MODULE II

Data link layer

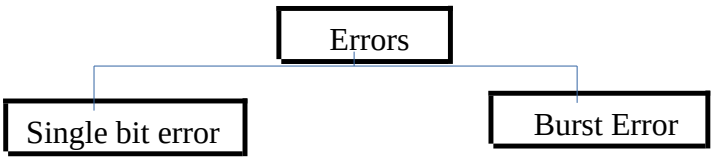
- The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-nodecommunication.
- Specific responsibilities of the data link layer include:
  - Framing
  - Addressing
  - Flowcontrol
  - Errorcontrol
  - Media accesscontrol
- The data link layer divides the stream of bits received from the network into manageable data units calledframes.
- The data link layer adds a header to the frame to define the addresses of the sender and receiver of theframe
- If the rate at which the data are absorbed by the receiver is less than the rate at whichdata are produced in sender, the data link layer imposes flow control mechanism to avoid overwhelming thereceiver.
- The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate or lostframes.
- When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any giventime.

Error detection and correction

- Networks must be able to transfer data from one device to another with acceptable accuracy.
- A system must guarantee that the data received are identical to the datatransmitted.
- Data can be corrupted during transmission. Some applications require that errors be detected andcorrected.
- Some applications can tolerate a small level of errors. For example, random errors in audio or video transmission may be tolerable, but when we transfer text, we expect a very high level ofaccuracy.

Types of errors, Single CSC error and Burst error

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal.



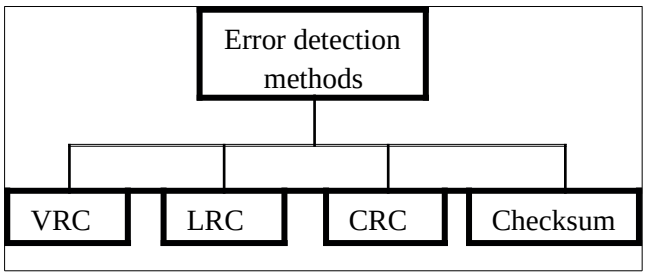
- ***Single bit error***
  - The term single bit error means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to1.
  - Single bit errors are least likely type of error in serial datatransmission.
  - To see why, imagine a sender sends data at 1Mbps.
  - This means that each bit lasts only 1/1000000 second. For a single bit error to occur, the noise must have a duration of only 1/1000000 second, which is very rare; noise normally lasts much longer than this.
  - single bit error can happen if we are sending data using parallel transmission.
  - Fig:10.1

- ***Burst error***
  - The term burst error means that 2 or more bits in the data unit have changed from1to0orfrom0to1.
  - Burst error is most likely to happen in a serial transmission. The duration of noise is longer than the duration of a bit, which means that when noise affects data, it effect a set ofbits.
  - Fig:10.2

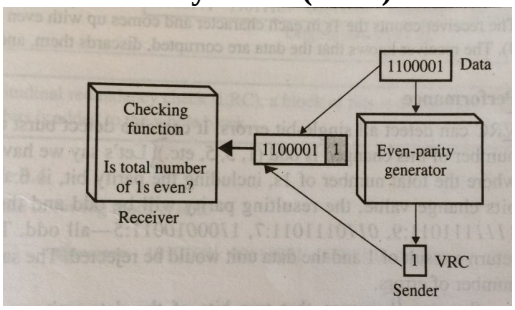
- *Redundancy bit*
  - The central concept of detecting or correcting errors is redundancy.
  - To be able to detect or correct errors, we need to send some extra bits with ourdata.
  - These redundant bits are added by the sender or removed by the receiver.
  - Their presence allows the receiver to detect or correct corruptedbits.

ERROR DETECTION

- In error detection, we are looking only to see if any error has occurred. The answer is simple yes or no. we are not even interested in the number of errors.
- Four types of redundancy checks are used in datacommunication:
  - Vertical Redundancy Check
  - Longitudinal redundancy check
  - Cyclic RedundancyCheck
  - Checksum



- **Vertical redundancy check (VRC)**



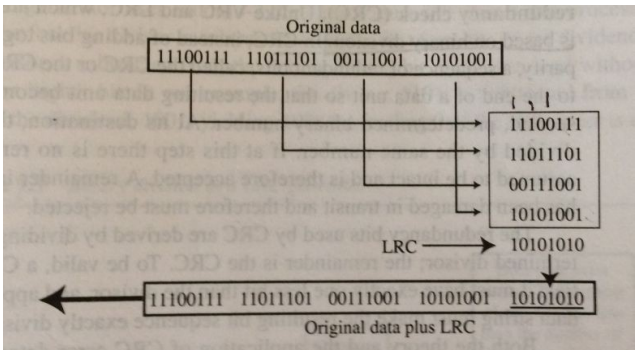
  - The most common and least expensive mechanism for error detection is the vertical Redundancy Check.
  - A redundant bit, called a parity bit, is appended to every data unit so that the total number of 1s in the unit becomes even
    - Suppose we want to transmit the binary data unit 1100001.
    - Adding together the number of 1s gives us 3, an odd number.
    - Before transmitting, we pass the data unit through a parity generator. The parity generator counts the 1s and appends the parity bit (a 1 in this case) to the end. The total number of 1s is now four, an even number.

- The system now transmits the entire expandedunit across the network link.
- When it reaches its destination, the receiver puts all eight bits through an even parity checking function.

- Some systems may use odd-parity checking, where the number of 1 should be odd.
- Example:
  "world"
  1110111 1101111 1110010 1101100 1100100
  w o r l d
  11101110 11011110 11001001 11100100 11011000

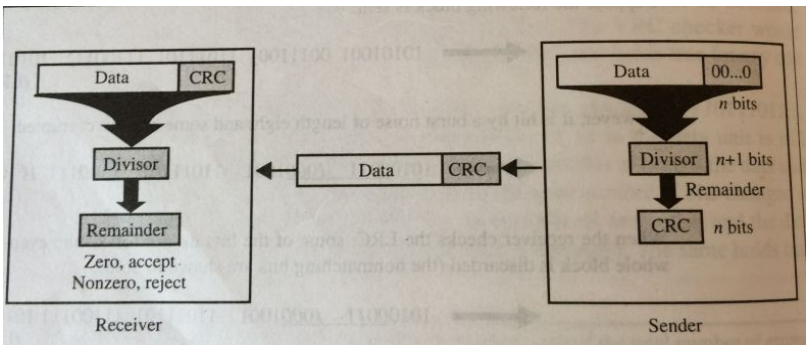
- ***Performance***
  - VRC can detect all single bit errors.
  - It can also detect burst errors as long as the total number of bits changed is odd.

- **longitudinal redundancy Check (LRC)**

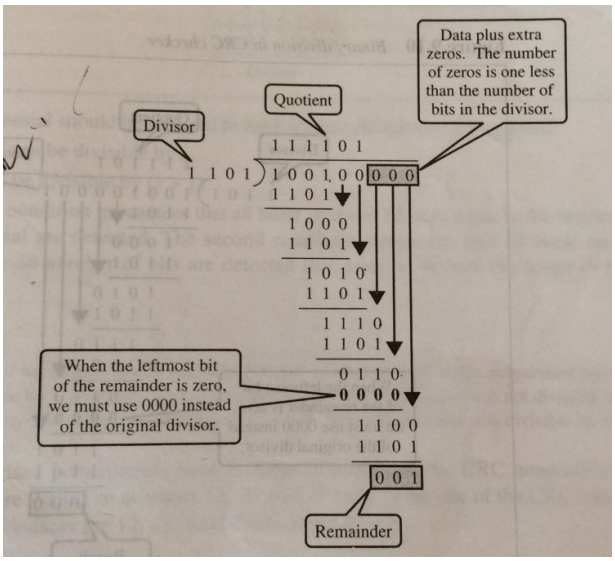


  - In Longitudinal Redundancy Check (LRC), a block of bits is organized in a table.
  - Instead of sending a block of 32 bits, we organize them in a table made of four rows and eight columns and create a new row of eight bits, which are the parity bits for the whole block.
  - Note that the first parity bit in the in the fifth row is based on all first bits. The second party bit is calculated based on all second bits, and so on.
  - ***Performance***
    - LRC increases the likelihood of detecting burst errors.
    - A burst error of more than n bits also detected by LRC with a very high probability.
    - If two bits in one data unit are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC detector will not detect an error.

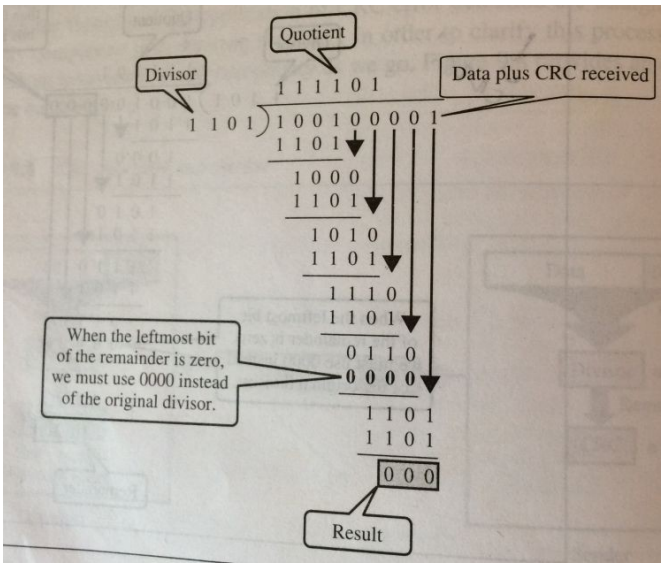
- **Cyclic Redundancy Check(CRC)**



- The most powerful of the redundancychecking techniques is the Cyclic Redundancy Check (CRC).
- Unlike VRC and LRC, which are based on addition, CRC is based on binary division.
- In CRC, instead of adding bits together to achieve a desired parity, a sequence of redundant bits, called the CRC or the CRC remainder, is appended to the end of a data unit so that the resulting data unit becomes exactly divisible by second, predetermined binary.
- At its destination, the incoming data unit is divided by the same number.
- If at this there is no remainder, the data unit assumed to be intact and is therefore
- accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.
- The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC. To be valid, a CRC must have two qualities:
  - It must have exactly one less bit than the divisor.
  - Appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.
- ***Steps:***
  - First, a string of n 0s is appended to the data unit. The number n is one less than the number of bits in the predetermined divisor, which is n+1 bits.
  - Second, the newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is the CRC.
  - Third, the CRC of n bits derived in step2 replaces the appended 0s at the end of the data unit.
  - The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder.
  - If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes. If the string has been changed in transit, the division yields a non-zero remainder and the data unit does not pass.
  - Binary division in CRC Generator



- Binary division in CRC Checker



- ***Performance***
  - CRC can detect all burst errors that affect an odd number of bits.
  - CRC can detect all burst errors of length less than or equal to the degree of the polynomial.
  - CRC can detect with a high probability burst errors of length greater than the degree of the polynomial.

CHECKSUM

- The error detection method used by the higher-layer protocols is called checksum.
- The sender follows these steps:
  - The unit is divided into k sections, each of n bits.
  - All sections are added together using one's complement to get the sum.
  - The sum is complemented and becomes the checksum.
  - The checksum is send with data.
- The receiver follows these steps:
  - The unit is divided into k sections, each of n bits.
  - All sections are added together using one's complement to get the sum.
  - The sum is complemented.
  - If the result is zero, the data are accepted:
  - otherwise, they are rejected.
- Example:
  - Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

    10101001 00111001
  - The numbers are added using one's complement arithmetic.

    10101001
    00111001
    sum 11100010
    checksum 00011101

    The pattern sent is:

    10101001 00111001 00011101
    checksum

- *Receiver side:*

Now suppose the receiver receives the pattern sent and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections together, it will get all 1s, which, after complementing is all 0s and shows there is no error.

	10101001
	00111001
	00011101
Sum	11111111
Complement	00000000

means that pattern is correct

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

ERROR CORRECTION

- Error correction is much more difficult than error detection. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.
- There are two main methods of error correction
  - *Forward error correction*: it is the process in which the receiver tries to guess the message by using redundant bits.
  - *Correction by retransmission:* it is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message.

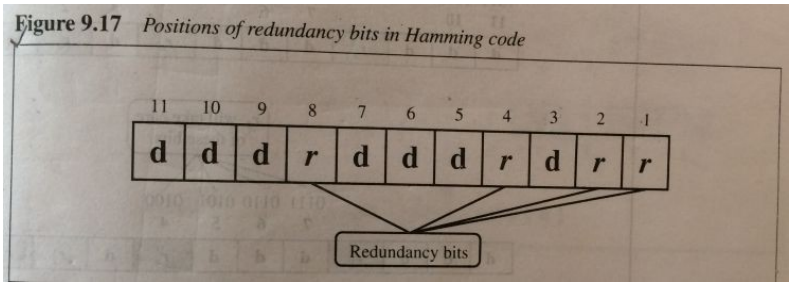
1.SINGLE BIT ERROR CORRECTION

  - single bit error can be detected by the addition of a redundant bit to the data unit.
  - A single additional bit can detect single bit errors in any sequence of bits because it must distinguish between only two conditions: error / no error.
  - To correct the error, the receiver simply reverses the value of the altered bit. To do so, it must know which bit is in error.
  - Ex: to correct a single bit error in an ASCII character, the error correction code must determine which of the 7 bits has changed.
  - We have to distinguish between eight different states: no error, error in position1, error in position2, and so on, up to error in position 7.
  - Three bit redundancy code should be adequate because three bits can show eight different states(000 to 111) and can therefore indicate the locations of eight different possibilities. But what if an error occurs in the redundancy bits themselves?
    - To calculate the number of redundancy bits (r) required to correct a given number of data bits(m), we must find the relationship between m and r.
    - If the total number of bits in a transmittable unit is m+r, then r must be able to indicate at least m+r+1 different states.
      - Of these, one state means no error and m+r states indicates the location of an error in each of the m+r positions.
    - m+r+1 states must be discoverable by r bits; and r bits can indicate 2^r different states.
    - Therefore, 2^r must be equal to greater than m+r+1:

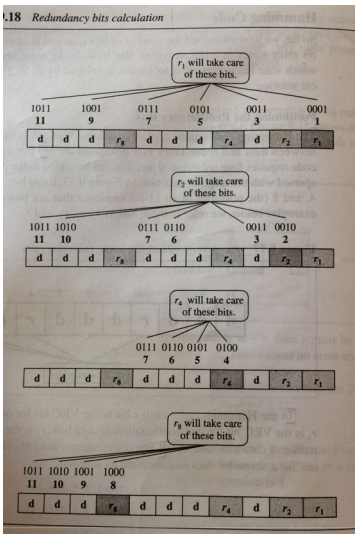
$$2^r >= m+r+1$$

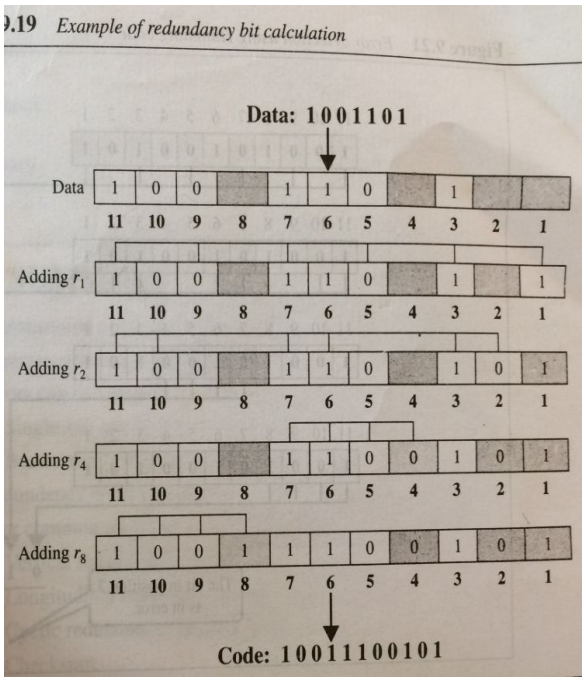
2. HAMMING CODE DATA COMPRESSION

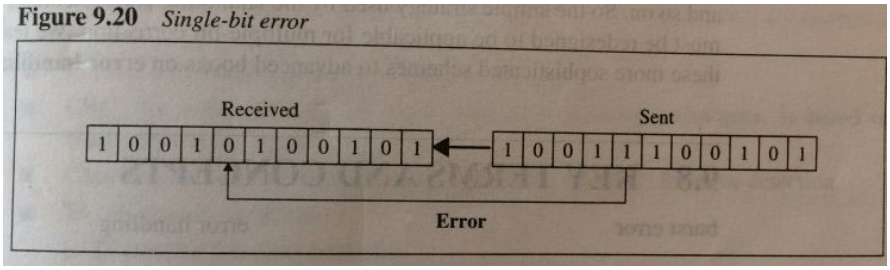
- It is a technique developed by RW Hamming. It provides a practical solution to the error correction.
- *Positioning Redundancy Bits*
- The hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits. (2r>=m+r+1).
- Example:

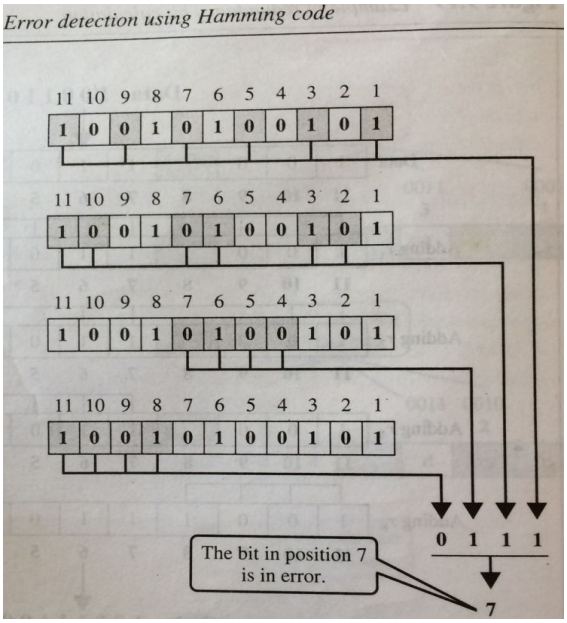


- In the hamming code, each r bit is the VRC bit for one combination of data bits, r1 is the VRC bit for one combination of data bits, r2 is the VRC bit for another combination of data bits, and soon.
- The combinations used to calculate each of the four r values for a seven bit data sequence are asfollows:
  R1 = bits 1, 3, 5, 7, 9, 11
  R2 = bits 2, 3, 6, 7, 10, 11
  R4 = bits 4, 5, 6, 7
  R8 = bits 8, 9, 10, 11
- Each data bit may be included in more than one CRC calculation. Here, each of the original data bits is included in at least two sets, while the r bits are included in onlyone.
- The r1 bit is calculated using all bit positions whose binary representations includes a 1 in the right most position. The r2 bit is calculated using all bit positions with a 1 in the second position, and so on.









3. HUFFMAN CODE

- It is a lossless data compression algorithm.
- We assign a variable length code to input characters, length of which depends on the frequency of characters.
- The variable-length code assigned to input characters are prefix code
- Eg:

{0,11} {0,1,11}
prefix code non prefix code

◦ ***Huffman tree***

- Create a leaf node for each unique character and build min heap of all leaf nodes.
- Extract two nodes with the minimum frequency from the min heap.
- Create a new internal node with frequency equal to the sum of the two nodes frequencies. Make the first extracted node as its left child and the other extracted node as its right child. Add this node to the minheap.
- Repeat step2 and 3 until the heap contains only one node. The remaining node is the root node and tree is complete.
- **Example**

Character	Frequency
A	5
B	9
C	12
D	13
E	16

F	45

STEP 1:

N1[14]

A[5] B[9]

STEP 2:

N2[25]

C[12] D[13]

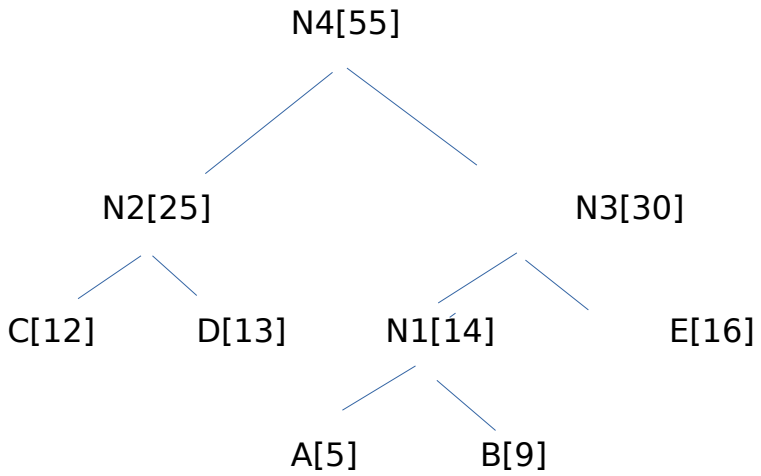
STEP 3:

N3[30]

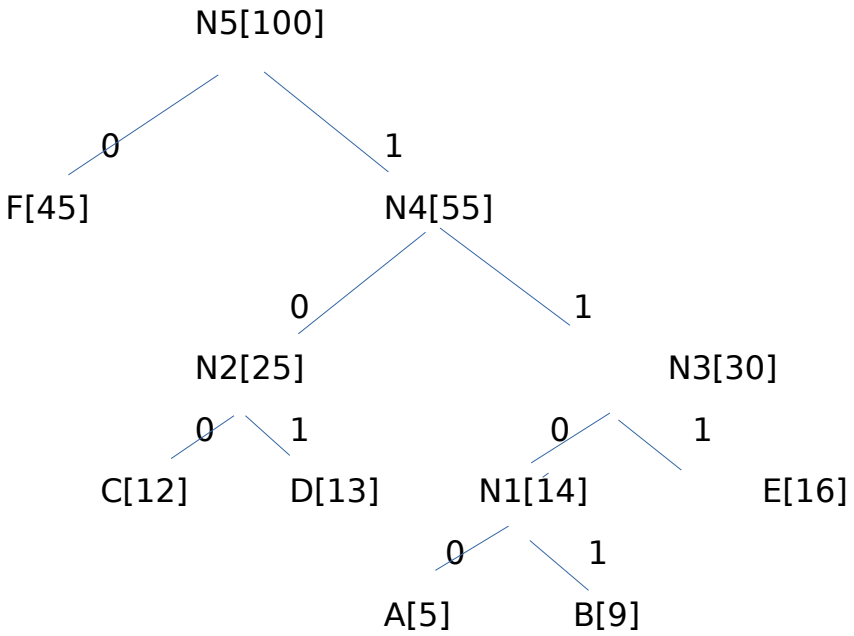
N1[14] E[16]

A[5] B[9]

STEP 4



STEP 5

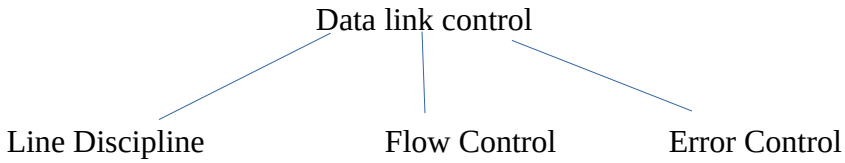


Encoded/compressed data

Character	Code
A	1100
B	1101
C	100
D	101
E	111
F	0

DATA LINK CONTROL

- The most important functions in the data link layer are flow control, error control and line discipline.
- Line discipline coordinates the link systems.It determines which device can send and when it can send.
- Flow control coordinates the amount of data that can be sent before receiving acknowledgement. It also provides the receiver's acknowledgement of frames received intact, and so is linked to error control.
- Error control means error detection and correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender.

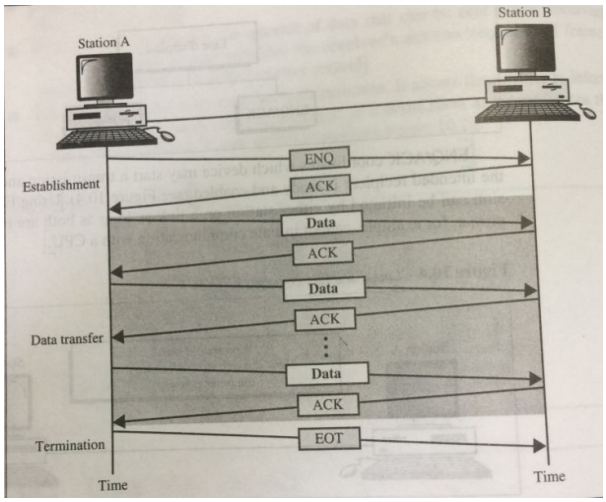


LINE DISCIPLINE

- The line discipline functions of the data link layer oversee the establishment of links and the right of a particular device to transmit at a given time.
- Line discipline can be done in two ways:
  - Enquiry / Acknowledgement
  - Poll / select

ENQ/ACK

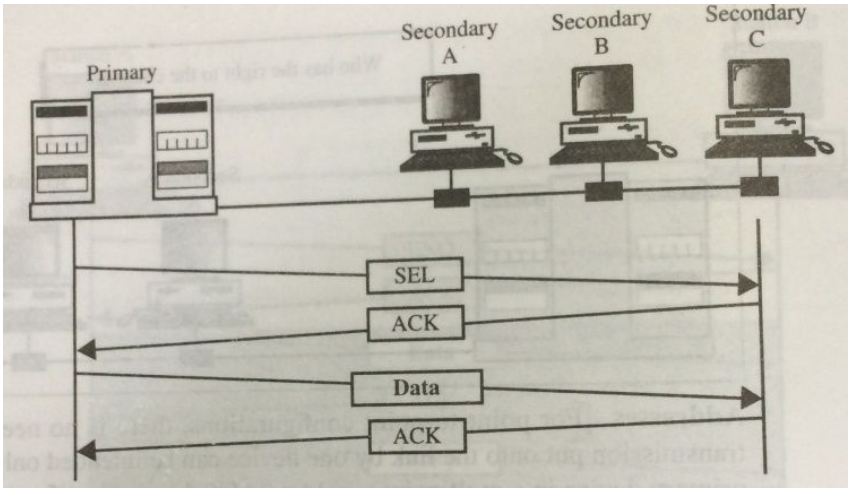
- This method is used in peer-to-peer communication.
- Enquiry/acknowledgement is used primarily in systems when there is a dedicated link between two devices so that the only device capable of receiving the transmission is intended one.
- ENQ/ACK coordinates which device may start a transmission and whether or not the intended recipient is ready and enabled.
- In both half-duplex and full-duplex transmission, the initiating device establishes the session.
  - In half-duplex, the initiator then sends its data while the responder waits. The responder may take over the link when the initiator is finished or has requested a response.
  - In full duplex, both devices can transmit simultaneously once the session has been established.
- How it works:



- The initiator first transmits a frame called an enquiry (ENQ) asking if the receiver is available to receive data.The receiver must answer either with an acknowledgement (ACK) frame if it is ready to receive or negative acknowledgement (NAK) frame if it is not.
- If neither an ACK or a NAK is received within a specified time limit, the initiator assumes that the ENQ frame was lost in transmit, disconnects, and sends a replacement.
- If the response to the ENQ is negative for three attempts, the initiator disconnects and begins the process again at another time.
- If the response is positive, the initiator free to sends it data.
- Once all of its data have been transmitted, the sending system finishes with an End of Transmission (EOT) frame.

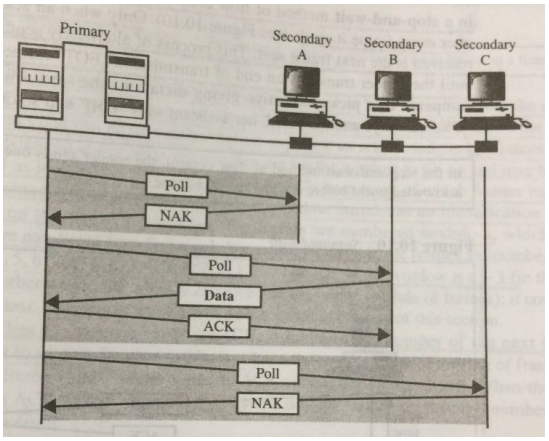
Poll / Select

- The poll/select method of line discipline works with topologies where one device is designated as primary station and the other devices are secondary stations.
- How it works:
  - Whenever a multipoint link consists of a primary device and multiple secondary devices using a single transmission line, all exchanges must be made through the primary device.
  - The primary device controls the link; the secondary devices follow its instructions.
  - If the primary wants to receive the, it asks the secondaries if they have anything to send; this function is called polling.
  - If the primary wants to send data, it tells the target secondary to get ready to receive; this function is called selecting.
- Addresses
  - For the primary device in a multipoint topology to be able to identify and communicate with a specific secondary device, there must be an addressing convention. Each secondary device has an address that differentiates it from the others.
  - In any transmission, that address will appear in a specified portion of each frame, called an address field or header depending on the protocol.
  - If the transmission comes from the primary device, the address indicates the recipient of the data. If the transmission comes from a secondary device, the address indicates the originator of the data.
- Select
  - The select mode is used whenever the primary device has something to send.



- Primary must alert the secondary to the upcoming transmission and wait for an acknowledgement of the secondary's ready status. Before sending data, the primary creates and transmits a select(SEL) frame, one field of which includes the address of the intended secondary.
- As a frame makes its way down the link, each of the secondary devices checks the address field. Only when a device recognizes its own address does it open the frame and read the data.
- If the secondary is awake and running, it returns an ACK frame to the primary. The primary then sends one or more data frames, each addressed to the intended secondary.

- Poll
  - If the primary wants to receive data, it asks the secondaries the if they have anything to send; this function is called polling.



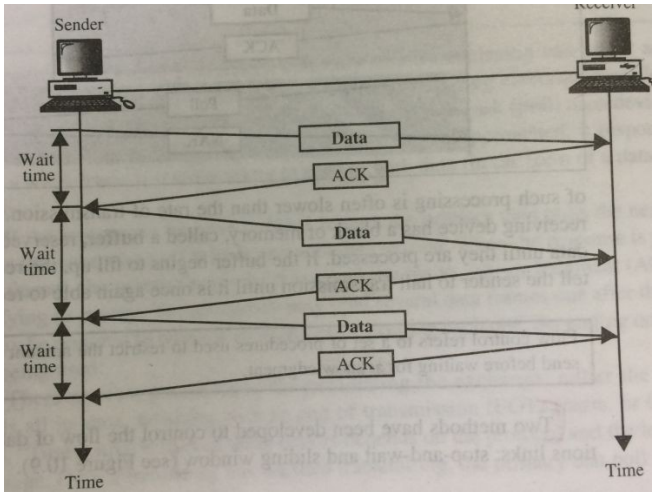
  - When the primary is ready to receive the data, it must ask (poll) each device in turn if it has anything to send.
  - The secondaries can reply with either NAK or data.
  - There are two possibilities for terminating the exchange: either the secondary sends all its data, finishing with an end of transmission(EOT) frame, or the primary says, "Time's up" .

Flow control

- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- The flow of data must not be allowed to overwhelm the receiver.
- Two methods have been developed to control the flow of data across communication links:
  - Stop-and-wait
  - Sliding window

Stop-and Wait

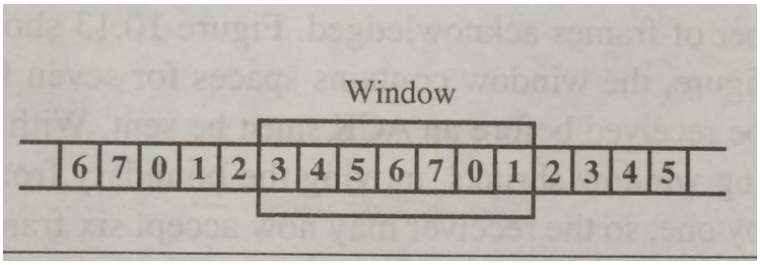
- In a stop-and-wait method of flow control, the sender waits for an acknowledgement after every frame it sends.



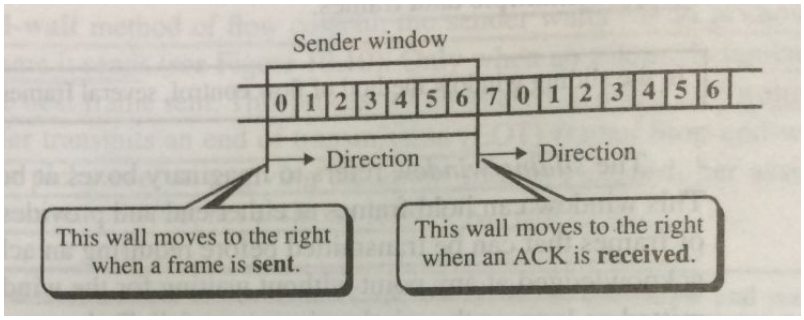
- Only when an acknowledgement has been received is the next frame sent.
- This process of alternatively sending and waiting repeats until the sender transmits an End Of Transmission (EOT) frame.
  - Advantage: simplicity
  - Disadvantage: inefficiency

Sliding Window

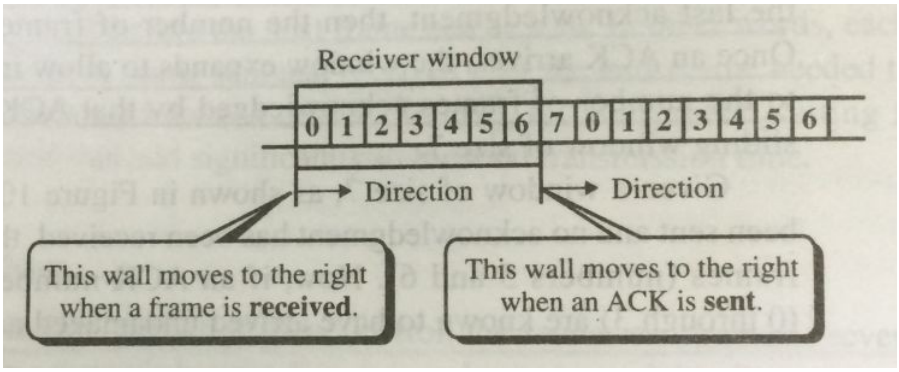
- In the sliding window method of flow control, the sender can transmit several frames before needing an acknowledgement.
- Frames can sent one right after another, meaning that the link can carry several frames at once and its capacity can be used efficiently.
- The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames.
- The sliding window refers imaginary boxes at both the sender and the receiver.
- This window can hold frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- Frames may be acknowledged at any point without waiting for the window to fill up and may be transmitted as long as the window is not yet full.
- To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window.



- The frames are numbered modulo-n, which means they are numbered from 0 to n-1.The size of the window is n-1. It covers one frame less.
- when the receiver sends an ACK, it includes the number of the next frame it expects to receive. [to acknowledge the receipt of a string of frames ending in frame 4, the receiver sends an ACK containing the number 5. When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.]
- ***sender window:***
- At the beginning of a transmission, the sender's window contains n-1 frames.
- As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window.
- Given a window of size w, if three frames have been transmitted since the last acknowledgement, then the number of frames left in window is w-3.



- Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by the ACK.
- ***Receiver window:***
- At the beginning of transmission, the receiver window contains not n-1 frames but n-1 spaces for frames.



- As new frames come in, the size of the receiver window shrinks.
- The receiver window therefore represents not the number of frames received but the number of frames that may still be received before an ACK must be sent.

ERROR CONTROL

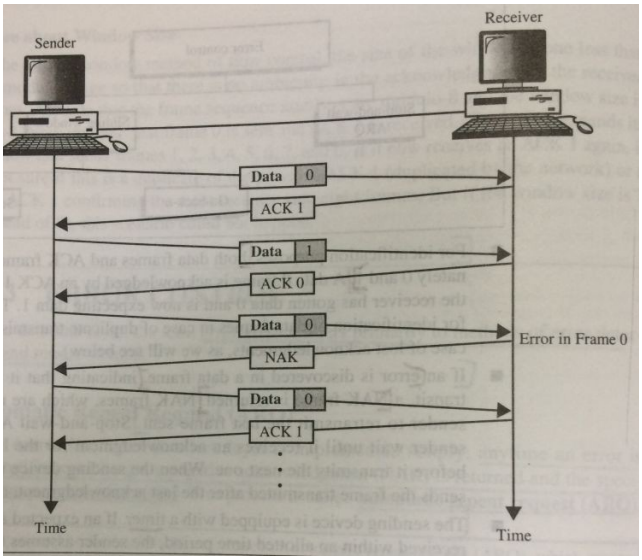
- Error control refers primarily to methods of error detection and retransmission.

Automatic Repeat Request

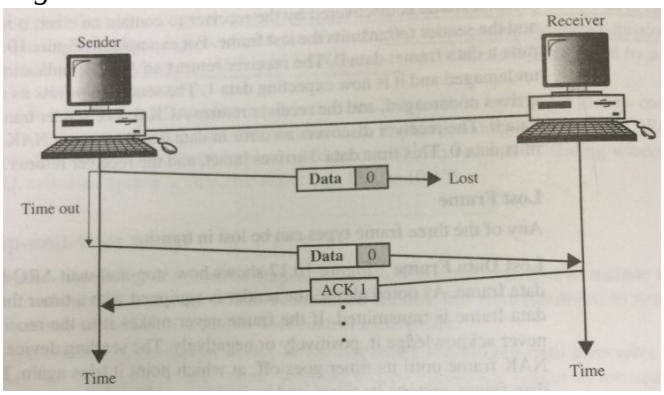
- Error control in the data link layer is based on automatic repeat request(ARQ), which means retransmission of data in three cases:
  - Damaged frame
  - Lost frame
  - Lost Acknowledgement
- ARQ error control is implemented in the data link layer as an adjunct to flow control.

- ***Stop- and –wait ARQ***
- For retransmission to work, four features are added to the basic flow control mechanism:
  - The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement.
  - For identification purpose, both data frames and ACK frames are numbered alternatively 0 and 1.
  - If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned.
  - The sending device is equipped with a timer. If an expected acknowledgement is not received within in an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again.

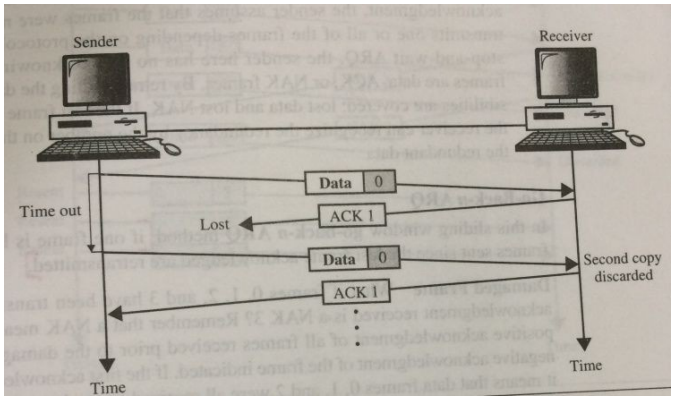
  - *Damaged Frames*



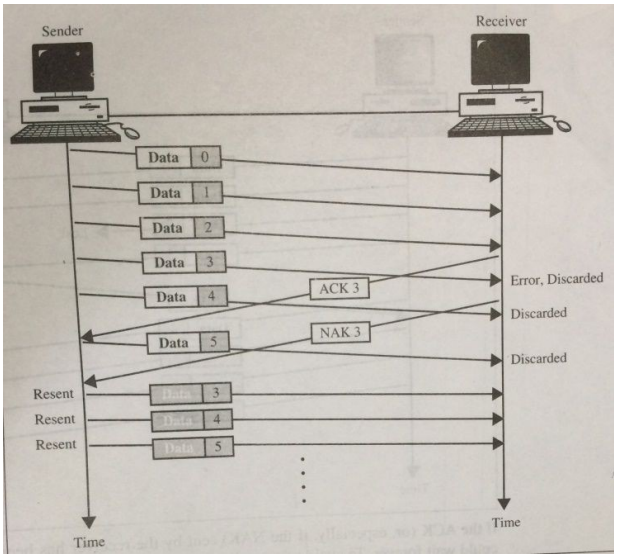
  - *Fig:*
  - *Lost Data Frame*
  - *Fig:*



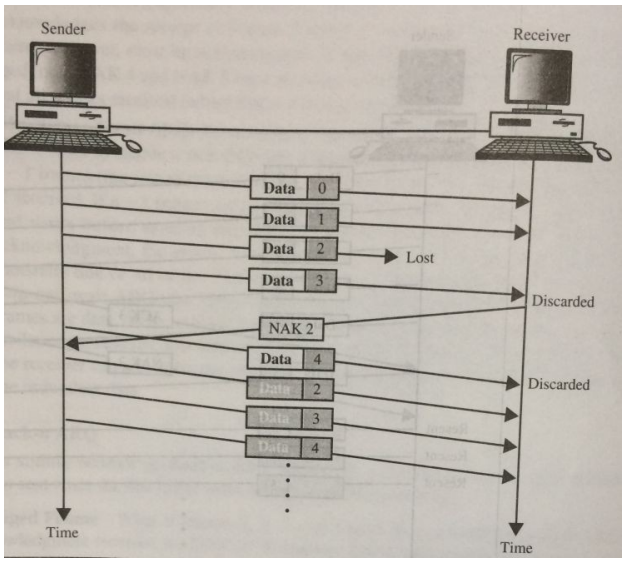
  - *Lost ACK/NAK frame*
  - *Fig:*



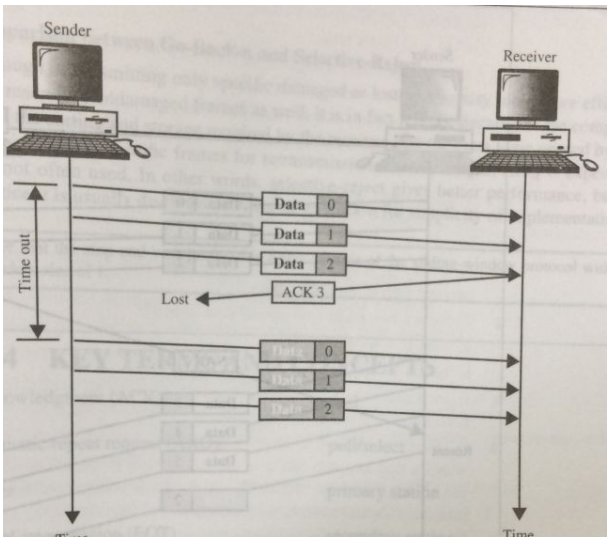
- ***Sliding Window ARQ***
- To extend sliding window to cover retransmission of lost or damaged frames, three features are added to the basic flow control mechanism:
  - The sending device keeps copies of all transmitted frames until they have been acknowledged.
  - In addition to ACK frames, the receiver has the option of returning a NAK frame if the data have been received damaged.
  - Like stop-and-wait ARQ, the sending device in sliding window ARQ is equipped with a timer to enable it to handle lost acknowledgements.
- ***Go-Back-n ARQ***
- If one frame is lost or damaged, all frames sent since the last frame acknowledged are retransmitted.
  - Damaged frame



- Lost Data Frame

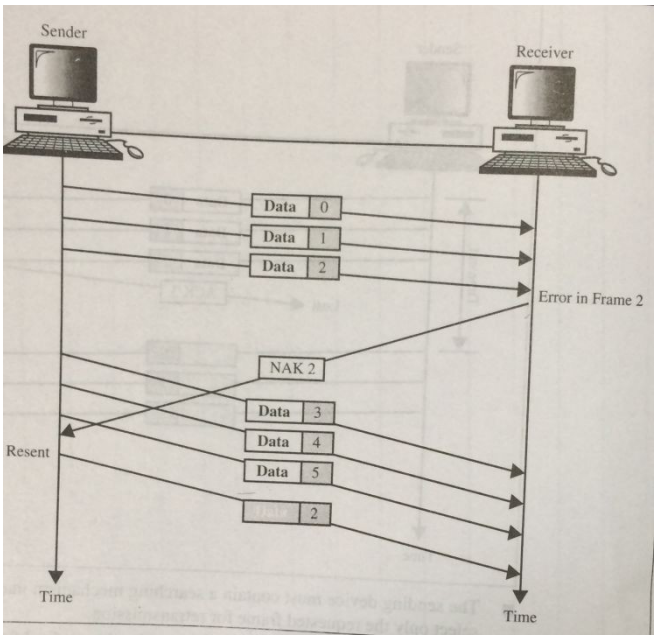


- Lost Acknowledgement



Selective- Reject ARQ

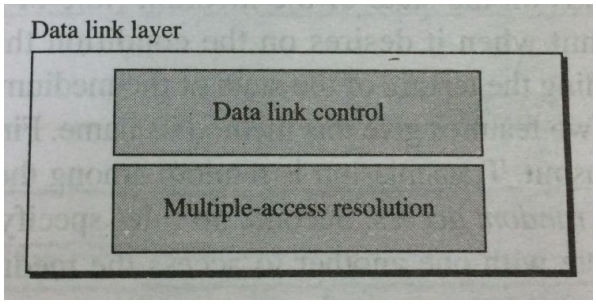
- In selective reject ARQ, only the specific damage or lost frame is retransmitted.
- If a frame is corrupted in transit, a NAK is returned and the frame is resent out of sequence.



- The receiving device must be able to sort the frames it has and insert the retransmitted frame into its proper place in the sequence. To make such selectivity possible, a selective reject ARQ system from a go-back-n ARQ system in the following ways:
  - The receiving device must contain sorting logic to enable it to render frames received out of sequence.
  - The sending device must contain a searching mechanism that allows it to find and select only the requested frame for retransmission.
  - A buffer in the receiver must keep all previously received frames on hold until all retransmissions have been identified and discarded.
  - To aid selectivity ACK numbers must refer to the frame received instead of the next frame expected.
  - This complexity requires a smaller window size than is needed by the go-back-n ARQ method if it is to work efficiently.

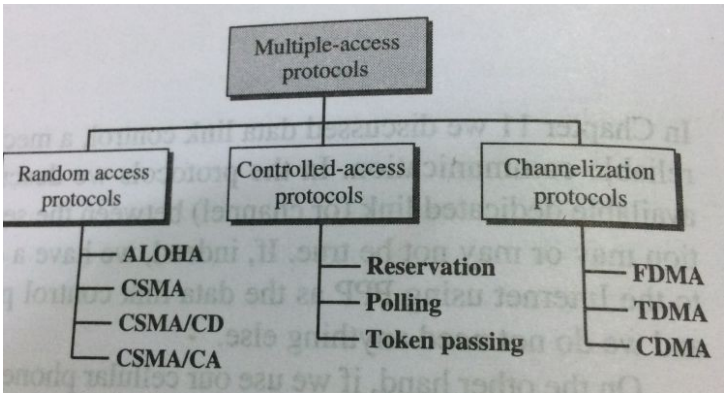
MULTIPLE ACCESS

- We can consider the data link layer as two sublayers. The upper sublayer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media.
- If the channel is dedicated, we do not need the lower sub layer.
- Fig:



- The upper sublayer that is responsible for flow and error control is called Logical Link Control layer; the lower sublayer that is mostly responsible for multiple access resolution is called the media access control layer.

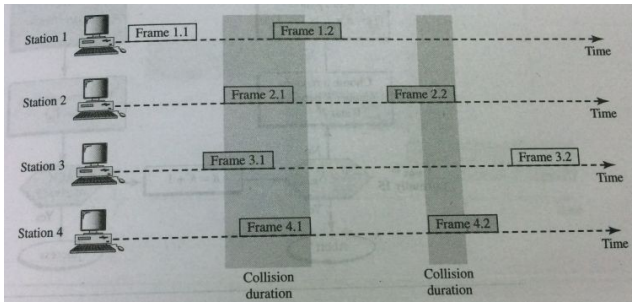
- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple access protocol to coordinate access to the link.
- We categorize them into three groups:



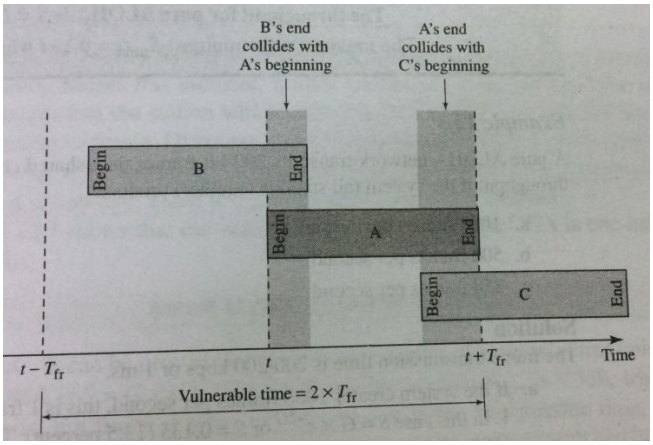
- Fig:

RANDOM ACCESS

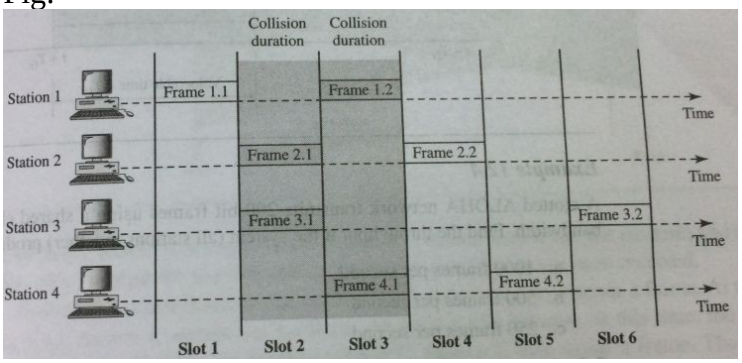
- Random access is also called contention methods.
- In this method, no station is superior to another station and none is assigned the control over another.
- A station that has to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle/busy).
- There is no schedule time for a station to transmit. Transmission is random among the stations. That is why the methods are called random access.
- No rules specify which station should send next. Stations compete with one another to access the medium.
- In a random access method, each station has the right to the medium without being controlled by any other station. However, if more than one station tries to send, there is an access conflict- collision – and the frames will be either destroyed or modified.
- Random Access protocols are:
  - ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- ***ALOHA***
- The earliest random access method.
- Developed at the University of Hawaii
- The medium is shared between the stations.
- When a station sends data, another station may attempt to do so at the same time. The data from two stations collide and become garbles.
  - *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. However, since there is only one channel to share, there is the possibility of collision between frames from different stations.
  - Fig:



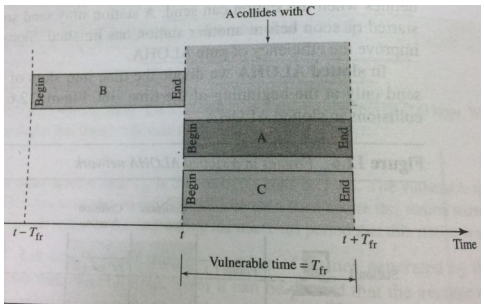
- The pure ALOHA protocol relies on acknowledgements from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgement. If the acknowledgement does not arrive after a time-out period, the station assumes that the frame has been destroyed and resends the frame.
- Pure ALOHA tries to avoid collision in two ways:
  - Each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions.
  - After a maximum number of retransmission attempts K max, a station must give up and try later.
- ***Vulnerable time: [length of the time, in which there is a possibility of collision.***
- Fig:



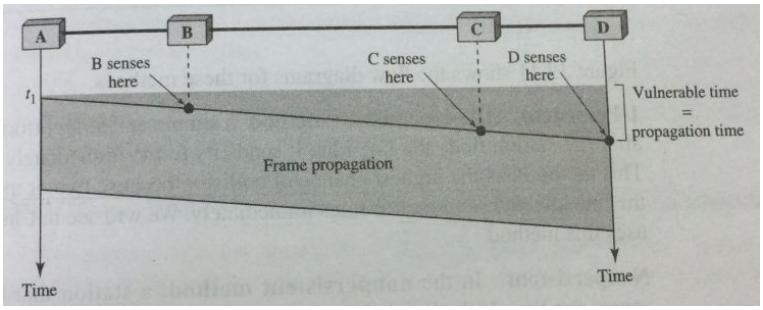
- ***Pure ALOHA vulnerable time = 2 x T fr***
- *Slotted ALOHA*
- Pure ALOHA has the vulnerable time of 2 x T fr. This is so because there is no rule that defines when the station can send.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA we divide the time into slots of T fr s and force the station to send only at the beginning of the time slot.
- Fig:



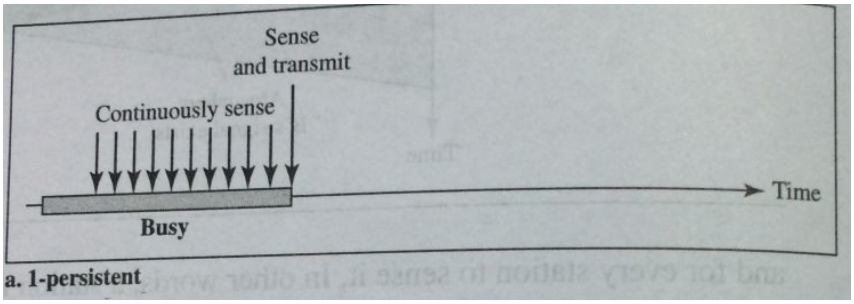
- There is still the possibility of collision if two stations try to send at the beginning of the same time slot.
- However, the vulnerable time is now reduced to one-half.
- ***Slotted ALOHA vulnerable time = T fr***



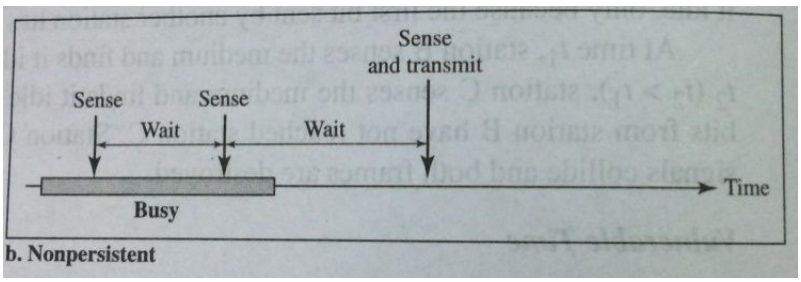
- ***Carrier Sense Multiple Access (CSMA)***
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier Sense Multiple Access requires that each station first listen to the medium before sending.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.
- The vulnerable time for the CSMA is the Propagation time.
- Fig:



- When the channel is busy or idle, the CSMA methods use persistent methods to decide what station will do.
  - *Persistent Methods*
    - *1- persistent Method*
    - In this method, after the station finds the line idle, it sends its frame immediately.
    - This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

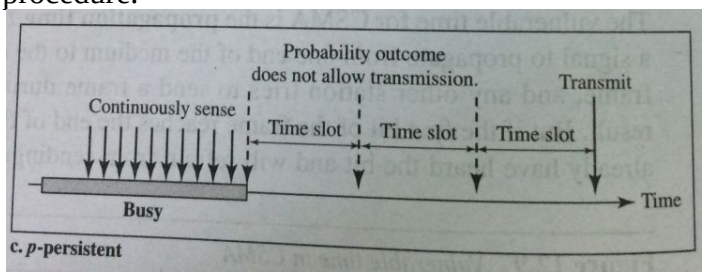


    - *Non persistent method*
    - In this method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.

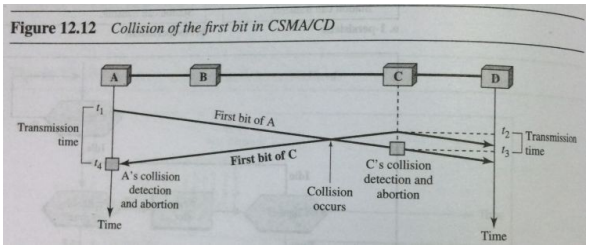


  - This method is used if the channel has time slots with a slot duration equal toor greater than the maximum propagation time.
  - In this method, after the station finds the line idle, it follows these steps:
    1. With probability p, the station sends its frame.

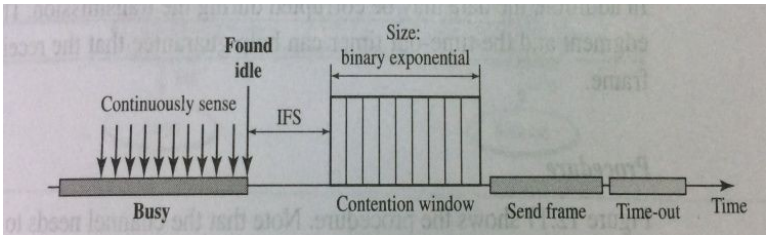
2. With probability q= 1-p, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts though a collision has occurred and uses the back off procedure.



- **Carrier Sense Multiple Access with Collision Detection(CSMA/CD)**
- In this method a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.
- Fig:



- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
- CSMA/CA was invented for the wireless networks because they cannot detect collision.
- Collisions are avoided through the use of CSMA /CAs three strategies:
  - Interframe Space(IFS)
  - The contention window
  - Acknowledgement.
- Fig:



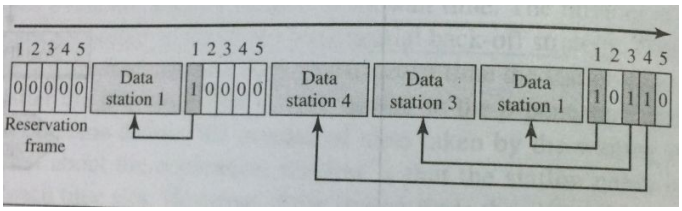
- ***Interframe Space(IFS)***
- When idle channel is found, the station does send immediately.
- It waits for a period of time called the IFS.
- Even through the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station.
- If after the IFS time the channel is still idle, the station can send, but it still needs wait a time equal to the contention time.

- *Contention Window*
- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as a wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy.

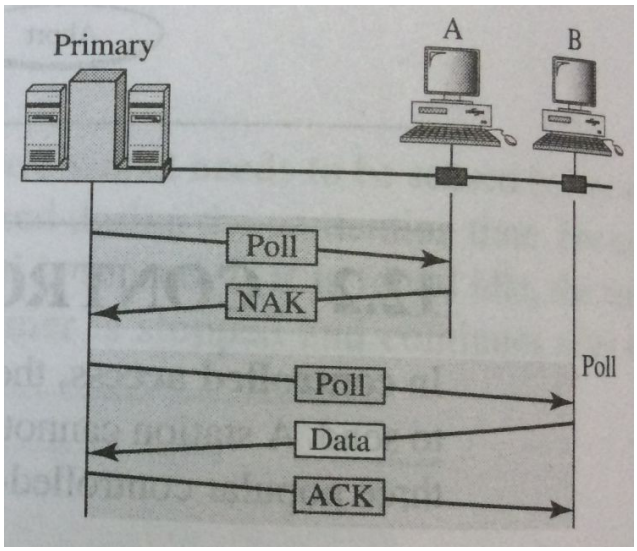
- *Acknowledgement*
- The data may be corrupted during the transmission.
- The positive acknowledgement and time-out timer can help guarantee that the receiver has received the frame.

CONTROLLED ACCESS

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.
- ***RESERVATION***
  - In the reservation method, a station needs to make a reservation before sending data.
  - Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.
  - Fig:

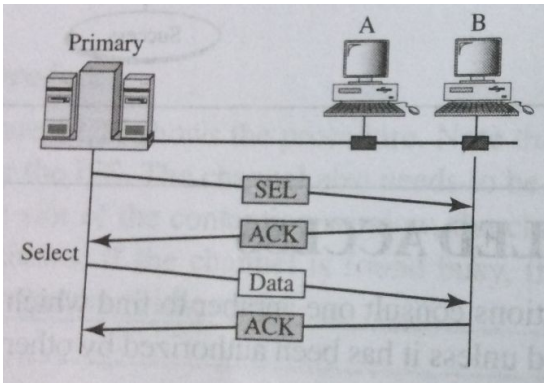


- ***POLLING***
  - Polling work with topologies in which one device is designated as a primary station and the other devices are secondary stations.
  - The primary device controls the link; the secondary devices follow its instructions.
  - If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function.
  - Fig:



  - If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

- Fig:



- ***TOKEN PASSING***
- In this method, the stations in a network are organized in a logical ring.
- For each station, there is a predecessor and successor. The predecessor is the station which is logically before the station in the ring; the successor is the station which is after the station in the ring.
- The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station. The right will be passes to the successor when the current station has no more data to send.
- A special packet called a token circulates through the ring, the possession of the token gives the station the right to access the channel and send its data.

CHANNELIZATION

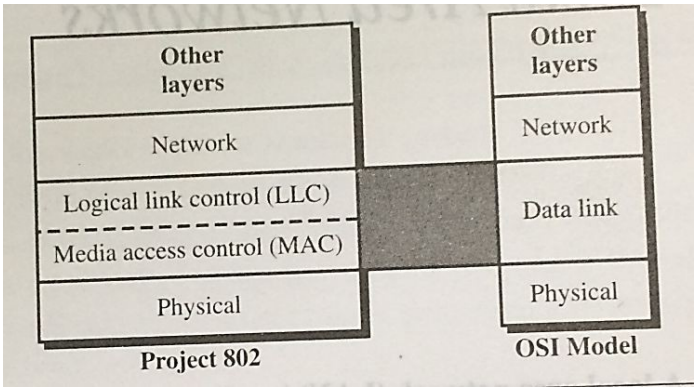
- Channelization is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.
- There are three channelization protocols:
  - FDMA
  - TDMA
  - CDMA
- ***Frequency Division Multiple Access(FDMA)***
  - In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to sends its data.
- ***Time Division Multiple Access(TDMA)***
  - In TDMA, the stations share a bandwidth of the channel in time. Each station is allocated a time slot during which it can send data.
- ***Code Division Multiple Access(CDMA)***
- In CDMA, one channel carries all transmissions simultaneously.

Wired LANs: ETHERNET

- Local Area Network (LAN) is a computer network that is designed for a limited geographic area such as building or a campus.
- The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI an ATM LAN but Ethernet is by far the dominant technology.

IEEE STANDARD

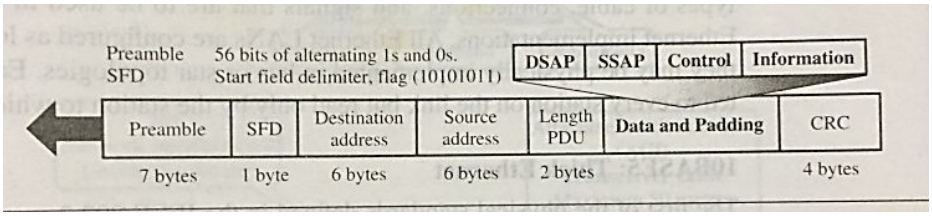
- Computer society of IEEE (Institute Of Electrical and Electronic Engineers) started a project called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.
- The standard was adopted by ANSI. The ISO also approved it as an international standard.
- The relationship of the 802 standard to the traditional OSI model.
- Fig:



- The IEEE has subdivided the data link layer into two sublayers:
  - Logical Link Control
  - Media Access Control
- **Logical Link Control**
- In IEEE 802, flow control, error control, and part of the framing duties are collected into one sub layer called the LLC.
- The LLC provides one single data link control protocol for all IEEE LANs. In this way the LLC is different from the media access control sublayer, which providesdifferent protocols for different LANs.
- Frame:

DSAP	SSAP	Control	Upper Layer data

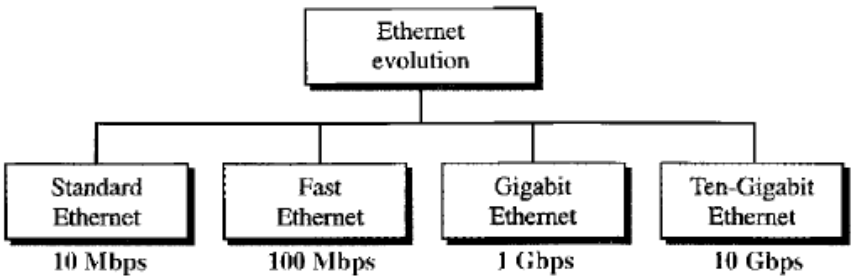
  - DSAP: Destination Service Access Point
  - SSAP: Source Service Access Point
  - Control: used to error control and flow control.
- **Media Access Control**
- IEEE 802 has created a sublayer called media access control that defines the specific access method for each LAN.
- Frame format:

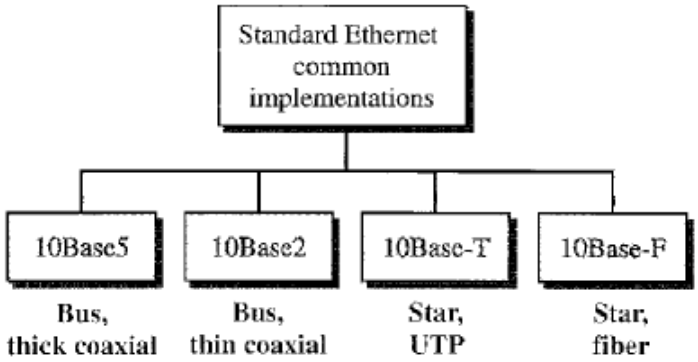


  - *Preamble*
  - It alerts the receiving system to the coming frame and enables it to synchronize its input timing.
  - *Start Frame Delimiter*
  - It signals the beginning of the frame.
  - The SFD warns the station or stations that this is the last chance for synchronization.
  - *Destination Address(DA)*
  - It contains the physical address of the destination station or stations to receive the packet.
  - *Source Address(SA)*
  - It contains the physical address of the sender of the packet.
  - *Length or type*
  - Length: to define the number of bytes in the data field.

- *Data*
- This field carries data encapsulated from the upper-layer protocols.
- 46- 1500 bytes capacity.
- *CRC*
- It contains error detection information.

- Standard has gone through four generations:
  - Standard Ethernet (lot Mbps)
  - Fast Ethernet (100 Mbps)
  - Gigabit Ethernet (I Gbps)
  - Ten-Gigabit Ethernet (10 Gbps)



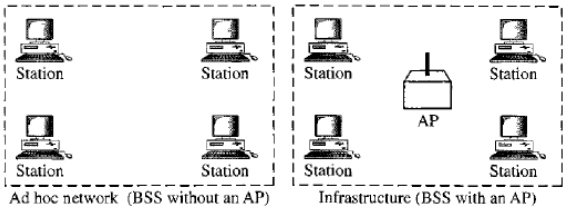


- **STANDARD ETHERNET COMMON IMPLEMENTATIONS**
  - ***10Base5: Thick Ethernet***
  - The first implementation is called lOBaseS, thick Ethernet, or Thicknet.
  - The nick-name derives from the size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.
  - ***10Base2: Thin Ethernet***
  - The second implementation is called 10Base2, thin Ethernet, or Cheapernet.
  - 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations.
  - ***lOBase-T: Twisted-Pair Ethernet***
  - lOBase-T uses a physical star topology.
  - The stations are connected to a hub via two pairs of twisted cable.
  - ***lOBase-F: Fiber Ethernet***
  - lOBase-F uses a star topology to connect stations to a hub.
  - The stations are connected to the hub using two fiber-optic cables

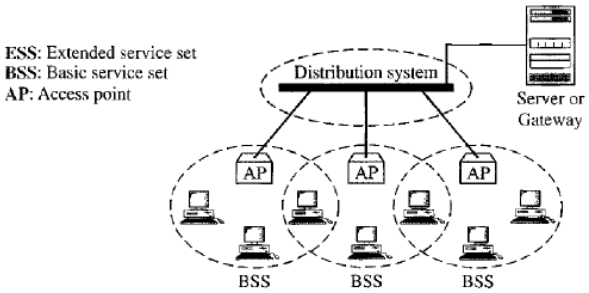
WIRELESS LANs

- Two promising wireless technologies for LANs:
  - IEEE 802.11 Wireless LANs [ethernet]
  - Bluetooth

- ***IEEE 802.11***
- *Architecture*
- The standard defines two kinds of services:
  - Basic Service Set (BSS)
  - Extended Service Set (ESS)
    - *Basic Service Set*
    - A Basic Service Set is made of stationary or mobile wireless stations and an optional central base station, known as Access Point(AP).



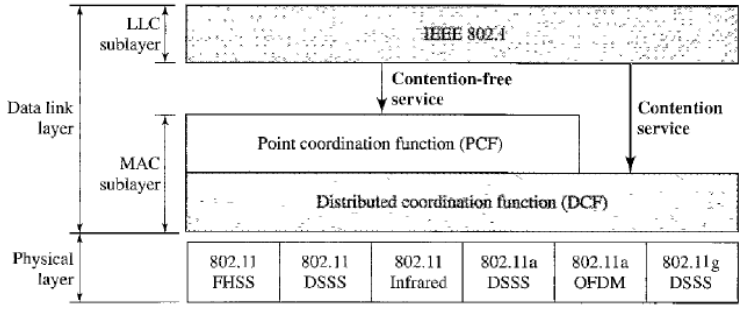
    - A BSS without an AP is called an ad hoc network.
    - A BSS with an AP is called an infrastructure network.
    - *Extended Service Set*
    - An Extended Service Set is made up of two or more BSSs with Aps.



    - In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.
    - The distribution system connects the APs in the BSSs.
    - The ESS uses two types of stations:
      - *Mobile*
        The mobile stations are normal stations inside a BSS.
      - *Stationary*
        The stationary stations are AP stations that are part of a wired LAN.
    - When BSS are connected , the stations within reach of one another can communicate without the use of an AP. However, communications between two stations in two different BSSs usually occur via two Aps.
- *STATION TYPES:*
  IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:
- *No-transition*
  A station with no-transition mobility is either stationary or moving only inside a BSS.
- *BSS-transition*
  A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS.
- *ESS-transition*
  A station with ESS transition mobility can move from one ESS to another
- *MAC Sublayer*

IEEE 802.11 defines two MAC sublayers:

- The Distributed Coordination Function
- Point Coordination Function
- Fig:



- ***Distributed Coordination Function***
- DCF uses CSMA/CA as access method
- Frame Exchange Time Line

  1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.

     a. The channel uses a persistence strategy with back-off until the channel is idle.

     b. After the station is found to be idle, the station waits for a period of time called the Distributed Interframe Space (DIFS); then the station sends a control frame called the Request To Send (RTS).

  2. After receiving the RTS and waiting a period of time called the Short InterframeSpace(SIFS), the destination station sends a control frame , called the Clear To Send(CTS) , to the source station.

  3. The source station sends data after waiting an amount of time equal SIFS.

  4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgement to show that the frame has been received.

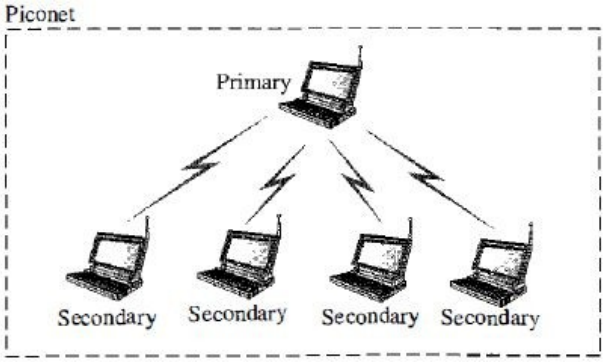
- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a Network Allocation Vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.
- ***Point Coordination Function***
- The PCF is an optional access method that can be implemented in an infrastructure network.
- PCF has a centralized, contention free polling access method.
- The AP performs polling for stations that are capable of being polled.
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium.
- To prevent this, a repetition interval has been designed to cover both contention free (PCF) and contention based(DCF) traffic.
- The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.
- *Frame Format*
- The MAC layer consist of nine fields:

- Frame Control
  - 2 byte long
  - Defines the type of frame and some control information.
  - Sub fields:
    - version
    - type
    - subtype
    - to DS
    - From DS
    - More Flag
    - Retry
    - pwrmgt
    - More data
    - Wired Equivalent Privacy
    - Rsvd
  - D
    - It defines duration of transmission.
  - Addresses
    - There are 4 address fields, each 6 bytes long.
  - Sequence Control
    - It defines the sequence number of the frame.
  - Frame Body
    - It contains information based on the type and subtype.
  - FCS
    - It contains a CRC-32 error detection sequence.

BLUETOOTH

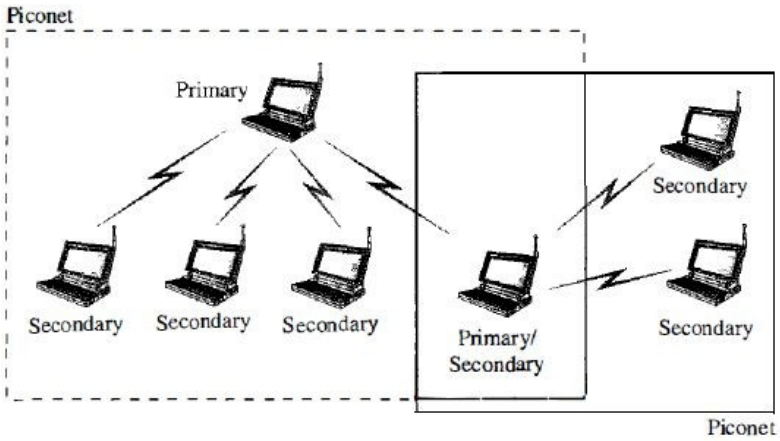
- Bluetooth is a wireless LAN technology designed to connect devices of different func-tions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- Bluetooth technology has several applications.
  - Peripheral devices such as a wire-less mouse or keyboard can communicate with the computer through this technology.
  - Monitoring devices can communicate with sensor devices in a small health care center.
- Bluetooth was originally started as a project by the Ericsson Company. It is named for HaraldBlaatand, the king of Denmark (940-981) who united Denmark and Norway.Blaatand translates to Bluetooth in English.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- *Architecture*

  Bluetooth defines two types of networks:
  - Piconet
  - scattemet.
  - ***Piconet***
    - A Bluetooth network is called a piconet, or a small net.
    - A piconet can have up to eight stations, one of which is called the primary; t the rest are called secondaries.
    - Fig:



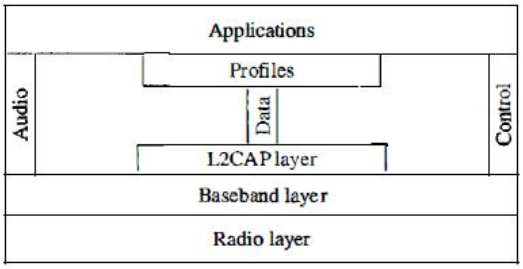
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- Apiconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state.
- A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the parked state.

- ***Scatternet***
  - Piconets can be combined to form what is called a scatternet.
  - A secondary station in one piconet can be the primary in another piconet.
  - A station can be a member of two piconets.
- Fig:



- ***Bluetooth Layers***

Bluetooth layers

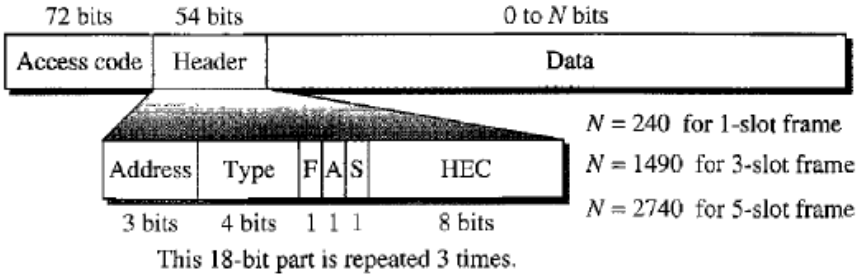


- ***Radio Layer***
  - The radio layer is roughly equivalent to the physical layer of the Internet model.

- ***Baseband Layer***
  - The baseband layer is roughly equivalent to the MAC sublayer in LANs.
  - The access method is TDMA.
  - The primary and secondary communicate with each other using time slots.
  - Bluetooth uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA).
  - TDD-TDMA is a kind of half-duplex communication in which the secondary and receiver send and receive data, but not at the same time.
  - *Single-Secondary Communication:* If the piconet has only one secondary,The primary uses even-numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5, ...).
  - *Multiple-Secondary Communication:*The process is a little more involved if there is more than one secondary in the piconet. Again, the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

- ***Physical links***
- Two types of links can be created between a primary and a secondary: SCO links and ACL links.
- A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).
- Asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency.

- ***Frame Format***



- *Access code.*
  - It contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.
- Header
  Subfields:
  - Address.
    It can define up to seven secondaries(1 to 7).
  - Type.
    It defines the type of data coming from the upper layers.
  - F: flow control.
  - A: acknowledgment.
  - S: sequence number.
  - HEC:error correction subfield, it is a checksum to detect errors
- Data