but does not affect nearby bits.
- A single bit error can occur in the presence of white noise, when a slight random deterioration of the signal to noise ratio is sufficient to confuse the receiver's decision of a single bit. Single bit errors are the least likely type of error in serial data transmission.

2) Burst error

- The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.
- Burst errors are more common and more difficult to deal with errors. Burst errors can be caused by impulse noise. Note that the effects of burst errors are greater at higher data rates.

2.2.1.1 Error Detection

- The simplest form of error detection is to append a single bit, called a **parity check**, to a string of data bits. This parity check bit has the value 1 if the number of 1's in the bit string is odd and has the value 0 (zero) otherwise. In other words, the parity check bit is the sum, modulo 2, of the bit values in the original bit string. In the ASCII character code, characters are mapped into strings of seven bits and then a parity check is appended as an eighth bit as shown in Fig. 2.2.1.

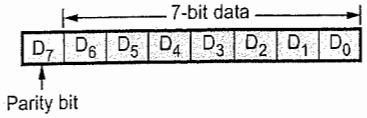


Fig. 2.2.1

- Note that the total number of 1's in an encoded string is always even. If an encoded string is transmitted and a single error occurs in transmission, then whether a 1 is changed to a 0 (zero) or a 0 to a 1 the resulting number of 1's in the string is odd and the error can be detected at the receiver. But receiver cannot tell which bit is in error, nor how many errors occurred. It simply knows that errors occurred because of the odd number of 1's.
- It is rather remarkable that for bit strings of any length, a single parity check enables the detection of any single error in the encoded string. Two errors in an encoded string always leave the number of 1's even so that the error cannot be detected. In general, any odd number of errors are detected and any even number are undetected.
- It is observed that, error detection requires redundancy in that the amount of information that is transmitted is over and above the required minimum. For a single parity check code of lengh k + 1, k bits are information bits and one bit is the parity bit. Therefore, the fraction 1/(k + 1) of the transmitted bits is redundant.
- Second observation is that every error detection technique will fail to detect some errors. The effectiveness of an error detection code is measured by the probability that the system fails to detect an error.

2.2.1.2 Redundancy

- Redundancy is a form of error detection where each data unit is sent multiple times, i.e. twice. At the receiver side, the two units are compared and if they are same, it is assumed that no transmission errors have occurred. Redundancy is a character redundancy and message redundancy.
- When the data unit is a single character, it is called **character redundancy,** whereas if the data unit is the entire message, it is called **message redundancy.**
- Another type of redundancy used with short messages is to transmit the same message several times. At the receiver side, if a given number of the messages are the same, it is assumed to be a successful transmission.

2.2.1.3 Detection versus Correction

- The ability to detect when a transmission has been changed is called **error detection**. When an error is detected it may actually be fixed without a second transmission. This is called **error correction.**
- The correction of errors is more difficult than the detection.
- The error detection, users are looking only to see if any error has occurred. A single bit error is the same as a burst error.
- In error correction, user need to know the exact number of bits that are corrupted and their location in the message.

2.2.1.4 Forward Error Correction versus Retransmission

- In **Forward Error Correction** (FEC), the transmitted bits contain the actual data along with checking bits which allow both the detection and correction of many errors. In an FEC system, the transmitted data are encoded so that the receiver can correct as well as detect errors. FEC techniques are used to correct errors on simplex channels.
- FEC is preferred on system with large transmission delays. There is no requirement for retransmitting the messages as long as the errors are infrequent. A burst type of interference destroying several bits cannot be corrected by this method. Whenever highest level of data integrity and confidence is needed, FEC is considered.
- Correction by **retransmission** is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message.

2.2.1.5 Coding

- Redundancy is achieved through various coding schemes. Coding schemes are divided into two class.
  a) Block coding b) Conventional coding
- Fig. 2.2.2 shows the general idea of the coding.

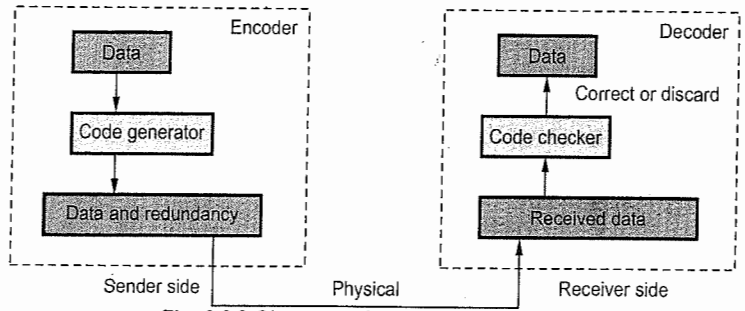


Fig. 2.2.2 Structure of encoder and decoder

2.2.1.6 Modular Arithmetic

- In modulo-N arithmetic, we use only the integers in the range 0 to N–1. For example, if the modulus is 12, we use only the integers 0 to 11.
- Addition and subtraction of modulo-2 is shown here.
- There is no carry when you add/subtract two digits in a column.

Addition

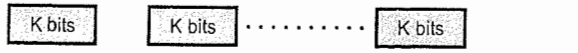
$$\begin{array}{r} 0 \\ +\,0 \\ \hline 0 \end{array} \quad \begin{array}{r} 0 \\ +\,1 \\ \hline 1 \end{array} \quad \begin{array}{r} 1 \\ +\,0 \\ \hline 1 \end{array} \quad \begin{array}{r} 1 \\ +\,1 \\ \hline 0 \end{array}$$

Subtraction

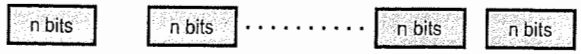
$$\begin{array}{r} 0 \\ -\,0 \\ \hline 0 \end{array} \quad \begin{array}{r} 0 \\ -\,1 \\ \hline 0 \end{array} \quad \begin{array}{r} 1 \\ -\,0 \\ \hline 1 \end{array} \quad \begin{array}{r} 1 \\ -\,1 \\ \hline 0 \end{array}$$

2.2.2 Block Coding

- In block coding, message is divided into blocks. Each block size is K bits and called as **datawords**. Redundant bits (r) is add to each block to make the length n = K + r. The resulting n-bit blocks are called **codewords**.
- Fig. 2.2.3 shows the datawords and codewords in block coding.
- With K bits, combination of 2^K datawords are possible and with n bits, 2^n codewords combination are possible. The block coding process is one-to-one; the same dataword is always encoded as the same codeword.



(a) Datawords



(b) Codewords

Fig. 2.2.3 Datawords and codewords

2.2.2.1 Error Detection

- Following steps are used for detecting errors in the block coding.
  1) The receiver has a list of valid codewords.
  2) The original codeword has changed to an invalid one.
- Fig. 2.2.4 shows the role of block coding in error detection.
- The sender creates codewords out of datawords by using a generator that applies the rules and procedures of encoding. Each codeword send to the receiver may change during transmission.
- If the received codeword is the same as one of valid codewords, the word is accepted; the corresponding dataword is extracted for use. If the received codeword is not valid, it is discarded.

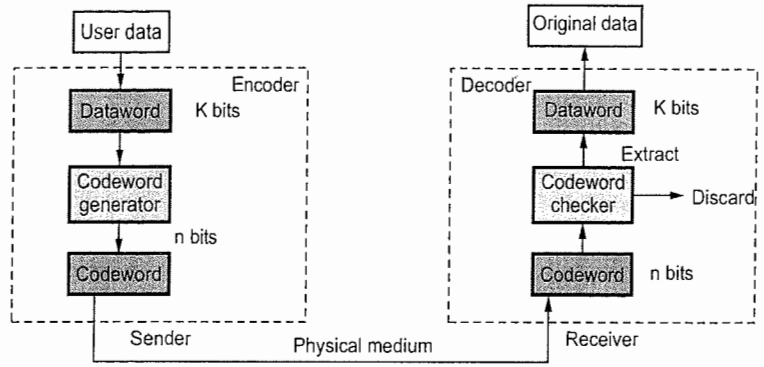


Fig. 2.2.4 Error detection process

- If the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.
- Block coding can detect only single errors. Two or more errors may remain undetected.

2.2.2.2 Error Correction

- Fig. 2.2.5 shows the error correction process. Error correction is much more difficult than error detection.

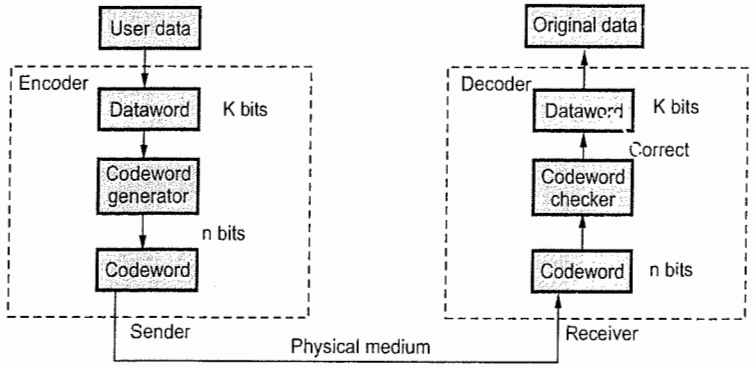


Fig. 2.2.5 Error correction in block coding

- In error correction, the receiver needs to find the original codeword sent. More number of redundant bits are required for error correction than for error detection.

2.2.2.3 Hamming Distance

- Hamming bits are inserted into the message at the random locations. Hamming code is a single error correcting code. It is most complex from the stand point of creating and interpreting the error bits. Let us consider a frame which consists of

m data bits and r check bits. The total length of message is then n = m + r. An n-bit unit containing data and checkbits is often referred to as an **n-bit codeword**.

- If 10001001 and 10110001 are two codewords, then the corresponding bits differ in these two codewords is 3 bits. The number of bit positions in which two codewords differ is called the **hamming distance.** If two codewords are a hamming distance d apart, it will require d single bit errors to convert one into the other. Determining the placement and binary value of the hamming bits can be implemented using hardware, but it is often more practical to implement them using software. The number of bits in the message are counted and used to determine the number of hamming bits to be used. The equation is used to count the number of hamming bits.

$$2^H \geq M+H+1 \quad \text{... (2.2.1)}$$

where M = Number of bits in a message

H = Hamming bits

- After calculating the number of hamming bits, the actual placement of the bits into the message is performed. Hamming code works as follows : Supose that frame consists of eight bits say $m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8$. If n parity checks are used, there are 2^n possible combinations of failures and successes. If we use 4-bit parity checks, then there are 16 possible combinations of parity successes and failures. Total 12 bits are sent which contain 8-bit original message and 4-bit parity bits. The four parity is inserted into the frame.

Four parity bits are $P_1\ P_2\ P_3$ and P_4. Let us consider following.

Data bit $m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8$

Hamming code	P_1	P_2	m_1	P_3	m_2	m_3	m_4	P_4	m_5	m_6	m_7	m_8
	1	2	3	4	5	6	7	8	9	10	11	12

- The parity bits are inserted into the message. Position of the parity bit is calculated as follows. Create a 4 bit binary number $b_4\ b_3\ b_2$ and b_1 where

$b_i = 0$ if the parity check for P_i succeeds

$b_i = 1$ otherwise

for i = 1, 2, 3, or 4.

1) The parity bit P_1 is inserted at bit position 1 for even parity for bit positions 1, 3, 5, 7, 9, 10. In these bit positions it contains even number of 0s or 1s.

2) The parity bit P_2 is inserted at bit position 2, for even parity for bit positions 2, 3, 6, 7, 10, 11.

3) The parity bit P_3 is inserted at bit position 4, for even parity of the bit positions 4, 5, 6, 7, 12.

4) The parity bit P_4 is inserted at bit position 8 for even parity of the bit positions 8, 9, 10, 11, 12.

- For inserting the parity bit even or odd parity can be used. Each parity bit is determined by the data bits it checks. When a receiver gets a transmitted frame, it performs each of the parity checks. The combination of failures and successes then determines whether there was no error or in which position an error occurred. Once the receiver knows where the error occurred, it changes the bit value in that position and the error is corrected.

Minimum hamming distance (d_{min})

- The minimum hamming distance is the smallest hamming distance between all possible pairs in a set of words.
- To find the value of d_{min}, we find the hamming distances between all words and select the smallest one.

Example 2.2.1 *Find the minimum hamming distance of the coding scheme given below.*

Dataword	*Codeword*
00	*000*
01	*011*
10	*101*
11	*110*

Solution : Hamming distances of given codeword is

d(000, 011) = 2

d(000, 101) = 2

d(000, 110) = 2

d(011, 101) = 2

d(011, 110) = 2

d(101, 110) = 2

The d_{min} = 2

Example 2.2.2 *What is the hamming distance for each of the following codewords :*
a. d (10000, 00000) b. d (10101, 10000) c. d (11111, 11111) d. d (000, 000)

Solution : a. d(10000, 00000) = **1** **b.** d(10101, 10000) = **2**

c. d(1111, 1111) = **0**

d. d(000, 000) = **0**

Example 2.2.3 *Using the code in Table, what is the dataword if one of the following codewords is received ?*

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

a. 01011 b. 11111 c. 00000 d. 11011

Solution : a. 01

b. Error

c. 00

d. Error

Example 2.2.4 *We need a dataword of at least 11 bits. Find the values of k and n in the hamming code C(n, k) with d_{min} = 3.*

Solution : We need to find k = 2m – 1 – m; Y 11. We use trial and error to find the right answer :

a. Let m = 1 k = 2 m – 1 – m = 21 – 1 – 1 = 0 (not acceptable)

b. Let m = 2 k = 2m – 1 – m = 22 – 1 – 2 = 1(not acceptable)

c. Let m = 3 k = 2m – 1 – m = 23 – 1 – 3 = 4 (not acceptable)

d. Let m = 4 k = 2m – 1 – m = 24 – 1 – 4 = 11 (acceptable)

Comment : The code is **C(15, 11)** with $\mathbf{d_{min} = 3}$.

Example 2.2.5 *Assuming even parity, find the parity bit for each of the following data units.*

a. 1001011 b. 0001100 c. 1000000 d. 1110111

Solution : We need to add all bits modulo-2 (X-ORing). However, it is simpler to count the number of 1s and make them even by adding a 0 or a 1. We have shown the parity bit in the codeword in color and separate for emphasis.

Dataword	Number of 1s	Parity	Codeword
1001011	4	0	**0** 1001011
0001100	2	0	**0** 0001100
1000000	1	1	**1** 1000000
1110111	6	0	**0** 1110111

2.2.3 Linear Block Coding

- In a linear block code, the exclusive OR(XOR) of any two valid codewords creates another valid codeword. Almost all block codes used today belong to a subset called linear block codes.

2.2.3.1 Minimum Distance for Linear Block Codes

- The minimum hamming distance is the number of 1s in the nonzero valid codeword with the smallest number of 1s.
- For example,

Datawords	Codewords
00	000
01	011
10	101
11	110

The number of 1s in the above nonzero codewords are 2, 2 and 2. (i.e. 011, 101, 110). So the minimum hamming distance is $d_{min} = 2$

- Let us consider the dataword and codeword

Dataword	Codeword
00	00000
01	01011
10	10101
11	11110

- In the above table, the numbers of 1s in the nonzero codewords are (01011) = 3, (10101) = 3 and (11110) = 4. So for this code we have $\mathbf{d_{min} = 3}$

2.2.4 Cyclic Redundancy Check

- Parity method detects only odd numbers of errors. To overcome this weakness polynomial codes error detection method is used. Polynomial codes involve generating check bits in the form of a Cyclic Redundancy Code (CRC). Therefore **polynomial also called Cyclic Redundancy Codes (CRCs).**
- The theory of polynomial code is derived from a branch of mathematics called algebra theory. The theory of CRC checksums is developed by using algebra and polynomials. These polynomials are equations which have the form of powers of X :

$$X^N + X^{N-1} + \ldots + X^2 + X^1 + X^0$$

- Polynomial codes are used with frame transmission schemes. A single set of check digits is generated for each frame transmitted, based on the contents of the frame and is appended by the transmitter to the tail of the frame. The receiver then performs a similar computation on a complete frame and check digits. If no errors have been induced, a known result should always be obtained, if a different answer is found, this indicates an error. Consider an example for binary, the polynomial for binary 10011001 is,

  $X^7 + X^4 + X^3 + X^0 \left(X^0 = 1\right)$

- The polynomial which represents the data bits is called the message polynomial, usually shown as G(X). There is a second polynomial, called the generator polynomial P(X). G(X) and P(X) both having same format. Combine two polynomials P(X) and G(X) to produce the CRC checksum polynomial F(X) calculating CRC error as follows :

  a) Multiply the G(X) by X^{n-k}, where $n-k$ is the number of bits in the CRC checksum.

  b) Divide the resulting product $X^{n-k}\,[G(X)]$ by the generator polynomial P(X).

  c) Add the remainder C(X) to the product to give the F(X), which is representated as $X^{n-k}\,[G(X)] + C(X)$.

  d) The division is performed in binary without carrying or borrowing. In this case, the remainder is always 1 bit less than the divisor. The remainder is the CRC and the divisor is the generator polynomial.

Working of CRC

- Let's now describe how CRC works. Suppose we want to send the bit string **1101011** and the generator polynominal is $\mathbf{G(x) = x^4 + x^3 + 1}$

Step 1 : Append 0s to the end of the string. The number of 0s is the same the degree of the generator polynominal G(x) (in this case, 4). Thus the string becomes 11010110000.

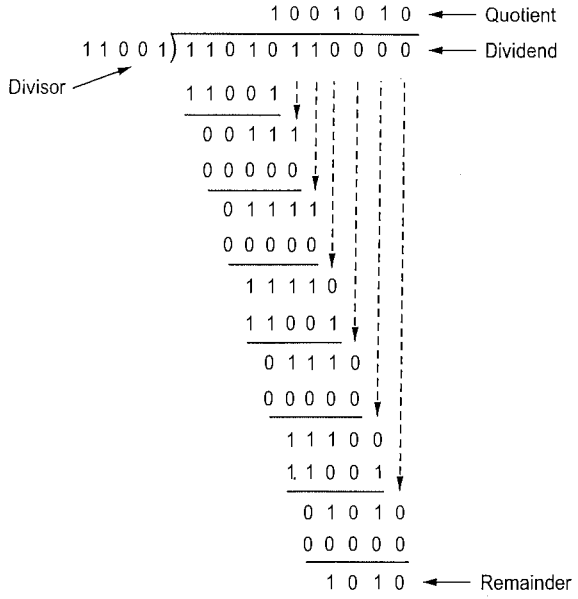
Step 2 : Divide B(x) by G(x). We can write this algebraically as

$$\frac{B(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$$

where Q(x) represent the quotient.

$G(x) = x^4 + x^3 + 1 = 11001$

String = 1101011 = After appending 11010110000



Step 3 : Define T(x) = B(x) – R(x). In this case,

B(x)	=	1 1 0 1 0 1 1 0 0 0	bit string B
– R(x)	=	1 0 1 0	bit string R
T(x)	=	1 1 0 1 0 1 1 1 0 1 0	bit string T

Note that the string T is actually the same as string B with the appended 0s replaced by R. The sender transmit the string T.

2.2.5 Polynomials

- A pattern of 0s and 1s can be represented as a polynomial with coefficients of 0 and 1. The power of each term shows the positions of the bit, the coefficient shows the value of the bit.
- In general it interprets the bit string

  $b_{n-1}\, b_{n-2}\, b_{n-3}\, \ldots\ldots\, b_2 b_1 b_0$

  as the polynomial

  $b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + b_{n-3}x^{n-3} + \ldots + b_2x^2 + b_1x + b_0$
- For example, the bit string 10010101110 is interpreted as,

  $x^{10} + x^7 + x^5 + x^3 + x^2 + x^1$

Since each b_j is either 0 or 1, we just write x^i when b_i is 1 and do not write any term when b_i is 0.

2.2.4.2 Degree of Polynomial

- The degree of polynomial is the highest power in the polynomial. For example, the degree of polynomial $x^5 + x + 1$ is 5.
- Following is an example of polynomial division T(X)/G(X) where,

  $T(X) = x^{10} + x^9 + x^7 + x^5 + x^4$ and

  $G(X) = x^4+x^3+1$

$$
\begin{array}{r}
 & & & & & & x^6 & & +x^3 & +x \\
\hline
x^4+x^3+1 \;\big)\; x^{10} & +x^9 & +x^7 & & +x^5 & +x^4 & & & & \\
 x^{10} & +x^9 & & +x^6 & & & & & & \\
\hline
 & & x^7 & +x^6 & +x^5 & +x^4 & & & & \\
 & & x^7 & +x^6 & & & +x^3 & & & \\
\hline
 & & & & x^5 & +x^4 & +x^3 & & & \\
 & & & & x^5 & +x^4 & & +x & & \\
\hline
 & & & & & & +x^3 & +x & &
\end{array}
$$

- In polynomial representation, the divisor is normally referred to as the **generator polynomial t(x).**

2.2.4.3 Cyclic Code Analysis

- Let us define the followings

  f(x) = Polynomial with binary coefficients

  d(x) = Dataword

  c(x) = Codeword

  g(x) = Generator

  e(x) = Error

  s(x) = Syndrome

- If s(x) is not zero, then one or more bits is corrupted. However, if s(x) is zero, either no bit is corrupted or the decoder failed to detect any errors.
- Let us first find the relationship among the sent codeword, error, received codeword and the generator we can say :

  Received codeword = c(x) + e(x)

- The received codeword is the sum of the sent codeword an error. The receiver divides the received codeword by g(x) to get the syndrome. We can write as this as,

$$\frac{\text{Received codeword}}{g(x)} = \frac{c(x)}{g(x)} + \frac{e(x)}{g(x)}$$

- A single bit error is $e(x) = x^i$, where i is the position of the bit. If the single bit is caught, then x^i is not divisible by g(x). If g(x) has at least two terms and the coefficient of x^0 is not zero, then e(x) cannot be divided by g(x).

2.2.4.4 Advantages of Cyclic Codes

1) Easily implemented in hardware and software.
2) Cyclic codes are faster when implemented in hardware.
3) It give good performance in detecting single bit errors, double errors, an odd number of errors and burst errors.

Standard polynomials

- CRC is widely used in Local Area Networks (LANs), where there are standard polynomials for G(X), such as following :

Sr. No.	Name	Polynomial	Application
1.	CRC-8	$x^8 + x^2 + x + 1$	ATM header
2.	CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
3.	CRC-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
4.	CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

Example 2.2.6 *Generate the CRC code for message 1101010101. Given generator polynomial* $g(x) = x^4 + x^2 + 1$

Solution : For polynomial division *T(X)/G(X)*

where $T(X) = 1\,1\,0\,1\,0\,1\,0\,1\,0\,1$
$(x^9 + x^8 + x^6 + x^4 + x^2 + 1)$

$G(X) = x^4 + x^2 + 1 = 1\,0\,1\,0\,1$

Polynomial division is done from an algebra.
Rules for addition and subtraction.

1. Addition	2. Subtraction
0 + 0 = 0	0 – 0 = 0
1 + 0 = 1	1 – 0 = 1
0 + 1 = 1	0 – 1 = 1
1 + 1 = 0	1 – 1 = 0

The steps are as follows :

Step 1 : Append 0 to the end of the string T(X).

The degree of polynomial $G(X) = x^4 + x^2 + 1 = 4$.

So we append 4 zeros to string $T(X)$.

The string becomes

1 1 0 1 0 1 0 1 0 1 0 0 0 0

Step 2 : Divide $B(X)$ by $G(X)$. After appending 0s to $T(X)$ it becomes $B(X)$. (Actually it is new $T(X)$ divided by $G(X)$).

```
              1110001110
        ┌──────────────
10101 ) 11010101010000
        11010
        10101
        ─────
        011111
         10101
         ─────
         010100
          10101
          ─────
          000011010
               10101
               ─────
               011110
                10101
                ─────
                010110
                 10101
                 ─────
                 000110      ← Remainder

 11010101010000
+           0110
 ──────────────
 11010101010110    ⇐ Codeword
```

Example 2.2.7 *Information to be transmitted is 110011 and the generator polynomial is represented as g (x) = 11001. Do a CRC check.*

Solution : Append by 4 bit 0 because coefficient of g(x) is 4.

The binary equivalent of d(x) = 1 1 0 0 1 1 0 0 0 0

```
              100001
        ┌──────────
11001 ) 1100110000
        11001
        ─────
        11001
        ─────
        0000010000
             11001
             ─────
             01001      ← Remainder
```

Remainder is added to d(x) to give f(x) i.e.

1 1 0 0 1 1 0 0 0 0 + 0 1 0 0 1 = 1 1 0 0 1 1 1 0 0 1 ← f(x)

f(x) is transmitted.

Example 2.2.8 *The message 11001001 is to be transmitted, using CRC error detection algorithm. Assuming the CRC polynomial to be $x^3 + 1$, determine the message that should be transmitted. If the second left most bit is corrupted, show that it is detected by the receiver.*

Solution : We take the message 11001001, append 000 to it and divide by 1001. The remainder is 011; what we transmit is the original message with the remainder appended, or 1100 1001 011.

```
          11010011
        ┌────────
1001 ) 11001001000
       1100
       1001
       ────
        1011
        1001
        ────
         1000
         1001
         ────
          1100
          1001
          ────
           1010
           1001
           ────
            011
```

Message transmit = 11001001000
                   011
                   ──────────
                   11001001011

2.3 DLL Protocol

- The protocols used for noiseless channel and noisy channels are as follows.

1. Noiseless channel protocols are,

a) Simplest

b) Stop and wait

2. Noisy channel protocol

a) Stop and wait ARQ

b) Go back N ARQ

c) Selective repeat ARQ

- Protocols in which the sender waits for a positive acknowledgement before advancing to the next data item are often called **Positive Acknowledgement with Retransmission** or **Automatic Repeat Request** (ARQ).
- In a real life network, the data link protocols are implemented as bidirectional; data flow in both directions.
- When data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet. The acknowledgement is attached to the outgoing data frame.
- In effect, the acknowledgement gets a free ride on the next outgoing data frame. The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame known as **piggybacking.**
- In ARQ scheme, the information word is coded with adequate redundant bits so as to enable detection of errors at the receiving end.
- If an error is detected, the receiver asks the sender to retransmit the particular information word.
- ARQ system is useful where the expected errors are bursty in nature or error rate of the channel is low, i.e. the channel is fairly reliable.
- Most often, the errors encountered in data communication systems are bursty in nature. Hence, ARQ schemes are used extensively in data networks.

Steps in ARQ

An ARQ protocol is characterized by four functional steps.

1) Transmission of frames.

2) Error checking at the receiver end.

3) Acknowledgement.

a) Negative if error is detected (NAK).

b) Positive if no error is detected (ACK).

4) Retransmission if acknowledgement is negative (NAK) or if no acknowledgement is received within a stipulated time.

- It may be noted that ARQ protocols require two way communication even if the information transfer is simplex, i.e. one way only. Information is exchanged in the form of frames, the beginning and the end of which are identified by means of flags or special characters.

2.4 Noiseless Channel

SPPU : Dec.-12, May-13

Assume that the channel is ideal in which no frames are lost, duplicated or corrupted.

2.4.1 Simplest Protocol

- In simplest protocol, there is no flow control and error control. It is a unidirectional protocol in which data frames are traveling in only one direction i.e. from the sender to receiver.
- We also assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible.
- The protocol consists of two distinct procedures a sender and a receiver. The sender runs in the data link layer of the source machine and the receiver runs in the data link layer of the destination machine. No sequence number or acknowledgements are used here.
- Fig. 2.4.1 shows the simplest protocol.

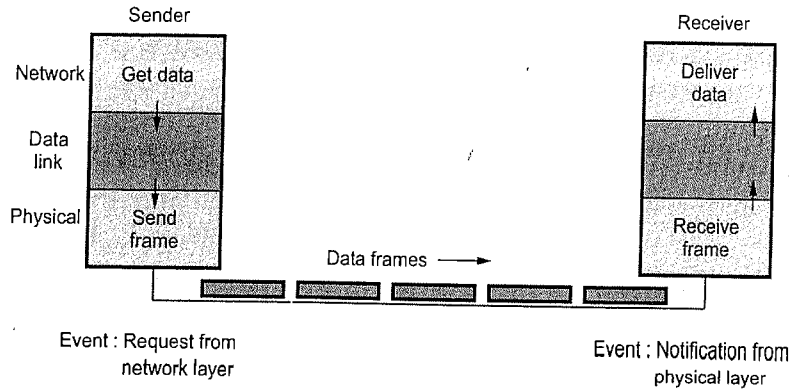


Fig. 2.4.1 Simplest protocol

- **Algorithm for sender**

```
void sender1 (void)
{
        frame s;
        packet buffer;
while(true){
from_network_layer(&bufer);
s.info=buffer;
to_physical_layer(&s);
}
}
```

- **Algorithm for receiver side**

```
void receiver1(void)
{
        frame r;
        event_type event;
        while(true){

wait_for_event (&event);
from_physical_layer(&r);

to_network_layer(&r.info);
}
}
```

- Fig. 2.4.2 shows the flow diagram for sender algorithm.

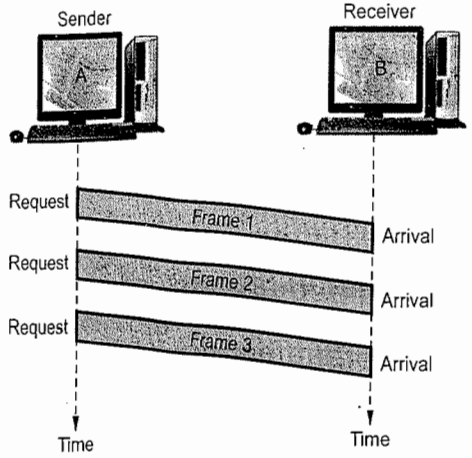


Fig. 2.4.2 Flow diagram for sender

2.4.2 A Simplex Stop-and-Wait Protocol

- Protocols in which the sender sends one frame and then waits for an acknowledgement before proceeding are called **stop-and-wait.**
- The communication channel is still assumed to be error free however and the data traffic is still complex.
- **Main problem :** How to prevent the sender from flooding the receiver with the data faster than the latter is able to process it.
- It is also assumed that there is no automatic buffering and queueing done within the receiver's hardware. The sender never transmit new frame until old one has been fetched by *from_physical_layer.*
- In some situations, delay is inserted by sender in the above protocol to slow it down sufficiently to keep from swamping the receiver.
- A more general solution to this dilemma is to have the receiver provide feedback (ACK) to the sender. After having passed a packet to its network layer, the receiver sends a little dummy frame back to the sender which, in effect, gives the sender permission to transmit the next frame.
- After having sent a frame, the sender is required by the protocol to bide its time until the little dummy (i.e., acknowledgement) frame arrives.
- Using feedback from the receiver to let the sender know when it may send more data is an example of the flow control.
- The simplest retransmission protocol is stop-and-wait. Transmitter (station A) sends a frame over the communication line and then waits for a positive or negative acknowledgement from the receiver (station B).
- If no errors occurred in the transmission, station B sends a positive acknowledgement (ACK) to station A.
- The transmitter can now start to send the next frame. If frame is received at station B with errors, then a negative acknowledgement (NAK) is sent to station A. In this case station A must retransmit the old packet in a new frame.
- There is also the possibility that information frames and/or ACKs can be lost. To account for this, the sender is equipped with a timer. If no recognizable acknowledgement is received when the timer expires at the end of time out interval t_{out}, then the same frame is sent again.
- Fig. 2.4.3 shows the design of stop and wait protocol.
- Protocols in which the sender sends one frame and then waits for an acknowledgement before process are called **stop and wait.**

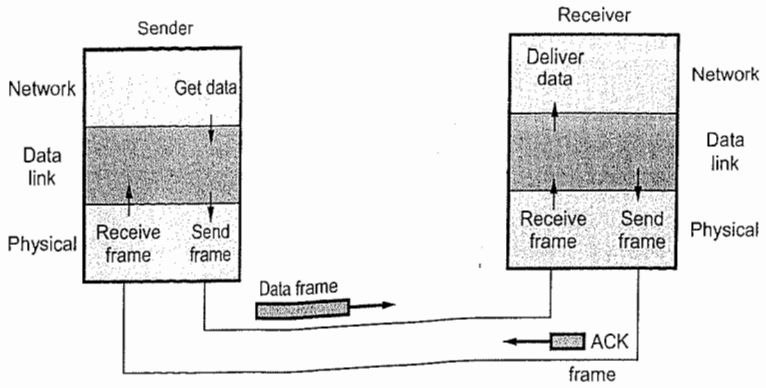


Fig. 2.4.3 Design of stop and wait protocol

- **Algorithm for sender**

```
void sender (void)
{
        frame s;
        packet buffer;
        event_type event;
while(true){
        from_network_layer(&buffer);
        s.info=buffer;
        to_physical_layer(&s);
        wait_for_event(&event);
}
}
```

- Fig. 2.4.4 shows the flow diagram.

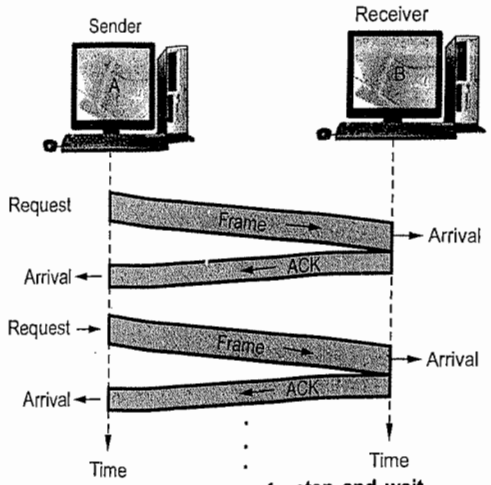


Fig. 2.4.4 Flow diagram for stop and wait

- **Algorithm for receiver side**

```
void receiver(void)
{
        frame r,s;
        event_type event;
while(true){

wait_for_event (&event);
from_physical_layer(&r);
to_network_layer(&r.info);
to_physical_layer(&s);
}
}
```

- **Major drawback of stop-and-wait flow control :**
  1) Only one frame can be in transmission at a time.
  2) This leads to inefficiency if propagation delay is much longer than the transmission delay.

University Questions

1. *State and explain the significance of sliding window protocol with an example.* **SPPU : Dec.-12, Marks 8**
2. *What is the peak throughput achievable by a source employing stop-wait flow control, when maximum packet size is 1000 kbytes and network span of 10 km.* **SPPU : May-13, Marks 8**

Ans. : Assuming a direct fiber-optic line between endpoints,

$$\text{Speed-of-light propagation delay} = 1/(0.7 \times 3 \times 10^5)\ s/k$$

Since the speed of light in fiber is approximately 0.7c, where c (the speed of light in vacuum) $3*10^5$ km/s. This works out to 4.76 us/km. Here we will ignore the effects of queuing and switching delays.

For a 10 km, the round-trip delay = 2×47.6

= 95.2 micro second

The maximum possible throughput = 1 packet/RTT

= 1000×8 bits/95.2 micro second

= 84.03 Mbps

2.5 Noisy Channel

SPPU : Dec. 13, 14, May 14

2.5.1 Sliding Windows Protocols

- Sliding windows is one of the methods of error correction. To increase the data rate, this method allows the sender to transmit a specific number of packets in continuous mode, i.e. at the maximum possible rate, without receiving positive acknowledgments for these packets.
- The number of packets that can be transmitted in such a way is known as the **window size.** Windows size can be constant parameters for this algorithm, which means that it is chosen at connection setup and does not change during the entire session.
- If the destination receives the packet with corrupted data, it might send a **Negative Acknowledgement (NACK),** specifying that the packet needs to be retransmitted.
- When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet. The acknowledgement is attached to the outgoing data frame.
- The acknowledgement gets a free ride on the next outgoing data frame. The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is known as **piggybacking.**
- The principal advantage of using piggybacking over having distinct acknowledgement frames is a better use of the available channel bandwidth. The **ack** field in the frame header costs only a few bits, whereas a separate frame would need a header, the acknowledgement and a checksum.
- In a sliding window protocol each outbound frame contains a sequence number in the range 0 to some maximum (MaxSeq). If **n** bits are allocated in the header to store a sequence number then the number range would be from 0 to $2^n - 1$.

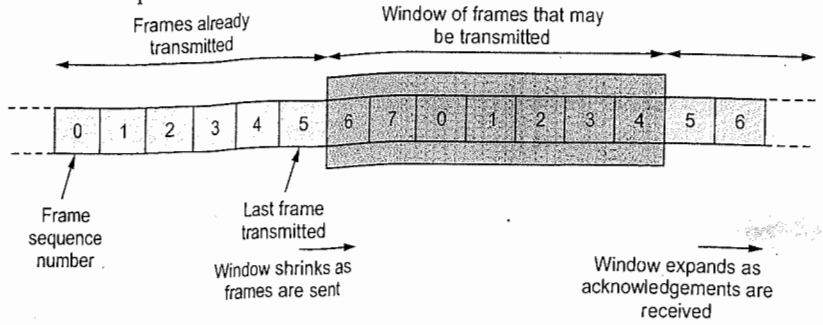


Fig. 2.5.1

For example : If a 3 bit number is used the sequence numbers would range from 0 to 7. The sender and receiver maintain a window.

- **Sending window :** It is a list of consecutive frame sequence numbers that can be sent by the sender or that have been sent and acknowledgments are waited for.
- When an ack arrives and all previous frames have already been acknowledged the window can be advanced and a new message obtained from the host to be transmitted with the next highest available sequence number. If ack arrives for a frame that is not within the 'window' it is discarded.
- **Receiving window :** It is a list of sequence numbers for frames that can be accepted by the receiver. When a valid frame arrives and all previous frames have already arrived the window is advanced. If a frame arrives that is not within the 'window' it is discarded.

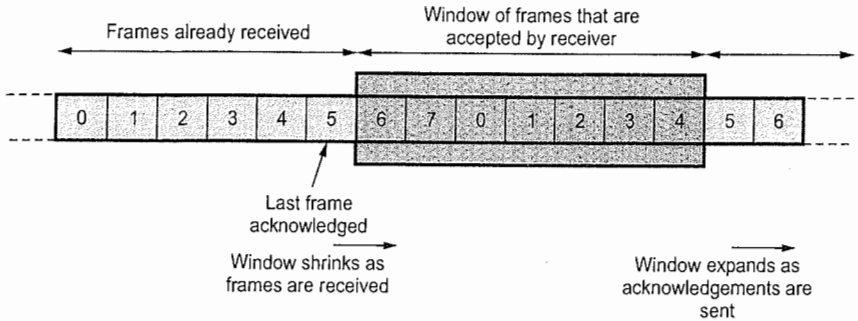


Fig. 2.5.2

Advantages of sliding windows protocol :

1) The sliding window is simpler, having only one set of parameters to manage.
2) Simultaneous communication in both directions is possible.
3) Better utilization of network bandwidth, especially if there are large transmission delays.
4) Traffic flow with reverse traffic data, known as piggybacking.

2.5.2 Stop and Wait ARQ Protocol

- This is the 'simplex protocol with sequence numbers and with the ack frame indicating the sequence number of the next frame expected'.
- In this sliding window protocol, the maximum window size of 1. Such a protocol uses stop-and-wait since the sender transmits a frame and waits for its acknowledgement before sending the next one.
- One-bit sliding window protocol is also called stop and wait ARQ.

- In a noisy communication channel if a frame is damaged in transit, the receiver hardware will detect this when it computes the checksum.
- If a damaged frame is received, it will be discarded and transmitter will retransmit the same frame after receiving a proper acknowledgement.
- If the acknowledgement frame gets lost and data link layer on A eventually times out. Not having received an ACK, it assumes that its data frame was lost or damaged and sends the frame containing packet 1 again. This duplicate frame also arrives at data link layer on B, thus part of file will be duplicated and protocol is said to be failed.
- A typical approach to solve this problem is the provision for a sequence number in the header of the message.
- The receiver can then check for the sequence number to determine if the message is a duplicate. Since only message is transmitted at any time.
- The sending and receiving station need only 1-bit alternating sequence of 0 or 1 to maintain the relationship of the transmitted message and its ACK/NAK.
- A modulo-2 numbering scheme is used where in frames are alternately labelled with 0 or 1 and positive acknowledgements are of the form ACK 0 and ACK 1.

Sequence numbers

- The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame.
- The sequence numbers are based on modulo-2 arithmetic.
- Fig. 2.5.3 shows the design of the stop and ARQ wait protocol. (See Fig. 2.5.3 on next page.)
- Stop-and-Wait ARQ is the simplest mechanism for error control and flow control.

Operation

- The sender transmits the frame, when frame arrives at receiver it checks for damage and acknowledges to the sender accordingly. While transmitting a frame there can be four situations.

a) Normal operation. b) The frame is lost.

c) The acknowledgement is lost. d) The acknowledgement is delayed.

a) Normal operation

- In normal operation the sender sends frame 0 and waits for acknowledgement ACK 1. After receiving ACK 1, sender sends next frame 1 and waits for its acknowledgement ACK 0. This operation is repeated. Fig. 2.5.4 shows this operation.

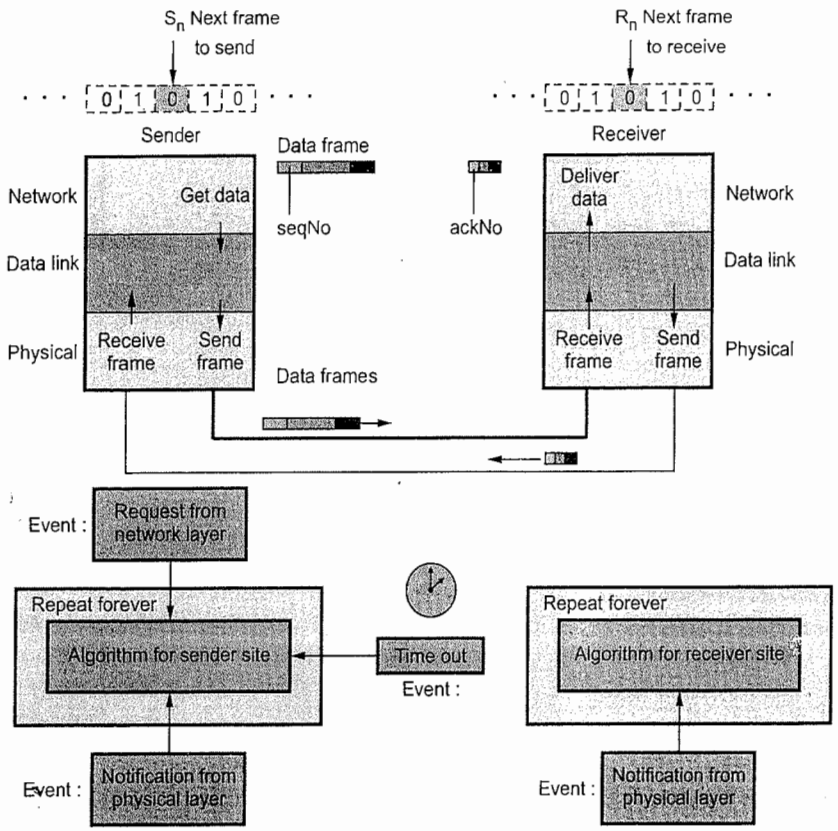


Fig. 2.5.3 Design of stop and wait ARQ protocol

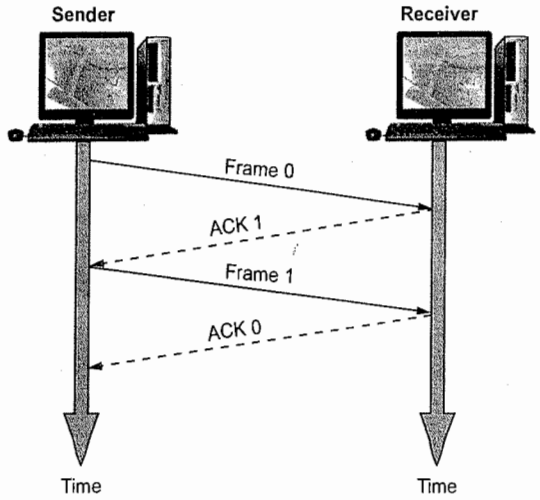


Fig. 2.5.4 Normal operation

- Usually a timer is set by sender after each frame is transmitted, its acknowledgement must be received before timer expires.

b) Lost or damaged frame

- When a receiver receives the frame and found it damaged or lost, it is discarded but retains its number. When sender does not receive its acknowledgement it retransmits the same frame. Fig. 2.5.5 shows Stop-and-Wait ARQ with lost frame.

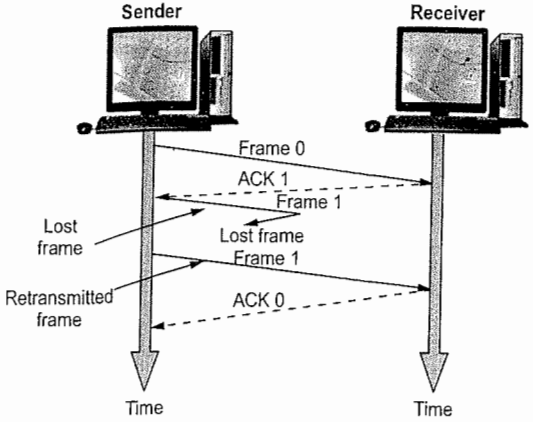


Fig. 2.5.5 Lost frame in Stop-and-Wait ARQ

c) Lost acknowledgement

- When an acknowledgement is lost, the sender does not know whether the frame is received by receiver. After the timer expires, the sender re-transmits the same frame. On the other hand, receiver has already received this frame earlier hence the second copy of the frame is discarded. Fig. 2.5.6 shows lost ACK.

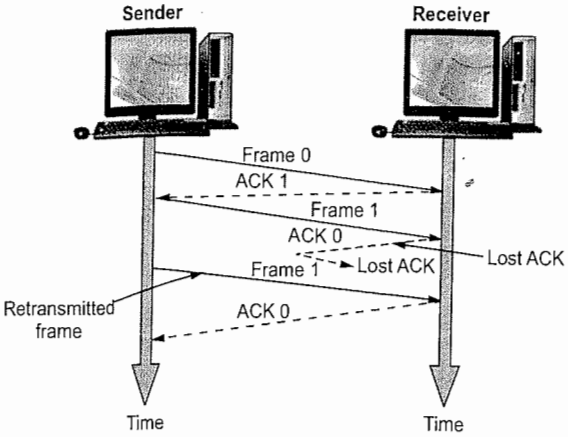


Fig. 2.5.6 Lost ACK

d) Delayed acknowledgement

- The ACK frame may be delayed due to some link problem. The ACK is received after the timer is elapsed. While the sender has already transmitted the same frame. Again second ACK is initiated by receiver for the retransmitted frame, hence the second ACK is discarded. To avoid duplication the ACKs must be numbered. Fig. 2.5.7 shows delayed ACK.

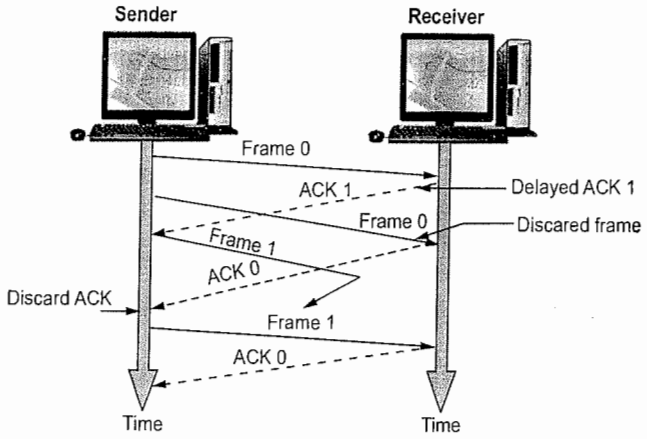


Fig. 2.5.7 Delayed ACK

2.5.2.1 Features of Stop-and-Wait ARQ

1) Sender keeps a copy of last transmitted frame until its ACK is received.
2) Both data frame and ACK frame are alternately numbered as 0 and 1 for identification of frame and to avoid duplication of frames.
3) In case of damage or loss of frame, the frames are discarded, no acknowledgment is sent.
4) The frames are numbered sequentially to avoid duplication.
5) The sender maintains a timer, if ACK is not received in time, sender assumes it it lost.
6) The receiver send only positive acknowledgement to the sender.

Shortcomings of Stop-and-Wait ARQ

1) If the sender's frame is lost, the receiver never sends an acknowledgement, and the sender will wait forever.
2) If the receiver's acknowledgement is lost, the same thing happens.
3) If the acknowledgement is damaged, the sender may draw the wrong conclusion and make protocol fail.
4) Both sender and receiver do a lot of waiting, it is just like teacher is giving one assignment question at a time. The student takes the question at home, works on it, brings it back to school, gives it to the teacher and waits for the next question.

2.5.3 Go-Back-N ARQ

- Go-Back-N uses the sliding window flow control protocol. If no errors occur the operations are identical to sliding window.
- A station may send multiple frames as allowed by the window size.
- Receiver sends a NAK i if frame i is in error. After that, the receiver discards all incoming frames until the frame in error was correctly retransmitted.
- If sender receives a NAK i it will retransmit frame I and all packets i+1, i+2,... which have been sent, but not been acknowledged.
- The need for a large window on the sending side occurs whenever the product of bandwidth x round-trip-delay is large. If the bandwidth is high, even for a moderate delay, the sender will exhaust its window quickly unless it has a large window.
- If the delay is high, the sender will exhaust its window even for a moderate bandwidth. The product of these two factors basically tells what the capacity of the pipe is and the sender needs the ability to fill it without stopping in order to operate at peak efficiency. This technique is known as **pipelining.**
- As in Stop-and-Wait protocol senders has to wait for every ACK then next frame is transmitted. But in Go-Back-N ARQ W frames can be transmitted without waiting for ACK. A copy of each transmitted frame is maintained until the respective ACK is received.

Additional features of Go-Back-N ARQ

1) Sequence numbers : Sequence numbers of transmitted frame are maintained in the header of each frame. If k is the number of bits for sequence number, then the numbering can range from 0 to $2^k - 1$ e.g. for k = 3. Sequence numbers are 0 to 7 $\left(2^3 - 1\right)$.

2) Sender sliding window : Window is a set of frames in buffer waiting for acknowledgment. This window keeps on sliding in forward direction. The window size is fixed. As the ACK is received, the respective frame goes out of window and new frame to sent come into window. Fig. 2.5.8 illustrates sliding of window for window size = 7.

3) Receiver sliding window : In the receiver side the size of the window is always one. The receiver is expecting to arrive frames in specific sequence. Any other frame received which is out of order is discarded. The receiver slides over after receiving the expected frame. Fig. 2.5.9 shows receiver sliding window.

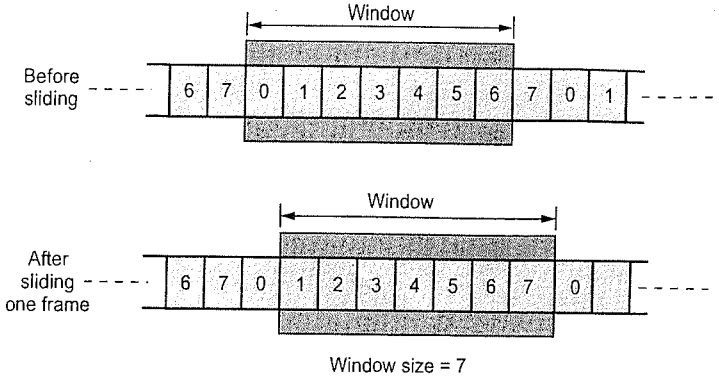


Fig. 2.5.8 Sender sliding window

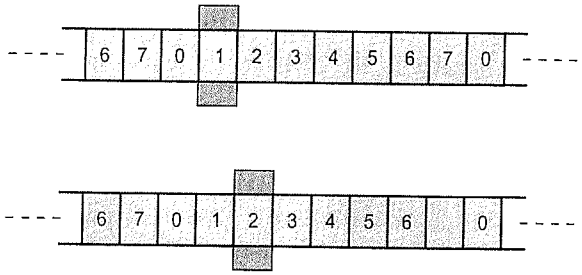


Fig. 2.5.9 Receiver sliding window

4) Control variables :

a) Sender variables

- The sender deals with three different variables.

S → Sequence number of recently sent frame.

S_F → Sequence number of first frame in window.

S_L → Sequence number of last frame in window.

∴ Window size $W = S_L - S_F + 1$

e.g. in previous feature, $W = 7 - 0 + 1 = 8$

b) Receiver variable

- The receiver deals with one variable only.

R → Sequence number of frame expected

If the number matches, then the frame is accepted otherwise not.

5) Timers

- The sender has a timer for each transmitted frame. The receiver don't have any timer.

6) Acknowledgment

- The receiver responds for frames arriving safely by positive acknowledgments. For damaged or lost frames receiver does not reply, the sender has to retransmit it when timer of that frame elapsed.
- The receiver may acknowledge once for several frames.

7) Resending of frames

- If the timer for any frame expires, the sender has to resend that frame and the subsequent frames also, hence the protocol is called Go-Back-N ARQ.

Operation

a) Normal operation

- The sender sends frames and update the control variables i.e. S_F, S, S_L and receiver updates variable R. Fig. 2.5.10 shows normal operation.

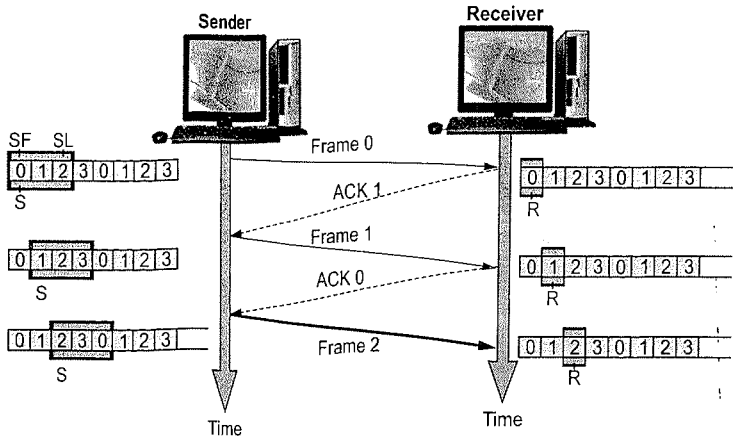


Fig. 2.5.10 Go-Back-N ARQ, normal operation

b) Damaged or lost frame

- Suppose frame 2 is damaged or lost and if receiver receives frame 3, it will be discarded since it is expecting frame 2. Sender retransmits frame 2 and frame 3. Fig. 2.5.11 shows this process.

(See Fig. 2.5.11 on next page.)

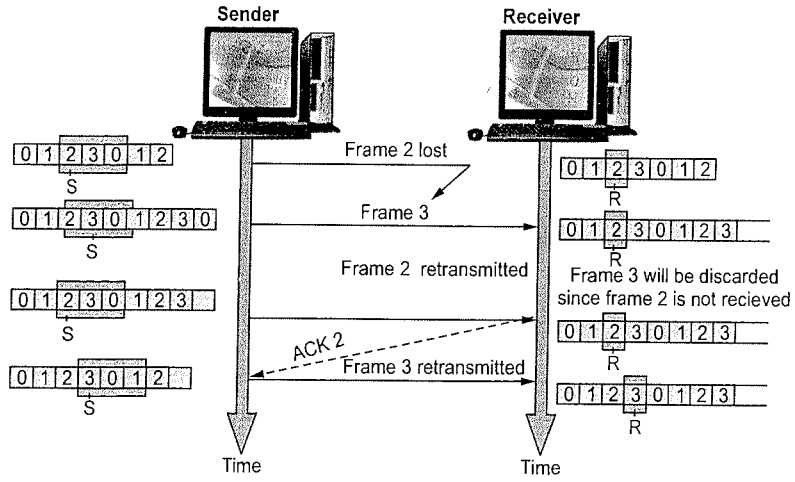


Fig. 2.5.11

2.5.4 Selective Repeat ARQ

- Selective repeat ARQ retransmitts only the damaged or lost frames instead of sending multiple frames. The selective retransmission increases the efficiency of transmission and is more suitable for noisy channel. The circuit complexities at the receiver side increases.
- The size of sender window is one half of 2^k. The receiver window size is of same length as that of sender. The receiver window includes the set of expected frames. The boundaries of receiver windows are defined by R_F and R_L. Fig. 2.5.12 shows the sender and receiver windows.

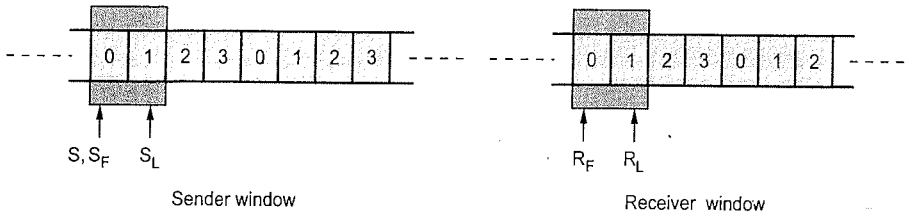


Fig. 2.5.12 Selective repeat windows

- Negative acknowledgement (NAK) is used for lost or damaged frames.

Operation

- In sequential transmission of frame 0, 1, 2, 3, suppose frame 2 is lost and the next frame 3 is already received then receiver sends NAK 2 frame to sender. Then sender retransmits frame 2 only. Fig. 2.5.13 shows operation of selective repeat ARQ.

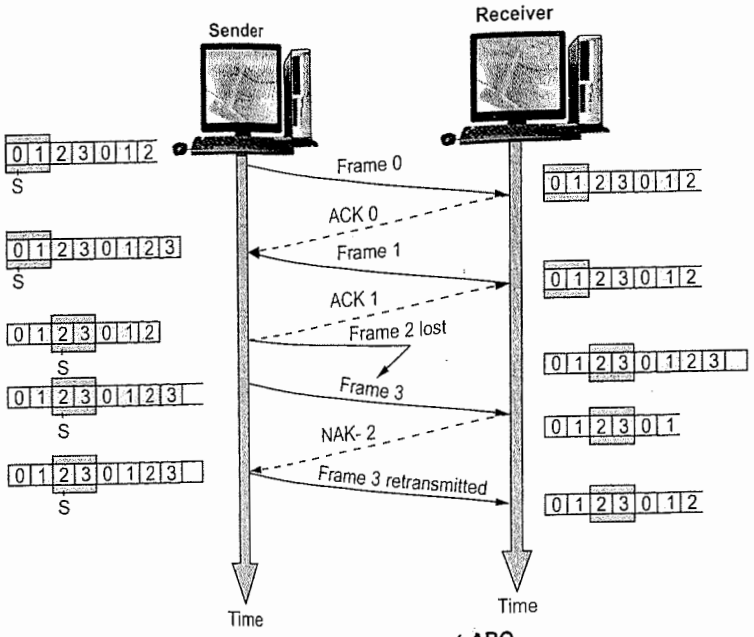


Fig. 2.5.13 Selective repeat ARQ

Advantage :

1) Fewer retransmissions.

Disadvantages :

1) More complexity at sender and receiver.
2) Each frame must be acknowledged individually (no cumulative acknowledgements).
3) Receiver may receive frames out of sequence.

2.5.5 Comparison of Flow Control Protocols

Sr. No.	Parameters	Stop-and-Wait protocol	Go-Back-N protocol	Selective repeat protocol
1.	Sending window size	One frame	Less than 2^k	Less than or equal to 2^k minus receiving window size
2.	Receiving window size	One frame	One frame	Less than or equal to 2^k minus sending window size

where k = Number of bits used for frame number.

2.5.6 Difference between Go-Back-N and Selective Repeat

Sr. No.	Go-Back-N	Selective repeat
1.	Go-back-N requires all retransmission of the succeeding frame along with the lost or damaged frame.	In selective repeat, only the specific damaged or lost frame is retransmitted.
2.	Sender does not require any logic to select the specific frame for retransmission.	Extra logic is required for searching and retransmission of specific frame.
3.	Receiver do not required any sort of storage and sorting mechanism.	The complexity of sorting and storage mechanism is required by the receiver.
4.	It is not expensive.	It is expensive.

Example 2.5.1 *Consider the use of 1000-bit frames on a 1 Mbps satellite channel with a 270 ms delay. What is the maximum link utilization for*

a) Stop-and-wait flow control ?

b) Sliding window flow control with a window size of 7 ?

c) Sliding window flow control with a window size of 127 ?

d) Sliding window flow control with a window size of 255 ?

Solution : Given data :

Frame = 1000 bits,

Channel data rate = 1 Mbps,

Propagation delay = 270 ms

a) Maximum link utilization with stop-and-wait flow control :

$$U = \frac{1}{1+2a}$$

where $a = \frac{t_{prop}}{t_{frame}}$

Since t_{prop} = 270 ms.

In order to find the value of U, we need to calculate t_{frame}

Frame = 1000 bits

Max bit rate = Channel bit rate = 1 Mbps then

$$t_{frame} = \frac{1000}{10^6}$$

$$U = \frac{1}{1+2a} = \frac{1}{1+2\times 270} = 1.85 \times 10^{-3} = 0.185\ \%$$

b) Maximum link utilization with flow control of windows size 7 :

Maximum link utilization for window flow control is U = 1 for W 2a + 1

$$U = \frac{W}{2a+1} \qquad \text{for } W < 2a + 1$$

Since W = 7 and a = 270

Then (2a + 1) = (2 × 270 + 1) = 541 which means that W < 2a + 1

$$U = \frac{W}{2a+1} = \frac{7}{541} = 0.013 = \mathbf{1.3\ \%}$$

c) Maximum link utilization with flow control of windows size 127 :

Maximum link utilization for window flow control is U = 1 for W 2a + 1

$$U = \frac{W}{2a+1} \qquad \text{for } W < 2a + 1$$

Since W = 127 and a = 270

Then (2a + 1) = (2 × 270 + 1) = 541 which means that W < 2a + 1

$$U = \frac{W}{2a+1} = \frac{127}{541} = 0.235 = 23.5\ \%$$

d) Maximum link utilization with flow control of windows size 255 :

Maximum link utilization for window flow control is U = 1 for W 2a + 1

$$U = \frac{W}{2a+1} \qquad \text{for } W < 2a + 1$$

Since W = 255 and a = 270

Then (2a + 1) = (2 × 270 + 1) = 541 which means that W < 2a + 1

$$U = \frac{W}{2a+1} = \frac{W}{2a+1} = 0.471 = \mathbf{47.1\ \%}$$

Example 2.5.2 *A channel has a data rate of 4 kbps and a propagation delay of 20 ms. For what range of frame sizes does stop-and-wait give an efficiency of at least 50 % ?*

Solution : Data rate = 4 kbps

Bit duration = $\frac{1}{4000}$ = 0.25 ms

Time to transmit frame is (t_{frame}) :

$$t_{frame} = \frac{\text{Frame size}}{\text{Bit rate}} = \text{Frame size} \times \text{Bit duration}$$

For stop and wait flow control, efficiency (U) = $\frac{1}{(2a+1)}$

Where $a = t_{prop} / t_{frame}$

t_{prop} = 20 ms

Solving this equation with respect to a

$$a = 0.5[(1/U) - 1]$$

For U ≥ 50 % = 0.5, then $a \le 0.5\left[(1/0.5)-1\right] \Rightarrow a \le 0.5$

Since $a = t_{prop}/t_{frame}$ then $t_{prop}/t_{frame} \le 0.5 \Rightarrow t_{frame} \ge 2t_{prop}$

But frame_size = t_{frame}/bit_ duration =>

Frame_size ≥ $2t_{prop}$ / bit_ duration = 2 × 20 ms / 0.25 ms = 160

University Questions

1. *Explain Go Back - N ARQ protocol and selective repeat ARQ protocol.* **SPPU : Dec.-13, Marks 8**
2. *Explain selective repeat ARQ protocol.* **SPPU : May-14, Marks 6**
3. *Explain bit stuffing in detail ? Explain GBN ARQ technique.* **SPPU : May-14, Marks 6**
4. *Explain simplest protocol and stop and wait ARQ protocol for noiseless channels with suitable diagram.* **SPPU : Dec.-14, Marks 8**

2.6 HDLC

SPPU : May-12, 14 Dec.-13

- HDLC is the most important data link control protocol, also it is the basis for many other important data link control protocols, which use the same or similar formats and the same mechanisms as employed in HDLC.
- The HDLC protocol is an international standard that has been defined by ISO for use on both point-to-point and multipoint data links.
- It supports full duplex, transparent mode operation and is now extensively used in both multipoint and computer networks.
- Although the acronym HDLC is now widely accepted, a number of large manufacturers and other standards bodies still use their own acronyms. These include IBM's SDLC (Synchronous Data Link Control) and ADCCP (Advanced Data Communications Control Procedure), which is used by the American National Standards Institute (ANSI).
- To satisfy a variety of applications, HDLC defines three types of stations. These are,

1) Primary station : Primary station has the responsibility for controlling the operation of the link. Frames issued by the primary are called **command.**

2) Secondary station : Secondary station operates under the control of the primary station. Frames issued by a secondary are called responses. The primary maintains separate logical links with each secondary station of the line.

3) Combined station : It combines the features of primary and secondary. A combined station may issue both commands and **responses.**

- Since HDLC has been defined as a general purpose data link control protocol. The stations can be configrated in different network configurations as,
  - i) Point-to-point with single primary and secondary.
  - ii) Multipoint with single primary and multiple secondaries.
  - iii) Point-to-point with two primaries and two secondaries.

  All above configurations are illustrated in Fig. 2.6.1 (a) and 2.6.1 (b).

i) Point-to-point with single primary and secondary

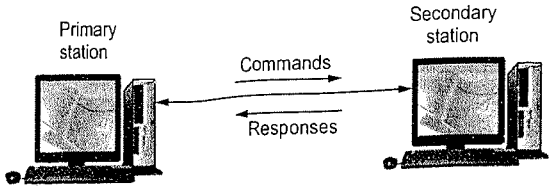


Fig. 2.6.1 Point-to-point link

ii) Multipoint with single primary and multiple secondaries

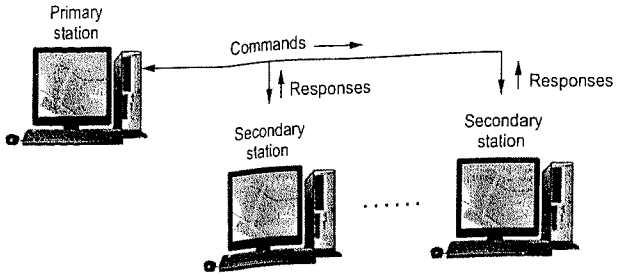


Fig. 2.6.1 (a) Multipoint link

iii) Point-to-point with two primaries and two secondaries

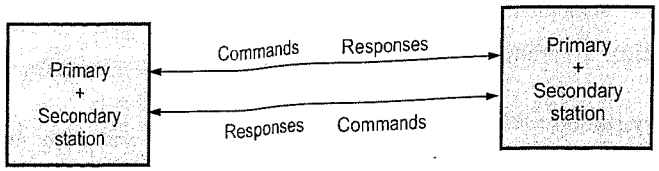


Fig. 2.6.1 (b) Point-to-point link between combined stations

- The frames sent by primary station to the secondary station are known as **commands** and those from the secondary to the primary as **responses.**

- Two configurations shown in part (i) and (ii) have a single primary station are known as **unbalanced configurations.** Unbalanced configuration supports both full duplex and half duplex transmission.
- The configuration in part (iii) has two primary stations and is known as **balanced configuration**. Balanced configuration supports both full duplex and half duplex transmission. Since each station has both a primary and a secondary, they are also known as **combined stations.**

2.6.1 Operational Mode of HDLC

HDLC has following data transfer modes :

1) Normal Response Mode (NRM).

2) Asynchronous Balanced Mode (ABM).

1) Normal Response Mode (NRM)

- This is used in unbalanced configurations. There are one primary station and multiple secondary stations.
- A primary station can send commands; a secondary station can only respond.
- Fig. 2.6.2 shows a Normal Response Mode (NRM).

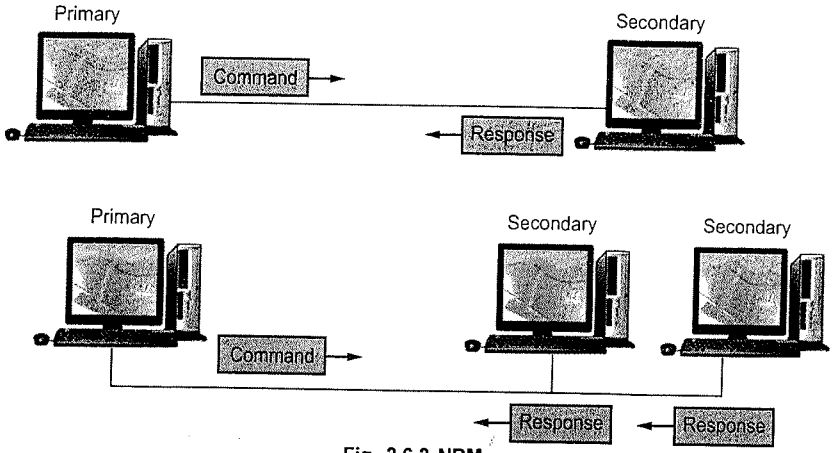


Fig. 2.6.2 NRM

- The NRM is used for both point-to-point and multipoint links.

2) Asynchronous Balanced Mode (ABM)

- In ABM, the configuration is balanced. The link is point to point and each station can functions as a primary and a secondary.
- Fig. 2.6.3 shows the ABM.

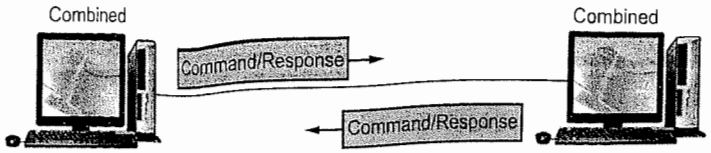


Fig. 2.6.3 ABM

- Either station can send data, control information or commands. This is typical in connections between two computers and in the X.25 interface standard.

2.6.2 Frames

In HDLC both data and control messages are carried in a standard format frame. Three classes of frame are used in HDLC.

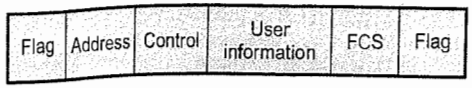
1) Unnumbered frames (U-frames) : These are used for functions such as link setup and disconnection. The name derives from the fact that they do not contain any acknowledgment information, which is contained in sequence numbers.

2) Information frames (I-frames) : These carry the actual information or data and are normally referred to simply as I-frames. I-frames can be used to piggy back acknowledgment information relating to the flow of I-frames in the reverse direction when the link is being operated in ABM or ARM.

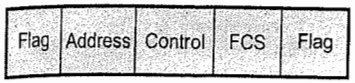
3) Supervisory frames (S-frames) : These are used for error and flow control and hence contain send and receive sequence numbers.

Frame structure

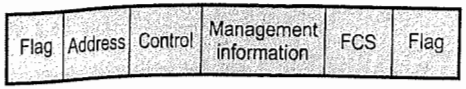
- HDLC uses synchronous transmission. All transmissions are in the forms of frames.
- Fig. 2.6.4 shows the structure of HDLC frame.
- The flag address and control bits before the information or data fields are known as a header. The FCS and flag fields following the data fields are referred as a trailer.



(a) I-frame



(b) S-frame



(c) U-frame

Fig. 2.6.4 HDLC frames

- **Flag fields :** It has a unique pattern at both the ends of the frame structure. It identifies the start of the frame and end of frame. The length of flag field is 8-bit.

- **Address fields :** Address field states the destination address. The address field is usually 8-bit long but can be extended.
- **Control fields :** Control fields contain frame numbers. Also it controls the acknowledgment of frames. Control field is 8 or 16 bits in length.
- **Information fields :** Data field contains the user data received from the network layer. It can be of variable length but in integral number of octets.
- **FCS (Frame Check Sequence) :** FCS is an error detecting code calculated from the remaining bits of the frame. FCS can be 16 bits or 32 bits long.

2.6.3 Control Field

Control field for I-frames

- I-frames are designed to carry user data from the network layer. This field also include flow and error control information.
- Fig. 2.6.5 shows the control field in I-frames.

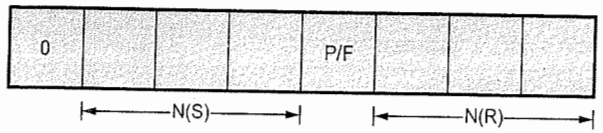


Fig. 2.6.5 Control field in I-frame

- The first bit defines the type. If it is 0, this means the frame is an I-frame.
- Next three bits define the sequence number (NCS). Sequence number range is in between 0 to 7.
- P/F field is 1-bit with dual purpose. This field is set when it is 1. It may be poll or final.
- Last 3-bit corresponds to the acknowledgement number when piggy backing is used.

Control field for S-frames

- S-frames do not have information fields. Fig. 2.6.6 shows the S-frame.

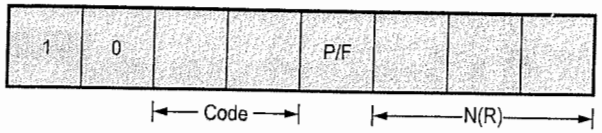


Fig. 2.6.6 S-frame

- If the first 2 bits of the control field is 10. This means the frame is an S-frame.
- The last 3 bits called N(R) corresponds to the acknowledgment number (ACK) or negative acknowledgment number (NAK) depending on the type of S-frame.
- The 2 bits called code is used to define the type of S-frame itself. Types of S-frames are :
  1) Receive Ready (RR)
  2) Receive Not Ready (RNR)
  3) Reject (REJ)
  4) Selective Reject (SREJ)

Code	S-frame type	Remarks
00	Receive ready	N(R) define ACK number
10	Receive not ready	N(R) define ACK number
01	Reject	N(R) define NAK number
11	Selective reject	N(R) define NAK number

Control Field for U-frames

- U-frames contain an information field, but one used for system management information, not user data.
- Fig. 2.6.7 shows U-frames.

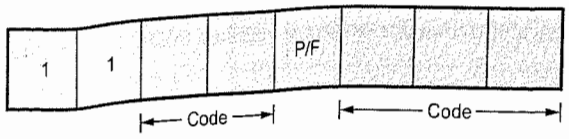


Fig. 2.6.7 U-frames

- U-frames codes are divided into two sections a 2-bit prefix before a P/F and a 3-bit suffix after the P/F bit.

University Questions

1. *Draw the HDLC frame format and explain in detail the control field used in HDLC protocol for different frame types.* **SPPU : May-12, Marks 8**
2. *Draw the HDLC frame format and explain in detail the control field used in HDLC protocol for different frame types.* **SPPU : Dec.-13, Marks 8**
3. *Draw and explain HDLC frame format in detail.* **SPPU : May-14, Marks 3**

2.7 PPP

- PPP is the most commonly used protocol for point-to-point transfer of data. The services provided by PPP are
  1) Formatting of frames to transfer.
  2) Negotiation between devices to establish link.
  3) Encapsulation of data in data link frame.
  4) Authentication of devices.
- PPP can operate between point-to-point transmission link in full duplex mode. Also PPP can be used as a data link control to connect two routers.

2.7.1 Frame Format

- PPP frame format is similar to HDLC. Fig. 2.7.1 shows PPP frame format. It has seven fields.

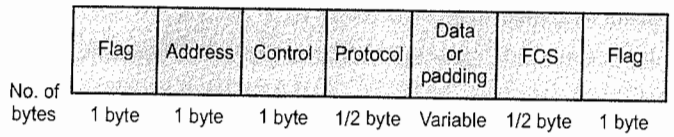


Fig. 2.7.1 PPP frame format

1) **Flag field :** The flag field identifies the boundaries of PPP frame i.e. each frame begins and ends with flag field. This field is 1 byte in length.
2) **Address field :** Address field indicates the address of destination. Address field is 1 byte (8-bits). When the address field contains "all 1's" i.e. 11111111, this indicates that all stations are to accept the frames (broadcast).
3) **Control field :** PPP normally runs in connectionless mode therefore control field is set to 11000000. This indicates unnumbered frames i.e. frame does not contain sequence numbers and there is no flow or error control.
4) **Protocol field :** Protocol field defines the information of data field. The protocol field is 1 or 2 bytes long.
5) **Data field :** The data field contains the actual data to transmit. The length of this field is variable.
6) **Frame Check Sequence (FCS) :** The FCS field is 24 byte long and contains CRC code. It checks length of all fields in frame.

2.7.2 Transition States

- The transition state is used to indicate the phases through which PPP connection passes. Fig. 2.7.2 shows PPP transition states.
- The PPP connection passes through five important states.
  1) Idle state
  2) Link establishing state
  3) Authenticate state
  4) Exchange of data state
  5) Terminate link state.

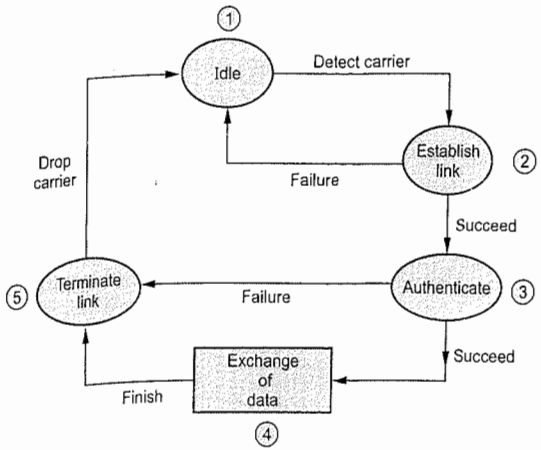


Fig. 2.7.2 Transition states for PPP

1) **Idle state :** In the idle state the link is not in use. The carrier is not activated in this state.
2) **Link establishing state :** When carrier is detected, one of the end points starts the transmission then connection enters into the link establishing state. Under this state there is negotiation between the devices. On successful negotiation, the connection enters into authenticate state otherwise it enters into idle state.
3) **Authenticate state :** The authenticate state is mutually decided by the stations. The stations sent several authentication packets. On successful authentication, the connection enters into exchange of data state otherwise to the terminate link state.
4) **Exchange of data state :** This state is also referred as networking state. In this state exchange of data started. The connection is terminated only after the any of the end points wants to terminate.
5) **Terminate link state :** After data exchange is over several packets are exchanged between and points for closing the link.

2.7.3 PPP Stack

- PPP uses a stack of other protocols for establishing link and to authentications. Two major protocols are used in PPP stack. These protocols are -
  1) Link Control Protocol (LCP)
  2) Network Control Protocol (NCP)

- During connection a PPP packet carry any of these protocols in its data field as shown in Fig. 2.7.3.

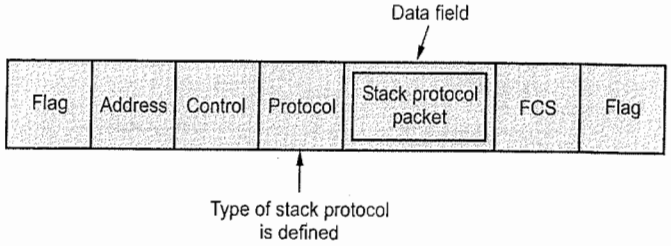


Fig. 2.7.3 PPP stack

2.7.4 Link Control Protocol (LCP)

- The LCP performs the function of establishing, maintaining, configuring and termination of links. LCP also involves in negotiating mechanism between stations. The PPP carries LCP packet in either establishing or terminating state i.e. when user data is not carried. Fig. 2.7.4 shows the frame format of LCP packet and how it is encapsuled in PPP frame.

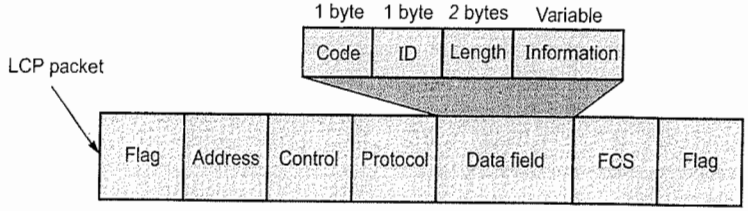


Fig. 2.7.4 LCP frame in PPP frame

1) **Code field :** Code field is 1 byte in length. The code field defines the type of LCP packet. There are three types of LCP packets - Configuration packets, link termination and link monitoring packets.
2) **ID :** ID field is 1 byte in length. ID field is used to match the request packet with its reply packet. The request end point inserts a value in this field which is copied in corresponding field in reply packet.
3) **Length :** The length field is 2 bytes. It defines the entire length of LCP packet.
4) **Information :** This is a variable length field. Any additional information needed by LCP packet is stored in this field.

LCP packet types

- The LCP packets can be categorized according to their function. Fig. 2.7.5 shows types of LCP packets.

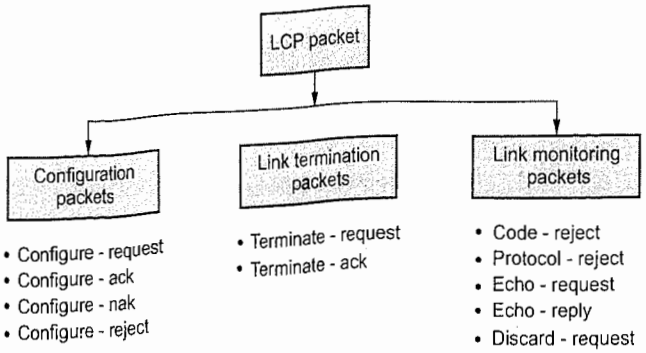


Fig. 2.7.5 LCP packet types

2.7.5 Network Control Protocol (NCP)

- The PPP uses Network Control Protocol (NCP) when it enters in exchange of data state. NCP is a set of protocols which allows encapsulation of data from network layer into PPP frame.
- PPP extends the negotiation not only in data link layer but in network layer also. The set of packets that establish and terminate a network layer connection for IP packets is called **Internetwork Protocol Control Protocol (IPCP).** The format of IPCP packet is shown in Fig. 2.7.6.

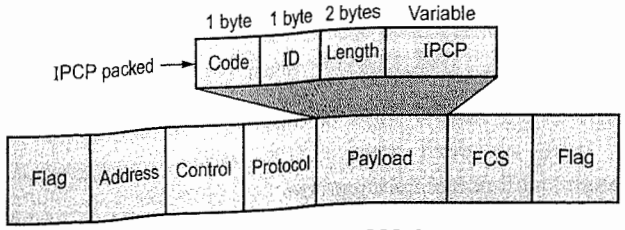


Fig. 2.7.6 IPCP packet in PPP frame

- The protocol field value for IPCP packet is $(8021)_H$. There exists seven types of IPCP packets, each having unique code value (1 byte). IPCP packets and their corresponding code values are shown in Table 2.7.1.

Code value	IPCP packets
01	Configure-request
02	Configure-ack
03	Configure-nak
04	Configure-reject
05	Terminate-request
06	Terminate-ack
07	Code-reject

Table 2.7.1 IPCP packets

2.7.6 Comparison of BISYNC and HDLC

Sr. No.	Feature	Characteristic	BISYNC	HDLC
1.	Transmission	Serial	Yes	Yes
		Asynchronous	No	No
		Synchronous	Yes	Yes
2.	Communication mode	Asynchronous	No	Yes
		Synchronous	Yes	Yes
3.	Directional mode	TWA	Yes	Yes
		TWS	No	Yes
4.	Configuration	Point-to-point	Yes	Yes
		Point-to-multipoint	Yes	Yes
5.	Flow control	-	Stop and wait	Sliding windows
6.	Flow control	Content errors	LRC/CRC	CRC
7.	Error detection and correction	Flow integrity errors	ACK-0/ACK-1	Sequence number
8.	Code set	-	ASCII/EBCDIC/Transcde	Any
9.	Control Character	-	Many	None

10.	Framing	Frame identifier	SYN SYN	Flag
		Frame delimiter	ETB/ETX	Flag
		Information field	Multiple bytes	Multiple bits
		Transparency	DLE stuffing	Zero stuffing

2.8 Media Access Control

SPPU : May-12, 13, Dec.-12, 13

- One feature of LAN is that its backbone is a shared channel or transmission link, which provides all user to access to the transmission facilities. It may be possible that two or more stations transmitting simultaneously, causing their signals to interfere and becomes garbled.
- To resolve these conflict, a number of different control mechanisms or access protocol have been devised. In order to handle the bursty nature of LAN, traffic asynchronous TDM is used.
- The asynchronous TDM mechanism is further divided into contention methods (random access) and deterministic methods (controlled methods).

Random access techniques are

i) ALOHA

ii) Carrier Sense Multiple-Access (CSMA)

iii) CSMA with Collision-Detection (CSMA/CD)

iv) Register insertion.

Controlled access to LAN can be performed in two types :

1) Centralized technique : In centralized technique master node decides which node is to access the channel at any one time.

e.g. Polling.

2) Distributed technique : In distributed technique each station is given an opportunity to transmit on the channel.

e.g. i) Token passing method

ii) Slotted ring method.

- Fig. 2.8.1 illustrates the typical multiple access communications where a number of user stations share a transmission medium.
- This sharing techniques are used in wired communications, and networks based on radio communication.

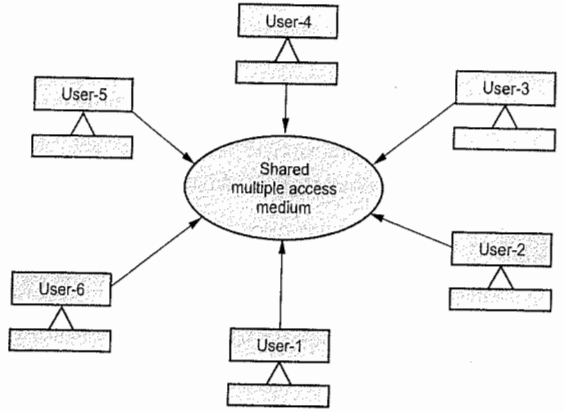


Fig. 2.8.1 Multiple access communication

- In wired communication multidrop cables are used in data networks to connected number of stations to a host computer.
- The host computer broadcasts information to the users on the outbound line.
- The stations transmit information to the host using the inbound line. This system is illustrated in Fig. 2.8.2.

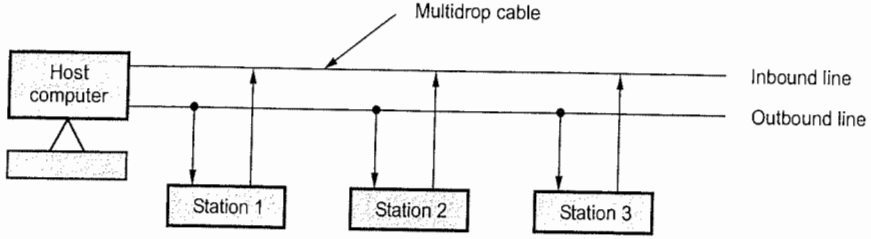


Fig. 2.8.2 Multidrop cable system for access control

- A Medium Access Control (MAC) protocol is developed for this system. Here the host computer issues polling messages to each stations, providing it with permission to transmit on the inbound line.

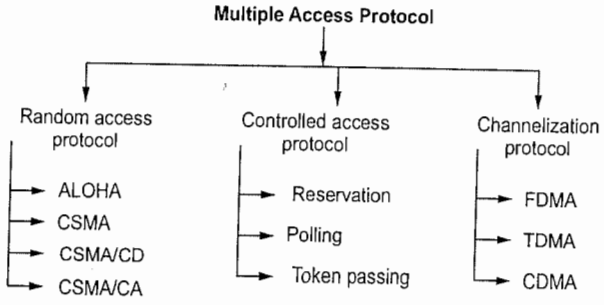


Fig. 2.8.3

- In radio communication several stations share two frequency bands, one for transmitting and one for receiving.
- In satellite communications each station is assigned a channel in an uplink frequency band that it uses to transmit to the satellite. The satellite sends back the signals on different frequency band called down link frequency band.

University Questions

1. *State and explain multiple access protocols in brief.* **SPPU : May-12, Marks 8**
2. *What are the responsibilities of MAC - Layer. Explain IEEE 802.3 MAC - Layer.* **SPPU : Dec.-12, Marks 8**
3. *How the problem of contention is avoided for the channel. Explain giving suitable example.* **SPPU : May-13, Marks 8**
4. *Define CSMA. What is the necessity of collision defect ? Suggest a collision free protocol using CSMA.* **SPPU : Dec.-13, Marks 8**

2.9 Random Access

- Access to the medium from many entry points is called contention. It is controlled with a **contention protocol.**
- In a random access method, each station has the right to the medium without being controlled by other station. However if more than one station tries to send, there is an access conflict, i.e. collision and the frames will be either destroyed or modified.

2.9.1 ALOHA

- The ALOHA protocol was developed at the university of Hawaii in the early 1970s. ALOHA was developed for packet radio networks. However, it is applicable to any shared transmission medium.
- In a system when multiple users try to send messages to other stations through a common broadcast channel random access or contention techniques are used.
- Random access means there is no definite or scheduled time for any station to transmit. This scheme is simplest possible and it is asynchronous. It is asynchronous because there is no co-ordination among users.
- The basic idea of ALOHA system is applicable to any system in which unco-ordinated users are competing for the use of a single shared channel.
- When a station send data, another station may attempt to do so at the same time. The data from the two station collide and become garbled. If two signals collided, so be it. Each station would simply wait a random time and try again.

2.9.1.1 Pure ALOHA

- The original ALOHA protocol is called pure ALOHA. The idea is that each station sends a frame whenever it has a frame to send. Since there is only one channel to share, there is the possibility of collision between frames from different stations.
- Fig. 2.9.1 shows the frame collisions in pure ALOHA.

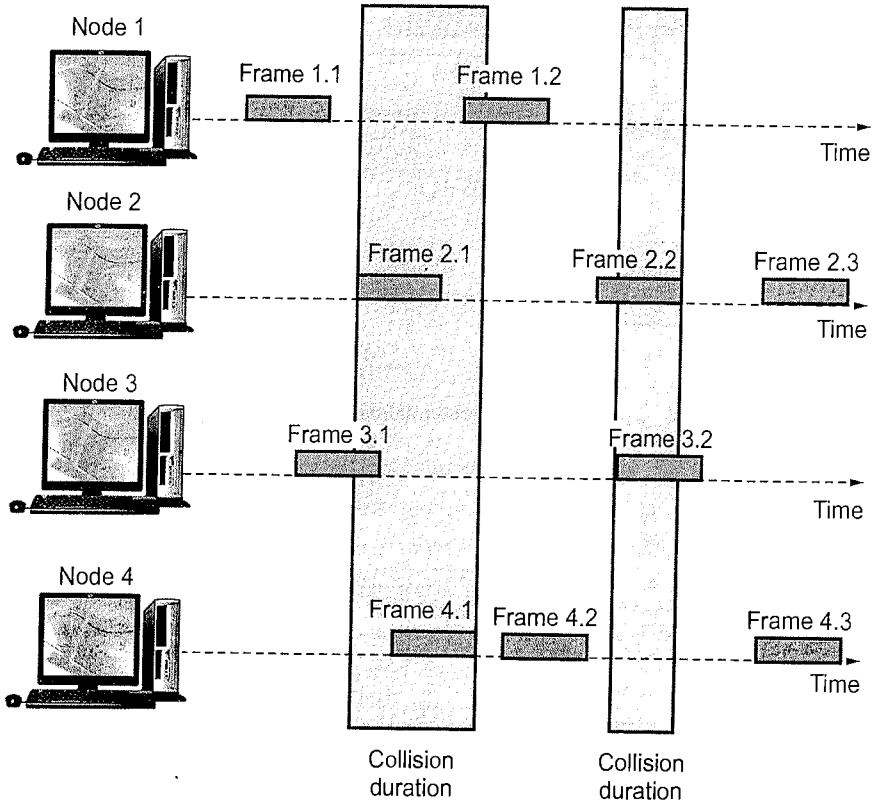


Fig. 2.9.1 Frames in pure ALOHA

- The pure ALOHA protocol relies on acknowledgements from the receiver. When a user sends a frame, it expects the receiver to send an acknowledgement. If the acknowledgement does not arrive after a time out period, the station assumes that the frame has been destroyed and resends the frame.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled. If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

- If all users try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each user waits a random amount of time before resending its frame. The randomness will help to avoid more collisions. This time is called as back-off time (T_B).
- Fig. 2.9.2 shows the procedure for pure ALOHA protocol.

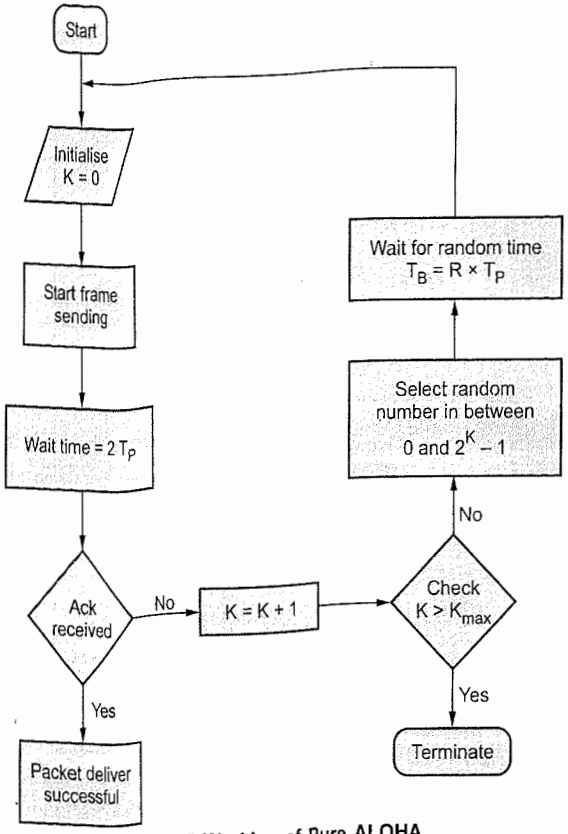


Fig. 2.9.2 Working of Pure ALOHA

- The time out period is equal to the maximum possible round trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations ($2 \times T_p$).
- Let all the packets have the same length. And each requires one time unit for transmission (t_p). Consider any user to send packet A at time t_0. If any other user B has generated a packet between time t_0 and $t_0 + t_p$, the end of packet B will collide with the beginning of packet A. Since in pure ALOHA packet, a station does not listen to the channel before transmitting, it has no way of knowing that above frame was already under way.

- Fig. 2.9.3 shows vulnerable periods during which packets can collide.

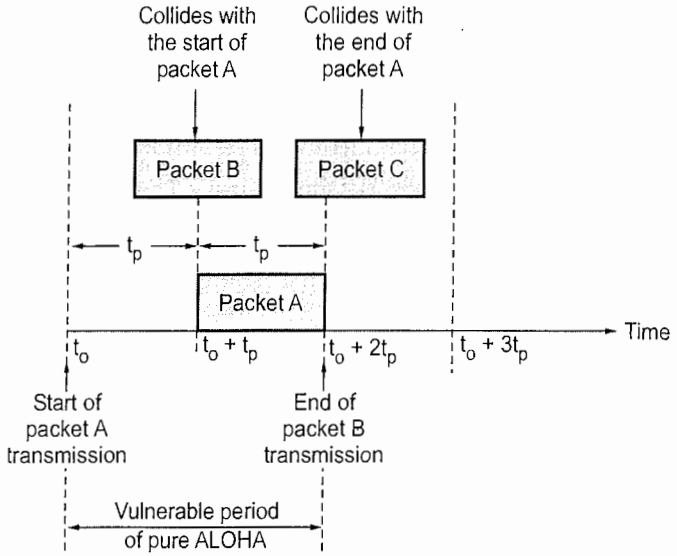


Fig. 2.9.3 Vulnerable period for packet A

- Similarly if another user wants to transmit between $(t_0 + t_p)$ and $(t_0 + 2t_p)$ i.e. packet C, the beginning of packet C will collide with the end of packet A. Thus if two packets overlap by even the smallest amount in the vulnerable period both packets will be corrupted and need to be retransmitted.

Throughput of pure ALOHA channel

1) Throughput :

- The throughput S is defined as average successful traffic transmitted between stations per unit time. The unit of time is slot-time, which is the time required to transmit a frame.
- Assuming all packets or frames are of same size. Since only one packet per slot can be transmitted, the maximum value of S is 1. When collision occurs, some of the packets are lost and part of available channel time is wasted. The resulting value of S is less than 1.

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

2) Offered traffic :

- The offered traffic is the average number of packets per slot time which are presented to the network for transmissions by users. It is denoted by G. The

throughput is expressed in terms of offered load or traffic G. Practically G can have any value between 0 to infinity.

3) Channel capacity :

- The maximum achievable throughput for a particular type of access scheme is called the capacity of the channel.
- To find the throughput of channel, let us assume that the probability (p_k) that k packets generated during a given slot-time follows a Poisson's distribution with a mean G per packet time is given by,

$$p_k = \frac{G^k \cdot e^{-G}}{k!} \quad \ldots (2.9.1)$$

The throughput S is then just the offered load G times the probability of a transmission being successful.

$$\therefore \quad S = G p_0 \quad \ldots (2.9.2)$$

where p_0 = Probability that a packet does not suffer a collision

The probability of no other traffic being initiated during the entire vulnerable period is thus given by

$$p_0 = e^{-2G} \quad \ldots (2.9.3)$$

From equation (2.9.2),

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

The maximum throughput occurs at G = 0.5,

i.e. $$S = \frac{1}{2e} = 0.184$$

- This means that the best channel utilization that can be achieved is around 18 % for pure ALOHA method.
- The advantage of pure ALOHA protocol is its simplicity, which can result in low cost user stations since no synchronization is required between stations in the system. Each station transmits a packet whenever its buffer has one. The disadvantage is somewhat inefficient channel utilization i.e. maximum channel utilization is only 18.4 % of the available capacity.

2.9.1.2 Slotted ALOHA

- In slotted ALOHA, the channel time is divided into time slots and the stations are allowed to transmit at specific instance of time. These time slots are exactly equal to the packet transmission time. All users are then synchronized to these time

slots, so that whenever a user generates a packet it must synchronize exactly with the next possible channel slot. Consequently the wasted time due to collisions can be reduced to one packet time or vulnerable period is reduced to half.

- Transmission attempts for four network user and random retransmission delays for colliding packets in slotted ALOHA is shown in Fig. 2.9.4.

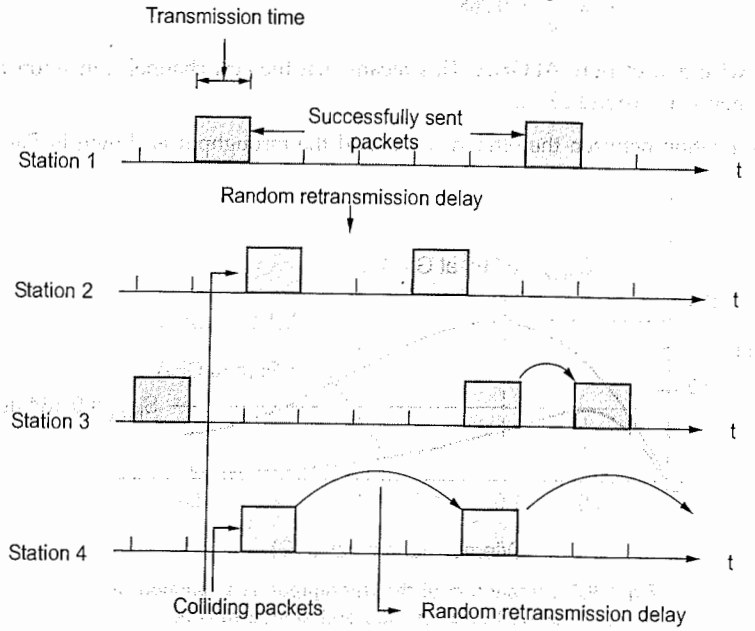


Fig. 2.9.4 Transmission attempts and random retransmission delays for colliding packets in slotted ALOHA

Slotted ALOHA

Assumptions :

1. All frames are of same size.
2. Time is divided into equal sized slots, a slot equals the time to transmit one frame.
3. Nodes start to transmit frames only at beginning of slots.
4. Nodes are synchronized.
5. If two or more nodes transmit in a slot, all nodes detects collision before the slot ends.

Throughput of slotted ALOHA channel

- In slotted ALOHA, the packets arrive in a synchronized fashion. The probability of single transmission during a slot time is,

$$p_0 = e^{-G} \quad \ldots (2.9.4)$$

From equation (2.9.2)

$$S = G \cdot e^{-G} \quad \ldots (2.9.5)$$

The maximum throughput occurs at G = 1,

i.e. $$S = \frac{1}{e} = 0.368$$

which is twice that of pure ALOHA. This means that the best channel utilization that can be achieved is around 37 %.

- The relation between the offered traffic and the throughput is shown in Fig. 2.9.5.

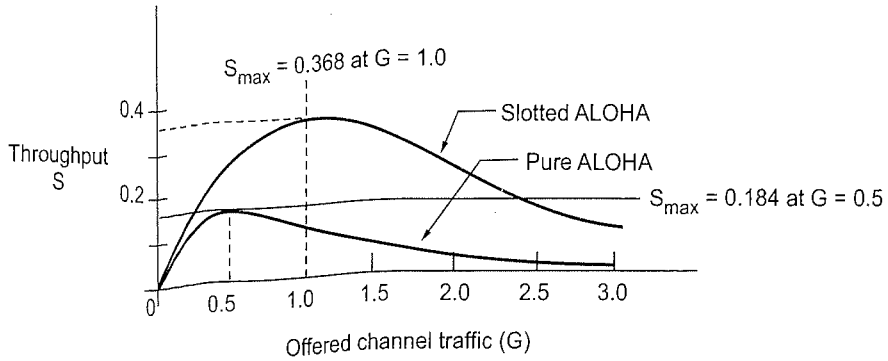


Fig. 2.9.5 Comparison of the throughput as a function of offered load for pure and slotted ALOHA

Pros and Cons of slotted ALOHA

Pros

1. Single active node can continuously transmit at full rate of channel.
2. Highly decentralized, each node independently decides when to retransmit.
3. Simple to implement.

Cons

1. Collisions waste slots.
2. Idle slots.

Example 2.9.1 *Calculate the throughput S for a pure ALOHA network if the offered traffic G is 0.75.*

Solution : For pure ALOHA, throughput S is given by,

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

$$\therefore \quad S = 0.75 * e^{-2 * 0.75} = 0.1673$$

or $$S = 16.73\ \%$$

Example 2.9.2 *A slotted ALOHA channel has an average 10 % of the slots idle.*

a) What is the offered traffic G ?

b) What is the throughput ?

c) Is the channel overloaded or underloaded ?

Solution : For slotted ALOHA channel,

a) Probability of single transmission during a slot time is = e^{-G}.

$$10\ \% = e^{-G}$$

$$0.1 = e^{-G}$$

$$\Rightarrow \quad -G = -2.3$$

$$\therefore \quad G = 2.3$$

b) $$S = G * e^{-G} = 2.3 * e^{-(2.3)} = 0.23$$

c) For slotted ALOHA, S is maximum at G = 1.

Here G = 2.3 and

S = 0.23

It is beyond G = 1, hence it is **overloaded**.

2.9.3 Difference between Pure ALOHA and Slotted ALOHA

Sr. No.	Pure ALOHA	Slotted ALOHA
1.	Frames are transmitted at arbitrary time.	Time is divided up into discrete slot, the frame is sent at the start of a slot.
2.	Throughput (s) = $G \times e^{-2G}$	Throughput (s) = $G \times e^{-G}$
3.	Vulnerable time is 2 times the frame transmission time.	Vulnerable time is one half that of pure ALOHA.
4.	The maximum utilization is about 18.4 %.	The maximum utilization is about 36.8 %.
5.	Global time is not required.	It requires global time for synchronization, as it is divided up into discrete slot.

6.	Simple to implement.	Implementation is complex due to the synchronization of all nodes.
7.	Cannot used for satellite, due to very low utilization.	It is used in broadcast satellites.

2.9.2 Carrier Sense Multiple Access Protocol

- The low maximum throughput of the ALOHA schemes is due to the wastage of transmission bandwidth because of frame collisions. This wastage can be reduced by avoiding transmissions that are certain to cause collisions. By sensing the medium for the presence of a carrier signal from other stations, a stations can determine whether there is an ongoing transmission.
- CSMA requires that each station first listen to the medium before sending. CSMA can reduce the possibility of collision, but it cannot eliminate it.
- The possibility of collision still exists because of propagation delay. A station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

Vulnerable Time

- The vulnerable time for CSMA is the propagation time (T_p). This is the time needed for a signal to propagate from one end of the medium to the other.
- Fig. 2.9.6 shows the vulnerable time for CSMA. Station A sends a frame at time t_1, which reaches the rightmost station D at time $t_1 + T_p$.

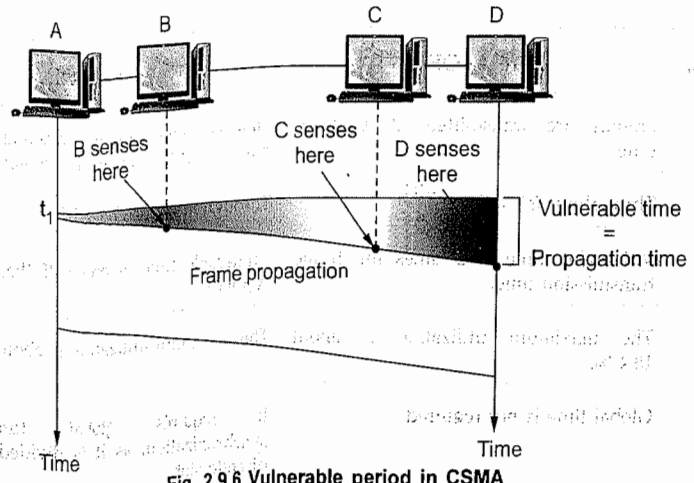


Fig. 2.9.6 Vulnerable period in CSMA

Persistence Methods

- These three protocols are
  1) Non-persistent CSMA.
  2) 1-persistent CSMA.
  3) p-persistent CSMA.

All three protocols are differing by the action to be taken by any station after sensing the readiness of the channel.

1) Non-persistent CSMA :

- In non-persistent CSMA, when a station having a packet (frame) to transmit and finds that the channel is busy, it backs off for a fixed interval of time. It then checks the channel again and if the channel is free then it transmits. The back-off delay is determined by the transmission time of a frame, propagation time and other system parameters. If the channel is already in use, the station does not continuously senses it for the purpose of seizing it immediately upon detecting the end of the previous transmission. But it waits a random period of time and again checks for activity.
- Fig. 2.9.7 shows flow diagram for non-persistent CSMA.

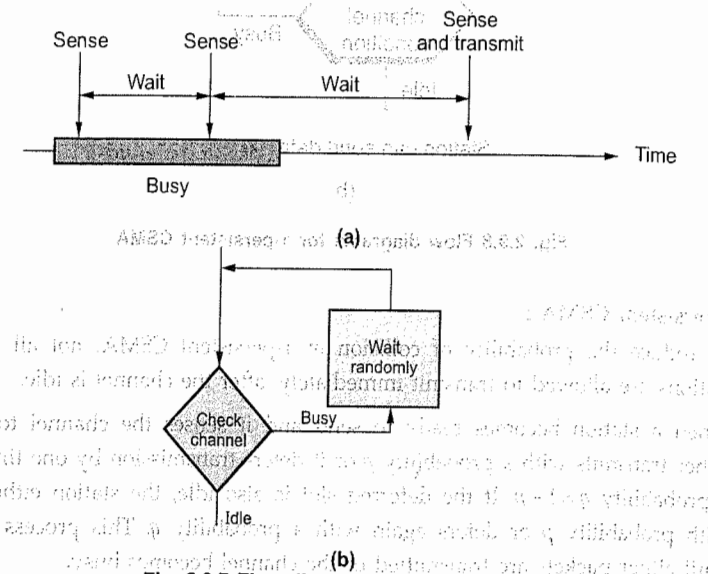


Fig. 2.9.7 Flow diagram for non-persistent

2) 1-persistent CSMA :

- Any station wishing to transmits, monitor the channel continuously until the channel is idle and then transmits immediately with probability one, hence the name 1-persistent.

- When two or more stations are waiting to transmit, a collision is guaranteed. Since each station will transmit immediately at the end of busy period. In this case each will wait a random amount of time and will then reattempt to transmit.
- As in the case with non-persistence CSMA, the performance of 1-persistent CSMA protocol depends on the channel delay time.
- Fig. 2.9.8 shows the flow diagrams for 1-persistent CSMA.

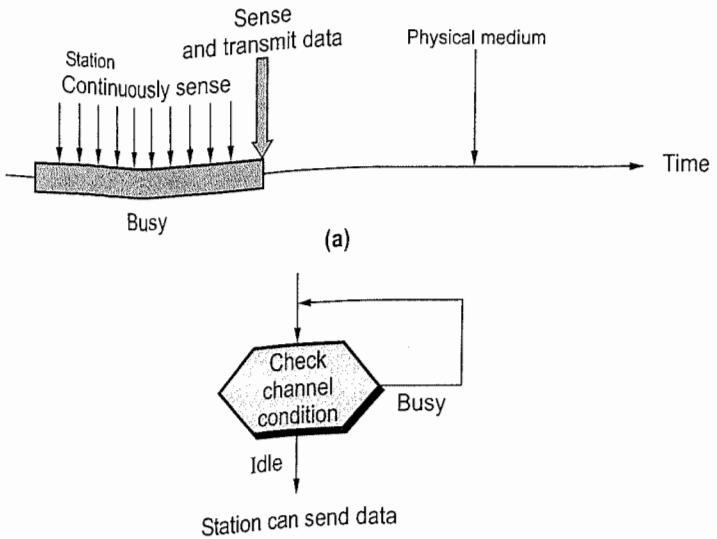


Fig. 2.9.8 Flow diagrams for 1-persistent CSMA

3) **p-persistent CSMA :**

- To reduce the probability of collision in 1-persistent CSMA, not all the waiting stations are allowed to transmit immediately, after the channel is idle.
- When a station becomes ready to send and it senses the channel to be idle, it either transmits with a probability p or it defers transmission by one time slot with a probability $q = 1 - p$. If the deferred slot is also idle, the station either transmits with probability p or defers again with a probability q. This process is repeated until either packets are transmitted or the channel becomes busy.
- Fig. 2.9.9 shows the flow diagram for p-persistent CSMA.

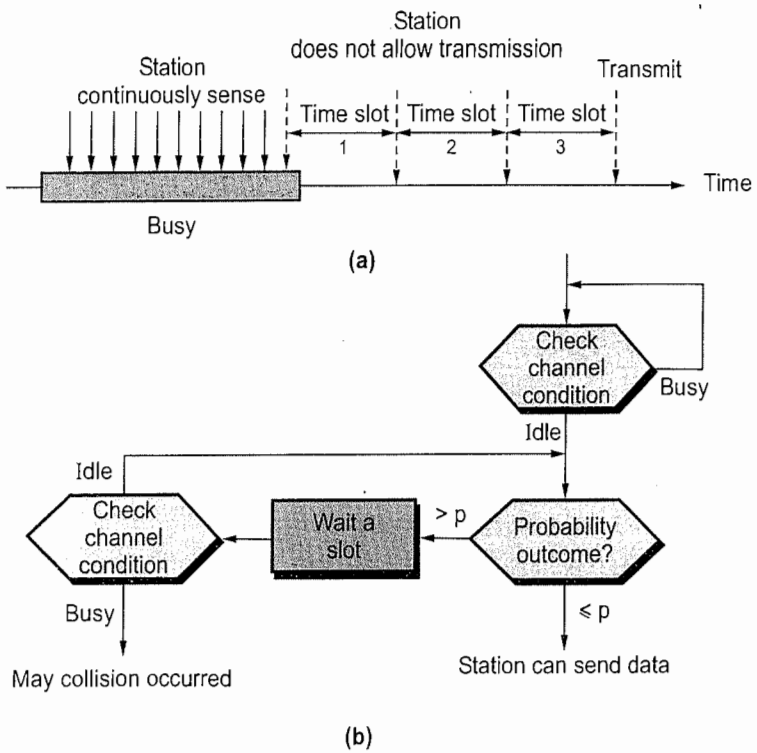


Fig. 2.9.9 Flow diagrams for p-persistent CSMA

2.9.3 Carrier Sense Multiple Access with Collision Detection

- In both CSMA and ALOHA schemes, collisions involve entire frame transmissions. If a station can determine whether a collision is taking place, then the amount of wasted bandwidth can be reduced by aborting the transmission when a collision is detected. The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) use this approach.
- CSMA/CD is the most commonly used protocol for LANs. CSMA/CD specifications were developed jointly by Digital Equipment Corporation (DEC), Intel and Xerox. This network is called as Ethernet. The IEEE 802.3 CSMA/CD standard for LAN is based on Ethernet specification.
- The basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending. If another station is sending, the second station must wait or defer, until the sending station has finished. Then it may send its message. If no station was sending at the time that it first listened, the station may send its message immediately. The term "carrier sense" indicates this "listening before transmitting" behaviour.

- If two or more stations have messages to send at the same time and they are separated by significant distances on the bus/channel, each may begin transmitting at roughly the same time without being aware of the other station. The signals from each station will superimpose on the channel and is garbled beyond the decoding ability of the receiving station. This is termed as "collision".
- A protocol is required for transmitting station to monitor the channel while sending each of its messages and to detect such "collisions".
- When a collision has been detected, each of sending stations must cease transmitting, wait for a random length of time, and then try again. Because of quick termination of transmission time and bandwidth is saved. Therefore CSMA/CD is more efficient than ALOHA, slotted ALOHA and CSMA.
- CSMA/CD networks work best on a bus, multipoint topology with bursty asynchronous transmission. All stations are attached to one path and monitor the signal on the channel through transreceiver attached to the cable.
- CSMA/CD has totally decentralized control and is based on contention access.
- Fig. 2.9.10 illustrates this technique. Station A and station D are the extreme ends of a bus structure.

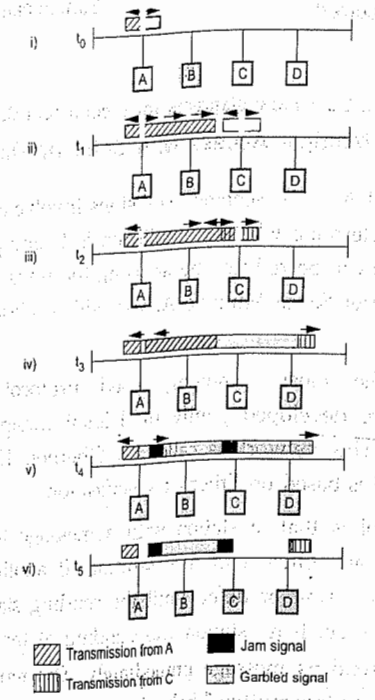


Fig. 2.9.10 CSMA/CD operation

i) Station A listens channel starts transmitting a packet addressing D.

ii) Station B and C are ready for transmission. B senses a transmission on channel so defers. C is unaware of transmission and begins its own transmission.

iii) Station A's transmission reaches C. C detects collision and ceases transmission. Sends jam signal.

iv) Effect of collision propagates back to A, A stops its transmission.

v) A sends jam signal.

vi) No station is transmitting but there are still signals on the bus.

- CSMA/CD supports both baseband and broadband system. CSMA/CD offers four options in terms of bit rate, signaling method and maximum electrical cable segment length. These are
  1) 10BASE5 2) 10BASE2 3) 10BROAD36 4) 1BASE5
- The numeric field in the beginning indicates the bit rate in Mbps, the middle term indicates type of signaling system i.e. baseband or broadband, the numeric field in the end indicates the electrical cable segment length in X 100 metres.
- Manchester signal code is used at the baseband level of transmission. In broadband transmission, Differential Phase Shift Keying (DPSK) is used to convert the Manchester encoded signal into analogue form.
- Fig. 2.9.11 shows the flowchart for CSMA/CD procedure.

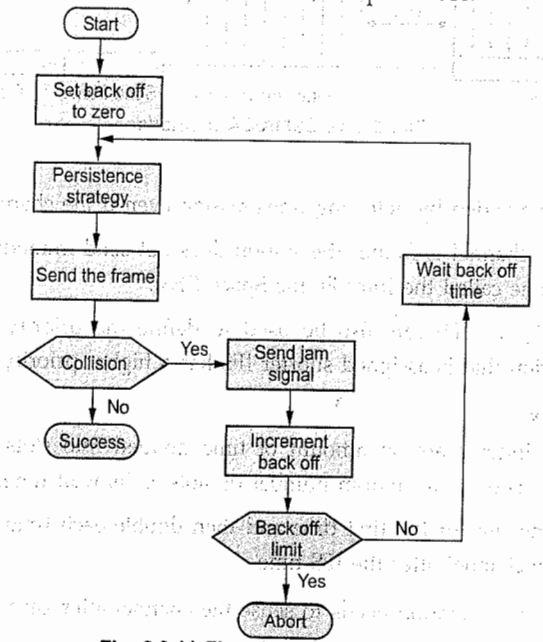


Fig. 2.9.11 Flowchart for CSMA/CD

CSMA/CD throughput

- The throughput of CSMA/CD is greater than that of pure or slotted ALOHA.
- For 1-persistent method, the maximum throughput is around 50 % when G = 1.
- For non-persistent method, the maximum throughput can go upto 90 % when G is between 3 and 8.

2.9.4 Carrier Sense Multiple Access with Collision Avoidance

- Wireless networks cannot use CSMA/CD in the MAC sublayer, since this requires the ability to receive and transmit at the same time - hence the use of CSMA/CA.
- In a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection. We need to avoid collision on wireless networks because they cannot be detected. So CSMA/CA was invented for this network.
- Collisions are avoided by using three methods.
  a. Inter-frame space b. Contention window c. Acknowledgments
- Fig. 2.9.12 shows the all three method of CSMA/CA

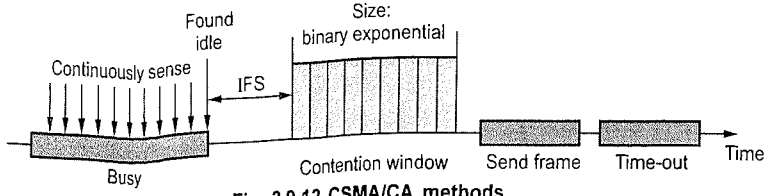


Fig. 2.9.12 CSMA/CA methods

Inter-frame space

- Collisions are avoided by deferring transmission even if the channel is found idle.
- When an idle channel is found, the station does not send immediately. It waits for a period of time called the Inter-Frame Space (IFS).
- In CSMA/CA, the IFS can also be used to define the priority of a station of a frame. A station that is assigned shorter IFS has a higher priority.

Contention window

- Contention windows are an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.
- Station set one slot for the first time and then double each time the station cannot detect an idle channel after the IFS time.
- In this method, 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 and restarts it when the channel is sensed as idle.
- This method gives the priority to the station with the longest waiting time.

Acknowledgments

- The data may be corrupted during the transmission. The positive acknowledgment and the time out can help guarantee that the receiver has received the frame.
- Fig. 2.9.13 shows the flowchart for CSMA/CA.

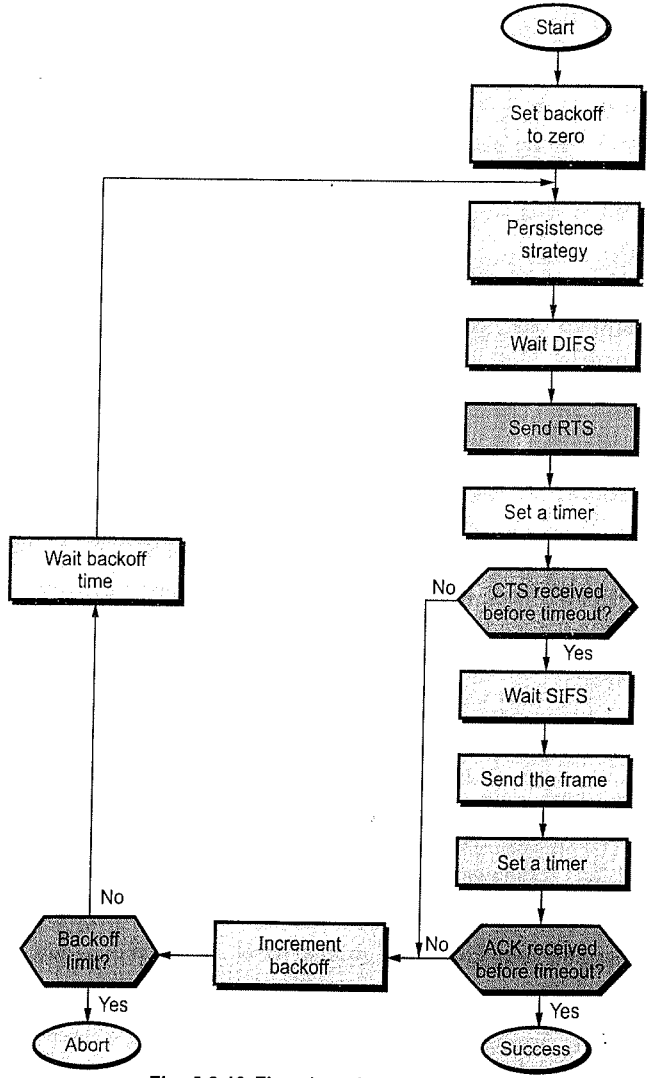


Fig. 2.9.13 Flowchart for CSMA/CA

Hidden Node Problem

- In the case of wireless network it is possible that A is sending a message to B, but C is out of its range and hence while "listening" on the network it will find the network to be free and might try to send packets to B at the same time as A. So, there will be a collision at B.
- The problem can be looked upon as if A and C are hidden from each other. Hence it is called the "hidden node problem".
- Fig. 2.9.14 shows node A is transmitting.

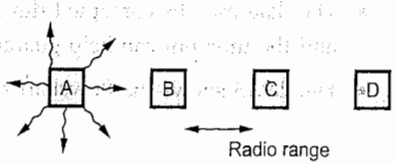


Fig. 2.9.14 A transmitting

Exposed Node Problem

- If C is transmitting a message to D and B wants to transmit a message to A, B will find the network to be busy as B hears C transmitting. Even if B would have transmitted to A, it would not have been a problem at A or D.
- CSMA/CD would not allow it to transmit message to A, while the two transmissions could have gone in parallel.
- Fig. 2.9.15 shows node B is transmitting.

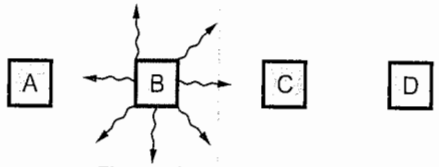


Fig. 2.9.15 B transmitting

2.10 Controlled Access

SPPU : May-14, Dec.-14

1. In this, the stations consult one another to find which station has the right to send.
2. A station cannot send unless it has been authorized by other stations.
3. Controlled access methods are :

   i. Reservation ii. Polling iii. Token passing.

2.10.1 Reservation

1. Before sending data, station needs to make a reservation.

   Fig. 2.10.1 shows the reservation access method.

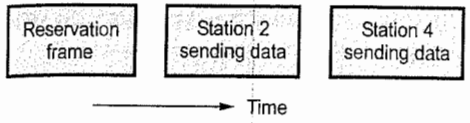


Fig. 2.10.1 Reservation access method

2. Number of reservation are equal to number of stations.
3. Each station have their own minislot in the reservation frame.
4. When station needs to send a data frame, it makes a reservation in its own minislot.

5. The stations that have made reservations can send their data frames after the reservation frame.
6. In the first slot, only station 1, 3 and 4 have made reservation.

2.10.2 Polling

1. Polling works with topology.
2. One device is designed as primary station and other devices are secondary station.
3. Link control is done by primary device.
4. All data exchange take place through primary device.
5. Primary device decides, which device is allowed to use the channel at a given time.
6. If primary device wants to receive data, it asks the secondaries if they have anything to send, this function is called **polling.**
7. Select mode and poll mode are the two functions of polling.
8. In polling, primary device receive the data.
9. In select mode, primary device sends data to secondary device.

Fig. 2.10.2 shows the select mode.

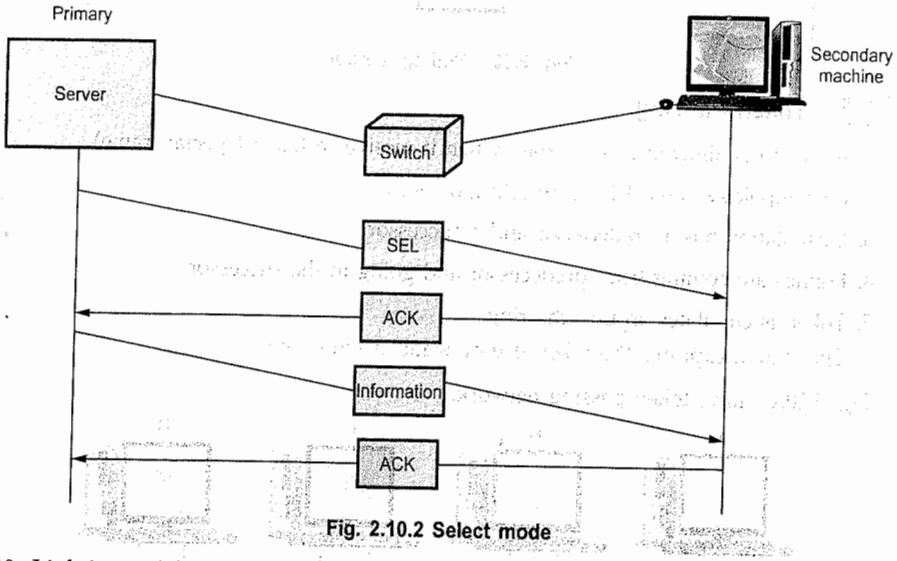


Fig. 2.10.2 Select mode

10. Link is available if primary device is not sending or receiving any data.
11. Before sending data, the primary creates and transmits a select (SEL) frame.
12. SEL frame includes address of the intended secondary device.

Fig. 2.10.3 shows the poll method.

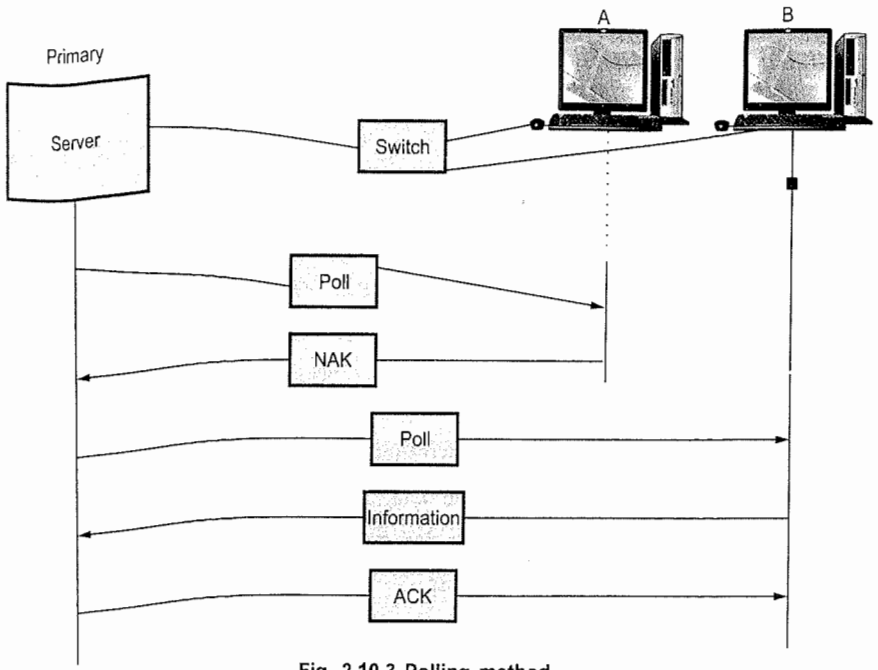


Fig. 2.10.3 Polling method

2.10.3 Token Passing

1. A station is allowed to send data when it receives a token (special frame).
2. Ring topology is used for connecting devices.
3. Each station has a predecessor and a successor.
4. Frames are coming from predecessor and going to the successor.
5. Token is circulates around the ring.
6. The station captures the token if they want to send data.

Fig. 2.10.4 shows token passing network.

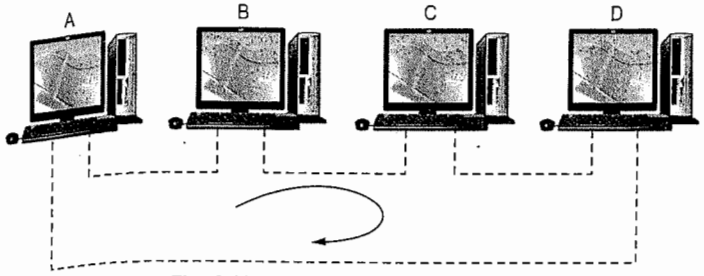


Fig. 2.10.4 Token passing network

7. Flowchart for token passing procedure is shown in Fig. 2.10.5.

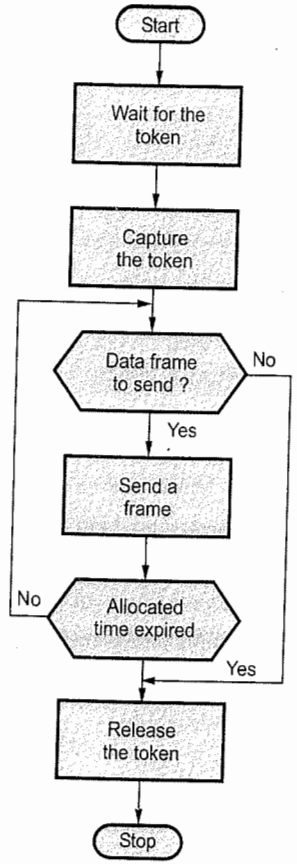


Fig. 2.10.5 Flowchart for token passing

Example 2.10.1 *A CSMA/CD bus spans a distance of 1.5 km. If the data rate is 5 Mbps what is the minimum frame size ?*

Solution : Typical propagation speed in LAN cables = 200 m/μs

End to end propagation delay t_p,

$$t_p = \frac{1500}{200} = 7.5\ \mu s$$

Minimum frame size = $2 \times 7.5 \times 10^{-6} \times 5 \times 10^{6} = 75$ bits

Example 2.10.2 *Compute the maximum channel utilization for a MAN which uses CSMA mechanism and has a length of 50 km, and operates at 50 Mbps with a frame length of 2000 bits.*

Solution : Assuming co-axial cable as the medium, the propagation delay is 5 μs/km

$$\therefore \quad t_f = \frac{2000}{5} = 40\ \mu s$$

$$A = \frac{t_p}{t_f} = \frac{250}{40} = 6.25$$

$$U_{max} = \frac{1}{1+A} = 0.14$$

University Questions

1. *Explain any controlled access technique in detail.* **SPPU : May-14, Marks 4**
2. *What are the different types of multiple access protocols ? Explain controlled access protocol.* **SPPU : Dec.-14, Marks 8**

2.11 Channelization

- Channelization is the multiple access method. Multiple access is the technique of sharing or dividing channel (transmission medium) for number of stations sharing it.
- Three most commonly used multiple access methods are -
  1. Frequency Division Multiple Access (FDMA)
  2. Time Division Multiple Access (TDMA)
  3. Code Division Multiple Access (CDMA)

2.11.1 Frequency Division Multiple Access (FDMA)

- In FDMA the available bandwidth is divided into M number of smaller frequency bands called **sub bands**. Each station transmits its information continuously on an assigned sub band. To reduce the co-channel interference, guard band between two sub bands is provided.

If W = Available BW of channel

R = Data rate of channel

M = Number of stations

Then the transmit rate of each station is $\frac{R}{M}$ bits/sec.

- FDMA transmissions are separated in frequency domain i.e. total available transponder bandwidth is shared by stations. Fig. 2.11.1 shows how FDMA stations use a fixed portion of frequency band all the time.

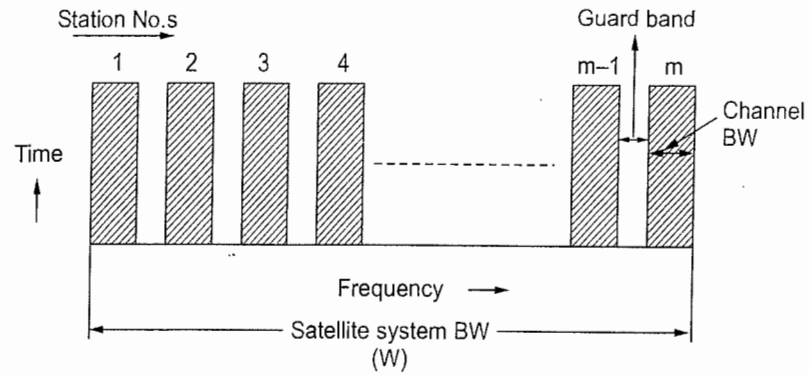


Fig. 2.11.1 FDMA

- FDMA is not suited for bursty traffic conditions because of inefficient use of transmission resources.

2.11.2 Time Division Multiple Access (TDMA)

- TDMA is a method of time-division multiplexing of digitally modulated carriers. In TDMA, each station transmits digitally modulated carriers during a preassigned time slots, making use of the entire transmission channel during its transmission. The stations are synchronized such that only one carrier is present on the channel at any given time. Thus avoiding collisions of stations. Sufficient guard bands are also provided to ensure collision avoidance.
- Each station spends most of the time accumulating packets and preparing them for transmission in a burst during the assigned time slot. The average bit rate of each channel is same because time slot available is same for each station.
- Fig. 2.11.2 shows how TDMA stations use a fixed portion of time slot in the frequency band.

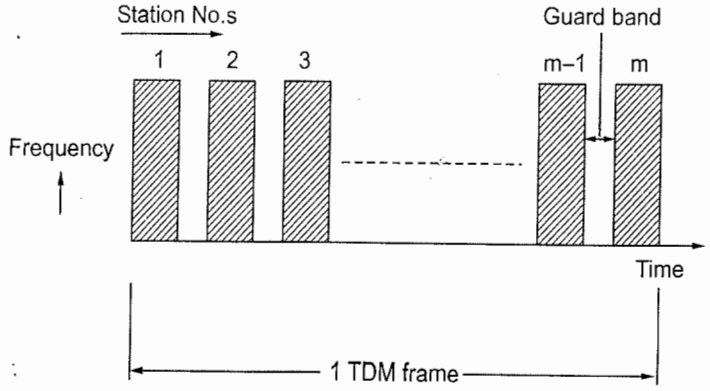


Fig. 2.11.2 TDMA

Advantages of TDMA :

1. At a given time only one carrier is present on the channel hence intermodulation distortion is eliminated.
2. TDMA transmission is separated in time domain. Processing of signal in time domain is easier.
3. TDMA is most efficient method of transmission because of efficient use of transmission resources.
4. TDMA can accomodate a wider range of bit rates by allowing a station to be allocated several slots. Thus TDMA is more flexible than FDMA.

Disadvantages of TDMA :

1. Precise synchronization between stations is required. Transmission of every station must occur during exact time slot.
2. Bit and frame timings must be maintained by TDMA.

2.11.3 Code Division Multiple Access (CDMA)

- In CDMA each station transmitter may transmit whenever it requires and can use entire bandwidth i.e. there are no restrictions on time and bandwidth. CDMA is also called as **spread spectrum multiple access** because transmission can spread throughout the bandwidth. Each station is assigned a unique binary code, this code is called as **chip code**. Each station and transmission is identified by its chip code. The receiver uses chip code to recover the signal from desired station. Fig. 2.11.3 shows conceptual view of CDMA technique.

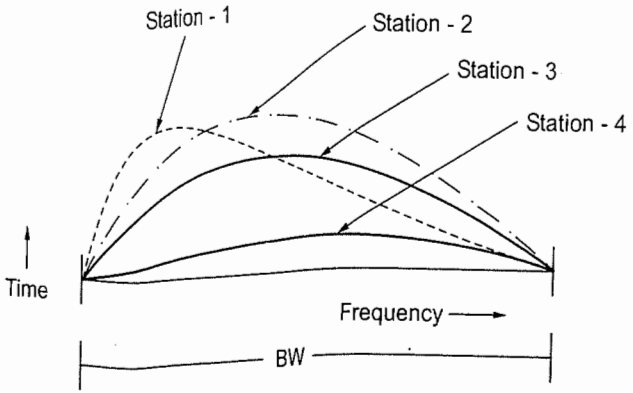


Fig. 2.11.3 CDMA Technique

Applications of CDMA :

1. CDMA is used for wireless systems with fixed base station and many mobile station at varying distance from it.
2. CDMA is used in satellite systems so that many signals can use a transponder; making it more efficient.
3. CDMA is used in digital cellular telephone services because it permits more users to occupy a given band.
4. Wideband CDMA (W-CDMA) is used for digital cell phone systems to accommodate voice transmission alongwith high speed data, FAX and internet communication.
5. CDMA is ideally suited for military application because of immunity to noise.

Advantages of CDMA :

1. Each station can use the entire bandwidth at any time.
2. High immunity for interference or jamming.

Disadvantages of CDMA :

1. The overall performance degrades with increase in number of users.
2. Time synchronization of stations is required.

2.11.4 Comparison between FDMA, TDMA and CDMA

Parameter	FDMA	TDMA	CDMA
Bandwidth	The bandwidth is divided into channels	The bandwidth is just one channel that is timeshared	Sharing of bandwidth and time
Synchronization between user	Not required	Required	Not required
Guard band/times between adjacent channel	Bands required	Guard times required	Both are required
Code word	Not required	Not required	Required

2.12 IEEE Standards

- The Institute of Electrical and Electronic Engineers (IEEE) publish several widely accepted LAN-recommended standards. These standards, collectively known as IEEE 802.

- Various IEEE 802 standards are as
  1) IEEE 802.I High Level Interface (MAC Bridges)
  2) IEEE 802.2 Logical Link Control (LLC)
  3) IEEE 802.3 CSMA/CD (Ethernet)
  4) IEEE 802.4 Token Bus
  5) IEEE 802.5 Token Ring
  6) IEEE 802.6 Metropolitan Area Networks
  7) IEEE 802.7 Broadband LANs
  8) IEEE 802.8 Fiber Optic LANs
  9) IEEE 802.9 Integrated Data and Voice Network
  10) IEEE 802.10 Security
  11) IEEE 802.11 Wireless Network.
- All of these standards have subsequently been adopted as international standards by International Organization for Standardization (ISO).
- Fig. 2.12.1 shows the IEEE standard for LAN.

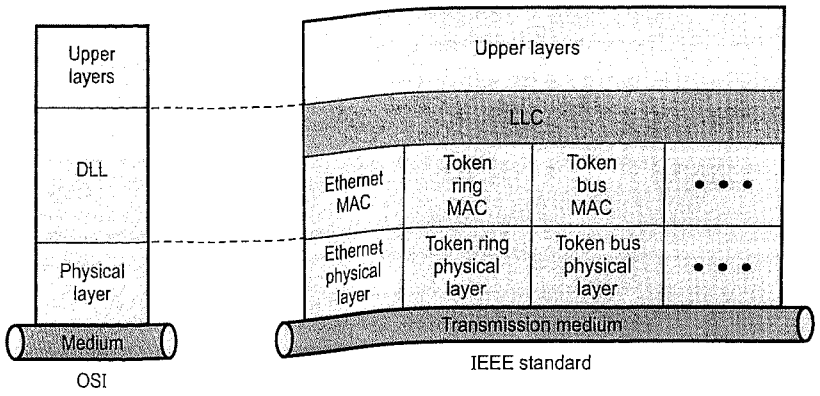


Fig. 2.12.1 IEEE standard for LAN

1. Data Link Layer

- Data link layer in the IEEE standard is divided into two sublayer : LLC and MAC.

Logical Link Control

- Data link control handles framing, flow control, error control. In IEEE 802, flow control, error control and part of the framing duties are collected into logical link control.

- Framing is handled in both the LLC sublayer and the MAC sublayer.
- The LLC provides one single data link control protocol for all IEEE LANs.

a) Framing : LLC defines a protocol data unit. The header contains a control field like the one in HDLC; this field is used for flow and error control. Other header fields are Destination Service Access Point (DSAP) and the Source Service Access Point (SSAP).

b) Need for LLC : The purpose of the LLC is to provide flow and error control for the upper layer protocols. However, the most upper layer protocols such as, IP do not use the services of LLC.

Medium Access Control (MAC)

- IEEE project 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- It defines CSMA/CD as the media access method for Ethernet LAN and the token passing method for Token Ring and Token BUS LANs.

2. Physical Layer

- The physical layer is dependent on the implementation and type of physical media used.
- IEEE defines detailed specifications for each LAN implementation.

2.13 Standard Ethernet

SPPU : May-12, Dec.-12, 13, 14

- The original Ethernet was created in 1976 at xerox's Palo Alto Research center.
- Generations of Ethernet
  a) Standard Ethernet (10 Mbps)
  b) Fast Ethernet (100 Mbps)
  c) Gigabit Ethernet (1 Gbps)
  d) Ten-Gigabit Ethernet (10 Gbps)

2.13.1 MAC Sublayer

MAC sublayer frames data received from the upper layer and passes them to the physical layer.

2.13.1.1 Frame Format

- Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.
- The frame format of the MAC is shown in Fig. 2.13.1.

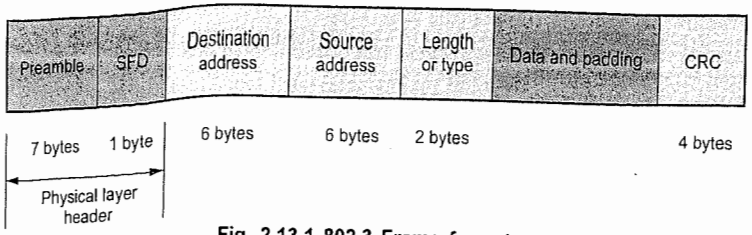


Fig. 2.13.1 802.3 Frame format

1. Preamble : A 7-byte pattern of alternating 0s and 1s used by the receiver to establish bit synchronization. Each frame contains the bit pattern 10101010. The pattern provides only an alert and a timing pulse. The preamble is actually added at the physical layer and is not part of the frame.

2. Start Frame Delimiter (SFD) : The sequence 10101011, which indicates the actual start of the frame and enables the receiver to locate the first bit of the rest of the frame.

3. Destination Address (DA) : The DA field is 6 bytes and specifies the station for which the frame is intended. It may be a unique physical address, a group address or a global address.

4. Source Address (SA) : The SA field is also 6 bytes and contains the physical address of the sender of the packet.

5. Length or Type : Length of LLC data field in octets, or Ethernet Type field, depending on whether the frame conforms to the IEEE 802.3 standard or earlier Ethernet specification. In either case, the maximum frame size, excluding preamble and SFD, is 1518 bytes.

6. Data : Data unit supplied by LLC. It is a minimum of 46 bytes and a maximum of 1500 bytes.

7. CRC : This field contains error detection information.

2.13.2 Frame Length

- An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer. Fig. 2.13.2 shows the minimum and maximum length of the frame.
- If we count 18 bytes of header and trailer i.e. 6 bytes of SA + 6 bytes of DA + 2 bytes of length + 4 bytes of CRC, then the minimum length of data from the upper layer is 64 – 18 = 46 bytes.
- If the upper layer packet is less than 46 bytes, padding is added to make up the difference.

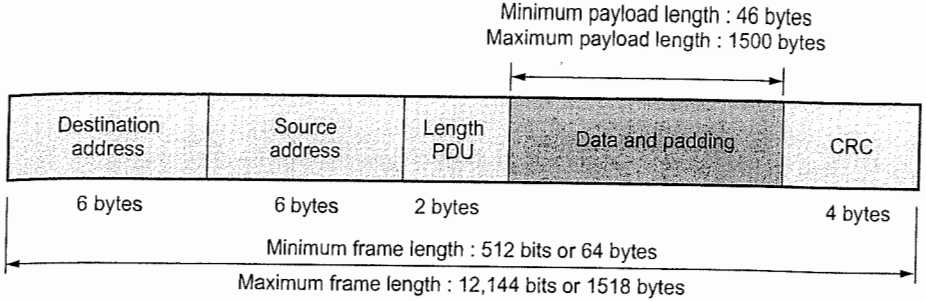


Fig. 2.13.2 Minimum and maximum lengths

- The standard defines the maximum length of a frame (without preamble and SFD) as 1518 bytes. If we subtract the 18 bytes of header and trailer, the maximum length of the payload is 1500 bytes.

Addresses

- A source address is always a unicast address, i.e. the frame comes from only one station. The destination address can be unicast, multicast or broadcast.
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

Access Method : CSMA/CD

- Standard Ethernet uses 1-persistent CSMA/CD.
  1. Slot time = Round trip time + Time required to send the jam sequence
  2. Maximum length = Propagation speed $\times \frac{\text{Slot time}}{2}$

Minimum frame size

- While a data field of 0 bytes is sometimes useful, it causes a problem. When a transceiver detects a collision, it truncates the current frame, which means that stray bits and pieces of frames appear on the cable all the time.
- Ethernet requires that valid frames must be atleast 64 bytes long, from destination address to checksum, including both.
- Reason for having a minimum length frame is to prevent a station from completing the transmission of a short frame before the first bit has even reached the far end of the cable, where it may collide with another frame.
- Fig. 2.13.3 shows collision detection.
- At time 0, station A, at one end of the network sends off a frame. Let us call the propagation time for this frame to reach the other end T. Just before the frame gets to the other end (i.e. at time T – ε), the most distant station B, starts transmitting.

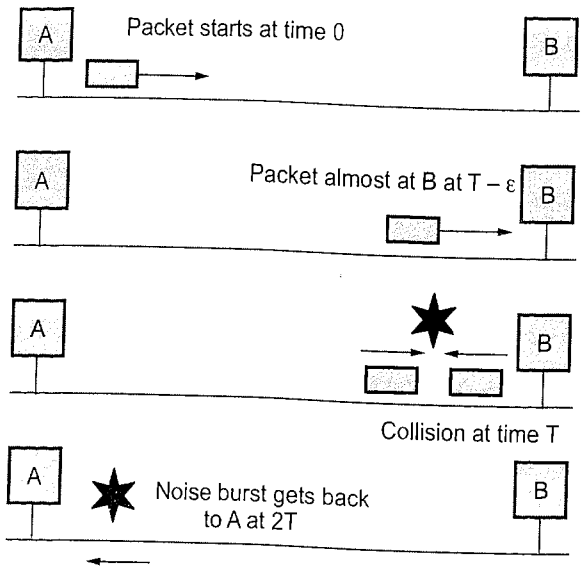


Fig. 2.13.3 Collision detection can takes as long as 2T

- When B detects that it is receiving more power than it is putting out, it knows that a collision has occurred, so it abort its transmission and generates a 48-bit noise burst to warn all other stations. In other words, it jams the either to make sure the sender does not miss the collision.
- Loss of bandwidth is 936×10^3 bytes/sec because we only transmit 64 bytes. The available bandwidth is 100 Mbps.

2.13.3 Ethernet Specifications

- CSMA/CD offers various options in terms of transmission medium, signalling technique, data rate and maximum electrical cable segment length.
- Table 2.13.1 summarizes these options defined for the IEEE 802.3 medium.

Sr. No.	Medium options	Transmission medium	Signaling technique	Data rate (Mbps)	Maximum segment length (m)
1.	10BASE5	Coaxial cable (50 ohm)	Baseband (Manchester)	10	500
2.	10BASE2	Coaxial cable (50 ohm)	Baseband (Manchester)	10	185

3.	1BASE5	Unshielded twisted pair	Baseband (Manchester)	1	250
4.	10BASET	Unshielded twisted pair	Baseband (Manchester)	10	100
5.	10BROAD36	Co-axial cable (75 ohm)	Broad band (DPSK)	10	3600
6.	10BASEF	Fiber optics	Baseband	10	2000

Table 2.13.1 IEEE 802.3 medium options

1) 10BASE5 : It is popularly called as **thick ethernet**. The notation 10BASE5 means that it operates at 10 Mbps, uses baseband signaling and can support segment upto 500 metres. The length of the network can be extended using repeaters. The standard allows a maximum of four repeaters in the path between any two stations, extending the effective length of the network to 2.5 km.

Application : 10BASE5 is generally used as low cost alternative for fiber optic media for use as a backbone segment with in a single building. Its extended length, higher attached device count and better noise resistance make 10BASE5 well suited for use as a network trunk for one or more floors in a building. However the high cost of connecting each device makes 10BASE5 too expensive for most LAN installations a single break or bad connection in the cable can bring the entire network down.

2) 10BASE2 : It is popularly called as **chepearnet** or thin ethernet. It uses thin co-axial cable. The thinner cable results in significantly cheaper cost, at the penalty of fewer stations and shorter length. Therefore 10BASE2 is limited to a maximum of 30 network devices per unrepeated network segment with a minimum distance of 0.5 m. And segment length is reduced to 185 metres.

Application : For small budget conscious installations, 10BASE2 is the most economical topology such as UNIX work stations.

The disadvantages of 10BASE2 is that any break in the cable or poor connection will bring the entire network down and repeaters are required if more than 30 devices are connected to the network or the cable length exceeds 185 m.

3) 1BASE5 : It is also known as **star LAN**. It specifies operation at 1 Mbps, using a passive star topology.

Application : This options is substantially lower in cost than either of coaxial cable options. This options could be appropriate for a departmental-level LAN.

4) 10BASET : 10BASET is 10 MHz ethernet running over UTP cable. It also uses passive star topology. The maximum cable segment allowed is 100 - 150 metres. There is no minimum distance requirements between devices, such devices cannot be connected serially but in star wired. Maximum 1024 stations can be connected to network.

Application : 10BASET is the most flexible topology for LAN's and is generally the best choice for network installations. 10BASET hubs or multi-hub concentraters, are typically installed in a central locations to the user community. The signalling technology is very reliable even in somewhat noisy environments it automatically shutdown the offending parts without affecting the rest of the network. Cabling is cheaper and requires less skill to install. Maintenance is easy.

The disadvantages are the hardware required is more expensive and maximum cable run from hub is 100-150 metre.

5) 10BROAD36 : It is a 10 Mbps broadband option. It provides support to more stations over greater distances than the baseband versions. The maximum cable run is restricted to 3600 m in two segments of 1800 m from the head end. Other services such as TV or voice can also be integrated on the same cable using FDM.

6) 10BASEF : 10BASEF is 10 Mbps running over fiber optic cabling. The maximum cable length depends on signaling technology and medium used but can go upto 2 km unrepeated segment. It is star wired so there is no minimum distance requirement between devices.

Application : 10BASEF is the only recommended topologies for inter-building links. However they need not be limited to this role, it can also run to desktop. It has excellent noise immunity.

The disadvantage is, it is very expensive due to the cost of connectors and terminators.

2.13.1.4 Manchester Encoding

- In order to transport digital bits of data across carrier waves, encoding techniques have been developed each with their own merits and demerits.
- Digital signal is a sequence of discrete, discontinuous voltage pulses. Data is represented in binary. These binary data is transmitted by encoding each data bit into signal elements.

Desirable Properties of Encoding Techniques

1. **Synchronization capability :** The ability to stay synchronized or to get re-synchronized.
2. Error detection capability.
3. **Immunity to noise :** Ability to separate noise from the transmitted signal.

1) Manchester Encoding : In Manchester encoding each bit period has both the high and low voltage values. If the data is a 1, the first half of the bit time period is sent at the positive level, and the second half of the period is at the negative level. For data bit of 0, first a negative signal and then a positive signal. There is a transition which can be

used for a synchronization. Sometimes this method is called self clocking encoding method. Fig. 2.13.4 shows manchester encoding waveform for the 8-bit data stream 11000101.

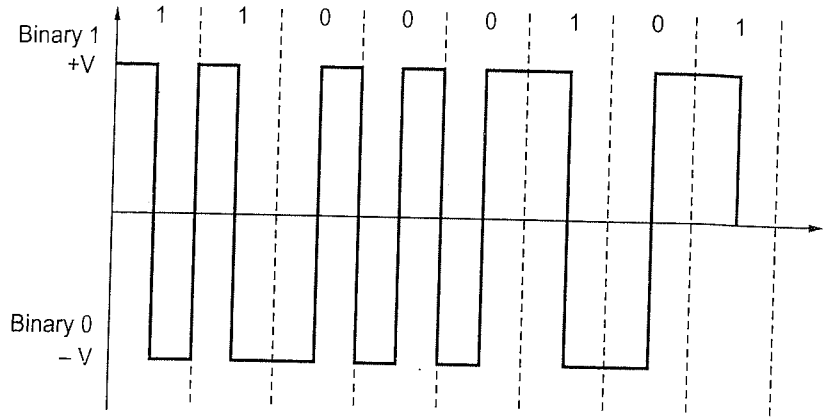


Fig. 2.13.4 Manchester encoding

2) Differential Manchester : In differential Manchester encoding, a binary 0 is marked by a transition at the beginning of an interval, whereas a 1 is marked by the absence of a transition. In this encoding method, detecting changes is often more reliable, especially when there is a noise in the channel. Fig. 2.13.5 shows the differential manchester encoding for 8-bit data stream 101011100.

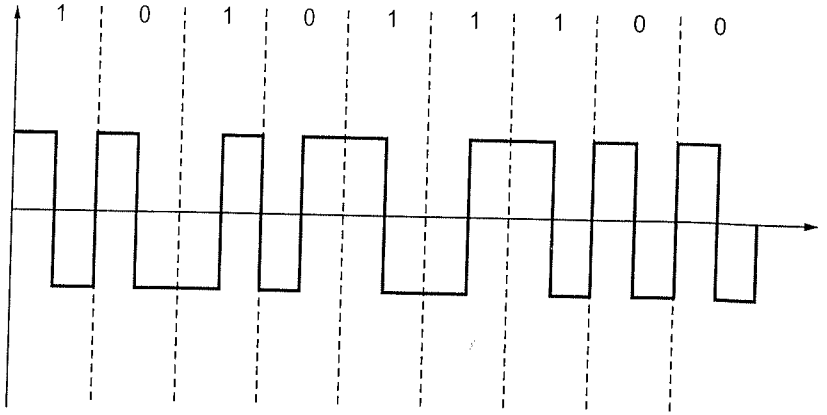


Fig. 2.13.5 Differential manchester

2.13.1.5 Binary Exponential Backoff Algorithm

- After a collision, time is divided into discrete slots whose length is equal to the worst-case round-trip propagation time on the either (2τ).

- **After first collision :** Each station was either 0 or 1 slot times before trying again. If two station collide and each one picks the same random number, they will collide again.
- **After second collision :** Each one picks either 0, 1, 2 or 3 at random and waits that number of slot times.
- **After third collision :** If a third collision occurs, then the next the number of slots to wait is chosen at random from the interval 0 to $2^3 - 1$.
- **After i^{th} collision :** A random number between 0 and $2^e - 1$ is chosen, and that number of slots is skipped.
- This algorithm, called **binary exponential backoff** was chosen to dynamically adapt to the number of stations trying to send.

2.13.16 Ethernet Performance

$$\text{Channel efficiency} = \frac{P}{P + 2\tau / A} \quad \ldots (2.13.1)$$

Rewrite the above formula in terms of the frame length (F), the network bandwidth (B), the cable length (L) and the speed of signal propagation (c) for the optimal case of e contention slots per frame. With P = F/B, then equation (2.13.1) becomes

$$\text{Channel efficiency} = \frac{1}{1 + 2BLe / cF} \quad \ldots (2.13.2)$$

University Questions

1. *What are the common standard ethernet implementations ? Explain.* **SPPU : May-12, Marks 8**
2. *State and explain common standard ethernet implementations.* **SPPU : Dec.-12,13, Marks 8**
3. *What are the common standard ethernet implementations ? Explain.* **SPPU : Dec.-14, Marks 8**

2.14 Fast Ethernet

SPPU : May-14

- Fast ethernet is backward compatible with standard ethernet. The goals of fast ethernet can be :
  1. Upgrade the data rate to 100 Mbps.
  2. Keep the same 48-bit address.
  3. Keep the same frame format.
  4. Make it compatible with standard ethernet.
  5. Keep the same minimum and maximum frame length.
- Fast ethernet refers to a set of specifications developed by the IEEE 802.3 committee to provide a low cost, ethernet compatible LAN operating at 100 Mbps.

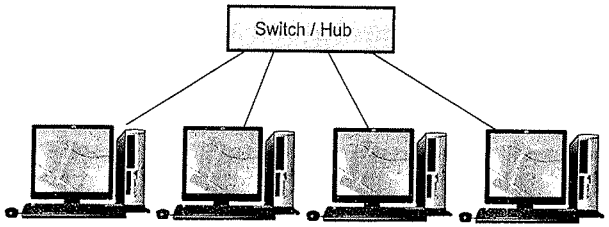
A traditional ethernet is half duplex : A station can either transmit or receive a frame, but it cannot do both simultaneously.

- Fast ethernet supports the full duplex with full duplex operation, a station can transmit and receive simultaneously. In fact, there is no collisions and the CSMA/CD algorithm is no longer needed.

Topology

- Fast ethernet is designed to connect two or more stations together. If there are only two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center. It is shown in the Fig. 2.14.1.

(a) Point-to-point



(b) Star

Fig. 2.14.1 Fast ethernet topology

Summary sheet of fast ethernet

Parameters	100BASE-TX		100BASE-FX	100BASE-T4
Transmission medium	STP	Cat 5 UTP	Fiber	Cat 3, 4, 5 UTP
Number of wires	4	4	2	4
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m
Line coding	MLT-3	MLT-3	4B5B	8B/6T/NRZ

University Question

1. *Explain the fast ethernet networks.* **SPPU : May-14, Marks 2**

2.15 Gigabit Ethernet

SPPU : May-14

- Goals of gigabit ethernet

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with standard or fast ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.

- It support the two different modes of operations.

i) Full duplex ii) Half duplex.

- In full duplex mode, there is a central switch connected to all computers or other switches. Each switch has buffers for each input port in which data are stored until they are transmitted. There is no collisions in this mode. This means that CSMA/CD is not used.
- Gigabit ethernet can also be used in half duplex mode. In this case, a switch can be replaced by a hub, which acts as the common cable in which a collision might occur. The half duplex approach uses CSMA/CD. For shared medium hub operation, there are two enhancements to the basic CSMA/CD scheme.
  1. **Carrier extension :** It defines the minimum length of a frame as 512 bytes.
  2. **Frame bursting :** It allows for multiple short frames to be transmitted consecutively, up to a limit, without relinquishing control for CSMA/CD between frames.

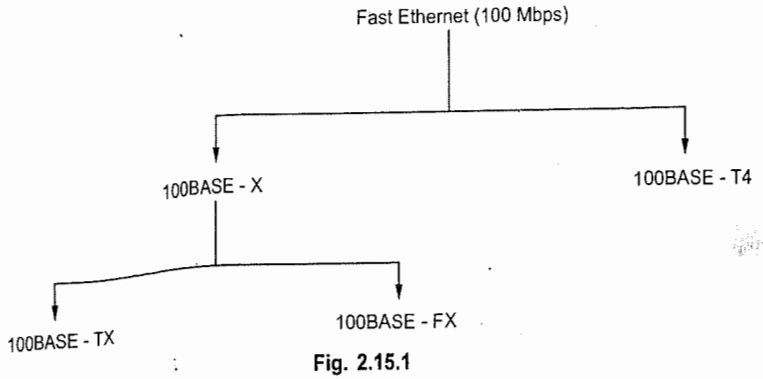


Fig. 2.15.1

Transmission Media

Summary sheet of gigabit ethernet

Parameters	1000Base-SX	100Base-LX	100Base-CX	1000Base-T
Transmission medium	Fiber short wave	Fiber long wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum segment length	550 m	500 m	25 m	100 m
Line coding	NRZ	NRZ	NRZ	4D-PAM5

Topology

- Gigabit ethernet is designed to connect two or more stations. If there are only two stations, thsey can be connected point-to-point. Fig. 2.15.2 shows the point-to-point connection.

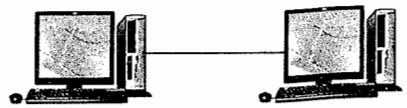


Fig. 2.15.2 Point-to-point

- Three or more stations need to be connected in a star topology with a hub or a switch at the center. This is shown in Fig. 2.15.3.

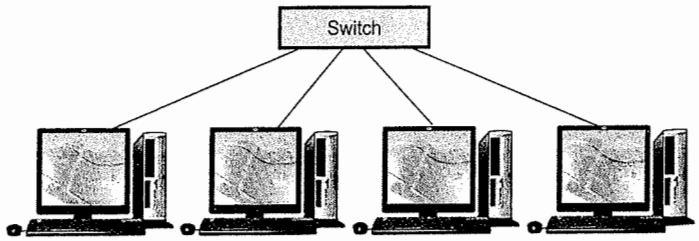


Fig. 2.15.3 Star

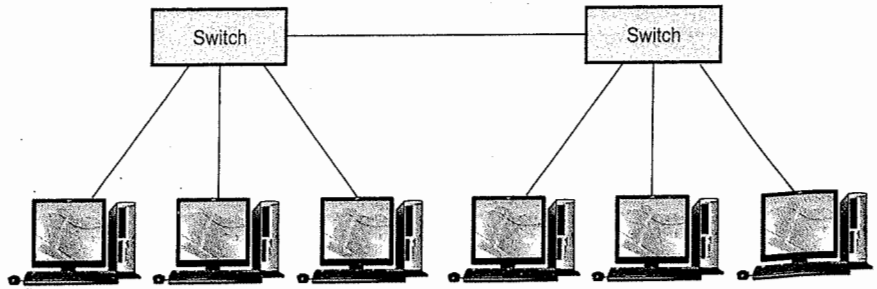


Fig. 2.15.4 Two stars

University Question

1. *Explain the gigabit ethernet networks.* **SPPU : May-14, Marks 2**

2.16 University Questions with Answers

(Regulation 2008)

May 2012

Q.1 *State and explain in brief the functions associated with data link layers in OSI model.* **(Refer section 2.1)** [8]

Q.2 *Draw the HDLC frame format and explain in detail the control field used in HDLC protocol for different frame types.* **(Refer section 2.6)** [8]

Q.3 *State and explain multiple access protocols in brief.* **(Refer section 2.8)** [8]

Q.4 *What are the common standard ethernet implementations ? Explain.* **(Refer section 2.13)** [8]

Dec. 2012

Q.5 *State and explain the significance of sliding window protocol with an example.* **(Refer section 2.4)** [8]

Q.6 *What are the responsibilities of MAC - Layer. Explain IEEE 802.3 MAC - Layer.* **(Refer section 2.8)** [8]

Q.7 *State and explain common standard ethernet implementations.* **(Refer section 2.13)** [8]

May 2013

Q.8 *What is the peak throughput achievable by a source employing stop-wait flow control, when maximum packet size is 1000 kbytes and network span of 10 km.* **(Refer section 2.4)** [8]

Q.9 *How the problem of contention is avoided for the channel. Explain giving suitable example.* **(Refer section 2.8)** [8]

Dec. 2013

Q.10 *Explain Go Back - N ARQ protocol and selective repeat ARQ protocol.* **(Refer section 2.5)** [8]

Q.11 *Draw the HDLC frame format and explain in detail the control field used in HDLC protocol for different frame types.* **(Refer section 2.6)** [8]

Q.12 *Define CSMA. What is the necessity of collision defect ? Suggest a collision free protocol using CSMA.* **(Refer section 2.8)** [8]

Q.13 *State and explain common standard ethernet implementations.* **(Refer section 2.13)** [8]

May 2014

Q.14 *Explain any framing technique in detail.* **(Refer section 2.1)** [6]

Q.15 *What are the functions of data link layer protocol ?* **(Refer section 2.1)** [3]

Q.16 *Explain selective repeat ARQ protocol.* **(Refer section 2.5)** [6]

Q.17 *Explain bit stuffing in detail ? Explain GBN ARQ technique.* **(Refer section 2.5)** [6]

Q.18 *Draw and explain HDLC frame format in detail.* **(Refer section 2.6)** [3]

Q.19 *Explain any controlled access technique in detail.* **(Refer section 2.10)** [4]

Q.20 *Explain the fast ethernet networks.* **(Refer section 2.14)** [2]

Q.21 *Explain the gigabit ethernet networks.* **(Refer section 2.15)** [2]

Dec. 2014

Q.22 *What are the different functions of data link layer ? Explain different types of framing techniques in detail.* **(Refer section 2.1)** [8]

Q.23 *Explain simplest protocol and stop and wait ARQ protocol for noiseless channels with suitable diagram.* **(Refer section 2.5)** [8]

Q.24 *What are the different types of multiple access protocols ? Explain controlled access protocol.* **(Refer section 2.10)** [8]

Q.25 *What are the common standard ethernet implementations ? Explain.* **(Refer section 2.13)** [8]

❑❑❑