UNIT 2

PHYSICAL LAYER AND DATA LINK LAYER

Introduction to Data Transmission, Guided Media: Twisted Pair, Coaxial Cable, Fiber Optic, Unguided (RF, Microwave, Satellite), Encoding Techniques – NRZ, RZ, Clock Synchronization, Manchester, Framing & Error Detection, MAC Protocols & Ethernet Standards, Applications: Ethernet in LAN/WAN setups, encoding in RFID readers, Wi-Fi MAC in homes and airports, CRC in packet verification, fiber media in ISP backbones.

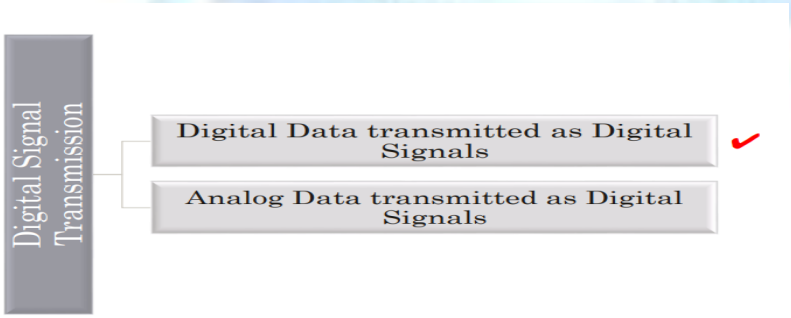
1. INTRODUCTION TO DATA TRANSMISSION, GUIDED MEDIA: TWISTED PAIR, COAXIAL CABLE, FIBER OPTIC, UNGUIDED (RF, MICROWAVE, SATELLITE)

(refer UNIT 1 Notes)

2. ENCODING TECHNIQUES – NRZ, RZ, CLOCK SYNCHRONIZATION, MANCHESTER

DIGITAL TRANSMISSION

- Digital transmission is the sending of information over a communications media in the form of digital signals
- Digital signals are a sequence of voltage pulses.
- They can propagate analog and digital data
- They offer better noise immunity, are cheaper to implement in hardware, more secure and also allow data compression, thereby optimally utilizing the transmission link.

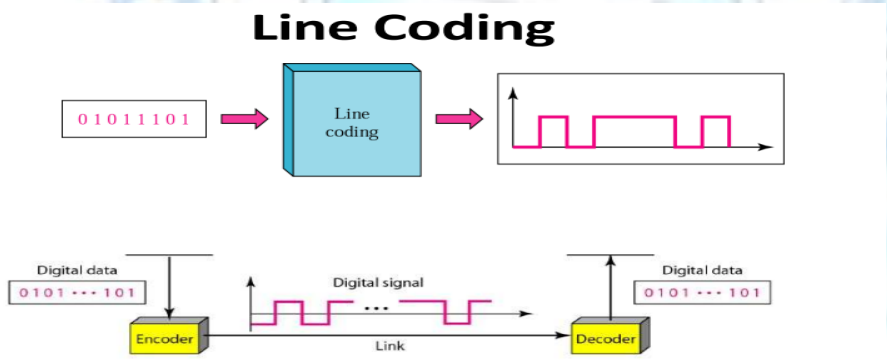


Digital Data Transmitted as Digital Signals

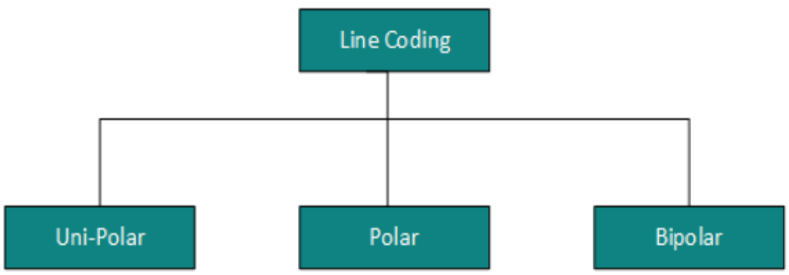
- To convert digital data into digital signals. It can be done in two ways, line coding and block coding.
- For all communications, line coding is necessary whereas block coding is optional.
- Here digital data is first encoded into a binary stream. These binary streams are then converted into digital signals by line coding techniques.

What is Line Coding?

- It is the process of converting binary data (a sequence of bits) to a digital signal.
- Different line codes have different attributes.
- Best line code has to be selected for a given application and channel condition.



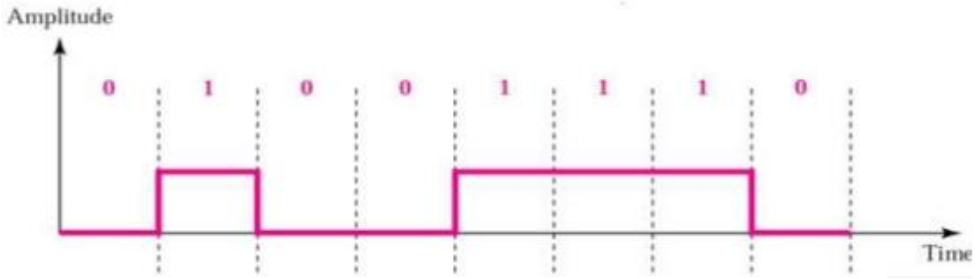
TYPES OF LINECODING



i) Unipolar Encoding

- Unipolar encoding uses only single voltage level to represent data.

- It is also called Unipolar-Non-return-to-zero, because there is no rest condition

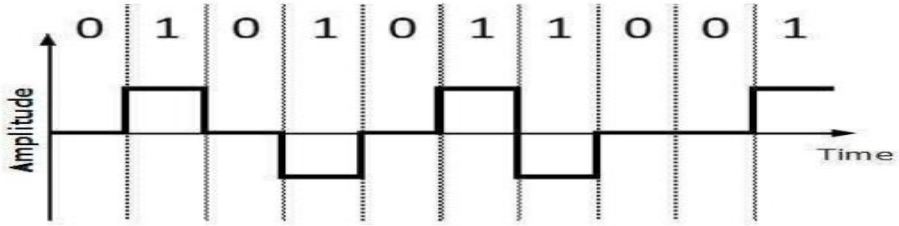


In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted

ii) Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero.

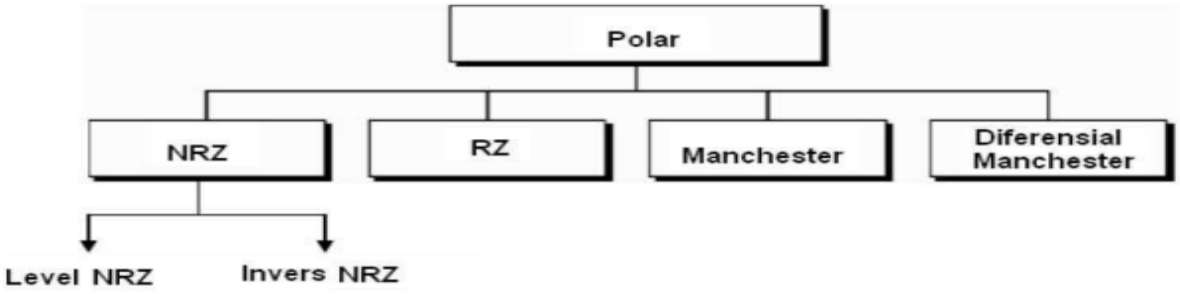
Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.



iii) Polar Encoding

Polar encoding uses two voltage levels (positive and negative).

- Polar encodings is available in four types:

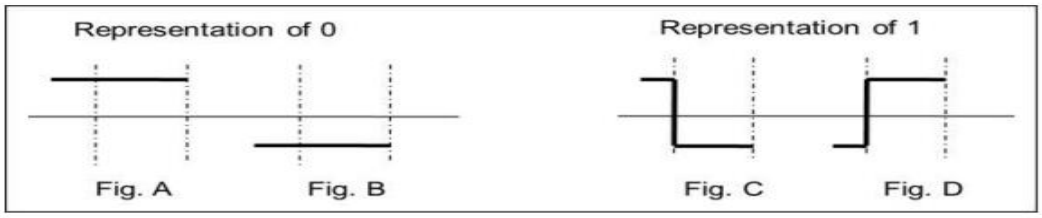


- ***Polar NRZL (Non Return to Zero) Level***

Bit 0 is mapped to a negative amplitude. –

Bit 1 is mapped to a positive amplitude.

- ***Polar NRZI (Non Return to Zero Inverted)***



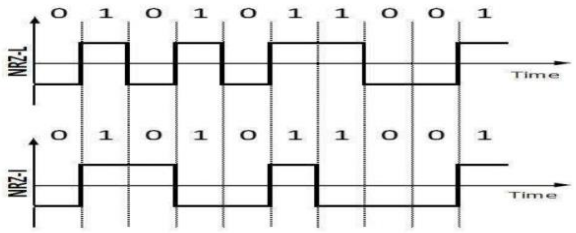
- Bit 0 mapped to no signal level transition.

- Bit 1 is mapped to signal level transition at the beginning of the bit interval.

Assumption: -

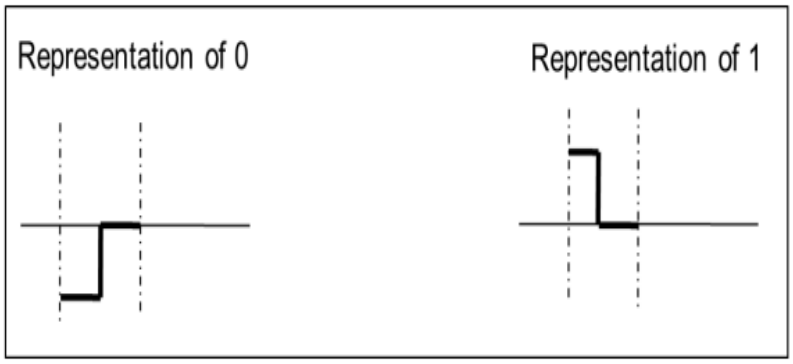
The signal level to the left of the bit is high – Fig. A and Fig. C

The signal level to the left of the bit is low – Fig. B and Fig. D



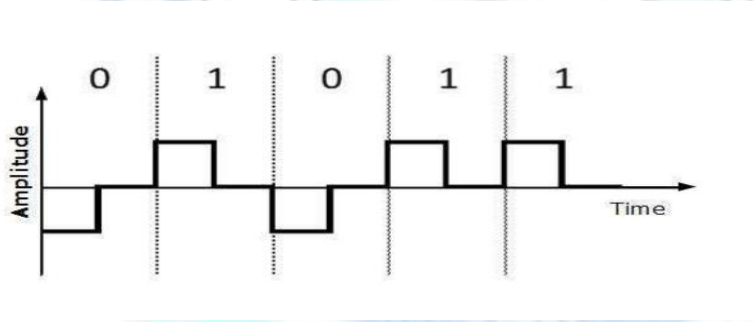
NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- ***Polar RZ (Return to Zero)***



Bit 0 is mapped to a negative amplitude - A for the first half of the symbol duration followed by a zero amplitude for the second half of the symbol duration. –

Bit 1 is mapped to a positive amplitude +A for the first half of the bit duration followed by a zero amplitude for the second half of the bit duration.

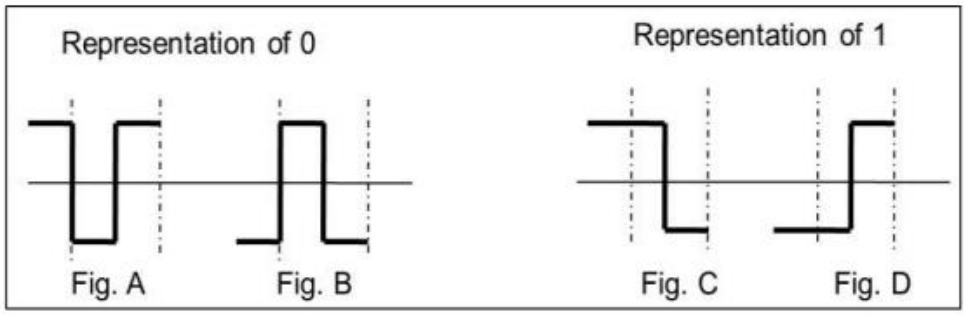


- ***Polar Manchester Coding***

-Bit 0 is sent by having a mid-bit transition from high to low.

- Bit 1 is sent by having a mid-bit transition from low to high.

- ***Polar Differential Manchester Coding***



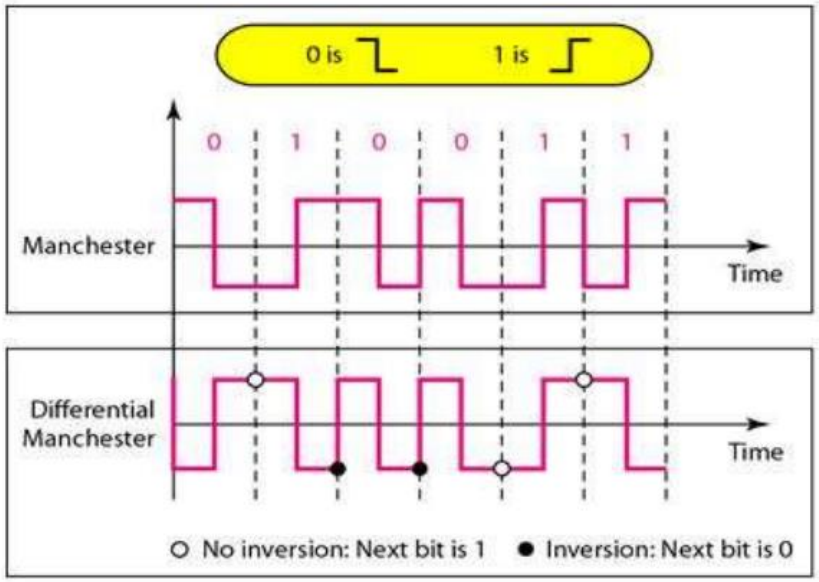
Bit 0 is mapped to signal level transition at the beginning of the bit interval. –

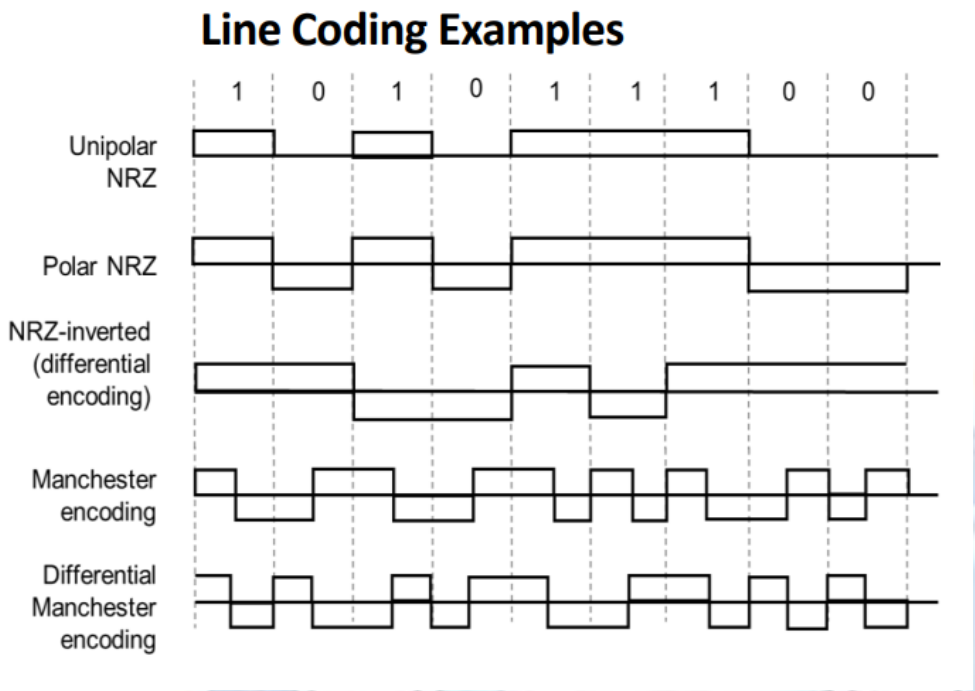
Bit 1 is mapped to absence of signal level transition at the beginning of the bit interval.

Assumption:

The signal level to the left of the bit is high – Fig. A and Fig. C

The signal level to the left of the bit is low – Fig. B and Fig. D





3. FRAMING, ERROR CONTROL AND FLOW CONTROL

The data link control (DLC) deals with procedures for communication between two adjacent nodes—node-to-node communication—no matter whether the link is dedicated or broadcast.

Data link control service include

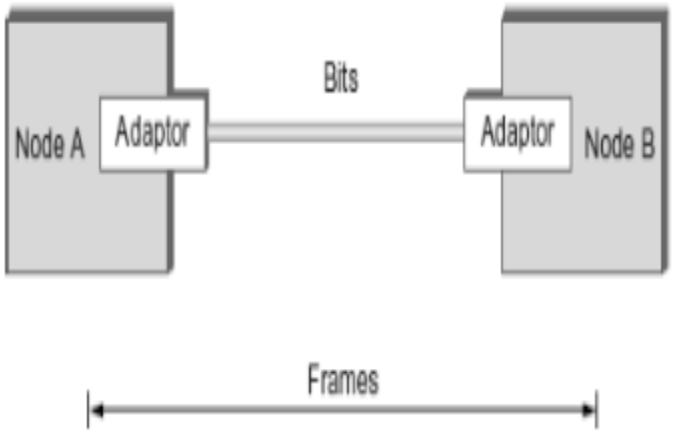
(1) Framing

(2) Flow Control

(3) Error Control

FRAMING

The data-link layer packs the bits of a message into frames, so that each frame is distinguishable from another.



- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole frame.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.
- Framing in the data-link layer separates a message from one source to a destination by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

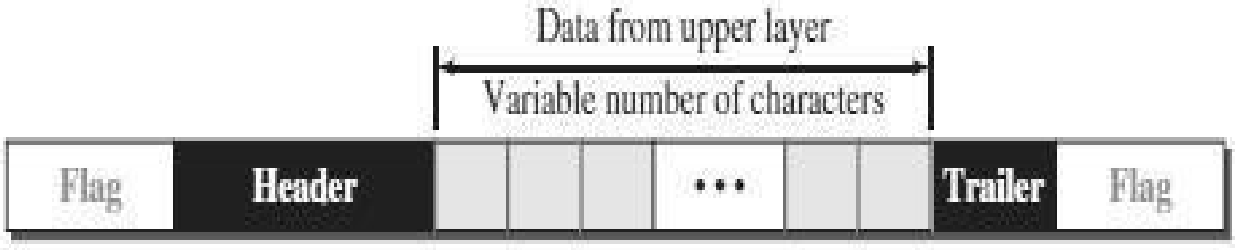
Frame Size

- Frames can be of **fixed or variable size**.
  - Frames of fixed size are called cells. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.
  - In variable-size framing, we need a way to define the end of one frame and the beginning of the next.
- Two approaches were used for this purpose:
  - a character-oriented approach and
  - a bit-oriented approach.

➢ ***Character-Oriented Framing***

- In character-oriented (or byte-oriented) framing, data to be carried are 8-bit characters.
- To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame.

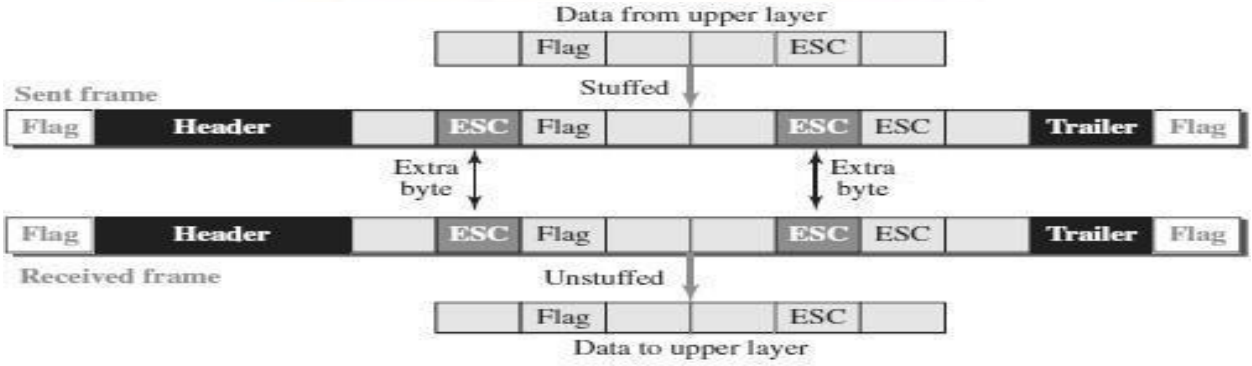
- The flag, composed of protocol-dependent special characters, signals the start or end of a frame.



- Any character used for the flag could also be part of the information.
- If this happens, when it encounters this pattern in the middle of the data, receiver thinks it has reached the end of the frame.
- To fix this problem, a **byte-stuffing strategy was added to character-** oriented framing.

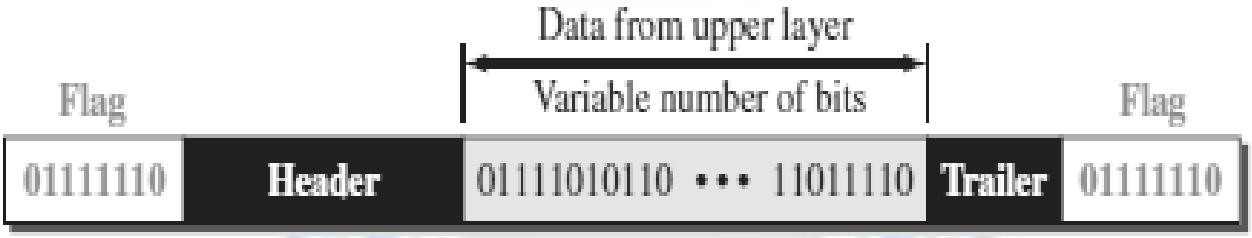
Byte Stuffing (or) Character Stuffing

- Byte stuffing is the process of adding one extra byte whenever there is flag or escape character in the text.
- In byte stuffing, a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC) and has a predefined bit pattern.
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not as a delimiting flag.



- ***Bit-Oriented Framing***

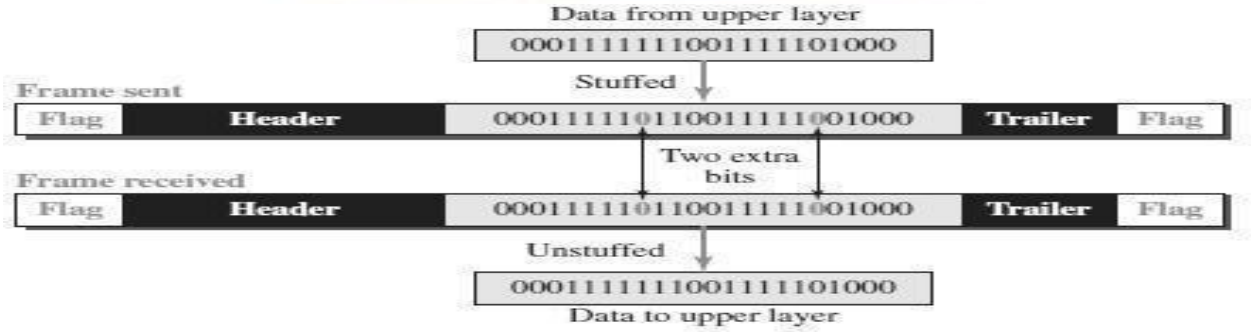
- In bit-oriented framing, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers and trailers), we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag, 01111110, as the delimiter to define the beginning and the end of the frame



- If the flag pattern appears in the data, the receiver must be informed that this is not the end of the frame.
- This is done by stuffing 1 single bit (instead of 1 byte) to prevent the pattern from looking like a flag. The strategy is called **bit stuffing.**

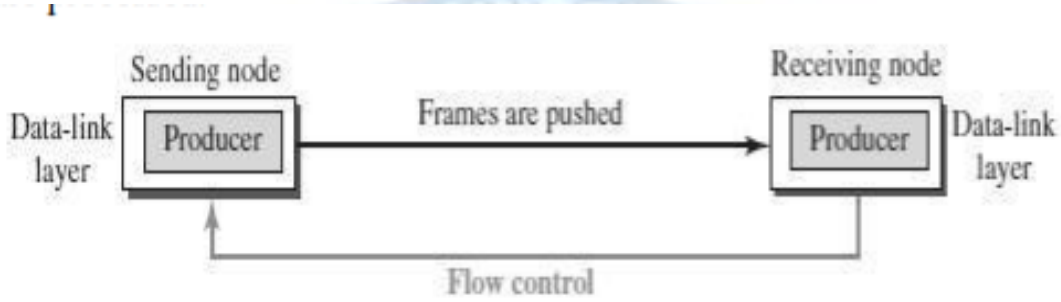
Bit Stuffing

- Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.
- In bit stuffing, if 0 and five consecutive 1 bits are encountered, an extra 0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.
- The extra bit is added after one 0 followed by five 1's regardless of the value of the next bit.
- This guarantees that the flag field sequence does not inadvertently appear in the frame.



FLOW CONTROL

- **Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.**
- The receiving device has limited speed and limited memory to store the data.
- Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed



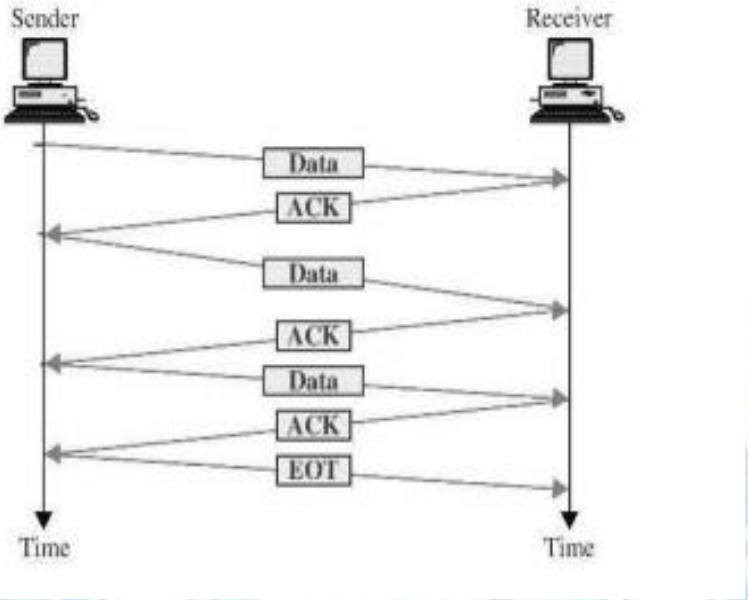
Two methods have been developed to control the flow of data:

o Stop-and-Wait

o Sliding Window

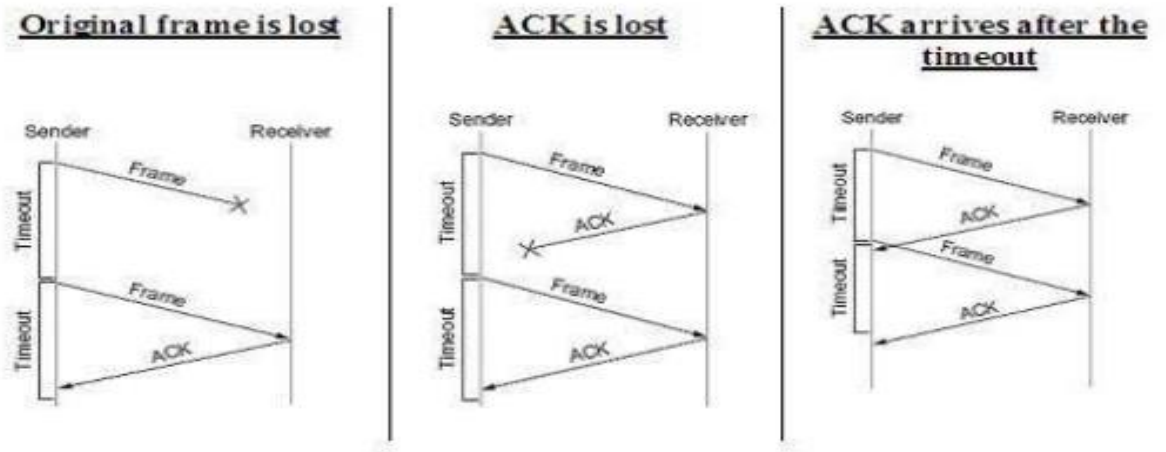
STOP-AND-WAIT

- The simplest scheme is the stop-and-wait algorithm.
- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent.
- The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.



- If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.
- The acknowledgement may not arrive because of the following three scenarios :

  1. Original frame is lost
  2. ACK is lost
  3. ACK arrives after the timeout



Advantage of Stop-and-wait

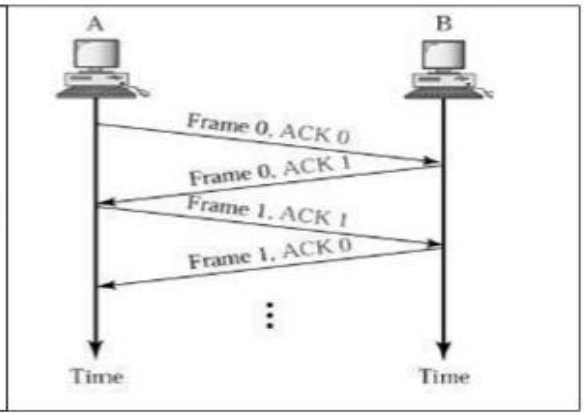
- The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent

Disadvantages of Stop-And-Wait

- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.

PIGGYBACKING

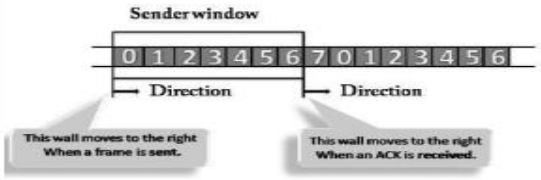
- A method to combine a data frame with ACK.
- Piggybacking saves bandwidth
- Station A and B both have data to send.
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing.



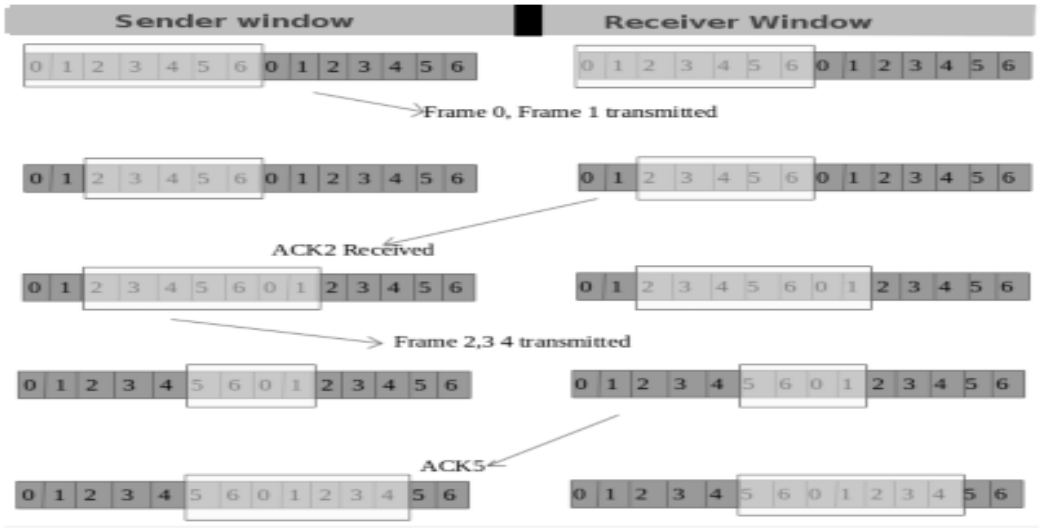
SLIDING WINDOW

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1.
- ***For example***, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.

- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive.
- For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5.
- When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window	Receiver Window
	
○ At the beginning of a transmission, the sender window contains n-1 frames. ○ When a frame is sent, the size of the window shrinks. ○ For example, if the size of the window is 'w' and if three frames are sent out, then the number of frames left out in the sender window is w-3. ○ Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.	○ At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames. ○ When the new frame arrives, the size of the window shrinks. ○ For example, the size of the window is w and if three frames are received then the number of spaces available in the window is (w-3). ○ Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

Example of Sliding Window



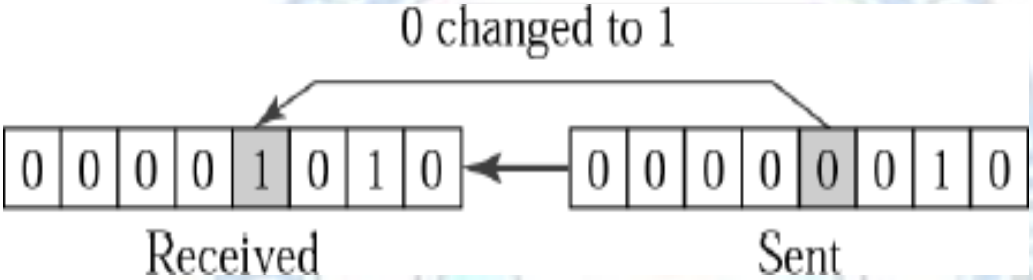
ERROR CONTROL

- Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.
- Error Control is a technique of error detection and retransmission.

TYPES OF ERRORS

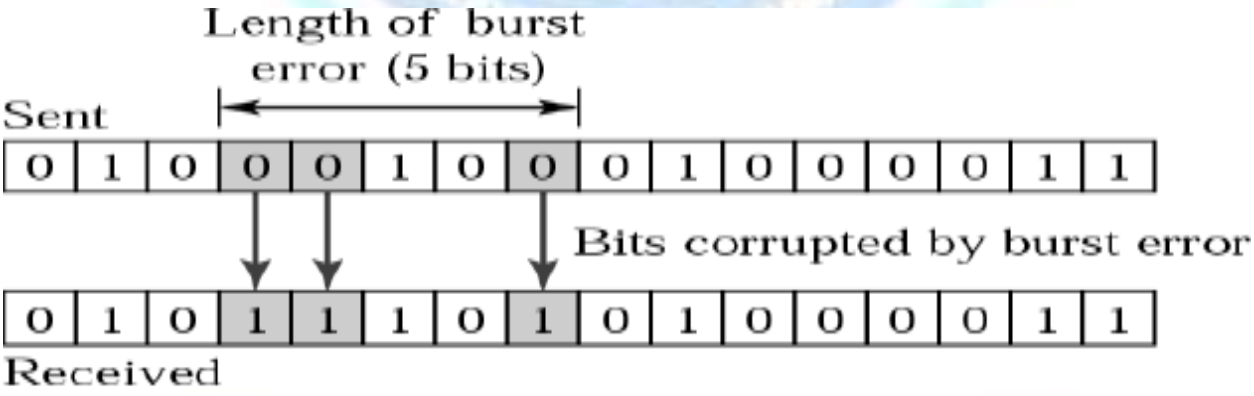
- ***Single-bit error***

The term Single-bit error means that only one bit of a given data unit (such as byte,character, data unit or packet) is changed from 1 to 0 or from 0 to 1



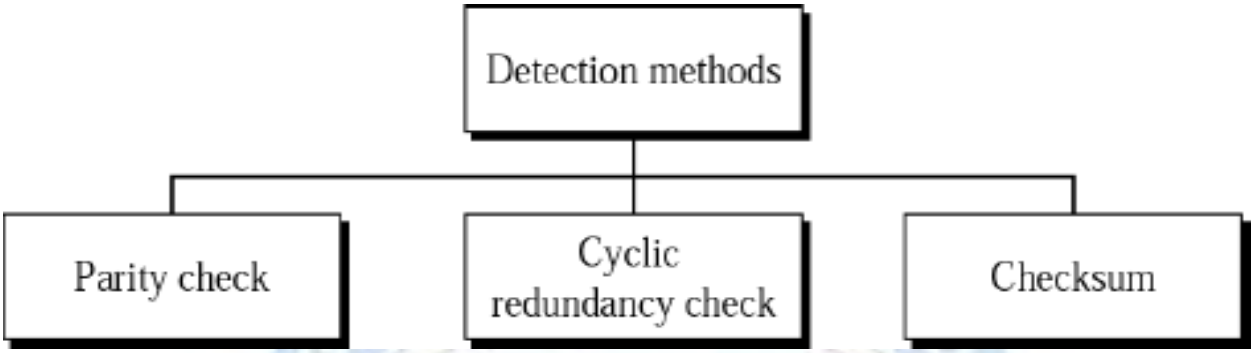
- ***Burst error***

The term Burst Error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1



ERROR DETECTION TECHNIQUES / METHODS

- The basic idea behind any error detection scheme is to add additional information to a frame that can be used to determine if errors have been introduced.



1. PARITY CHECK

One bit, called parity bit is added to every data unit so that the total number of 1's in the data unit becomes even (or) odd.

The source then transmits this data via a link, and bits are checked and verified at the destination.

Data is considered accurate if the number of bits (even or odd) matches the number transmitted from the source.

This techniques is the most common and least complex method.

1. *Even parity – Maintain even number of 1s*

E.g., 1011 → 1011 **1**

2. ***Odd parity – Maintain odd number of 1s***

E.g., 1011 → 1011 **0**

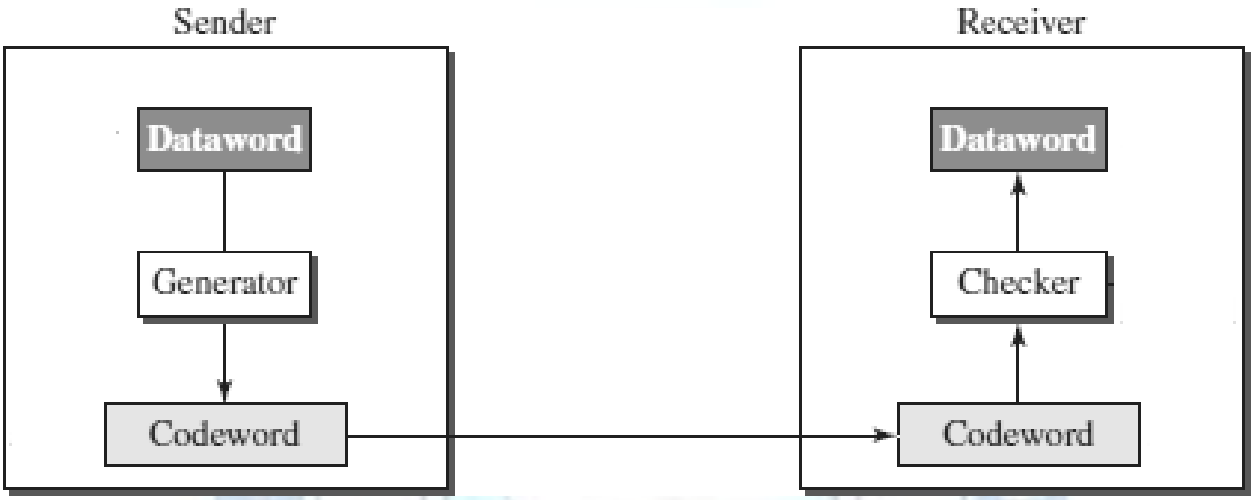
2. CYCLIC REDUNDANCY CHECK

- Cyclic codes refer to encoding messages by adding a fixed-length check value.
- CRCs are popular because they are simple to implement, easy to analyze mathematically and particularly good at detecting common errors caused in transmission channels.

Steps Involved:

- Consider the original message (data word) as M(x) consisting of 'k' bits and
- the divisor as C(x) consists of 'n+1' bits.
- The original message M(x) is appended by 'n' bits of zeros. Let us call
- this zero-extended message as T(x).

- Divide T(x) by C(x) and find the remainder.
- The division operation is performed using XOR operation.
- The resultant remainder is appended to the original message M(x) as CRC and sent by the sender(code word).



Example 1:

· Consider the Data word / Message M(x) = 1001

· Divisor C(x) = 1011 (n+1=4)

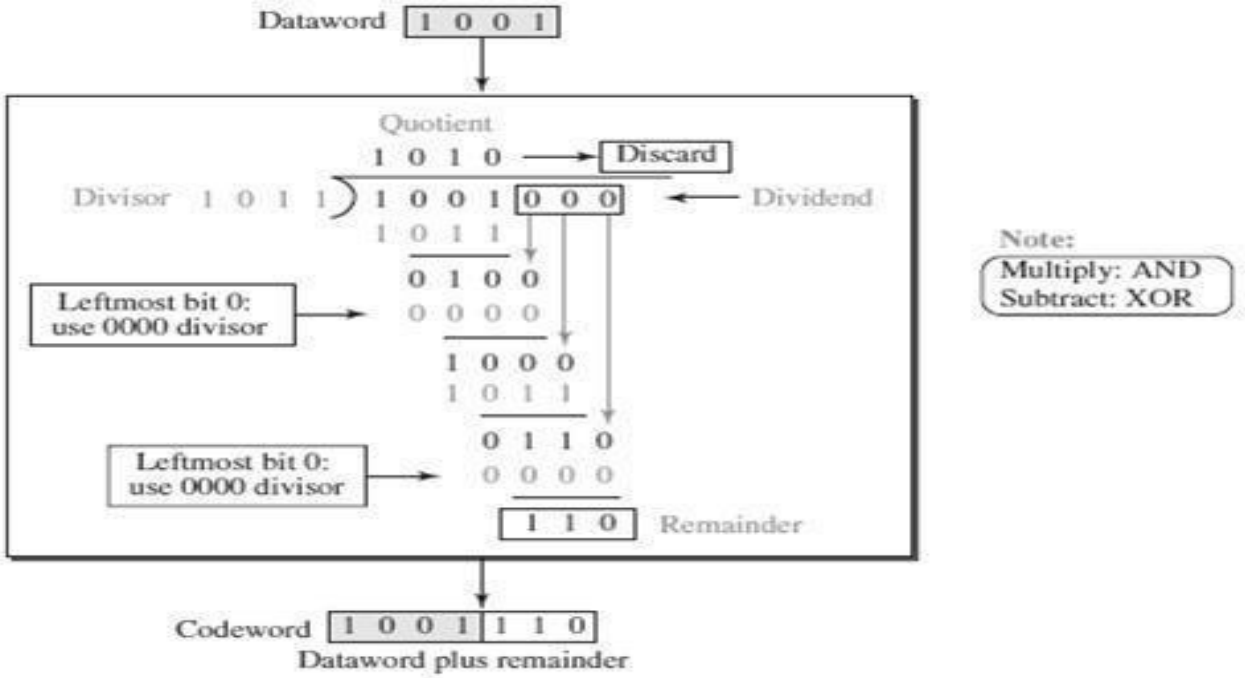
· Appending 'n' zeros to the original Message M(x).

· The resultant messages is called T(x) = 1001 **000. (here n=3)**

· Divide T(x) by the divisor C(x) using XOR operation.

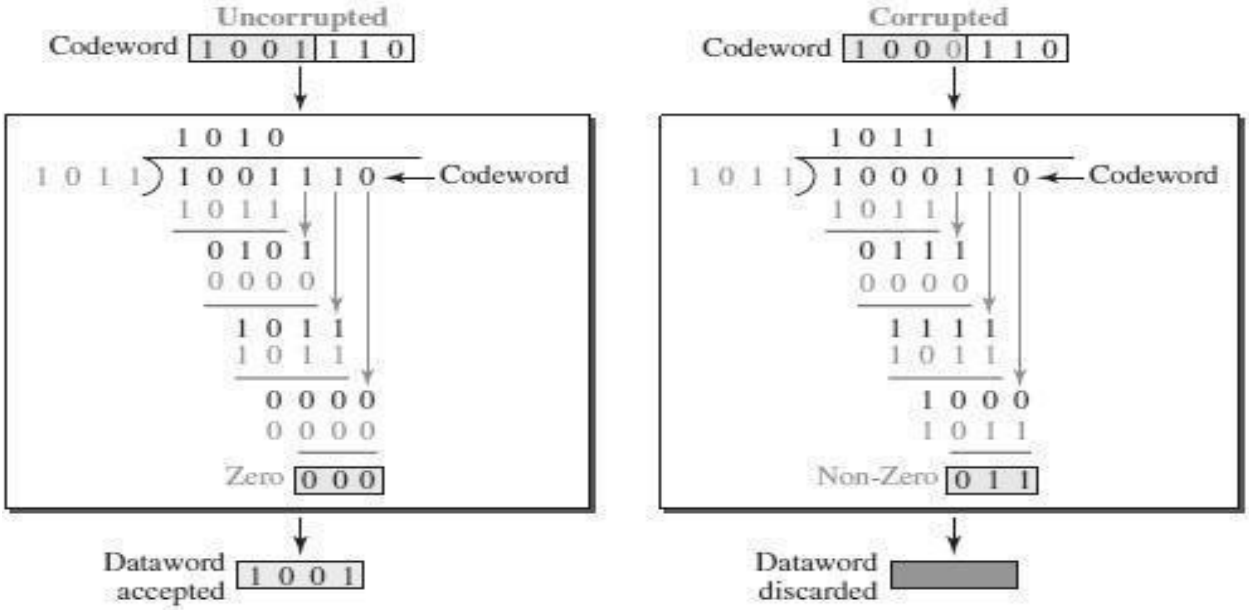
Input A	Input B	XOR Output
0	0	0
0	1	1
1	0	1
1	1	0

Sender Side:



ReceiverSide:

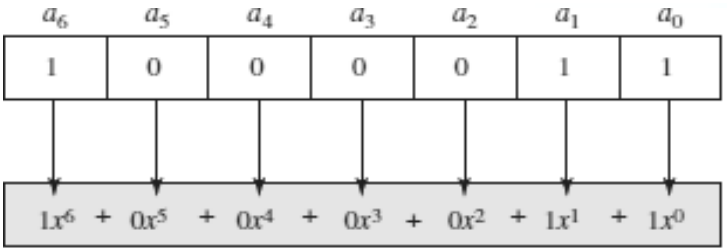
(For Both Case – Without Error and With Error)



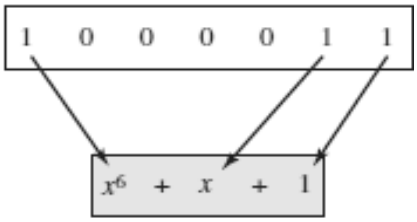
Polynomials

· 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 position of the bit; the coefficient shows the value of the bit.



a. Binary pattern and polynomial



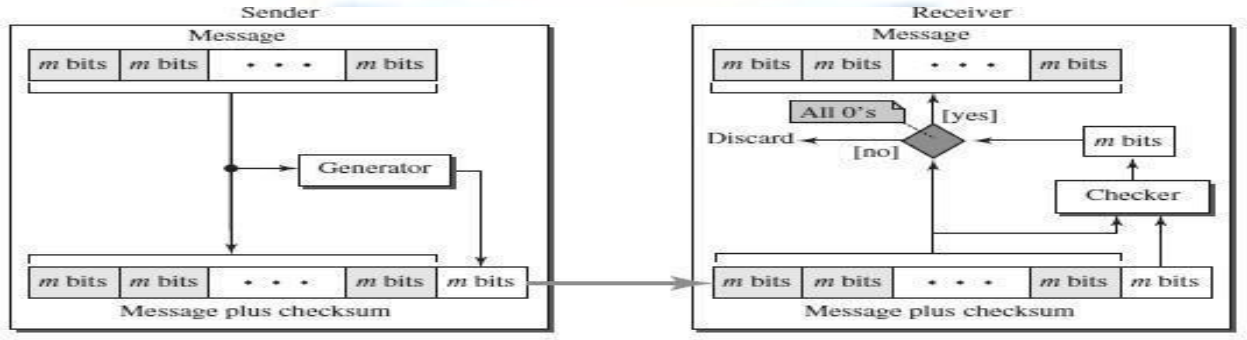
b. Short form

3. INTERNET CHECKSUM

· Checksum is a calculated value that is used to determine the integrity of data.

Procedure to calculate the traditional checksum

Sender	*Receiver*
1. The message is divided into 16-bit words. 2. The value of the checksum word is initially set to zero. 3. All words including the checksum are added using one's complement addition. 4. The sum is complemented and becomes the checksum. 5. The checksum is sent with the data.	1. The message and the checksum are received. 2. The message is divided into 16-bit words. 3. All words are added using one's complement addition. 4. The sum is complemented and becomes the new checksum. 5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.

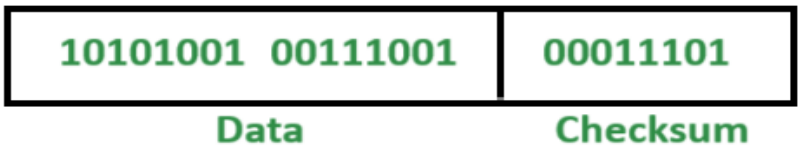


Example: If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

Sender Site:

```
10101001        subunit 1
00111001        subunit 2
11100010        sum (using 1s complement)
00011101        checksum (complement of sum)
```

Data transmitted to Receiver is:



Receiver Site:

```
10101001        subunit 1
00111001        subunit 2
00011101        checksum
11111111            sum
00000000     sum's complement
```

Result is zero, it means no error.

ERROR CONTROL

- Error control includes both error detection and error correction.
- Whenever an error is detected, specified frames are retransmitted
- It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender.

- Includes the following actions:

o **Error detection**

o Positive Acknowledgement (**ACK): if the frame arrived with no** errors

o Negative Acknowledgement (**NAK): if the frame arrived with errors**

o Retransmissions after **Timeout: Frame is retransmitted after certain** amount of time if no acknowledgement was received

- Error control in the data link layer is based on automatic repeat request(ARQ).

Categories of Error Control

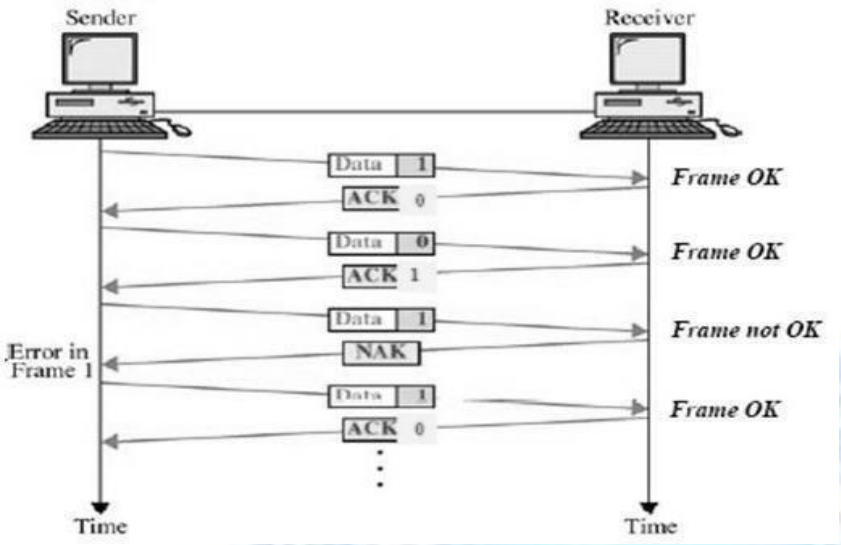
STOP-AND-WAIT ARQ

- Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.
  - This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame
- Two possibilities of the retransmission in Stop and Wait ARQ:

Damaged Frame:

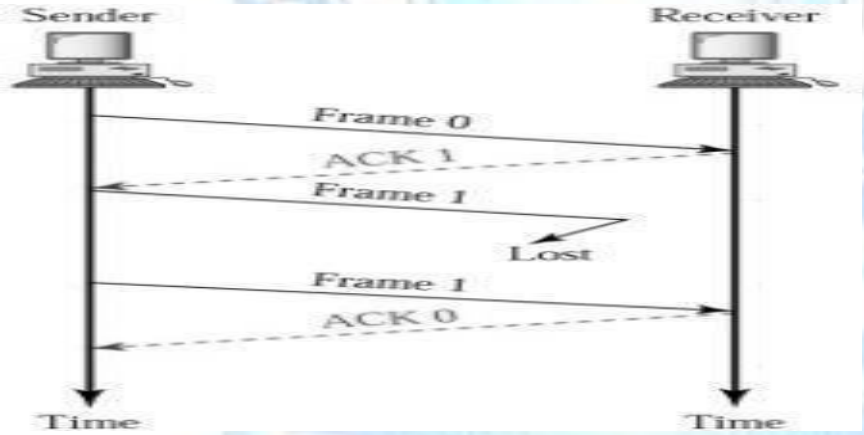
- When the receiver receives a damaged frame(i.e., the frame contains an error), then it returns the NAK frame.

For example, when the frame DATA 1 is sent, and then the receiver sends the ACK 0 frame means that the data 1 has arrived correctly. The sender transmits the next frame: DATA 0. It reaches undamaged, and the receiver returns ACK 1.The sender transmits the third frame: DATA 1. The receiver reports an error and returns the NAK frame. The sender retransmits the DATA 1 frame.



Lost Frame:

- Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it cannot be acknowledged either positively or negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

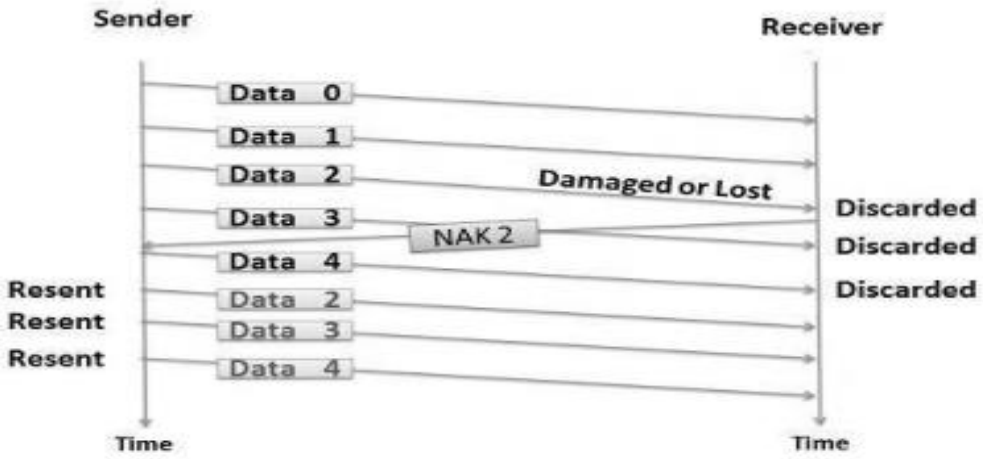


SLIDING WINDOW ARQ

- Sliding Window ARQ is a technique used for continuous transmission error control.
- Two protocols used in sliding window ARQ:

GO-BACK-N ARQ

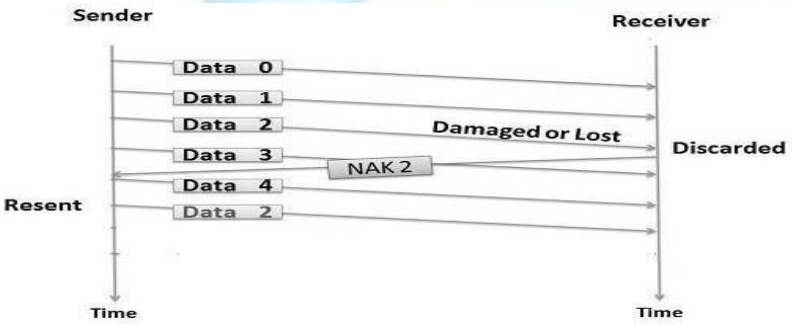
- In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.



- In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.
- The receiver discovers the error in Data 2 frame, so it returns the NAK 2 frame.
- All the frames including the damaged frame (Data 2,3,4) are discarded as it is transmitted after the damaged frame.
- Therefore, the sender retransmits the frames (Data2,3,4).

SELECTIVE-REJECT(REPEAT) ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



In the above figure, three frames (Data 0,1,2) have been transmitted before an error discovered in the third frame.

- The receiver discovers the error in Data 2 frame, so it returns the NAK 2 frame.
- The damaged frame only (Data 2) is discarded.
- The other subsequent frames (Data 3,4) are accepted.
- Therefore, the sender retransmits only the damaged frame (Data2).

Four protocols have been defined for the data-link layer controls.

They are

1. Simple Protocol

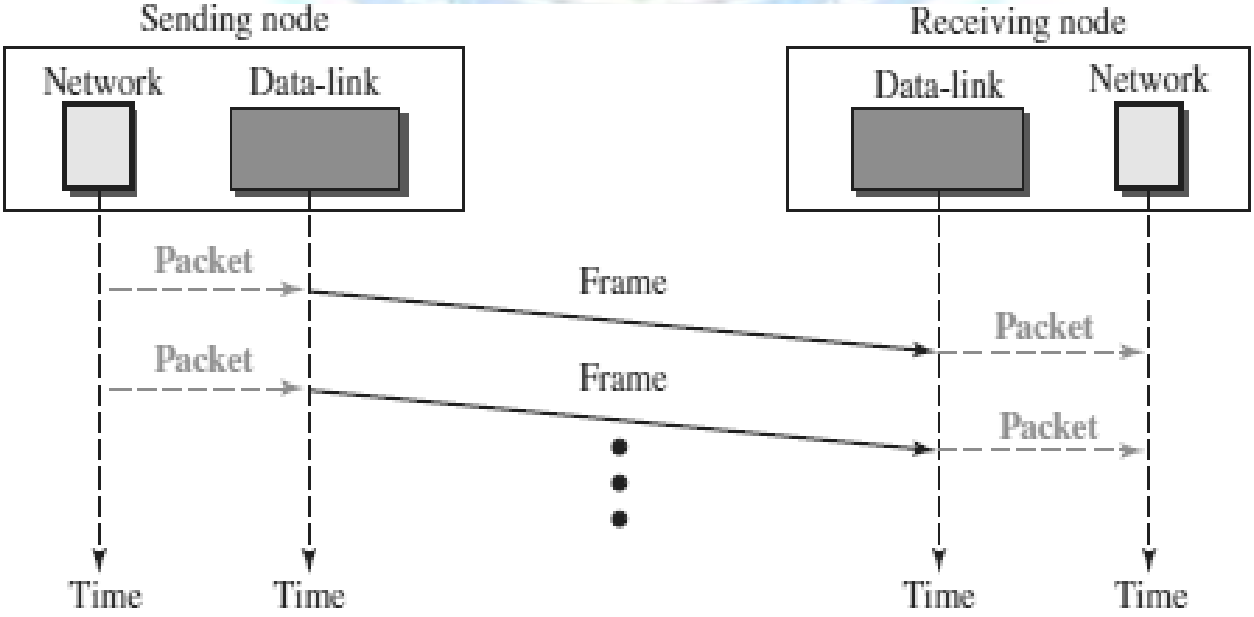
2. Stop-and-Wait Protocol

3. Go-Back-N Protocol

4. Selective-Repeat Protocol

1. SIMPLE PROTOCOL

- The first protocol is a simple protocol with neither flow nor error control.
- We assume that the receiver can immediately handle any frame it receives.
- In other words, the receiver can never be overwhelmed with incoming frames.
- The data-link layers of the sender and receiver provide transmission services for their network layers.



The data-link layer at the sender gets a packet from its network layer, makes a frame out of it, and sends the frame.

o The data-link layer at the receiver receives a frame from the link, extracts the packet from the frame, and delivers the packet to its network layer.

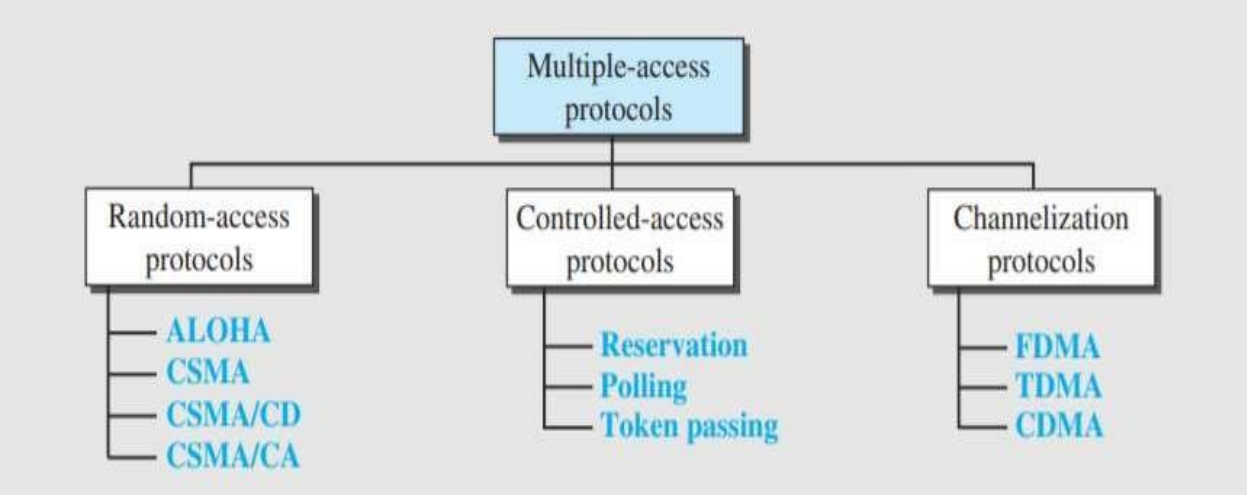
2. Stop-and-Wait Protocol (Refer Previous topic)

3. Go-Back-N Protocol (Refer Previous topic)

4. Selective-Repeat Protocol (Refer Previous topic)

4. MEDIA ACCESS CONTROL

Set of procedures to determine when a device or user is allowed to begin communication when the link is shared by more than two devices.



A) RANDOM-ACCESS OR CONTENTION METHODS

- ***No station is superior to another station*** and none is assigned control over another.
- First, there is ***no scheduled time*** for a station to transmit.
- Transmission is random among the stations.
- Second, ***no rules specify*** which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.
- If more than one station tries to send, there is an access conflict***/collision***—and the frames will be either destroyed or modified.
- To avoid access conflict or to resolve, ***each station follows a procedure*** that answers the following questions:

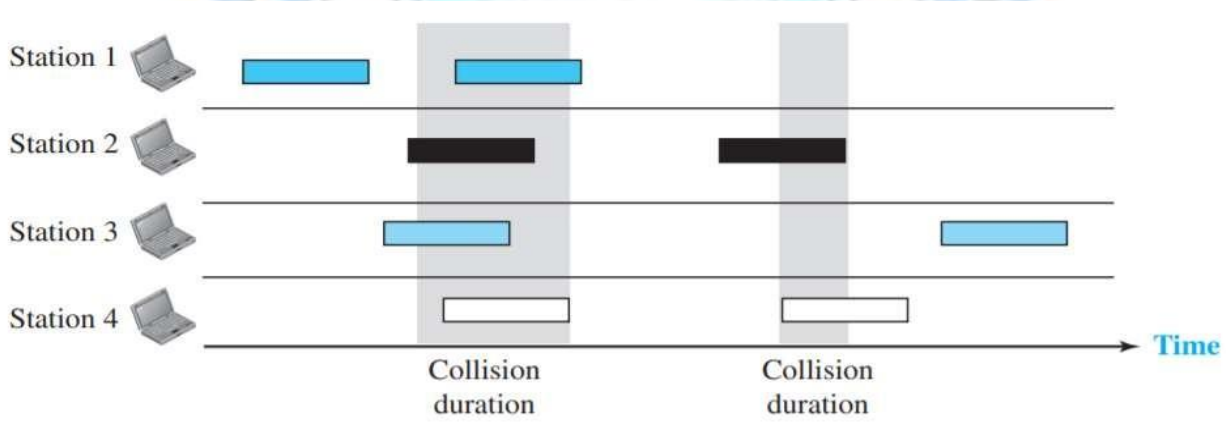
- When can the station access the medium?
- What can the station do if the medium is busy?
- How can the station determine the successor failure of the transmission?
- What can the station do if there is an access conflict?

ALOHA

- Earliest random access method, developed at the University of Hawaii in early 1970.
- Designed for a ***radio (wireless) LAN***, but it can be used on any shared medium.
- 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 the two stations collide and become garbled.

a) Pure ALOHA

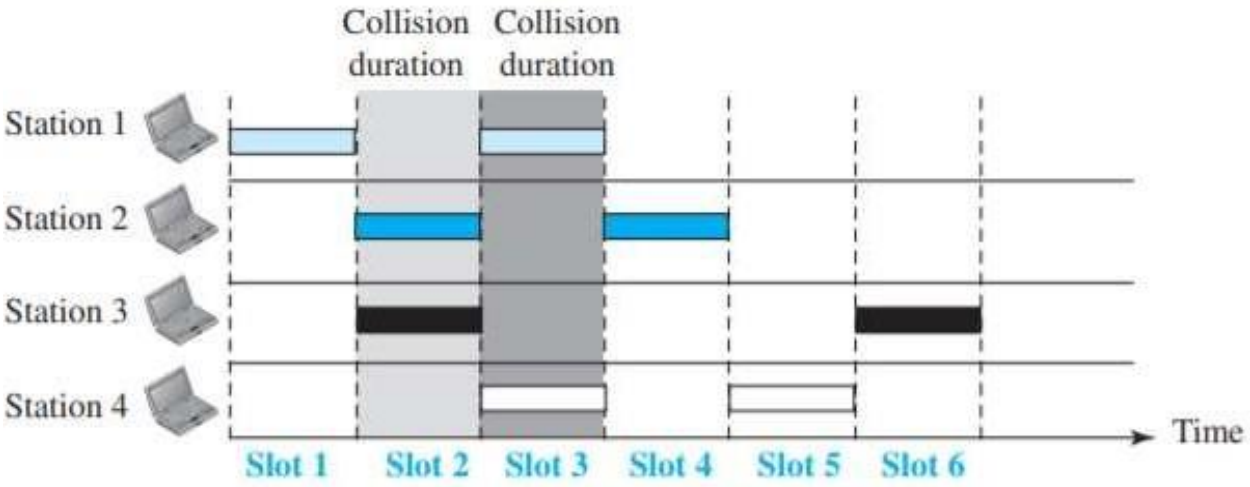
- The original ALOHA protocol is called pure ALOHA.
- Simple but elegant protocol.
- The idea is that each station sends a frame whenever it has a frame to send (***multiple access***).



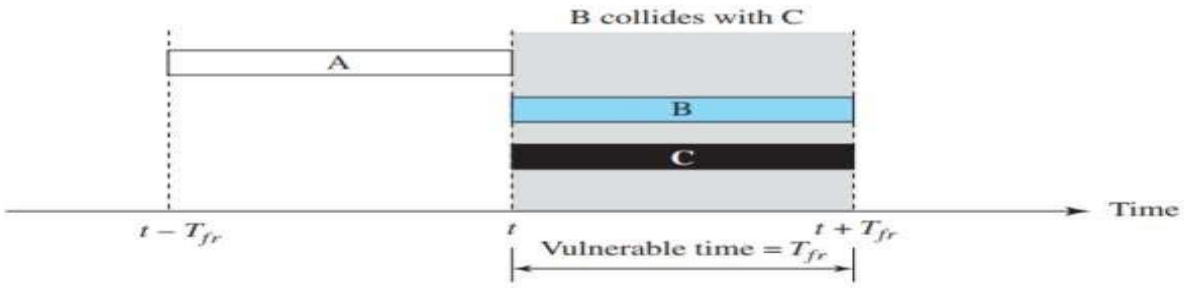
- Dictates that when the ***time-out period passes***, each station waits ***a random amount of time*** before resending its frame. The randomness will help avoid more collisions and the time is known as backoff time TB.
- After a maximum number of retransmission attempts Kmax, a station must give up and try later.

b) Slotted ALOHA

- Pure ALOHA has a vulnerable time of $2 \times T_{fr}$.
- Slotted ALOHA was invented to ***improve the efficiency of pure ALOHA.***
- The ***time is dividedinto slots*** of T_{fr} seconds and force the
- station to send only at the beginning of the time slot.



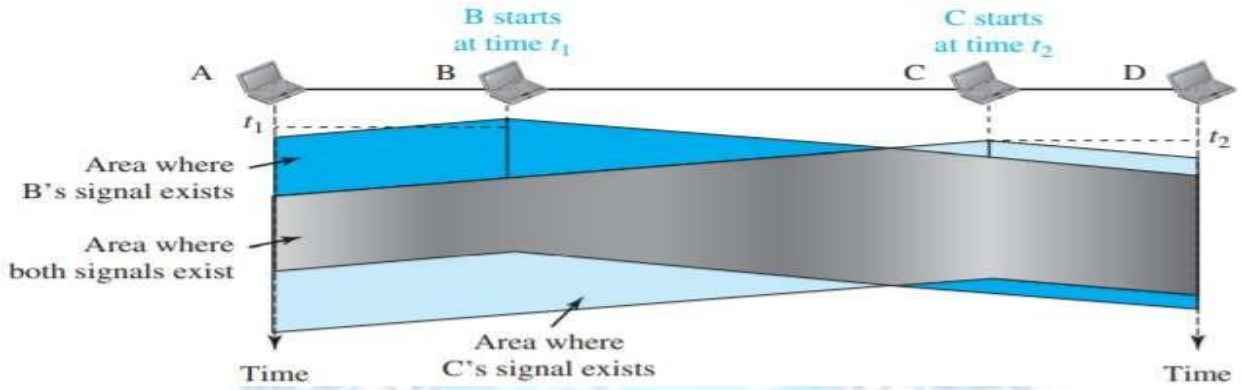
- A station is allowed to ***send only at the beginning of the synchronized time slot***.
- If a station misses this moment, it must wait until the beginning of the next time slot.
- The station which started at the beginning of this slot has already finished sending its frame.
- Still the ***possibility of collision*** if two stations try to send at the beginning of the same time slot.



c) Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision and to increase the performance.
- The chance of collision can be reduced, if a ***station senses the medium*** before trying to use it.

- Requires that each station first listen to the medium (or check the state of the medium) before sending.
- If the ***media is idle***, the station is allowed to transmit or use it. Otherwise, the station has to wait until the station becomes idle.



CSMA-Persistence Methods

- What should a station do if the channel is busy?
- What should a station do if the channel is idle?
- **Three methods**
  - 1-persistent method
  - Non persistent method
  - P-persistent method

1-Persistent

- Is simple and straightforward.
- After the station finds the line idle, it sends its frame immediately (with ***probability 1***).
- Has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

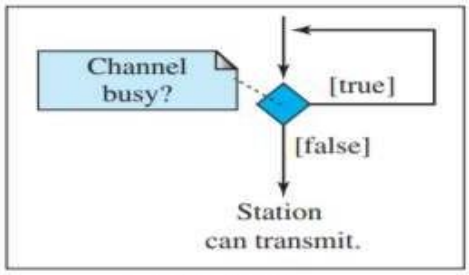
Non persistent

- 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.
- Reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- Reduces the efficiency of the network because the medium remains idle, when there may be stations with frames to send.

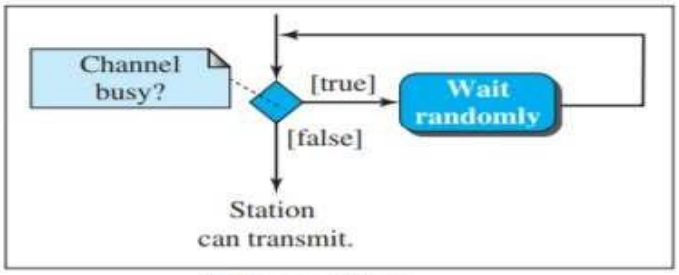
P-Persistent

- Is used, if the channel has ***time slots with a slot*** duration equal to or greater than the maximum propagation time.

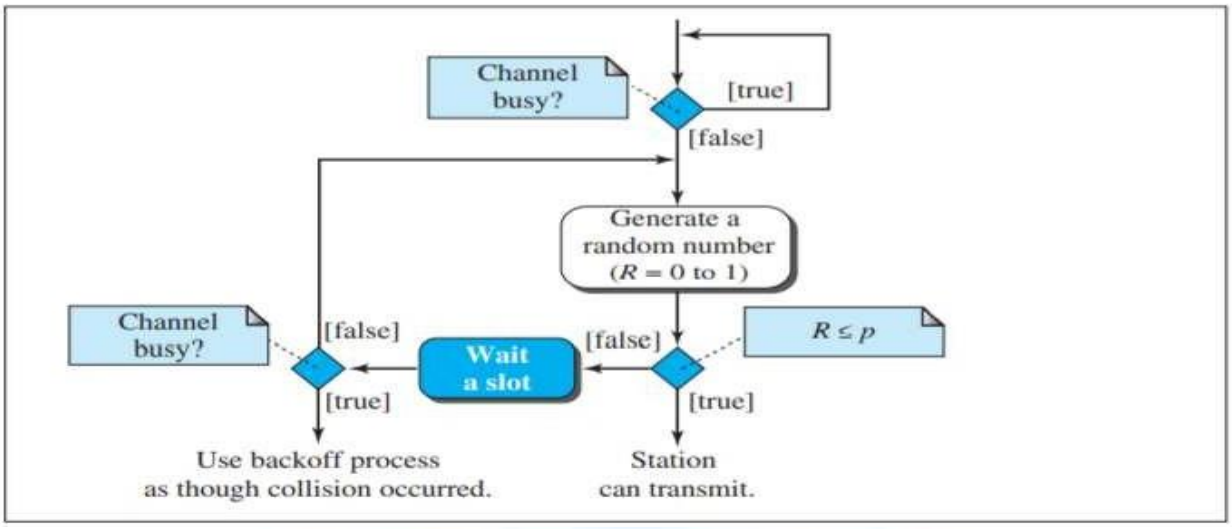
- Combines the advantages of the other two strategies.
- Reduces the chance of collision and improves efficiency.
- After the station finds the line idle, it follows t2.
- With probability q=1−p, the station waits for the beginning of the next time slot and checks the line again.
- If the line is idle, it goes to step 1.
- If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.



a. 1-Persistent

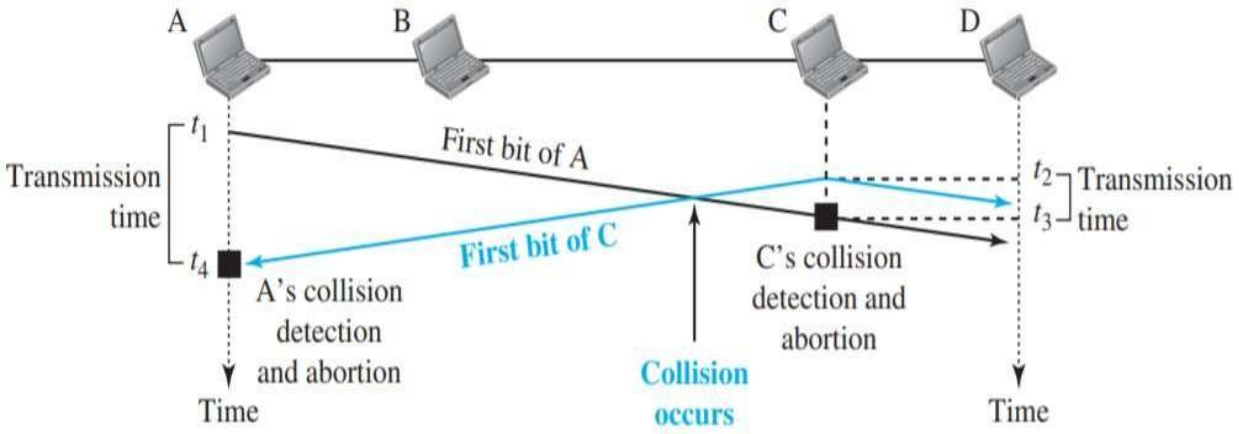


b. Nonpersistent

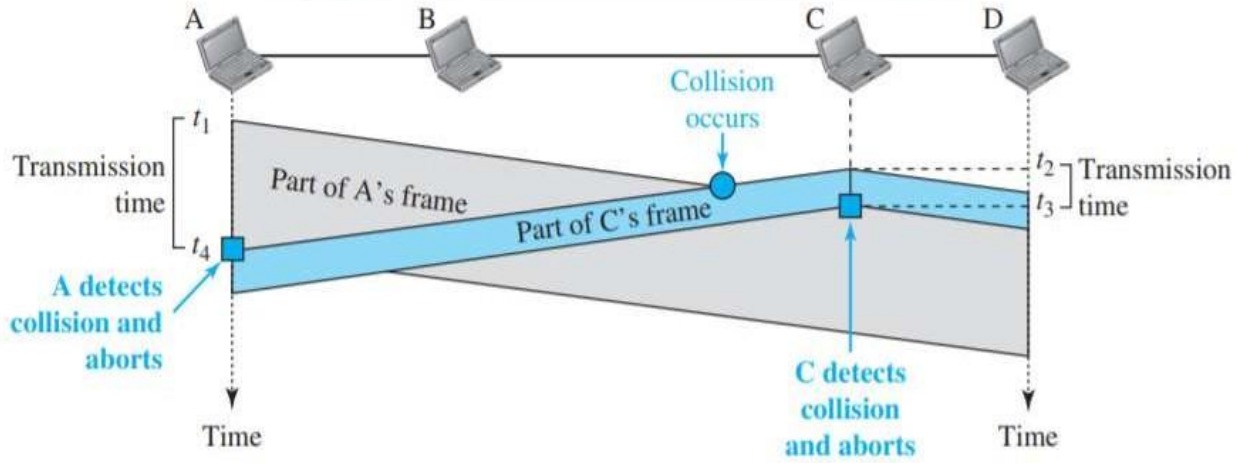


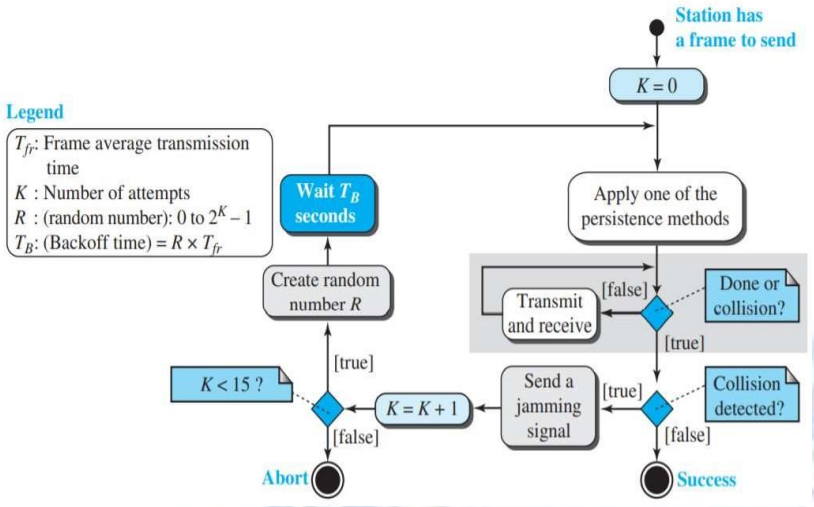
d) ***Carrier Sense Multiple Access With Collision Detection (CSMA/CD)***

- ***Augments the algorithm*** to handle the collision.
- 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 resent.



- At time t1, station A has executed its persistence procedure and starts sending the bits of its frame.
- At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time t2.
- Station C detects a collision at time t3, when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission.
- Station A detects collision at time t4, when it receives the first bit of C's frame; it also immediately aborts transmission.
- In the figure, we see that A transmits for the duration t4 − t1; C transmits for the duration t3 − t2.
- Augments the algorithm to handle the collision.
- 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 resent.



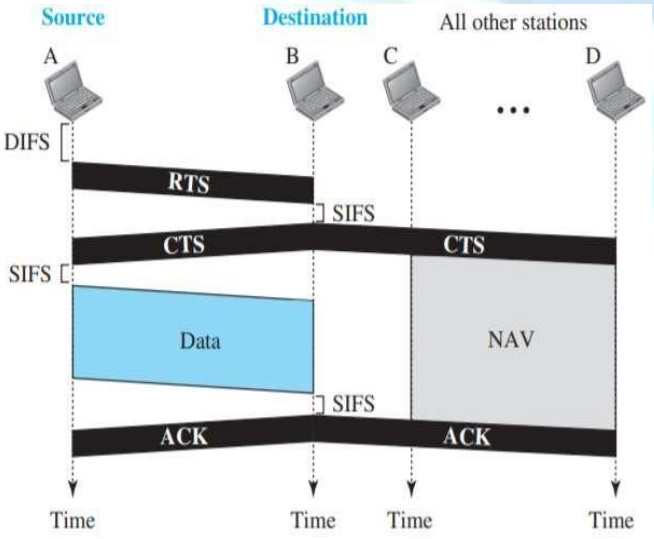


e) ***Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)***

- Invented for ***wireless networks.***
- Collisions are avoided through the use of CSMA/CA's **three strategies**:
  - **the inter frame space**
  - **the contention window**
  - **and acknowledgments**

Key Terms

- Short Inter Frame Space (SIFS)
- DCF Inter Frame Space (DIFS)
- Request To Send (RTS)
- Clear To Send (CTS)

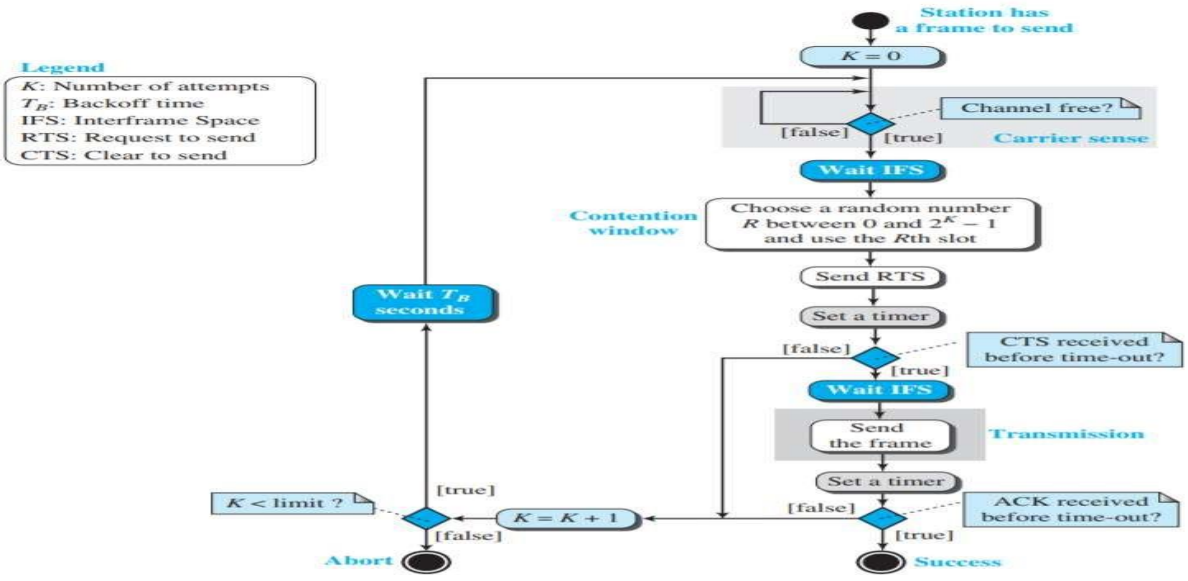


CSMA/CA -Frame Exchange Time Line

- Before sending a frame, ***the source station senses the medium*** by checking the
- energy level at the carrier frequency.
- The channel uses ***a persistence strategy*** with backoff until the channel is idle.
- After the station is found to be idle, the station waits for a period of time called the ***DCF interframe space (DIFS);*** then the station sends a control frame called the request ***to send (RTS).***
- After receiving the RTS and waiting a period of time, ***short interframe space (SIFS),*** the destination station sends a control frame, called ***the clear to send (CTS),*** to the source station. This control frame indicates that the destination station is ready to receive data.
- The source station sends data after waiting an amount of time equal to SIFS.
- The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. ***Acknowledgment is needed in this protocol*** because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived. station is ready to receive data.

CSMA/CA-Network Allocation Vector (NAV)

- How is the collision avoidance aspect of this protocol accomplished?
- The key is a feature called **NAV.**
- When a station sends an RTS frame, it includes the duration ***of time*** that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a NAV that shows how much time must pass before these stations are allowed to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

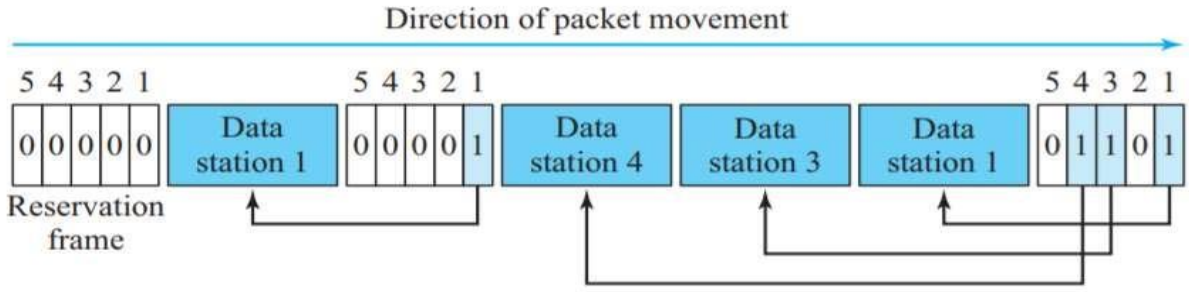


B) CONTROLLED ACCESS

- 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.
- Controlled-access methods:
  - **Reservation**
  - **Polling**
  - **Token Passing**

a) Reservation:

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

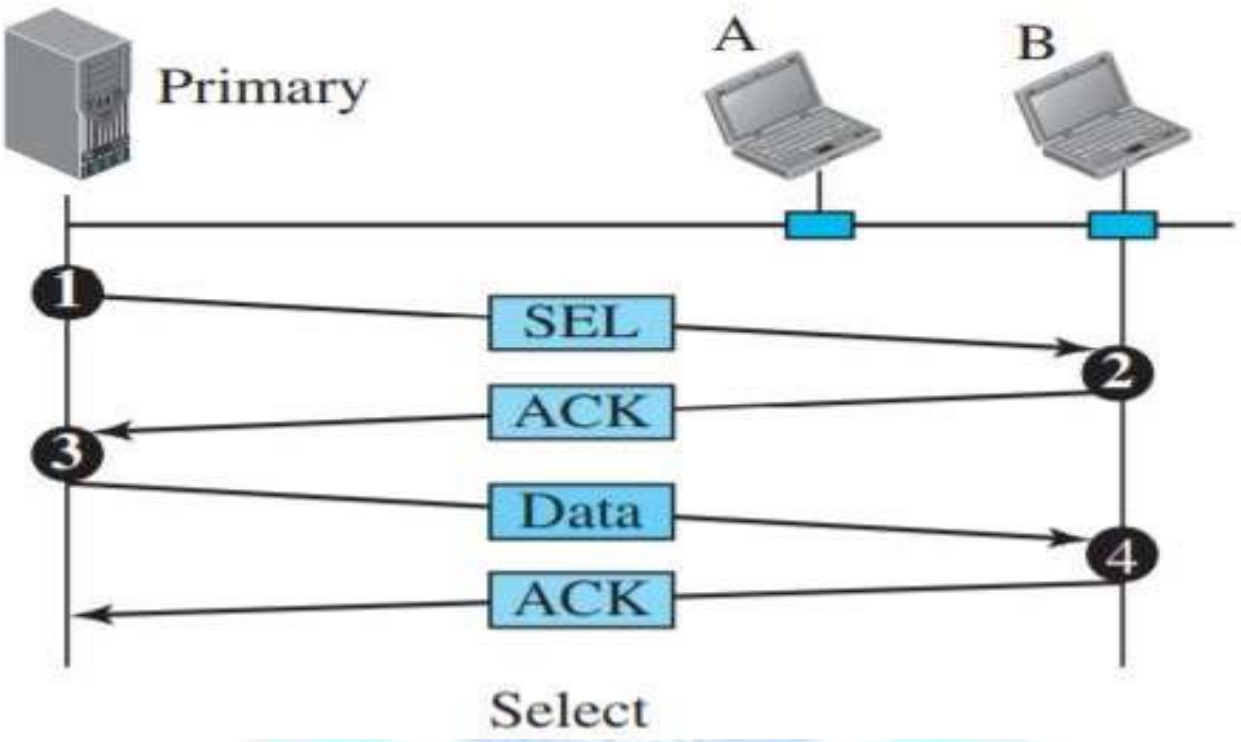


b) Polling

- ***Works with topologies*** in which one device is designated as a **primary station** and the other devices are **secondary stations.**
- All **data exchanges** must be made through the **primary device** even when the ultimate destination is a secondary device.
- The ***primary device controls the link***; the secondary devices follow its instructions.
- Primary device determine which device is allowed to use the channel at a given time.
- The primary device, is always the initiator of a session.
- This method uses poll and select functions to prevent collisions
- Major drawback is if the primary station fails, the system goes down.

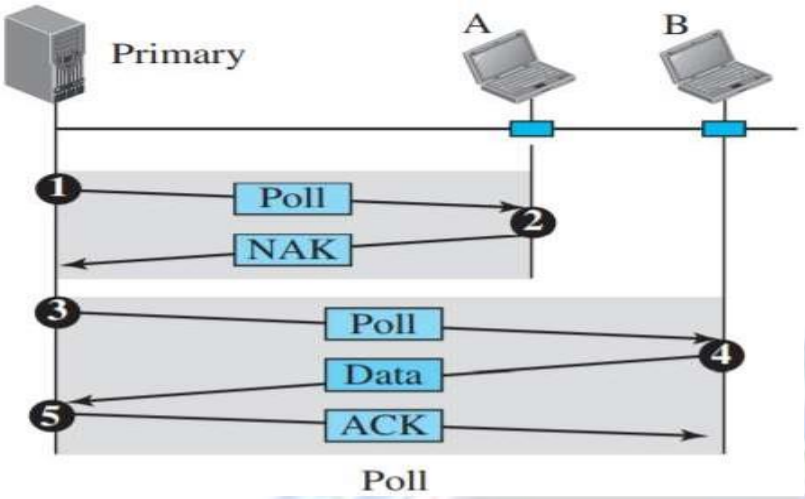
1. ***Polling - Select***

- Is used whenever the primary device has something to send.
- Primary controls the link.
- If the primary is neither sending nor receiving data, it knows the link is available. If it has something to send, the primary device sends it.
- The primary must alert the secondary to the upcoming transmission and wait for an acknowledgment 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.



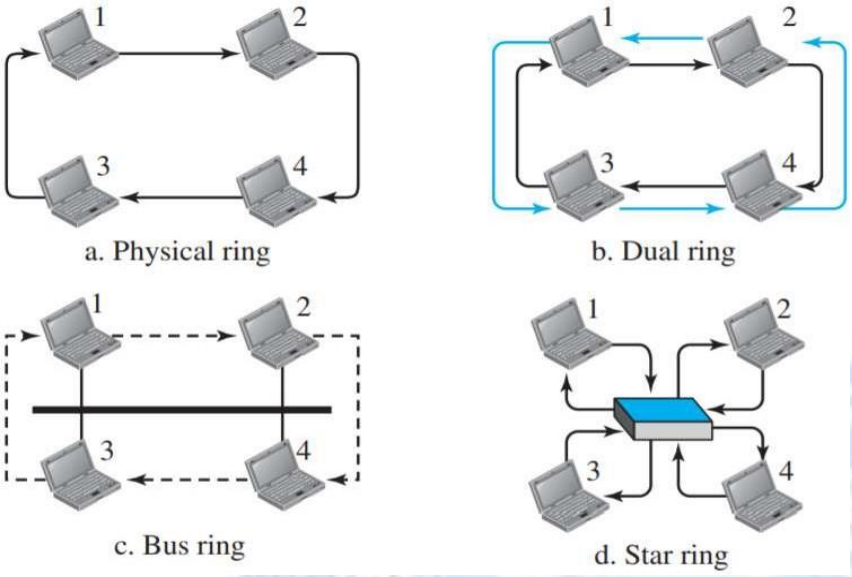
2. ***Polling - Poll***

- Is used by the primary device to solicit transmissions from the secondary devices.
- When the primary is ready to receive data, it must ask (poll) each device in turn if it has anything to send.
- When the first secondary is approached, it responds either with a **NAK frame**, if it has nothing to send or with data (in the form of a data frame) if it does.
- If the response is negative (a NAK frame), then the primary polls the next secondary in the same manner until it finds one with data to send.
- When the response is positive (a data frame), the primary reads the frame and returns an acknowledgment (ACK frame), verifying its receipt.



c) Token Passing

- The stations in a network are organized in a logical ring (each station,there is a predecessor and a 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.
- A special packet called a **token** circulates through the ring.
- The possession of the token gives the station the right to access the channel and send its data.
- When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data.
- When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.
- When a station receives the token and has no data to send, it just passes the data to the next station.
- Token management is needed for this access method. Stations must be limited in the time they can have possession of the token.
- The token must be monitored to ensure it has not been lost or destroyed.
- Token management is needed to make low-priority stations release the token to high-priority stations.



Ring topology

- When a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line.
- This means that the token does not have to have the address of the next successor.
- If one of the link(i.e the medium between two adjacent station)fails, the whole system fails.

Dual ring topology

- The uses a second(auxiliary) ring which operates inthe reverse direction compared with the main ring.
- The second ring is for emergencies only.
- If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring.
- After the failed link is restored, the auxiliary ring becomes idle again.
- Note that for this topology to work, each station needs to have two transmitter ports and two receiver ports.
- The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.

Bus ring topology (Token bus)

- The stations are connected to a single cable called a bus. They make a logical ring, as each station knows the address of its successor.
- When a station has finished sending its data, it releases the token and inserts the address of its successor in the token.
- Only the station with the address matching the destination address of the token gets the token to access the shared media.
- Eg.The Token Bus LAN, standardized by IEEE.

Star ring topology

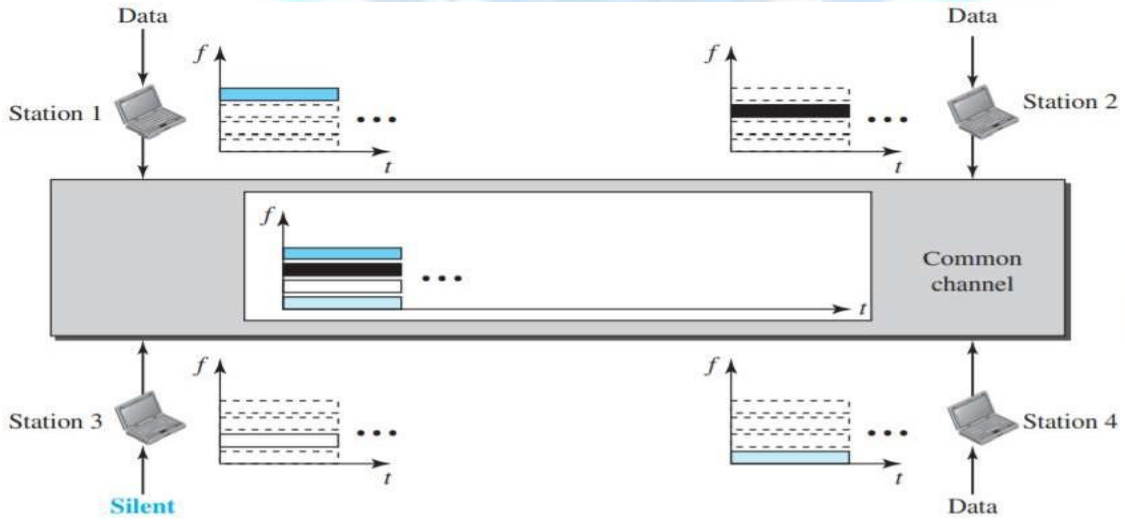
- The physical topology is a star. Hub acts as the connector.
- The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections.
- Makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate.
- Adding and removing stations from the ring is easier.
- Eg. Token Ring LAN designed by IBM.

C) CHANNELIZATION

- Is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.
- Three channelization protocols:
  - **FDMA**
  - **TDMA**
  - **CDMA.**

a) Frequency-Division Multiple Access (FDMA)

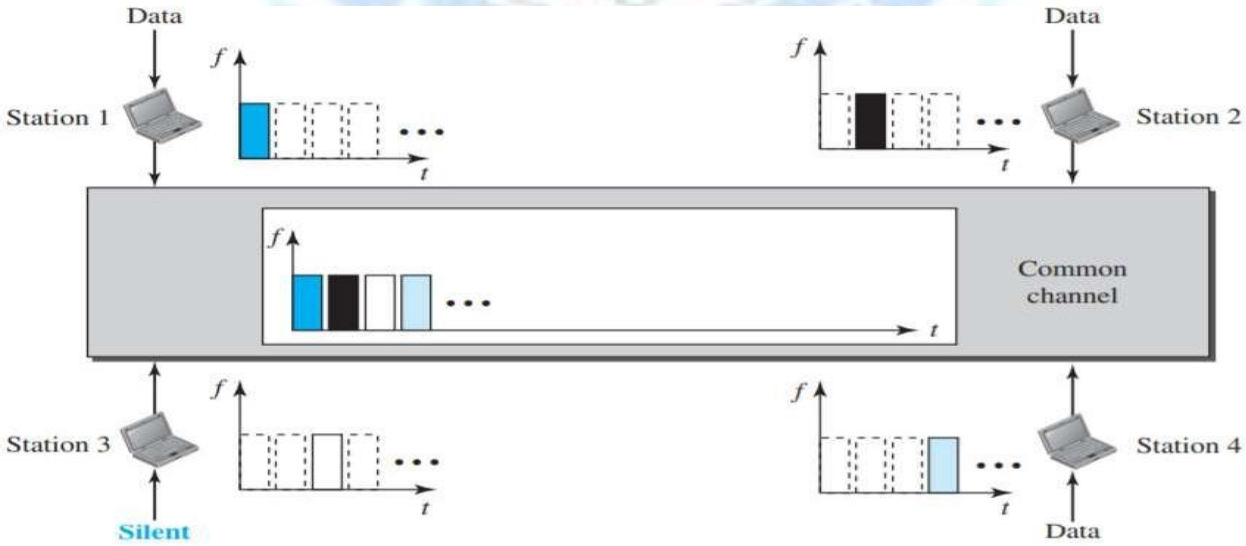
- The available bandwidth is divided into frequency bands.
- Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time.
- Each station also uses a band pass filter to confine the transmitter frequencies.
- To prevent station interferences, the allocated bands are separated from one another by small guard bands.



- Specifies a predetermined frequency band for the entire period of communication.
- Stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA.
- The multiplexer modulates the signals, combines them, and creates a band pass signal.
- The data link layer in each station tells its physical layer to make a band pass signal from the data passed to it.
- The signal must be created in the allocated band.
- The signals created at each station are automatically band pass-filtered. They are mixed when they are sent to the common channel.

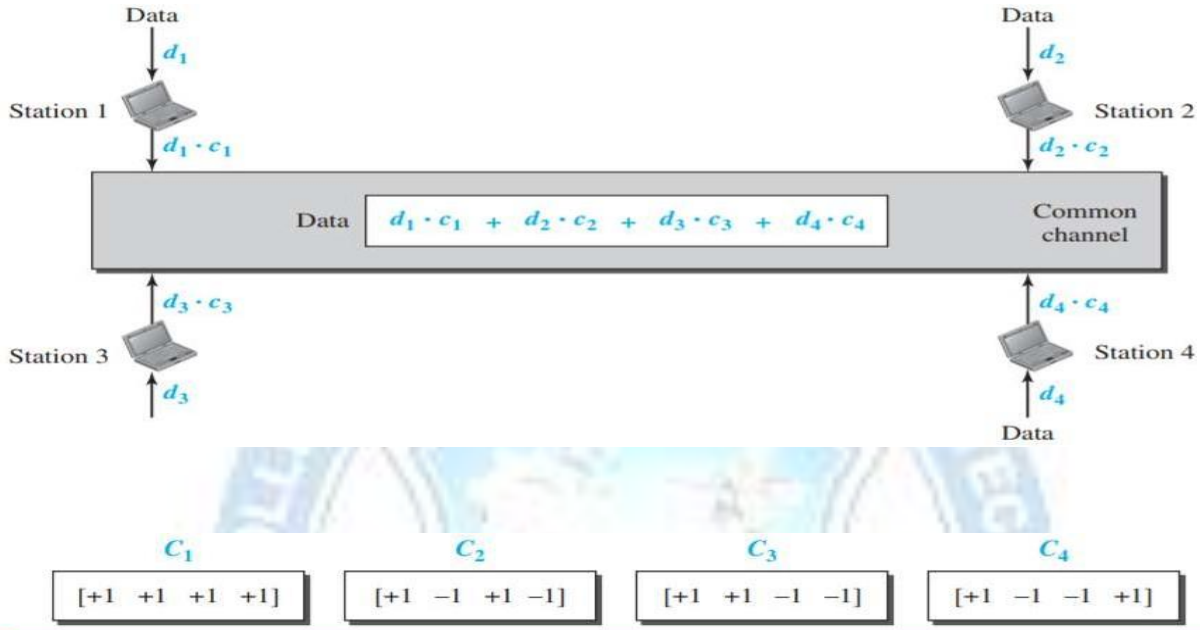
b) Time-Division Multiple Access (TDMA)

- The bandwidth is just one channel that is timeshared between different stations.
- Stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data.
- Each station transmits its data in its assigned time slot.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Synchronization is normally accomplished by having some synchronization bits (normally referred to as preamble bits) at the beginning of each slot.
- Each station needs to know the beginning of its slot and the location of its slot.
- To compensate for the propagation delays, guard times are inserted.



c) Code-Division Multiple Access (CDMA)

- One channel carries all transmissions simultaneously.



1. Each sequence is made of N elements, where N is the number of stations.
2. If we multiply a sequence by a number, every element in the sequence is multiplied by that element. This is called multiplication of a sequence by a scalar. For example,

$$2 \cdot [+1\ +1\ -1\ -1] = [+2\ +2\ -2\ -2]$$

3. If we multiply two equal sequences, element by element, and add the results, we get N, where N is the number of elements in each sequence. This is called the ***inner product*** of two equal sequences. For example,

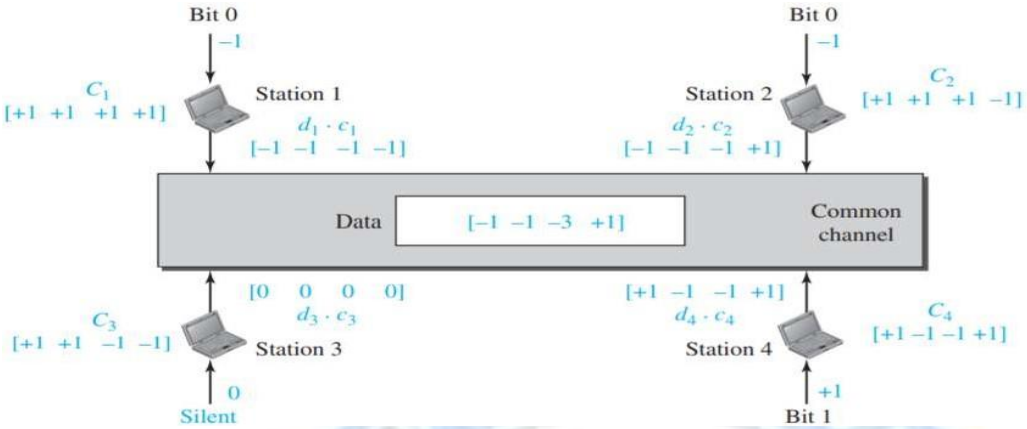
$$[+1\ +1\ -1\ -1] \cdot [+1\ +1\ -1\ -1] = 1 + 1 + 1 + 1 = 4$$

4. If we multiply two different sequences, element by element, and add the results, we get 0. This is called the *inner product* of two different sequences. For example,

$$[+1\ +1\ -1\ -1] \cdot [+1\ +1\ +1\ +1] = 1 + 1 - 1 - 1 = 0$$

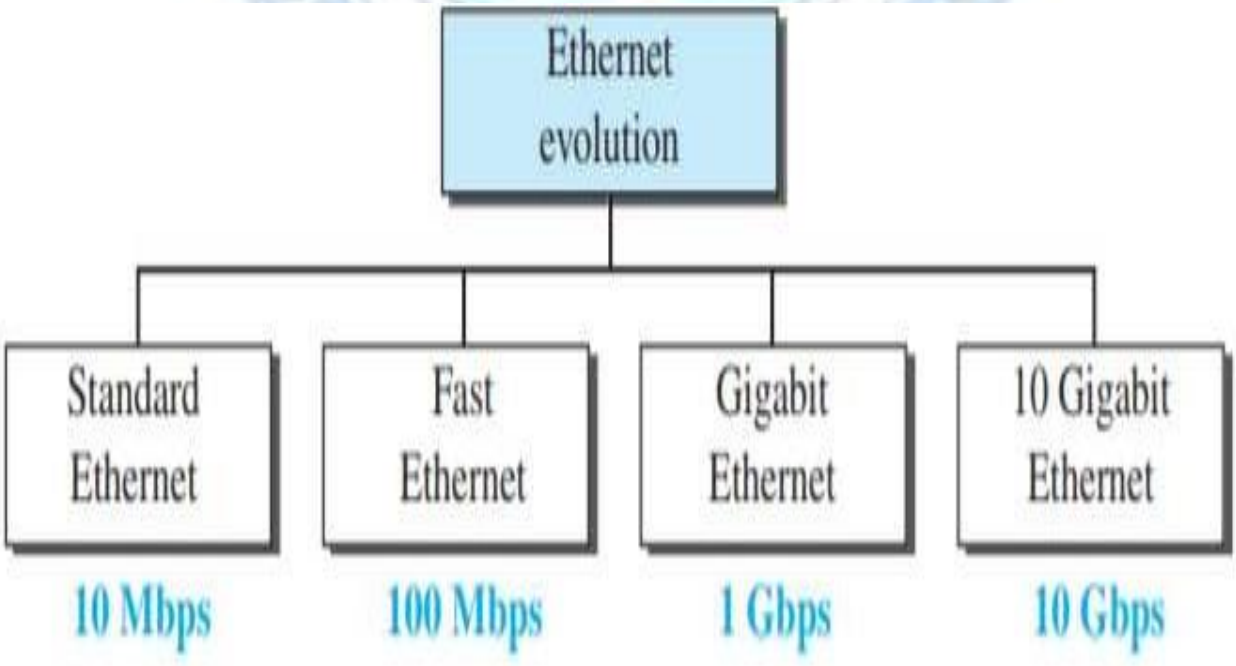
5. Adding two sequences means adding the corresponding elements. The result is another sequence. For example,

$$[+1\ +1\ -1\ -1] + [+1\ +1\ +1\ +1] = [+2\ +2\ 0\ 0]$$



5.WIRED LANS-ETHERNET STANDARDS

- Ethernet Evolution
  - The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.



A) Standard Ethernet

CHARACTERISTICS

i) Connectionless and Unreliable Service

Connectionless Service

- Provides a connectionless service, which means each frame sent is independent of the previous or next frame.
- If a frame drops, the sender will not know about it.
- In the transport layer if UDP is used, the frame is lost and
- salvation may only come from the application layer.
- In the transport layer if TCP is used, the sender TCP does not
- receive acknowledgment for its segment and sends it again.

Unreliable Service

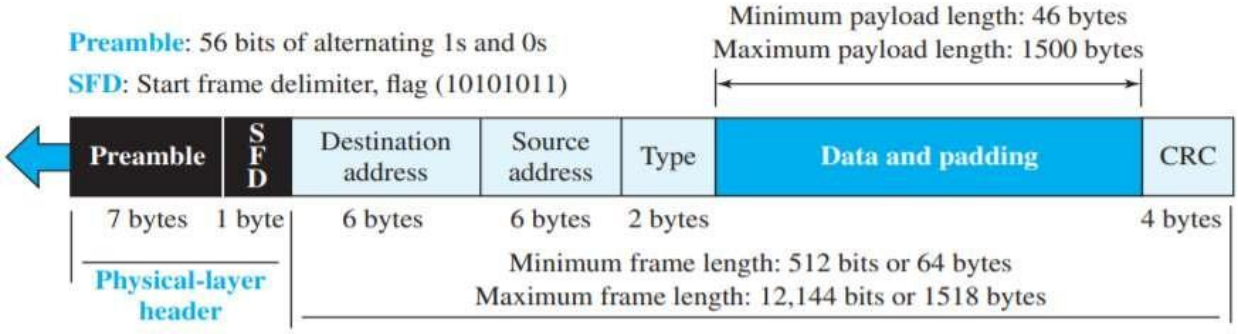
Ethernet is also unreliable like IP and UDP.

If a frame is corrupted during transmission using CRC-32,

the receiver drops the frame silently.

It is the duty of high-level protocols to find out about it.

FRAME FORMAT



Fields:

Preamble.– Contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization.

Start Frame Delimiter (SFD).– Is (1 byte: 10101011) and signals the beginning of the frame.

Destination Address (DA)– Is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet.

Source Address (SA)– Is also six bytes and contains the link-layer address of the sender of the packet.

Type.–Defines the upper-layer protocol (IP, ARP, OSPF, and so on) whose packet is encapsulated in the frame.

Data.– Carries data encapsulated from the upper-layer protocols. It is a minimum of 46 bytes and a maximum of 1500 bytes.

CRC.– The last field contains error detection information, in this case a CRC-32.

ADDRESSING

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own ***Network Interface Card (NIC).***
- The NIC fits inside the station and provides the station with a link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

ACCESS METHOD

- Is a broadcast network and uses the standard Ethernet protocol?
- Uses CSMA/CD with 1-persistent method.

EFFICIENCY OF STANDARD ETHERNET

Is defined as the ratio of the time used by a station to send data to the time the medium is occupied by this station.

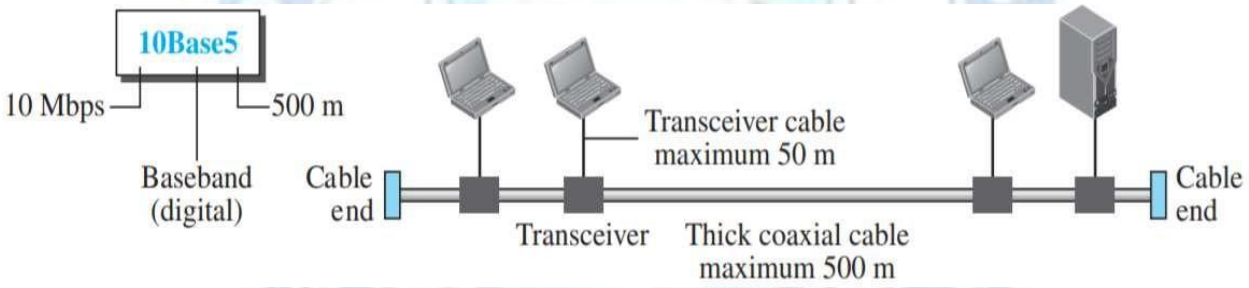
IMPLEMENTATION

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

a) 10Base5: Thick Ethernet

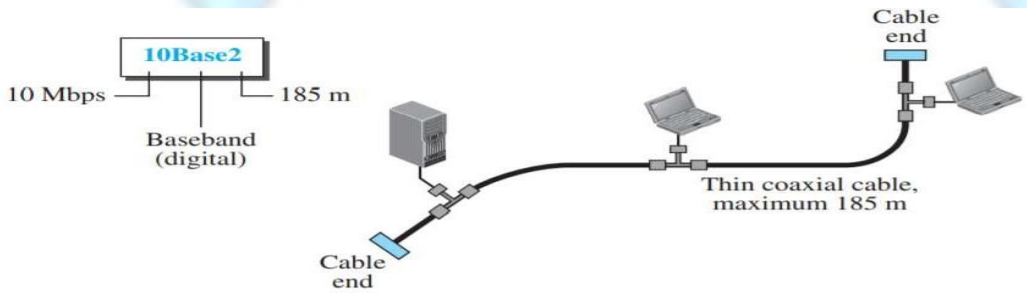
- Size of the cable, which is roughly the size of a garden hose and too stiff to bend with your hands.
- The first Ethernet specification to use a ***bus topology*** with an external ***transceiver (transmitter/receiver)*** connected via a tap to a thick coaxial cable.
- The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that ***collision can only happen in the coaxial cable.***
- The **maximum length** of the coaxial cable must not exceed **500 o**therwise, there is excessive degradation of the signal.
- If a length of more than 500 m is needed, up to five segments, each a maximum of 500 meters, can be connected using repeaters.

10Base5: Thick Ethernet



b) 10Base2 : thin Ethernet or Cheaper net

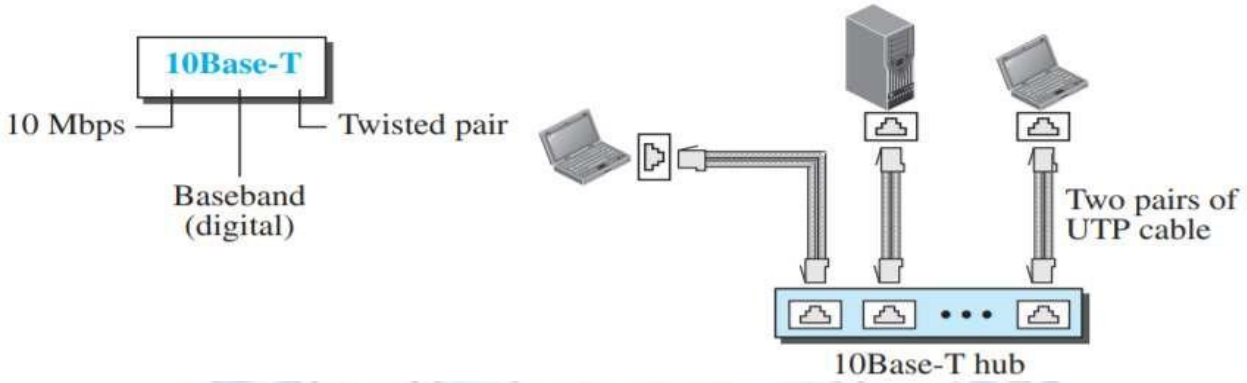
- Uses a bus topology, but the cable is much thinner and more flexible.
- The cable can be bent to pass very close to the stations.
- The **transceiver** is normally ***part of the network interface card (NIC),*** which is installed inside the station.
- Is less expensive than thick coaxial and the 'T' connections are much cheaper than taps.
- Installation is simpler because the thin coaxial cable is very flexible.
- The **length** of each segment ***cannot exceed 185 m (close to 200 m)*** due to the high level of attenuation in thin coaxial cable.



c) 10Base-T: Twisted-Pair Ethernet

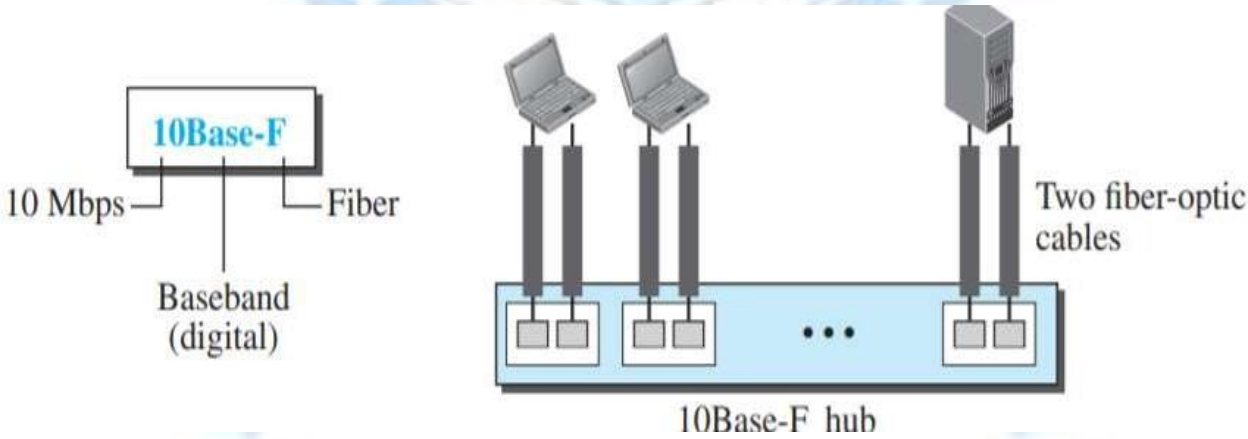
Uses a physical ***star topology***.

- Two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub.
- Any collision here happens in the hub. Hub actually replaces the coaxial cable as far as a collision is concerned.
- The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.



d) 10Base-F: Fiber Ethernet

- Most common is called 10Base-F.
- Uses a star topology to connect stations to a hub.
- The stations are connected to the hub using two fiber- optic cables.



B) Fast Ethernet (100 Mbps)

- New generation increasing the transmission rate to 100 Mbps.
- The designers of the Fast Ethernet needed to make it compatible with the Standard Ethernet.

- The MAC sub layer was left unchanged.(same frame format and the maximum and minimum size).
- Need to reconsider on the **transmission rate, access method, and implementation.**

Goals of Fast Ethernet

- Upgrade the data rate to 100 Mbps.
- Make it compatible with Standard Ethernet.
- Keep the same 48-bit address.
- Keep the same frame format.

A) ACCESS METHOD

- Operation of the CSMA/CD depends on the transmission rate, the minimum size of the frame, and the maximum network length.
- If we want to keep the minimum size of the frame, the maximum length of the network should be changed.
- If the minimum frame size is still 512 bits, and it is transmitted 10 times faster, the collision needs to be detected 10 times sooner, which means the maximum length of the network should be 10 times shorter (the propagation speed does not change).

Two solutions:

- To totally drop the bus topology and use a passive hub and star topology, but make the maximum size of the network 250 meters instead of 2500 meters as in the Standard Ethernet.
- To use a link-layer switch with a buffer to store frames and a full-duplex connection to each host to make the transmission medium private for each host. No need for CSMA/CD because the hosts are not competing with each other.

AUTONEGOTIATION

- Allows a station or a hub a range of capabilities
- Allows two devices to negotiate.
- Designed particularly for these purposes:
    - To allow incompatible devices to connect to one another. (a device with a 10 Mbps can communicate with a device with a 100 Mbps capacity).
- To allow one device to have multiple capabilities.
- To allow a station to check a hub's capabilities.

PHYSICAL LAYER

– To be able to handle a 100 Mbps data rate

TOPOLOGY

- Fast Ethernet is designed to connect two or more stations.
- 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.

ENCODING

- Uses 4B5B, NRZ-I and 8B/6T based on implementation.

Implementation	Medium	Medium Length	Wires	Encoding
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

C) GIGABIT ETHERNET (1000 MBPS)

- Data transfer rate of 1000 Mbps.
- Called as Standard 802.3z.

GOALS

- Upgrade the data rate to 1 Gbps.
- Make it compatible with Standard or Fast Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame lengths.
- Supports autonegotiation.

MAC SUB LAYER

- Gigabit Ethernet has two distinctive approaches for medium access:

Half-duplex

- A switch can be replaced by a hub, which acts as the common cable in which a collision might occur.
- Uses CSMA/CD. Uses three methods namely, traditional, carrier extension, and frame bursting.

Full duplex

- Is a central switch connected to all computers or other switches.
- For each input port, each switch has buffers in which data are stored until they are transmitted.
- Since the switch uses the destination address of the frame and sends a frame out of the port connected to that particular destination, there is no collision.
- CSMA/CD is not used.
- Lack of collision implies that the maximum length of the cable is determined by the signal attenuation in the cable and not by the collision detection process.

i) PHYSICAL LAYER TOPOLOGY

- designed to connect two or more stations.
- 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.
- Another possible configuration is to connect several star topologies or let one star topology be part of another.

ii) IMPLEMENTATION

- Gigabit Ethernet can be
- Categorized as either a two-wire or a four-wire implementation.
- The two-wire implementations use fiber-optic cable (1000Base-SX, short-wave, or 1000Base-LX, long-wave), or STP (1000Base-CX).
- The four-wire version uses category 5 twisted-pair cable (1000Base-T). In other words, we have four implementations.
- 1000Base-T was designed in response to those users who had already installed this wiring for other purposes such as Fast Ethernet or telephone services.

iii) ENCODING

- Uses NRZ, 8B/10B and 4D-PAM5.

Implementation	Medium	Medium Length	Wires	Encoding
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

D) 10 GIGABIT ETHERNET

- To extend the technology, the data rate, and the coverage distance so that the Ethernet can be used as LAN and MAN (metropolitan area network).
- IEEE committee created 10 Gigabit Ethernet and called it Standard 802.3ae.

GOALS

- upgrading the data rate to 10 Gbps, keeping the same frame size and format, and allowing the interconnection of LANs, MANs, and WAN possible.
- This data rate is possible only with fiber-optic technology at this time.
- The standard defines two types of physical layers:
- LAN PHY: To support existing LANs
- WAN PHY: Defines a WAN with links connected through SONET OC-192.

IMPLEMENTATION

– 10 GigabitEthernet operates only in full-duplex mode.

Implementation	Medium	Medium Length	Number of wires	Encoding
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

WIRELESS LANS-IEEE 802.11 PROJECT

A) **IEEE 802.11 Project**

- Specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers.
- Also called as **wireless Ethernet**.
- **WiFi** (Wireless Fidelity) as a synonym for wireless LAN.
- WiFi, is a wireless LAN that is certified by the WiFi Alliance. (Global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.

A) ARCHITECTURE

- Defines two kinds of services:
  - Basic Service Set (BSS)
  - Extended Service Set (ESS).

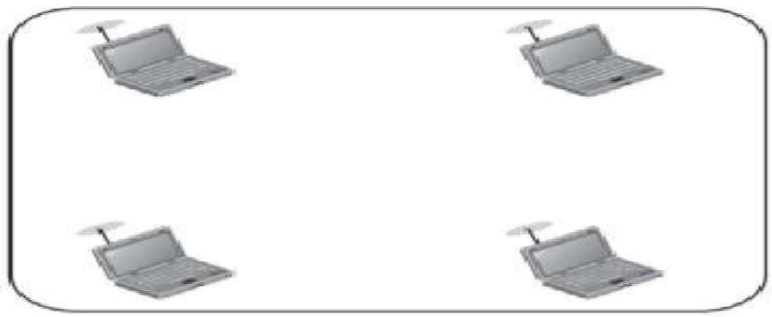
i) Basic Service Set

- IEEE 802.11 defines the basic service set (BSS) as the building blocks of a wireless LAN.
- A basic service set is made of stationary or mobile wireless stations and an optional central Base Station, known as the Access Point (AP) data-link layers.
- It is sometimes called wireless Ethernet.

a) Architecture-Basic Service Set

1. Stand-alone network (ad-hoc architecture)

- The BSS without an AP is a stand-alone network and cannot send data to other BSSs.
- It is called an ad-hoc architecture.
- In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS.



Ad hoc BSS

2. Infrastructure BSS

– A BSS with an AP is sometimes referred to as an infrastructure BSS.

ii) ***Extended Service Set (ESS)***

- Is made up of two or more BSSs with APs.
- The BSSs are connected through a distribution system, which is a wired or a wireless network.
- The distribution system connects the APs in the BSSs.
- Does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet.
- The extended service set uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.
- When BSSs are connected, the stations within reach of one another can communicate without the use of an AP.
- Communication between a station in a BSS and the outside BSS occurs via the AP.
- Mobile station can belong to more than one BSS at the same time.

MAC SUBLAYER

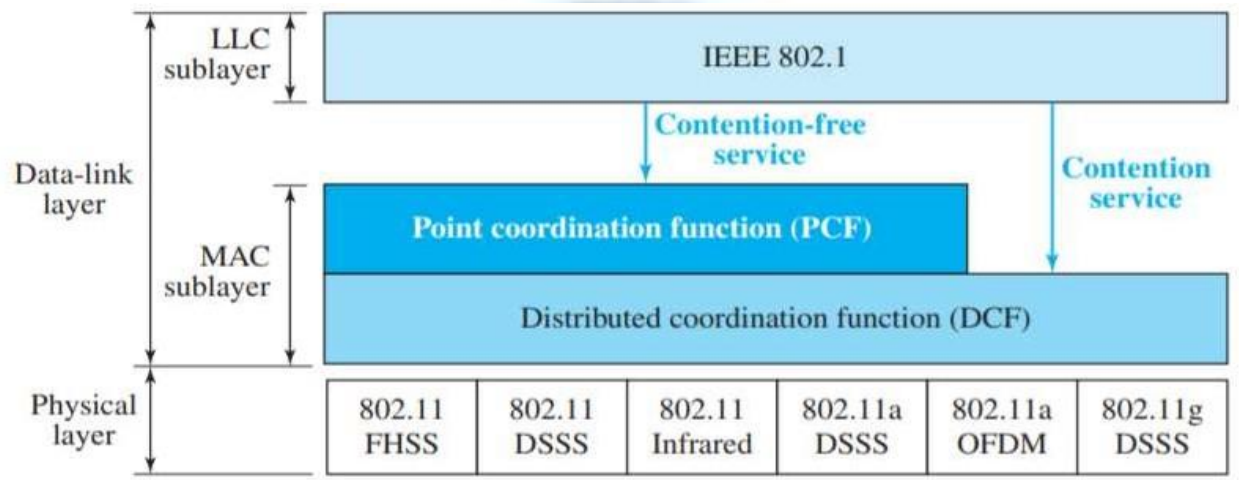
- Defines two MAC sublayers:

Distributed Coordination Function (DCF)

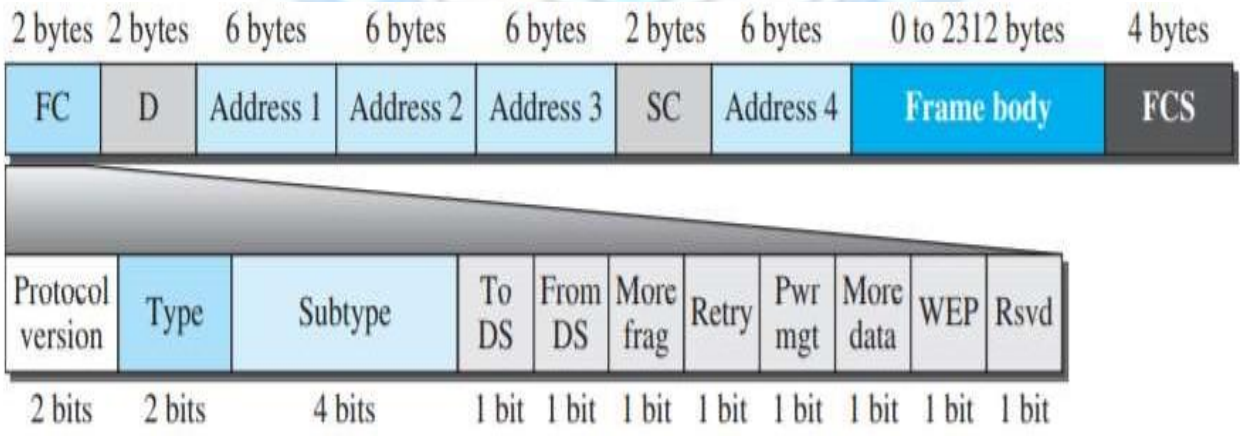
- Uses CSMA/CA as the access method

Point Coordination Function (PCF)

- Is an optional access methodthat can be implemented in an infrastructure network.
- Implemented on top of the DCF and is used mostly for time-sensitive transmission.



MAC Layer Frame format



Frame control (FC)-Is 2 bytes long and defines the type of frame and some control information.

D-Defines the duration of the transmission that is used to set the value of NAV. In one control frame, it defines the ID of the frame.

***Addresses*-**There are four address fields, each 6 bytes long. The meaning of each address field depends on the value of the To DS and From DS subfields and will be discussed later.

***Sequence Control (SC)*-**SC field, defines a 16-bit value. The first four bits define the fragment number; the last 12 bits define the sequence number, which is the same in all fragments.

***Frame body*-**Shall be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

***FCS*-**Is 4 bytes long and contains a CRC-32 error-detection sequence.

Frame Types

Management frames:

- Used for the initial communication between stations and access points.

Control Frames:

- Used for accessing the channel and acknowledging frames.

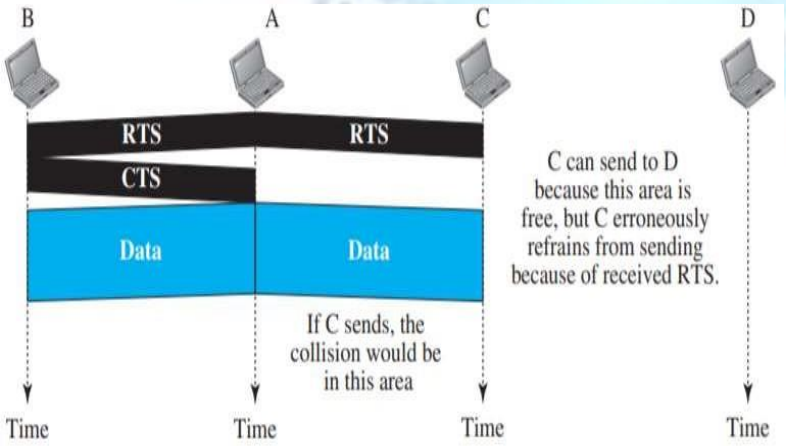
Data Frames:

- Used for carrying data and control information.

Addressing Mechanism

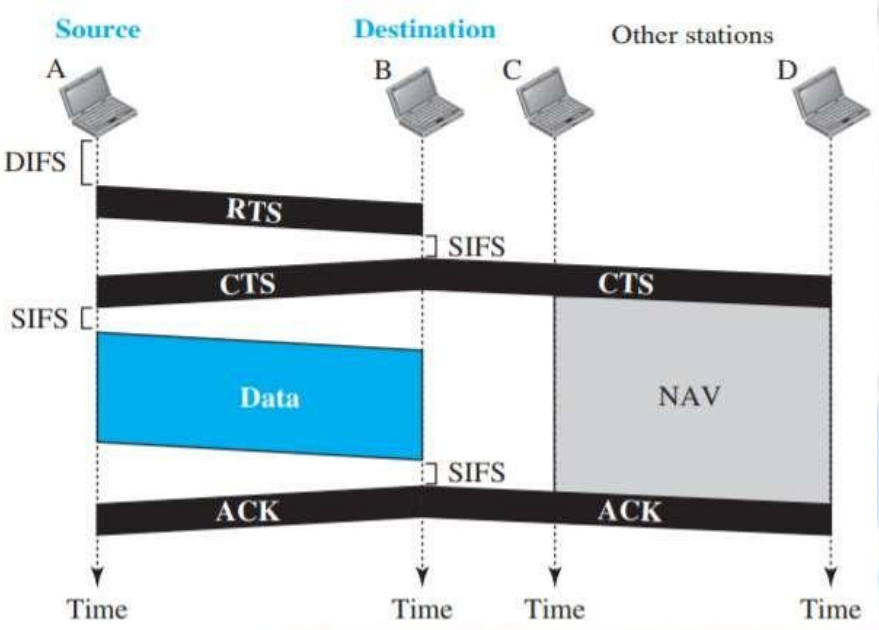
To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

c) Exposed Station Problem



- Station A is transmitting to station B.
- Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B.
- However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending.
- Station C is too conservative and wastes the capacity of the channel.
- Station C hears the RTS from A and refrains from sending, even though the communication between C and D cannot cause a collision in the zone between A and C; station C cannot know that station A's transmission does not affect the zone between C and D.

d) Hidden Station Problem



- RTS message from B reaches A, but not C.
- As both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A, reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

e) Physical Layer

Six specifications are given in Table.

IEEE	Technique	Band	Modulation	Rate (Mbps)
802.11	FHSS	2.400–4.835 GHz	FSK	1 and 2
	DSSS	2.400–4.835 GHz	PSK	1 and 2
	None	Infrared	PPM	1 and 2
802.11a	OFDM	5.725–5.850 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.400–4.835 GHz	PSK	5.5 and 11
802.11g	OFDM	2.400–4.835 GHz	Different	22 and 54
802.11n	OFDM	5.725–5.850 GHz	Different	600

WIRELESS LANS-BLUETOOTH

Introduction

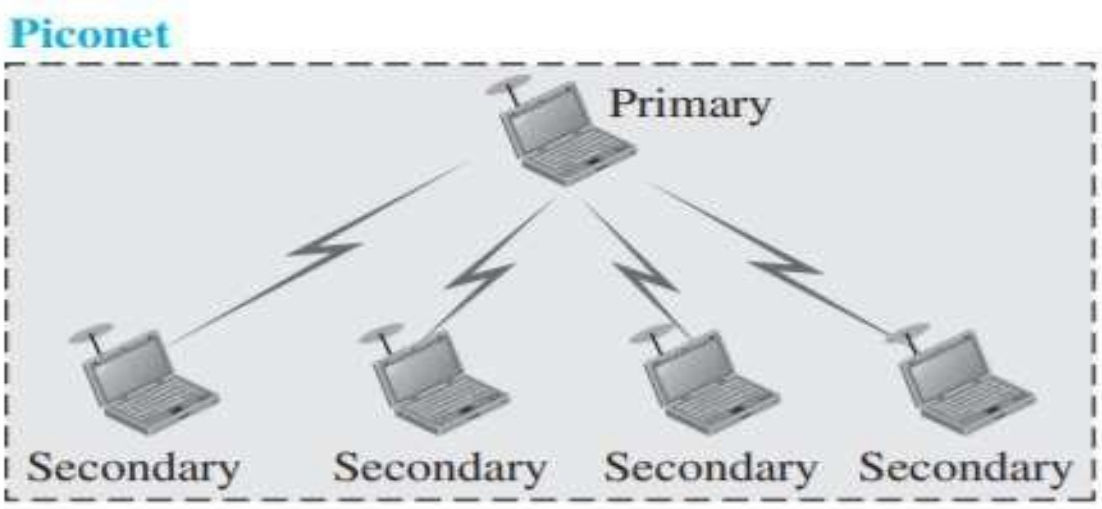
- Originally started as a project by the Ericsson Company.
- Is the implementation of a protocol defined by the IEEE 802.15 standard.
- Defines a wireless Personal-Area Network (PAN) operable in an area the size of a room or a hall.
- Is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when at a short distance from each other.
- A Bluetooth LAN is an ad hoc network, the devices, (gadgets), find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.
- A Bluetooth LAN, by nature, cannot be large.

A) Architecture

- defines two types of networks:
    1. Piconet
    2. Scatter net

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; the rest are called secondaries.



- Bluetooth defines two types of networks:

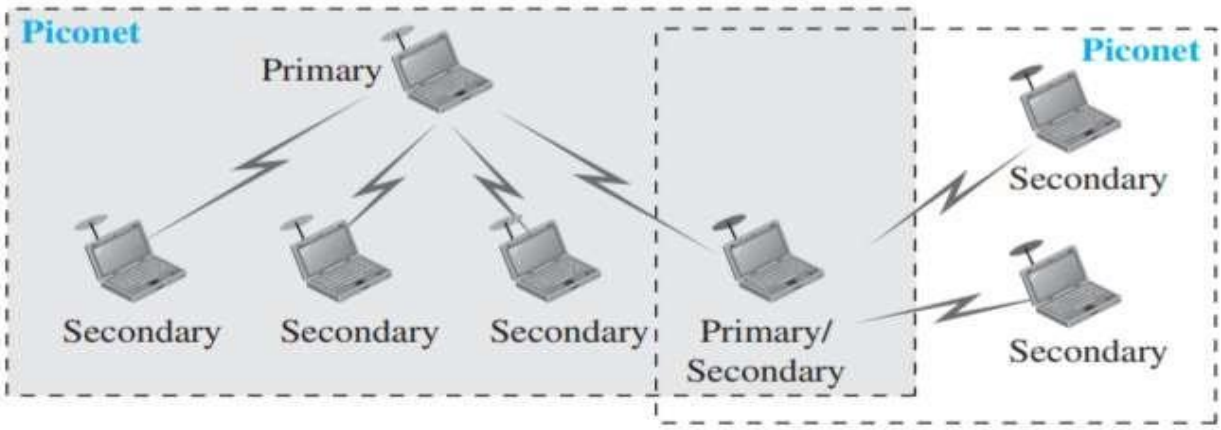
Picone t and Scatternet

i) Piconet

- All the secondary stations synchronize their clocks and
- hopping sequence with the primary.
- The communication between the primary and secondary stations can be one-to-one or one-to-many
- Although a picont have a maximum of seven secondaries, additional 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 to the active state.
- Only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

ii) Scatternet

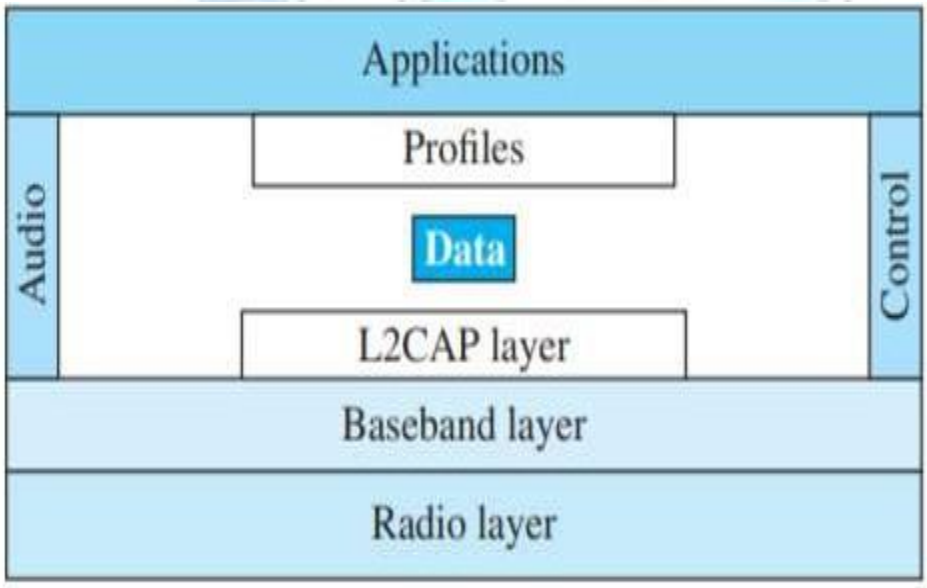
- Piconets can be combined to form a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.



Bluetooth Layers

Logical Link Control and Adaptation Protocol (L2CAP)

- Is roughly equivalent to the LLC sublayer in LANs.
- It is used for data exchange on an ACL link; SCO channels do not use L2CAP.



Frame Format:

Length

16-bit length field defines the size of the data, in bytes, coming from

the upper layers.

Data

Data can be up to 65,535 bytes.

Channel ID (CID)

Defines a unique identifier for the virtual channel created at this level.

Functions of L2CAP

- **Multiplexing**
  - At the sender site, it accepts data from one of the upper-layer protocols, frames them, and delivers them to the baseband layer.
  - At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol layer.
- ***Segmentation and Reassembly***
  - The maximum size of the payload field in the baseband layer is 2774 bits, or 343 bytes.
  - The L2CAP divides these large packets into segments and adds extra information to define the location of the segments in the original packet. The L2CAP segments the packets at the source and reassembles them at the destination.
- **QoS**
  - Bluetooth allows the stations to define a quality-of-service level.
- **Group Management**
  - To allow devices to create a type of logical addressing between themselves.
  - Two or three secondary devices can be part of a multicast group to receive data from the primary.

ii) Baseband Layer

- Baseband layer is roughly equivalent to the MAC sub-layer in LANs.
- Access method is TDMA.
- Primary and secondary stations communicate with each other using time slots.
- Length of a time slot is exactly the same as the dwell time, 625 μs.
- This means that during the time that one frequency is used, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.
- Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.

Links

- Two types of links can be created between a primary and a secondary: SCO links and ACL links.

i) A synchronous connection-oriented (SCO) link:

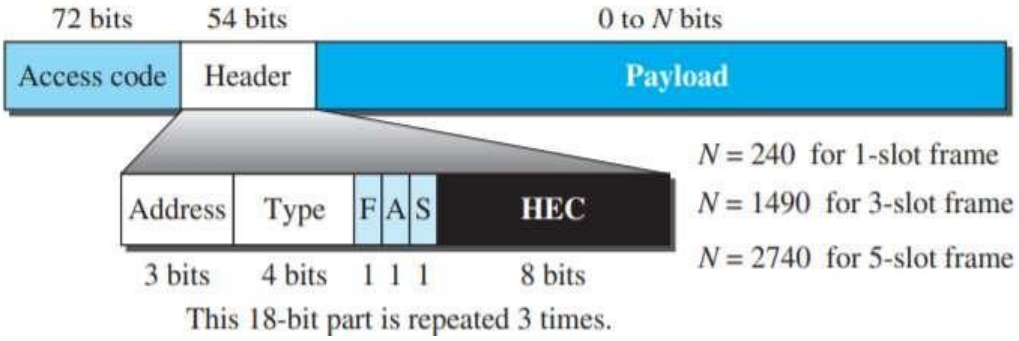
- Is used when avoiding latency (delay in data delivery) is more important than
- integrity (error-free delivery).
- A physical link is created between the primary and a secondary by reserving
- specific slots at regular intervals.
- The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted.
- A secondary can create up to three SCO links with the primary, sending digitized
- audio (PCM) at 64 kbps in each link.

ii) An asynchronous connectionless link (ACL):

- Is used when data integrity is more important than avoiding latency.
- If a payload encapsulated in the frame is corrupted, it is retransmitted.
- A secondary returns an ACL frame in the available odd-numbered slot if the previous slot has been addressed to it.
- ACL can use one, three, or more slots and can achieve a maximum data rate of 721kbps.

FRAME FORMAT

- A frame can be one of three types: one-slot, three-slot, or five slot.
- In a one-slot frame exchange, 259 μs is needed for hopping and control mechanisms.
- This means that a one-slot frame can last only 625 − 259, or 366 μs.
- With a 1-MHz bandwidth and 1 bit/Hz, the size of a one slot frame is 366 bits.



Access code-This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.

Header-This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:

Address.-The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.

Type. The 4-bit type subfield defines the type of data coming from the upper layers. We discuss these types later.

F. This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).

Header.

- A This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and- Wait ARQ; 1 bit is sufficient for acknowledgment.
- S. This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and- Wait ARQ; 1 bit is sufficient for sequence numbering.
- HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section. The header has three identical 18-bit sections. The receiver compares these three sections, bit by bit. If each of the corresponding bits is the same, the bit is accepted; if not, the majority opinion rules.

Payload.

This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

iii) Radio Layer

- Is roughly equivalent to the physical layer of the Internet model.
- Bluetooth devices are low-power and have a range of 10 m.
- Band Uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- Bluetooth uses the frequency-hopping spread spectrum (FHSS)
- method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.
- A device uses a frequency for only 625 μs (1/1600 s) before it hops to another
- frequency; the dwell time is 625 μs.
- Modulation

- Uses a sophisticated versionof FSK, called GFSK (FSK with Gaussian bandwidth filtering.
- GFSK has a carrier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit 0 is represented by a frequency deviation below the carrier.

$$f_c = 2402 + n \text{ MHz} \qquad n = 0, 1, 2, 3, \ldots, 78$$

6.APPLICATIONS: ETHERNET IN LAN/WAN SETUPS, ENCODING IN RFID READERS ,WI-FI MAC IN HOMES AND AIRPORTS, CRC IN PACKET VERIFICATION, FIBER MEDIA IN ISP BACKBONES.

Ethernet in LAN/WAN Setups

Ethernet is a standard networking technology that provides wired connections in Local Area Networks (LANs) and Wide Area Networks (WANs).

- Connectivity and Resource Sharing: It allows devices (computers, printers, servers, RFID readers) within an office, campus, or factory to connect and share resources and information efficiently.

- Internet Access: Ethernet connects end-user devices to the internet via routers or switches, forming the physical layer of many TCP/IP networks.

- Power over Ethernet (PoE): A significant application is the use of a single Ethernet cable to provide both a data connection and electrical power to devices like security cameras, VoIP phones, and networked RFID readers, simplifying installation and reducing cabling costs.

- Industrial Automation: Ethernet is widely adopted in industrial settings for reliable, highspeed communication between various automation devices, including Programmable Logic Controllers (PLCs) and sensors.

Encoding in RFID Readers

Encoding refers to the process of writing specific, organized data onto an RFID tag's memory banks so that readers can identify and interact with it correctly.

- Unique Identification: The primary application is assigning a unique identifier (ID) to each physical item (assets, inventory, tools, people). This ID is then linked to detailed information in a database or software system.

- Supply Chain Management: In logistics and inventory tracking, specific encoding schemes and standards like the GS1 Tag Data Standard (TDS) or RAIN ISO numbering (EPC Class 1 Gen2V2)

are used to ensure global compatibility and organization of product information, such as lot numbers, serial numbers, and manufacturing dates.

- Access Control: For door access systems, RFID cards or tags are encoded with unique identifiers that the reader verifies to grant or deny entry, often working in conjunction with a central control system.

- Data Logging and Real-time Monitoring: Data can be written to a tag as an item moves through different processes (e.g., in a manufacturing line), with readers at various points collecting this information in real time to monitor workflow and status.

Wi-Fi MAC in homes and airports

A Wi-Fi MAC address is a unique hardware identifier used for local network communication and device management, while a Cyclic Redundancy Check (CRC) is an error-detection code used to verify the integrity of data packets during transmission. Wi-Fi MAC Addresses in Homes and Airports A Media Access Control (MAC) address is a unique, 48-bit physical address "burned into" a device's network interface card (NIC) by the manufacturer. It operates at the data link layer (Layer 2) of the OSI model and is used for communication within a local area network (LAN).

- Local Identification: MAC addresses ensure that data frames are delivered to the correct physical device on the same local network segment (e.g., within a home or a single area of an airport terminal). Network switches and access points use MAC address tables to learn which devices are connected to which ports and forward traffic efficiently.

- Access Control (Filtering): Network administrators, in both home and airport settings, can use MAC address filtering as a basic security measure to restrict network access to only approved devices. However, this is not a strong security measure on its own as MAC addresses can be easily "spoofed" (changed in software).

- Network Management: In home networks, the router might use a device's MAC address to assign a consistent IP address via the Dynamic Host Configuration Protocol (DHCP). In enterprise environments like airports, network teams use MAC addresses for inventory, monitoring, and troubleshooting to pinpoint the physical location of a device causing problems.

- Privacy and Tracking: Static MAC addresses can be used to track a device's movement across different physical locations, which has significant privacy implications in public spaces like airports. To counter this, modern operating systems use MAC address randomization, where a device uses a random, locally administered MAC address when scanning for or connecting to public Wi-Fi networks.

CRC in Packet Verification

A Cyclic Redundancy Check (CRC) is an efficient mathematical method used to detect accidental errors or changes in digital data that may occur during transmission or storage due to noise or interference. Mechanism: CRC works by treating a block of data as a binary polynomial.

- The sender calculates a short, fixed-length checksum (or Frame Check Sequence) based on a division of the data by a predetermined "generator polynomial" using modulo-2 arithmetic.

- This CRC checksum is appended to the data and transmitted as part of the data packet or frame.

- The receiver performs the same calculation on the received data. The expected result (remainder) should be zero. Error Detection: o If the calculated remainder at the receiver is zero, the data is assumed to be error-free and is accepted. o If the remainder is non-zero, it means an error was detected during transmission, and the receiver can request that the sender retransmit the data.

- Application: CRC is a crucial component in many network protocols, including Wi-Fi and Ethernet frames, where a CRC-32 checksum is typically used to ensure high data integrity. It is effective at detecting common errors like single-bit and burst errors. CRC is only for error detection, not correction, and does not protect against intentional data tampering.

Fiber media in ISP backbones

Fiber optic media is the universal and primary choice for Internet Service Provider (ISP) backbones due to its unmatched high speed, massive bandwidth capacity, and signal integrity over long distances. It has largely replaced traditional copper cabling in this critical infrastructure role. Role and Importance in ISP Backbones

The internet backbone is a core network of the largest and fastest interconnections that link major routers, data centers, and internet exchange points (IXPs) across cities, countries, and continents. Fiber media is the foundational pillar of this network, enabling global data exchange by:

- Handling Enormous Data Volumes: Fiber cables can carry vast amounts of data simultaneously (up to terabits per second) as pulses of light, which is essential for modern data demands like cloud computing and video streaming.

- Ensuring Long-Distance Transmission: Data transmitted through fiber experiences minimal signal loss (attenuation) compared to other media, allowing it to cover thousands of kilometers with fewer repeaters and ensuring data integrity across the globe.

- Providing High Speed and Low Latency: Data travels through fiber at speeds close to the speed of light, which minimizes latency (signal delay). This is crucial for real-time applications and smooth global internet traffic flow.

- Offering Reliability and Immunity to Interference: Because fiber uses light signals instead of electrical ones, it is immune to electromagnetic interference (EMI) and crosstalk. This results in highly stable and reliable connections, which is a critical requirement for a global network backbone.

Key Technologies and Components

ISPs and telecom companies use several technologies and components to leverage fiber media in their backbones:

- Single-Mode Fiber (SMF): This is the predominant type used in long-haul backbone networks. It has a small core and transmits a single beam of light from a laser, enabling very high data rates over long distances.

- Wavelength-Division Multiplexing (WDM): This technology allows multiple channels of information to be sent through a single fiber strand using different wavelengths (colors) of light, dramatically increasing the network's total capacity

- High-Performance Routers and Switches: Powerful networking equipment is used at connection points to manage and direct the immense volume of data traffic efficiently across the network.

- Internet Exchange Points (IXPs) and Points of Presence (PoPs): These are the physical locations where different backbone networks and ISPs interconnect and exchange data, often in neutral, high-performance facilities.

- Submarine Communications Cables: Extensive networks of armored fiber optic cables laid on the ocean floor are used to connect different continents, forming the physical global internet infrastructure.