Chapter 3 Self Note (pg - 132)

S.No.	Contents	Check it (if Study)	Page	Spend Time in Hour
3.1	Functions of Data Link Layer	✓	126	1
3.2	Data Link Control: Framing, Flow and Error Control		126	1
3.3	Error Detection and Correction		156	1
3.4	High-Level Data Lin k Control(HDLC) & Point - to - Point protocol(PPP)		161	1
3.5	Channel Allocation Problem		167	0.5
3.6	Multiple Access: Radom Access(ALOH A, CSMA, CSMN CD, CSMA/CA), Controlled Access(Reservation, Polling, Token Passing), Channelization (FDMA, TDMA, CDMA)		168	1
3.7	Wired LAN: Ethernet Standards and FDDI		190	1
3.8	Wireless LAN : IEEE 802.11x and Bluetooth Standards		193	1
3.9	Token Bus, Token Ring and Virtual LAN		198	0.5

Table of Content

3.1 Functions of Data-link layer

- Framming the packets and transmitting them over a physical layer
- Hanlde error detection and flow control
- Uses error detection bit to detect error and correct them at receiving site
- Regulating the flow of data so that slow receiver are not swamped by fast sender (Flow control)
- Reliable transfer of each message

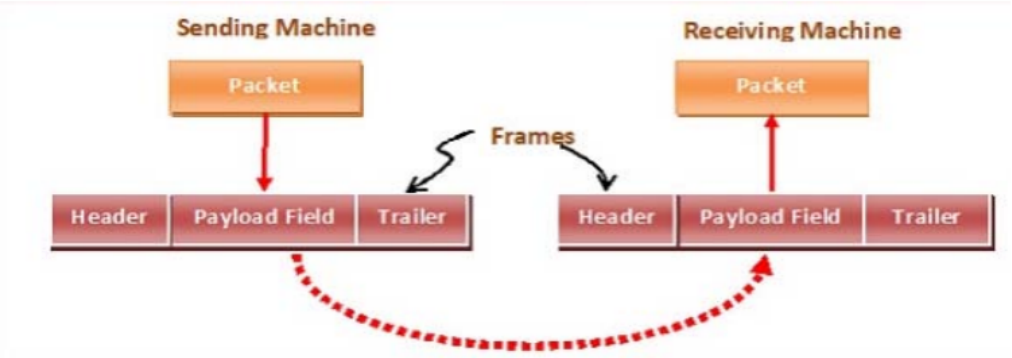
Framing

It is a process of diving large data into smaller manageable unit called frames for transmission over a network.

It consist of three parts

- Header
  Contains information like source and destination address, error detection code

- Payload
  Carries actual data
- Trailer
  A piece of information that is added to the end of a data packet to shows the packet's destinatio
  n.



- **Frame Header** – It contains the source and the destination addresses of the frame.
- **Payload field** – It contains the message to be delivered.
- **Trailer** – It contains the error detection and error correction bits.
- **Flag** – It marks the beginning and end of the frame.

Its divided into Two sublayers

▼ MAC (Media Access Control)

Fig : General MAC frame Format

Functions of MAC

1. Device Interaction
2. Frame Addressing
   Assign physical address
3. Error Detection
   CRC use to detect error

Common MAC

- Ethernet
- WI-FI

▼ LLC (Logical Link Control)

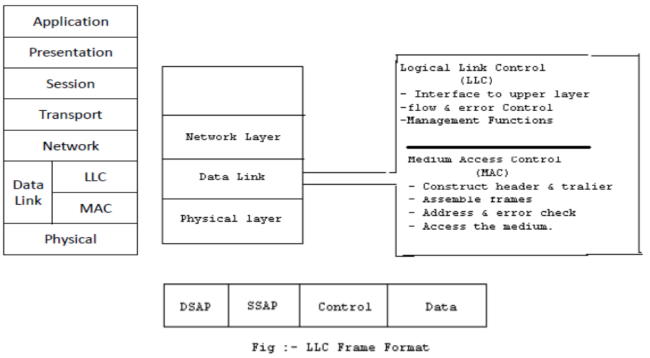


Fig :- LLC Frame Format

Functions

1. Error control

   Provide mechanisms to correct error at receiving site and ensure data integrity

2. Flow control

   Regulating the flow of data so that slow receiver are not flooded by fast sender

3. Acknowledgements

   Sends ACKs to confire data received

Frame Format

1. **DSAP**
   - Destination service access point
   - 8 Byte identifying the DSAP
2. SSAP
   - Source service access point
   - 8 Byte identifying SSAP
3. Control
   - 1 or 2 byte containing control information frame LLC layer such as
     - Frame type
     - flow control
     - Sequencing
4. Data

Type of Framing

▼ Fixed Size

- The frame is of fixed sized
- length of frame acts like delimiter (seperate one piece of data from another).
- There is no need to provide boundaries to frame

Drawback

It suffer from internal fragmentation if the size is less than frame size.

Solution

Padding

▼ Variable Size

It is a technique for dividing data into frames (packets) that can be of varying lengths.

Header	Payload	Trailer	Header	Payload	Trailer
Frame 1			Frame 2		

Figure : Frame Format in Variable Size frame

It can be done in two ways:

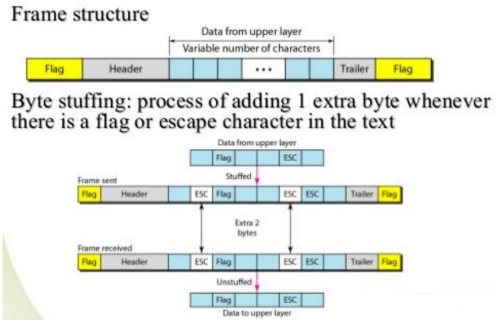
1. **Length Field :**
   - To show length of frame.
   - Problem : length field might get corrupted

2. **End Delimeter :**
   - To show end of the frame

   It can be solved using

   1. Byte Stuffing

      A byte is stuffed in the message to differentiate from the delimiter.
      This is also called
      character-oriented framing.



   2. Bit Stuffing

      A pattern of bits of arbitrary length is stuffed in the message to differentiate from the

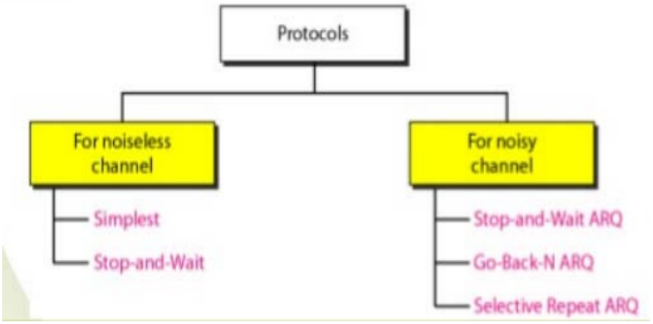
      delimiter.

      This is also called **bit – oriented framing.**

Flow and Error Control

- **Data link control = flow control + error control**
- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement
- Error control in the data link layer is based on automatic repeat request (ARQ), which is the retransmission of data
- ACK, NAK(Negative ACK), Piggybacking (ACKs and NAKs in data frames)

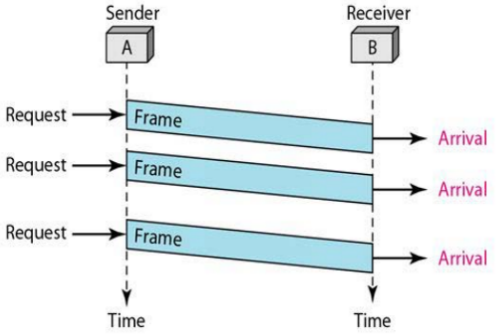
▼ Flow Control



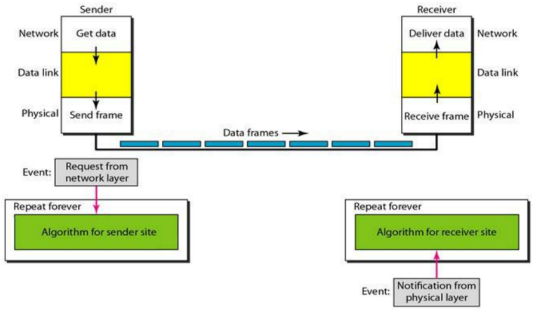
> Easy to remember → noisey has ARQ at back || noiseless has no ARQ

Simplest

- It has no flow or error control
- it is a unidirectional protocol
  (data frames are traveling in only one direction-from the sender to receiver.)
- We assume that the receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible.
- The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately.

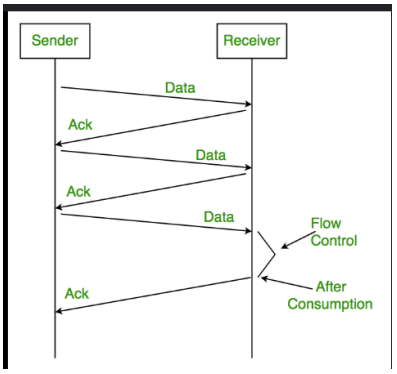


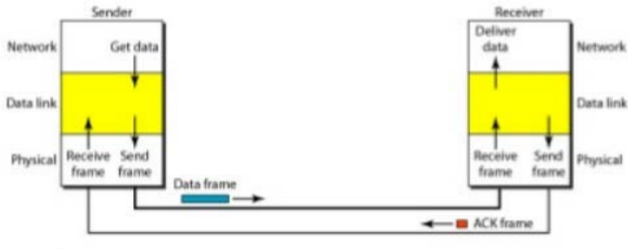
Simplest protocol with no flow or error control



Stop & Wait

- Flow control added , Error control added and token for ACK



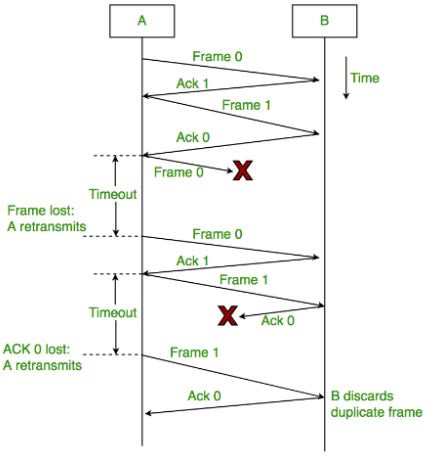


Stop and wait ARQ (Automatic Repeat Request)

- Build upon the foundation of stop and wait
- Error correction is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires (time out)

Mechanisum:

- Sender transmit frame with sequence number (0 or 1)
- Receiver check for error using CRC or Checksum
- If error free, receiver sends ACK with same sequence number
- If error, receiver sends NAK
- Sender wait for ACK or NAK
- If ACK, sender sends next frame with opposite sequence number
- If NAK or timeout , sender retransmits previous frame.



Go Back N ARQ

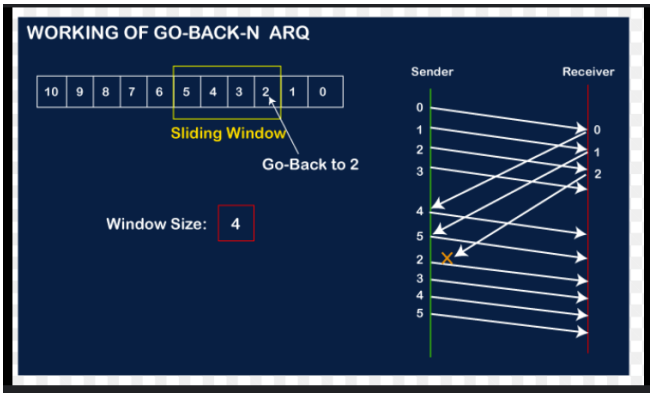
Go-Back-N ARQ (Automatic Repeat Request) is a data link layer protocol used for reliable data transmission over unreliable channels.
It's a type of
error correction technique that employs a sliding window mechanism to achieve reliable and sequential delivery of data frames.

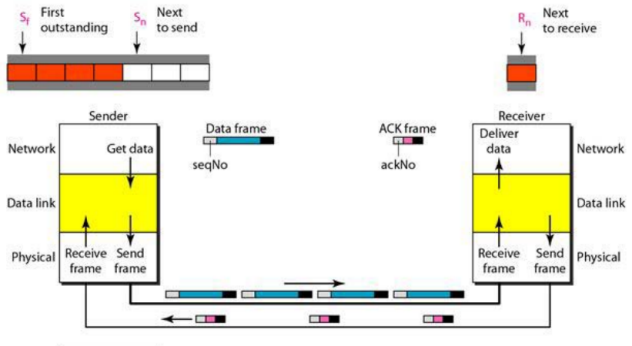
Core principle:

- The sender transmits multiple data frames continuously within a specific window size (N) before waiting for an acknowledgment (ACK) from the receiver.
- The receiver acknowledges frames sequentially.
  If it encounters an error or doesn't receive an expected frame, it sends a negative acknowledgment (NAK) indicating the sequence number of the next expected frame.

When to use Go-Back-N ARQ:

- It's a simpler protocol compared to Selective Repeat ARQ, which might be preferable for complex scenarios.
- Go-Back-N ARQ is suitable for situations with moderate error rates where some level of re-transmission is acceptable.





Selective repeat ARQ

Selective Repeat ARQ (Automatic Repeat Request), also known as Selective Reject ARQ

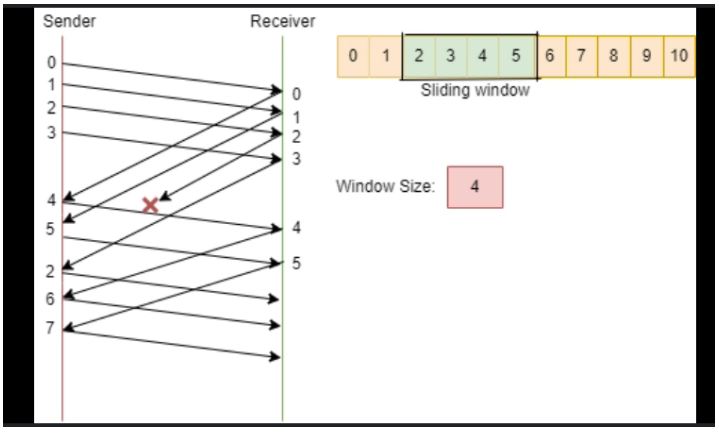
> It used in the data link layer for reliable data transmission.
> It builds upon the concepts of Go-Back-N ARQ but offers improved efficiency, particularly in channels with
> higher error rates.

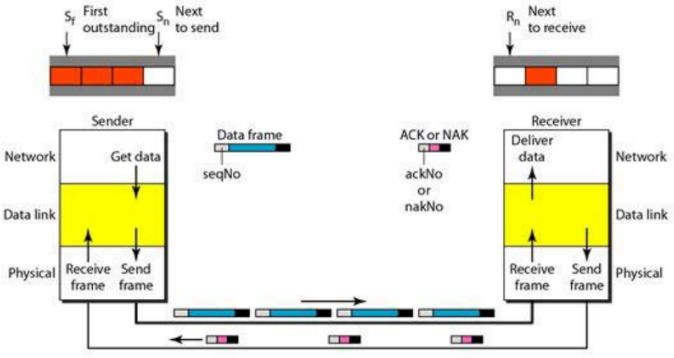
Key improvements over Go-Back-N ARQ:

- **Selective retransmission:**
  Unlike Go-Back-N, where the
  entire window is retransmitted upon receiving a NAK (Negative Acknowledgment),
  Selective Repeat only
  retransmits the specific frames that were lost or corrupted.
  This reduces wasted bandwidth on frames that were already received correctly.
- **Receiver buffering:** (in order accept)
  The receiver in Selective Repeat maintains a buffer to store received frames.
  Even if frames arrive out of order, the receiver can buffer them and deliver them to the higher layer in the correct sequence.
  This allows for more efficient utilization of the channel.

Working mechanism of Selective Repeat ARQ:

1. **Windowing:**
   Similar to Go-Back-N, both sender and receiver maintain windows.
   The sender's window size (Ws) defines the number of frames it can send continuously, while the receiver's window size (Wr) specifies the number of frames it's prepared to receive out-of-order.
2. **Sending and Acknowledging:**
   The sender transmits frames within its window.
   The receiver indivisually acknowledge frame, even if they arrive out of order.
3. **Error handling (Selective retransmission):**
   If a frame is lost or corrupted, the receiver discards it and sends a NAK for the specific missing sequence number. The sender only retransmits the NAKed frame, not the entire window.
4. **Out-of-order delivery:** The receiver buffers frames arriving out of order. Once it receives all frames required to construct a complete sequence, it delivers them to the higher layer in the correct order.





Sliding Window

- It allows multiple frames or packets to be transmitted without waiting for indivisual ACK for each other.
- Improves Effiency
  - Reducing Idel time
  - Increasing throught-put
- Common use:
  - Go Back N ARQ
  - Selective repeat ARQ
  - TCP
  - HLDC
  - PPP

Window Size:

The size of the sender and receiver window must be at most one-half of 2m

Piggybacking Protocol

- To improve the efficiency of the bidirectional protocols.
- Piggybacking in Go-Back-N ARQ

▼ Error Control

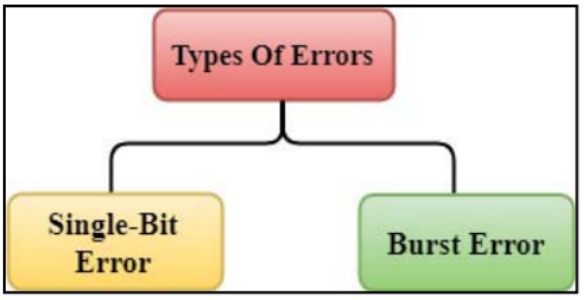
Error

It is unintented alteration or corruption of data that occur during transmission from a sender to receiver.

They can be caused

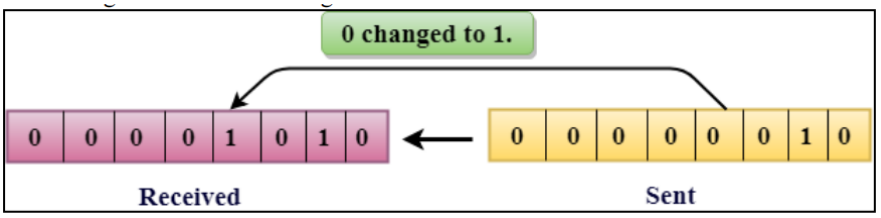
1. Noise in communication channel
2. Interference from other signal
3. Faulty hardware or software
4. Human Error

#Type of Errors



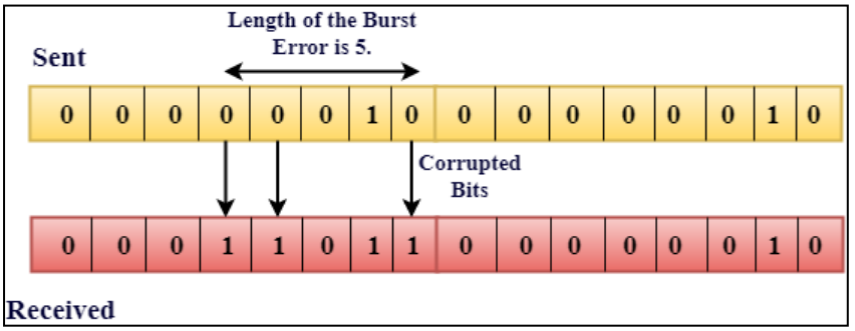
1. Single Bit Error

- Only one bit of data unit is changed (0 or 1)

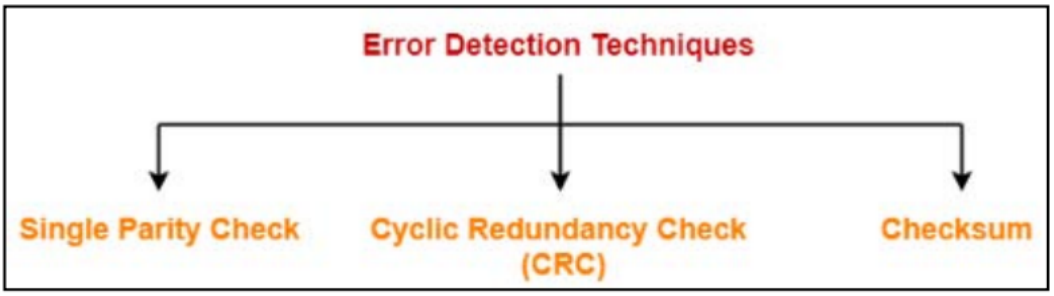


2. Burst Error

- Multiple consicutive bits are affected.



#Error Detection Technique

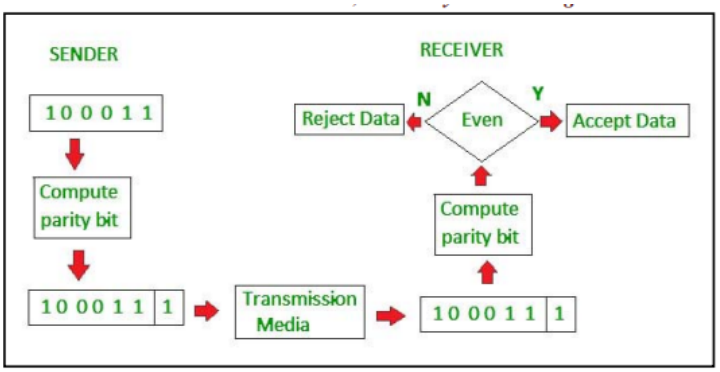


1. Single Parity Check

Adds extra bit to each data unit to make total of 1’s even or odd.

Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



2. Check sum

> The data is divided into k segments each of m bits.
> Mostly 4 segments of 8 bits

▼ **Gemini**

Imagine you're sending a box of chocolates across town. To check if any get eaten along the way, you add up the total number before sending it. That's kind of like a checksum in computer networking, but for data!

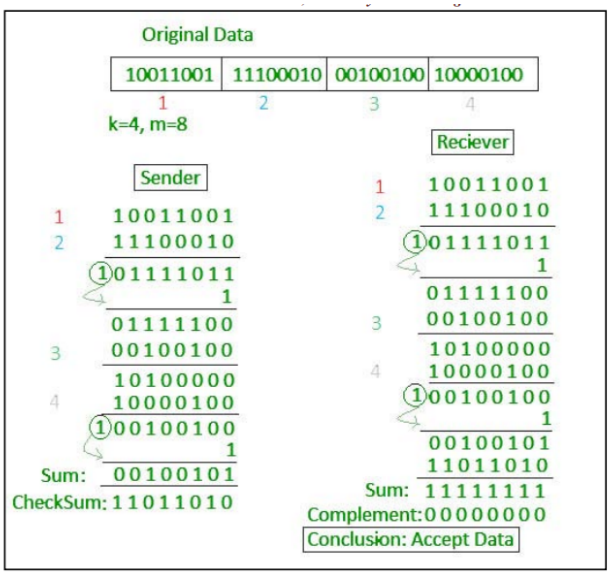
Here's a simplified explanation of checksums:

- **Goal:** Detect errors in data transmission over networks.
- **Process:**
  1. **Sender's Side:**
     - The data is divided into smaller chunks.
     - A checksum is calculated by adding these chunks together (using a specific method).
     - This checksum is like a quick fingerprint of the original data.
     - The checksum is sent along with the actual data.
  2. **Receiver's Side:**
     - The received data and checksum are added together.
     - If the result is ZERO, it likely means the data arrived without errors.
     - If the result is NOT ZERO, there's a good chance the data is corrupt.
- **Think of it as a quick check:** It's not perfect, but it catches many errors before they cause problems.

Key Points:

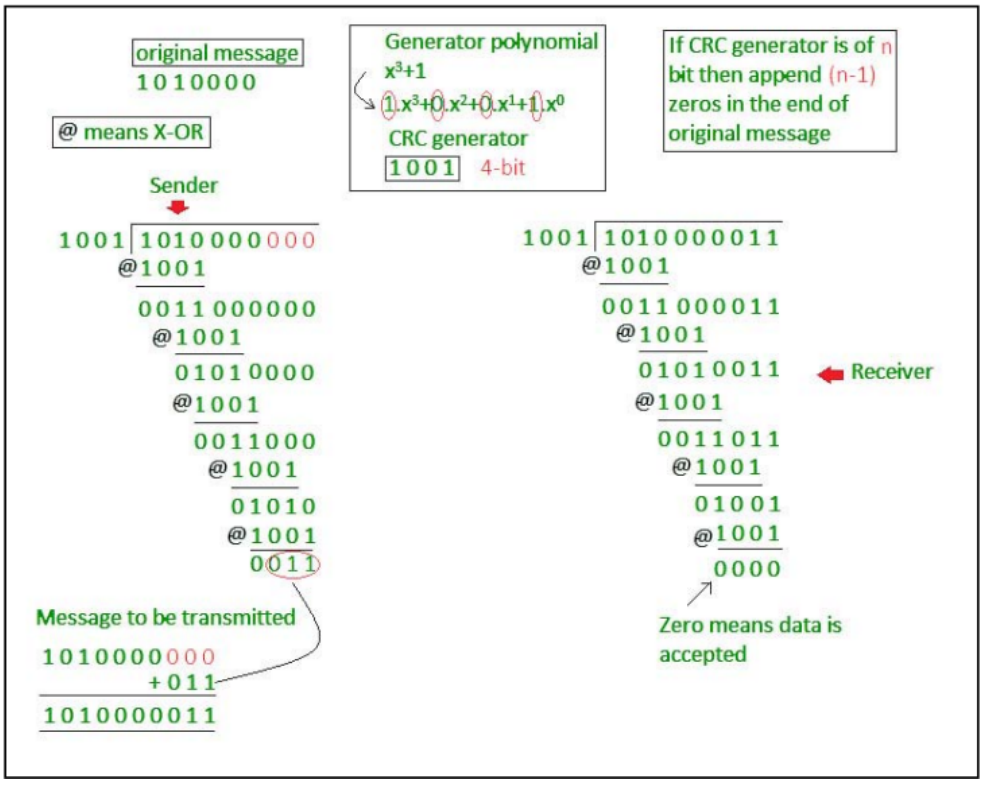
- Checksum is an error detection technique, not correction.
- It's a simple and efficient way to identify data corruption during transmission.
- While not foolproof, it's widely used in various network protocols.

• In the sender’s end the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
• The checksum segment is sent along with the data segments.
• At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum.
The sum is complemented.
• If the result is zero, the received data is accepted; otherwise discarded



3. Cyclic redundancy check (CRC)

- CRC is based on binary division.
- A sequence of redundant bits (CRC bits) are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number.
- If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected



pg: 151 for steps of all the techniques

3.3 Error Detecing codes and Error Correcting codes

Error Detecting code

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is **parity check**.

Error Correction code

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.
In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

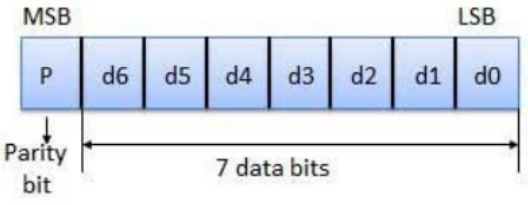
How to Detect and Correct Errors?

To detect and correct the errors, additional bits are added to the data bits at the time of transmission.

- The additional bits are called **parity bits**. They allow detection or correction of the errors.
- The data bits along with the parity bits form a **code word**.

Parity Checking of Error Detection0

It is the simplest technique for detecting and correcting errors.
The MSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits.
The parity of 8-bits transmitted word can be either even parity or odd parity.



Even parity

Even parity means the number of 1's in the given word including the parity bit should be even

(2,4,6,....).

Odd parity

Odd parity means the number of 1's in the given word including the parity bit should be odd

(1,3,5,....).

Use of Parity Bit

The parity bit can be set to 0 and 1 depending on the type of the parity required.

- For even parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is even. Shown in

fig. (a).

- For odd parity, this bit is set to 1 or 0 such that the no. of "1 bits" in the entire word is odd. Shown in

fig. (b)

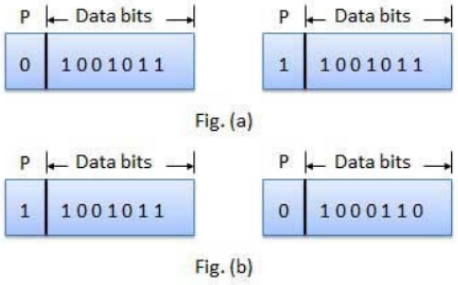


Fig. (a)

Fig. (b)

Hamming Code

It is a type of error-correction code used to detect and sometimes correct errors that may occur during data transmission across a network.

Here's how it works:

- **Redundant bits:**
  Hamming code adds extra bits, called parity bits, to the original data. These parity bits are calculated based on the data bits and help identify errors.
- **Encoding and Decoding:**
  The sender encodes the data by adding the calculated parity bits.
  The receiver then decodes the received data, including the parity bits, to check for errors.
- **Error detection and (sometimes) correction:**
  By analyzing the parity bits and the data bits, the receiver can determine if any errors occurred during transmission. In some Hamming code variations, the specific pattern of the error can also be identified, allowing for correction of the corrupted data bit.

▼ Code Smasher (incompleted)

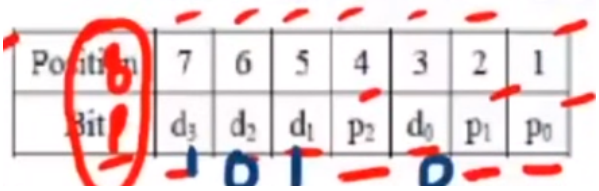
Lec-30: Hamming Code for Error Detection & Correction both with easiest examples
👉Subscribe to our new channel:https://www.youtube.com/@varunainashots

Hamming codes are used to detect and correct errors in transmitted or stored data. They
https://youtu.be/V5Iu52tbZEQ?si=RUx3SUxff6H6AyRM&t=36

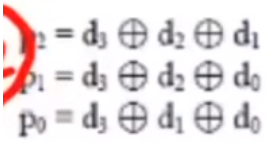
Position	7	6	5	4	3	2	1
Bit	d_3	d_2	d_1	p_2	d_0	p_1	p_0

- If we have 7 hamming code , 4 for data and 3 for parity
- To find out which is parity and which is data
- We use 2 ^ n where n is (0 , 1, 2 …) is parity and other are data
  - 2^0 ⇒ 1 is parity
  - 2^1 ⇒ 2 is parity
  - 2^2 ⇒ 4 is parity etc

- now suppose we have data as “ 1010 “, its placed as :



Now to calculate po, that sign is xor. Take the value of



▼ Neso acadimy

Data transmited by transmitter and received by the receiver.

There is the channel between them so there is possible of noise

- Given by RW hamming
- Easy to implement
- 7 bit hamming code is used commonly.

Rule:

- We use 2 ^ n where n is (0 , 1, 2 … 7) is parity and other are data
  - 2^0 ⇒ 1 is parity p1
  - 2^1 ⇒ 2 is parity p2
  - 2^2 ⇒ 4 is parity p4 etc

> In 7 bit we have Data bit ⇒ 4 and Parity bit ⇒ 3

Data bit:

- Data that we want to trasmit

Parity bit:

- It is extra bit to detect error

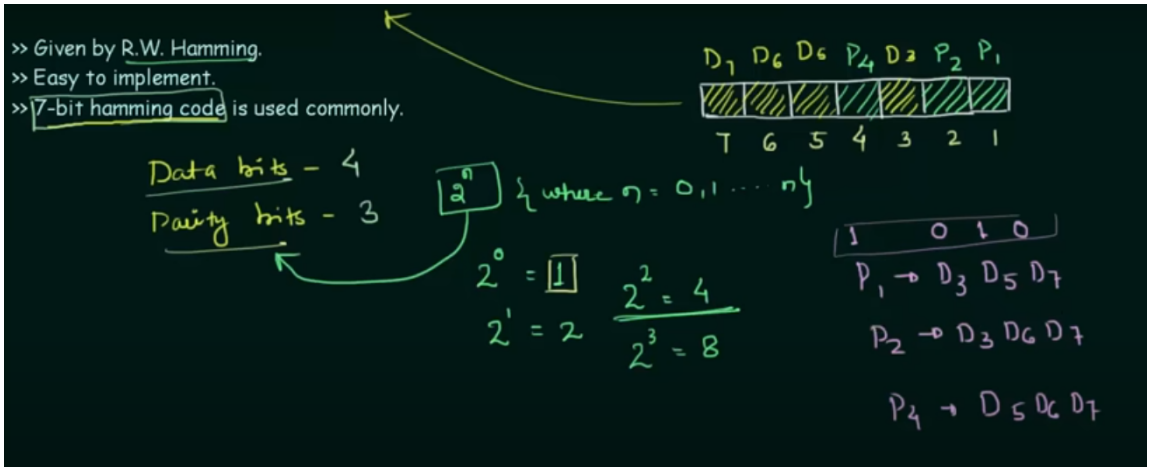
WE have to remember

p1⇒ D3 D5 D7

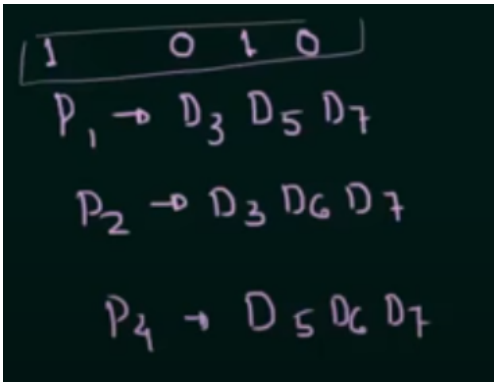
p2⇒ D3 D6 D7

p4⇒ D5 D6 D7

▼ Error Detection

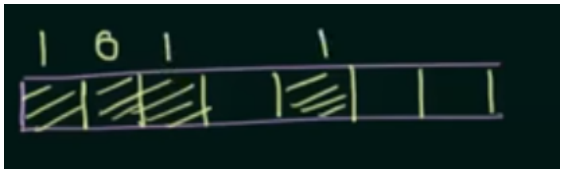


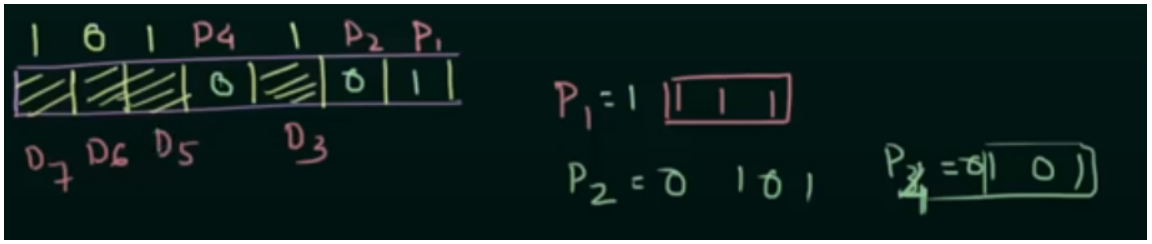
Here,



Suppose we have to make it even parity, we need to make the p1 addjusted according to it.
As in this example, p→ D3 D5 D7 (0 1 0) , we put p1 as 1 so that it will have 1 as even (1 0 1 0).

Question:

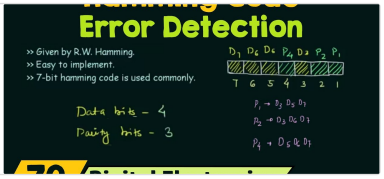




Hamming Code | Error Detection

Digital Electronics: Hamming Code | Error Detection Part.
Hamming Code-Error Correction Part: http://youtu.be/wbH2VxzmoZk

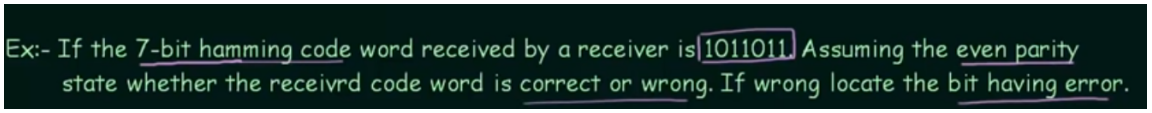
https://youtu.be/1A_NcXxdoCc?si=YdS3GxO1n1tTpljf&t=596

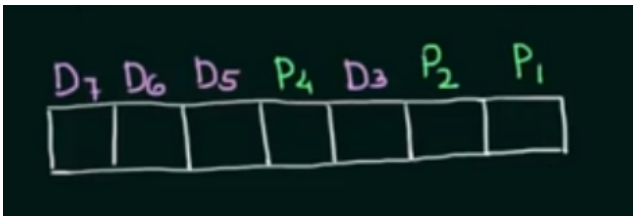


Watch from here to understand more..

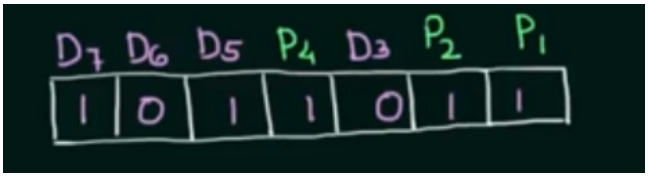
▼ Error Correction

Question

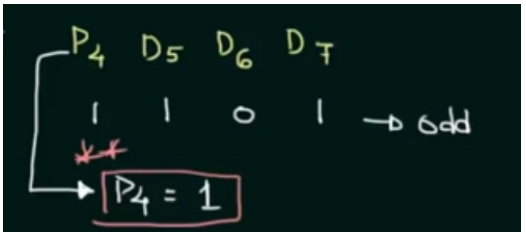




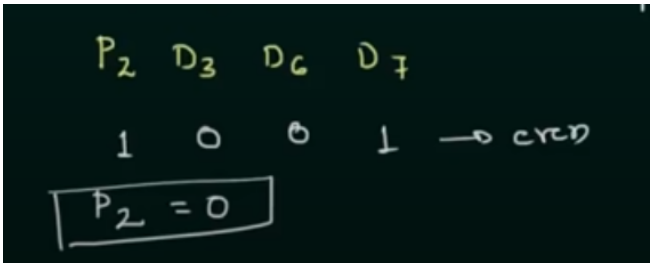
Steps



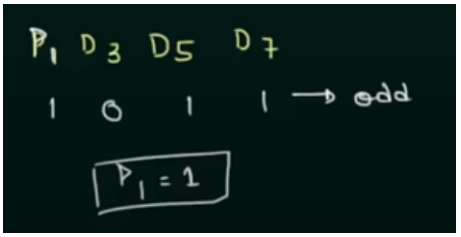
- First we have the received data 1011011 and its assuming that its even parity.
- First we check `p4 → D5 D6 D7` what we got is
  - Is Odd as number of 1 is odd. But we assumed to get even



  - we Put p4 as 1 as its odd not even
- now, we check `p2 → D3 D6 D7`
  - It is even, no error



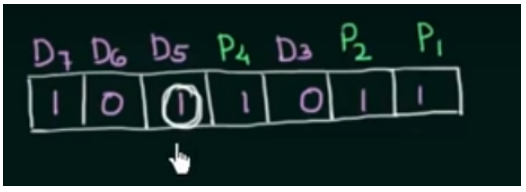
- now, we check `p4→ D3 D5 D7`
  - Its odd



Now lets write them

`p4 p2 p1` = `101` in binary ⇒ `5` in decimal.

So it mean its having 5th bit as error.



So our answer is `( 1001011 )`

3.4 High Level Data Link Control (HDLC)

> It is a group of communication protocol that works at datalink layer.

It defines how data is packed and trasmisted between network device accross physical layer.

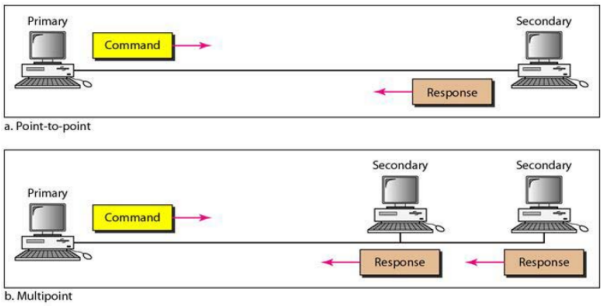
Different transfer modes

1. **Normal Response Mode (NRM)**

   Two types of stations are there,

   - Primary station that send commands
   - Secondary station that can respond to received commands.

   It is used for both point - to - point and multipoint communications.

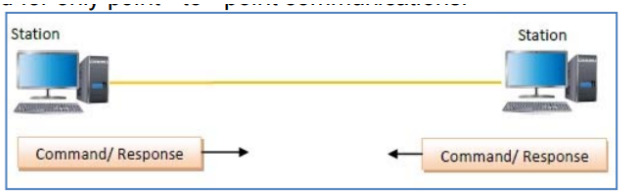


2. **Asynchronous balanced mode (ABM)**

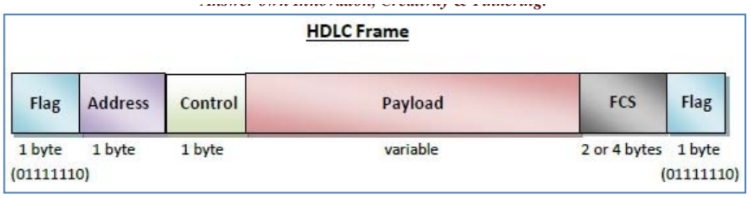
   Here, the configuration is balanced, i.e.

   each station can both send commands and respond to commands.

   It is used for only point - to - point communications.



HDLC Frame Format (FAC IF)



1. ***Flag***

   It is an 8-bit sequence that marks the beginning and the end of the frame

   The bit pattern of the flag is `01111110`.

2. ***Address***

   It contains the address of the receiver.

   If the frame is sent by the primary station, it contains the address(es) of the secondary station(s).

3. ***Control***

   It is 1 or 2 bytes containing flow and error control information.

4. ***Information (payload)***

   This carries the data from the network layer.

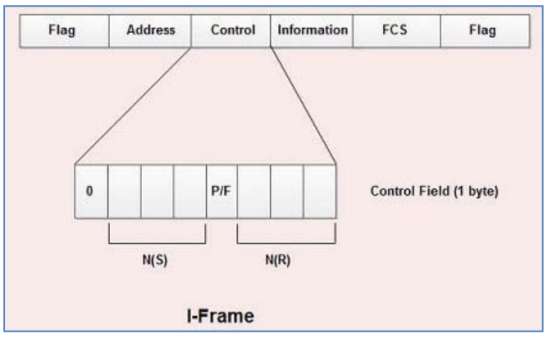
   Its length may vary from one network to another.

5. ***Frame check sequence (FCS)***

   It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

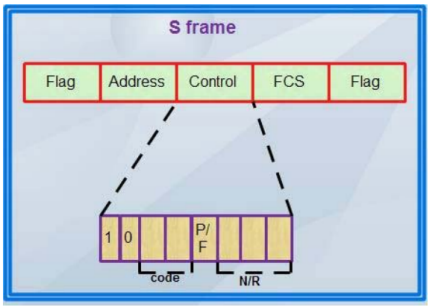
HDLC Frames Types

1. ***I-Frame***
    - Information Frame
    - It carries user data from network layer
    - It also has flow and error control information that is piggybacked



---

2. ***S-Frame***
    - Supervisory frame
    - It does not carry user data.
    - It is used for flow and eror control when piggybacking is not required



---

3. ***U-Frame***
    - Un-numbered frame
    - Does not carry user data.
    - Its used for link managemnet task
        - initialization
        - configuration
        - disconnect

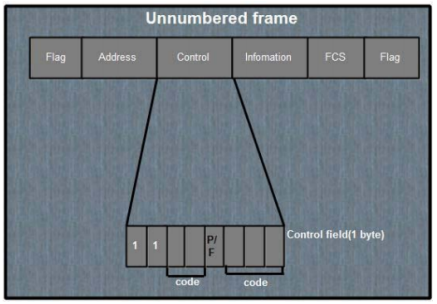


Table: Types of S-frame

Code	Command
00	RR Receive Ready
01	REJ Reject
10	RNR Receive Not Ready
11	SREJ Selective Reject

3.4 Point to Point (PPP)

> It is communication protocol of data link layer that is used to transmit multiprotocol data between two directly connected point to point computers.

It is a **byte-oriented protocol** that is widely used in broadband communications having heavy loads and high speeds.

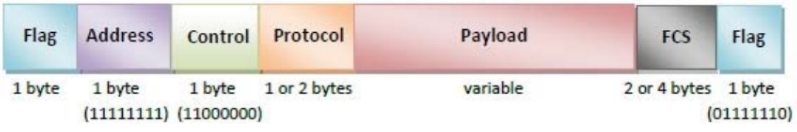
PPP defines/provides

- the format of the frame to be exchanged between devices
- how two devices negotiate the establishment of the link and the exchange of data
- how network layer data are encapsulated in the data link frame
- how two devices can authenticate each other
- multiple network layer services
- connection over multiple links
- Network address configuration

But, several services are missing for simplicity

- no flow control
- simple error control (detection and discard)
- no sophisticate addressing for multipoint configuration

PPP Frame (FAC PIF)



1. ***Flag***

   Marks the beginning and the end of the frame.

   The bit pattern of the flag is `01111110`

---

2. ***Address***

   It is set to `11111111` in case of broadcast.

---

3. ***Control***

Set to a constant value of `11000000`.
(No need because PPP has no flow control and limited error control)

4. ***Protocol***

   `1 or 2 bytes` that define the type of data contained in the payload field

5. ***Information (Payload)***

   This carries the data from the network layer.
   The maximum length of the payload field is 1500 bytes.
   However, this may be negotiated between the endpoints of communication.

6. ***FCS***

   It is a `2 byte or 4 bytes` frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

Components of PPP

1. ***Link Control Procol (LCP)***

   - It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission.
   - Detect and recovers from Link erros through monitoring and control message

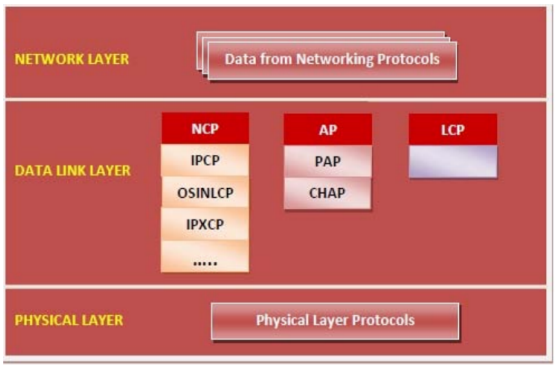
2. ***Network Control Protocol (NCP)***

   - These protocols are used for negotiating the parameters
   - Facilities for the network layer.

   Some of the NCPs of PPP are:
   o Internet Protocol Control Protocol (IPCP)
   o OSI Network Layer Control Protocol (OSINLCP)
   o Internetwork Packet Exchange Control Protocol (IPXCP)
   o DECnet Phase IV Control Protocol (DNCP)
   o NetBIOS Frames Control Protocol (NBFCP)
   o IPv6 Control Protocol (IPV6CP)

3. ***Authentication Protocols (AP)***

   - These protocols authenticate endpoints for use of services.
   - The two authentication protocols of PPP are:
     - Password Authentication Protocol (PAP)
     - Challenge Handshake Authentication Protocol (CHAP)



3.5 Channel Allocation Problem

When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users.

> Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.

There are user's quantity may vary every time the process takes place

If there are N number of users and channel is divided into
N equal-sized sub channels, Each user is assigned one portion.

If the number of users are small and don't vary at times, than ***Frequency Division Multiplexing*** can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.

Channel allocation schemes:

1. Static Channel Allocation

> A fixed portion of the *frequency channel* is allotted to each user.

For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment

It is not efficient to divide into fixed number of chunks.

```
T = 1/(U*C-L)

T(FDM) = N*T(1/U(C/N)-L/N)
```

Where,

```
T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time
```

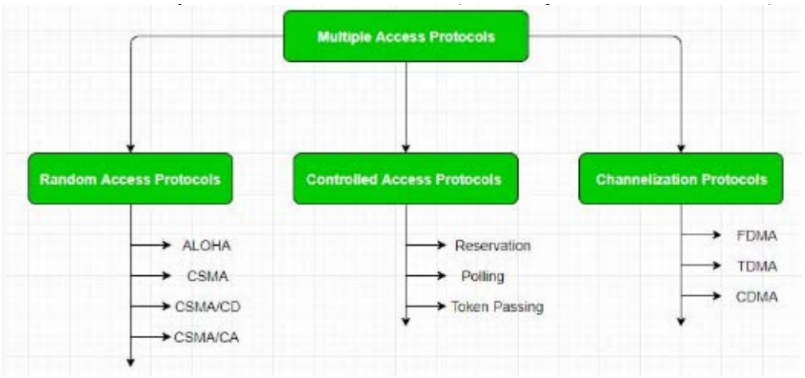
---

2. Dynamic Channel Allocation

Frequency bands are ***not permanently assigned*** to the users.
Instead channels are
allotted to users dynamically as needed, from a **central pool**.
The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimizes bandwidth usage and results is faster transmissions.

3.6 Multiple Access:



1.Random Access

- All devices compte for the channel access equally.
- Multiple devices share a single channel to transmit data.

Unlike controlled access methods, random access doesn't involve any scheduling or coordination between devices.
This means any device can transmit data whenever it has something to send, but it also increases the chance of collisions where multiple devices try to transmit simultaneously.

▼ Aloha

A simple protocol where devices transmit whenever they have data.
It's inefficient due to high collision rates.
Different versions are:

1. ***Pure Aloha***

> It is an un-slotted, decentralized, and simple to implement a protocol.

- **Transmission:**
  Stations can transmit data at any time whenever they have a packet ready.
- **Time:**
  Time is continuous and
  not synchronized between devices.
- **Collisions:**
  Due to random transmissions, collisions are highly likely.
  If a collision occurs, the data packets are corrupted and need to be retransmitted later.
- **Efficiency:**
  Pure Aloha has a low maximum throughput (around 18.4%) because of frequent collisions.

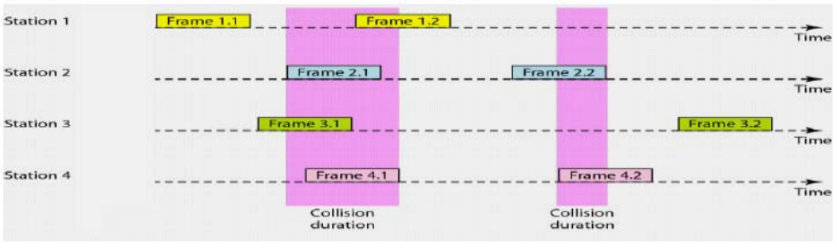


Figure 4-1. In pure ALOHA, frames are transmitted at completely arbitrary times.

2. ***Slotted Aloha***

   - **Transmission:**
     An improvement over Pure Aloha.
     Time is divided into
     fixed-sized intervals called **slots**.
     Stations can only transmit data at the beginning of a slot.
   - **Time:**
     Time is discrete and
     synchronized across all devices.
   - **Collisions:**
     By
     restricting transmissions to slots, Slotted Aloha reduces the probability of collisions compared to Pure Aloha.
     However,
     collisions can still happen if multiple stations try to transmit in the same slot.
   - **Efficiency:**
     Slotted Aloha offers better throughput (around 36.8%) compared to Pure Aloha due to fewer collisions.

Difference between Pure and Slotted

Feature	Pure Aloha	Slotted Aloha
Transmission Time	Any time	Beginning of a time slot
Time Synchronization	Not required	Globally synchronized
Collision Probability	High	Lower than Pure Aloha
Throughput	Low (around 18.4%)	Higher than Pure Aloha (around 36.8%)

▼ CSMA

- Carrier Sense Multiple Access
- Simple Rules for
  1. Listen before taking
  2. If someone else begins talking at the same time as you, stop talking
- A node should not send if another node is already sending(Carrier Sensing)
- If the channel is busy, they wait until it becomes available before transmitting.
  This reduces the chances of collisions where multiple devices transmit simultaneously, corrupting their data.

These methods define different strategies for stations to handle channel busy situations and attempt retransmission to reduce collisions.
Here are the three main CSMA persistence methods:

1. **I-Persistent (Non-preemptive):**
   - In this method, a **station** with data to send continuously **listens** (carrier sense) to the **channel**.
   - If the channel is busy, the station keeps listening without backing off (non-preemptive).
   - As soon as the channel becomes idle, the station immediately transmits its data (persistent).
   - This method is aggressive and can lead to high collision rates if many stations are contending for the channel.
2. **Non-Persistent:**

- This method takes a more cautious approach.
- A **station** with data **listens** to the **channel**.
- If the channel is busy, the **station waits** for a **random amount of time** before trying to listen again (backing off).
- Once the channel is idle, the station transmits its data immediately.
- This method reduces collisions compared to I-Persistent but can introduce delays due to random backoff times.

3. **P-Persistent:**
   - This method **combines elements of both I-Persistent and Non-Persistent.**
   - A station with **data listens to the channel.**
   - If the channel is busy, the station enters **a probabilistic (based on probability) mode.**
   - **With a probability of 'p'**, the station **transmits immediately** upon finding an idle slot (like 1-Persistent).
   - **With a probability of 1-p (q)**, the station **waits for a random amount of time** and tries listening again (like Non-Persistent).
   - The value of 'p' (persistence probability) can be adjusted to achieve a balance between reducing collisions and minimizing delays.

▼ CSMA/CD

- Carrier sense multiple access with collision detection
- A device with data listens to the channel.
- If the channel is free, it transmits data.
- While transmitting, the device also listens for collisions.
- If a collision is detected (another device transmits at the same time), both devices stop transmitting immediately.
- After a random amount of time, both devices try to retransmit their data again using CSMA/CD.

▼ CSMA/CA

- Carrier sense multiple access with collision avoidance
- A network protocol used in wireless networks for controlling access to a shared medium, like a radio channel.

The key difference between CSMA/CA and CSMA/CD (Collision Detection) is how they handle collisions, which occur when multiple devices try to transmit data at the same time.

- **Collision Avoidance:** Unlike CSMA/CD, which detects collisions after they happen, CSMA/CA tries to prevent them altogether. Here's how:
  - Once the channel is idle, the device waits for a short inter-frame gap before transmitting.
  - Some CSMA/CA protocols use a technique called exponential backoff. If a collision is detected (usually through failed acknowledgement from the receiver), the device waits for a random amount of time before retrying. This waiting time increases exponentially with each retry attempt, reducing the chance of multiple devices trying again at the same time

Difference between CSMA/CD and CSMA/CA

s.no	CSMA/CD	CSMA/CA
1	**CSMA / CD is effective after a collision.**	**Whereas CSMA / CA is effective before a collision.**
2	**CSMA / CD is used in wired networks.**	**CSMA / CA is commonly used in wireless networks.**
3	**It only reduces the recovery time.**	**Whereas CSMA/ CA minimizes the possibility of collision**
4	~~CSMA / CD resend the data frame whenever a conflict occurs.~~	~~Whereas CSMA / CA will first transmit the intent to send for data transmission.~~
5	**Collision detection**	**No collision detection**
6	**No Collision avoidance**	**Collision avoidance**
7	**Effience moderate**	**More Efficient**
8	**Eg: Ethernet**	**EG: Wi-Fi**

2. Controlled Access

> The stations consults each other to find which station has right to send.

It grants permission to send only one node at a time, to avoid collision of messages on the shared medium.

A station cannot send data unless it is authorized by the other stations.

Imagine a busy highway with only one lane. Without any rules, vehicles would constantly collide trying to enter the lane. Multiple access protocols are like traffic regulations for this single-lane highway, ensuring data packets from various devices don't collide and reach their destinations effectively.

Methods:

▼ Reservation

- It **avoids collisions** by letting devices **reserve a time slot** to transmit on a **shared medium.**
- This ensures predictable **performance** for **real-time applications** like video calls.
- **Time** is **divided** into **intervals with reservation frames** followed by data transmission periods.
- **Devices signal their intent to transmit during the reservation frame** using dedicated mini-slots to avoid collisions.
- While reservation offers predictability and fairness, it can be complex and introduce overhead compared to simpler protocols.

▼ Polling

Master and Slaves:
Polling
operates on the principle of a central controller, often called a master station, and multiple peripheral devices, known as slave stations.
The master station dictates communication flow.

Taking Turns:

The core concept of polling is like a roll call in a classroom.
The master station systematically queries each slave station in a predetermined order, asking if they have data to transmit.

There are two general polling policies:
i. Round Robin Order
ii. Priority Order

▼ Token Passing

A Station is authorized to send data when it receives a special frame called a Token.

Stations are arranged around a ring (physically or logically)

- A Token circulates around a ring
- If a station needs to send data ,it waits for the token
- The Station captures the token and sends one or more frames as long as the allocated time has not expired
- It releases the token to be used by the successor station

Difference between Reservaton, Polling and Token passing

Feature	Reservation Method	Polling Method	Token Passing Method
Access Mechanisum	Device “Reserve” Slots in advance	Primary device polls secondary device sequentially	Token circulates among devices,only device with token transmit
Efficiency	High for predictable,low collision	moderate for predictable,polling delay	High for predictable, no collision
Fairness	Fair with proper slot allocation	Unfair to high speed device if polling interval is fixed	high fair
Complexity	Requires coordiation and negotiation among device	Simple implementation but central device needed	Complex
EG	Ethernet	USB	Token ring network

3. Channelization

> The channel is divided into sub channels (time, frequency, code) assigned to different devices, allowing simulation transmission.

Methods

▼ FDMA

- Frequency Division Multiple Access
- **It is a channelization technique used to share a limited bandwidth among multiple users in a communication system**

Applications of FDMA:

- **Cellular Networks:** Earlier generations of cellular networks (like AMPS) employed FDMA for channelization.
- **Satellite Communication:** FDMA is used in some satellite communication systems to allocate channels for multiple users.
- **Radio and Television Broadcasting:** Different radio and TV channels occupy specific frequency bands, essentially using FDMA for channelization.

▼ TDMA

- Time division multiple access
- Unlike FDMA which divides the frequency spectrum, TDMA divides the available time on a single channel into slices, allowing multiple users to transmit data within their designated time slots.

Think of it this way:
Imagine a single lane highway with short time intervals instead of frequency sub-bands.Each user gets exclusive use of the lane for a brief period to transmit their data packet, like cars taking turns on the highway.

We can divide TDM into two different schemes:
synchronous and statistical.

▼ Synchronous TDM (STDM):

- **Fixed-size time slots:** The channel is divided into equal-sized time slots, and each user is assigned a specific slot in a predetermined frame.
- **Scheduled access:** Think of it like a round-robin schedule. Users transmit data only during their assigned slots, regardless of whether they have data or not. Unused slots are wasted bandwidth.
- **Simpler to implement:** Requires less complex logic compared to statistical TDM.
- **Suited for constant bit rate traffic:** Works well for applications with predictable data flow, like voice calls.

▼ Statistical TDM (STAM):

- **Dynamic time slot allocation:** Slots are allocated on demand based on a user's need for data transmission. There's no fixed assignment.
- **More efficient bandwidth usage:** Slots are only used when there's data to transmit, minimizing wasted bandwidth.
- **Increased complexity:** Requires additional logic to manage slot requests and allocation.
- **Better for bursty traffic:** Ideal for applications with variable data rates, like data transfer.

In a nutshell, synchronous TDM offers a simpler and more predictable channel access scheme, while statistical TDM provides more efficient bandwidth utilization for bursty traffic.

▼ CDMA

- Code division multiple access

Unlike FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access) which divide the channel into frequency bands or time slots respectively, **CDMA allows multiple users to share a single channel simultaneously.**

Here's how CDMA achieves this magic:

- **Spread Spectrum:** CDMA utilizes a technology called spread spectrum. In simple terms, user data is spread over a much wider bandwidth than the information itself. Imagine stretching a message across a large billboard instead of whispering it.
- **Unique Codes:** Each user is assigned a unique mathematical code, like a secret handshake. This code is used to spread the user's data across the entire channel bandwidth.
- **The Decoder Ring:** Receivers employ the same codes to differentiate between different users' signals. They act like decoder rings, filtering out unwanted signals and recovering the intended data based on the specific code.

Applications of CDMA:

- **Cellular Networks:** CDMA is used in some cellular network technologies like CDMA2000 and is a key component of 3G networks.
- **Wi-Fi:** Certain Wi-Fi standards utilize CDMA for improved capacity and interference resistance.
- **GPS:** CDMA is employed in the coarse acquisition code (C/A code) of the Global Positioning System (GPS) to distinguish GPS signals from background noise.

Difference between FDMA, TDMA, CDMA

Feature	FDMA	TDMA	CDMA
Full form	Frequency division multiple access	Time divison multiple access	Code division multiple access
Multiple users transmit	No	No	No
Synchronization require	No	Yes	No
Complexity	Moderate	Moderate	High
Fairness	Limited	Moderate	High
Interference	Sensitive	Moderate	Resistence
EG:	Analog Tv	GSM	3G, 4G

3.7 Wired LAN: Ethernet Standards and FDDI

Ethernet Standards

The Ethernet standards come under the **IEEE 802 section** which deal with **local area networks** and **metropolitan area networks.**

In particular, **IEEE 802.3 defines Ethernet.**

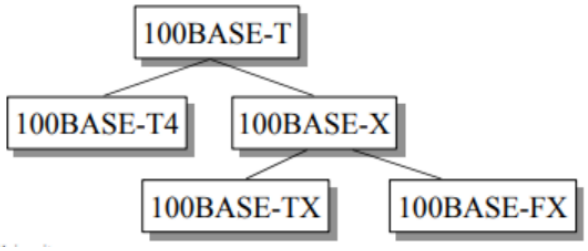
The different standards with their numbers are outlined in the table below:

Standard Ethernet Code

Guide to Ethernet Coding

10	at beginning means the netowkr operates at 10mbps
BASE	means the type of signaling used is baseband
2 or 5	at the end indicates the **maximum cable length in meters.**
T	the end stands for twisted-pair cable
X	at the end stands for full duplex capable cable
FL	at the end stands for fiber optic cable

Some of Ethernet version numbering:



- 10BASE5: 10 Mb/s over coaxial cable (ThickWire)
- 10BROAD36: 10 Mb/s over broadband cable, 3600 m max segments
- 10BASE5: 1 Mb/s over 2 pairs of UTP
- 10BASE2: 10 Mb/s over thin RG58 coaxial cable (ThinWire), 185 m max segments
- 10BASE-T: 10 Mb/s over 2 pairs of UTP
- 10BASE-FL: 10 Mb/s fiber optic point-to-point link
- 10BASE-FB: 10 Mb/s fiber optic backbone (between repeaters). Also, known as synchronous Ethernet.

Baisc Frame Format

- **PREAMBLE –** Ethernet frame starts (PRE).
- ***Start frame delimiter (SFD).*** This field (1 byte: 10101011) signals the beginning
- of the frame.
- ***Type.*** This field defines the upper-layer protocol whose packet is encapsulated in
- the frame.
- ***Data.*** This field carries data encapsulated from the upper-layer protocols. For example, a datagram has a field that defines the
- length(padding) of the data.
- **Cyclic Redundancy Check (CRC):** The last field contains error detection information

---

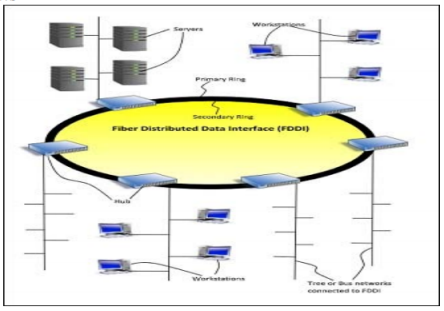
Fiber Distributed Data Interface (FDDI)

> It is a set of ANSI and ISO standards for transmission of data in LAN over fiber optic cables.

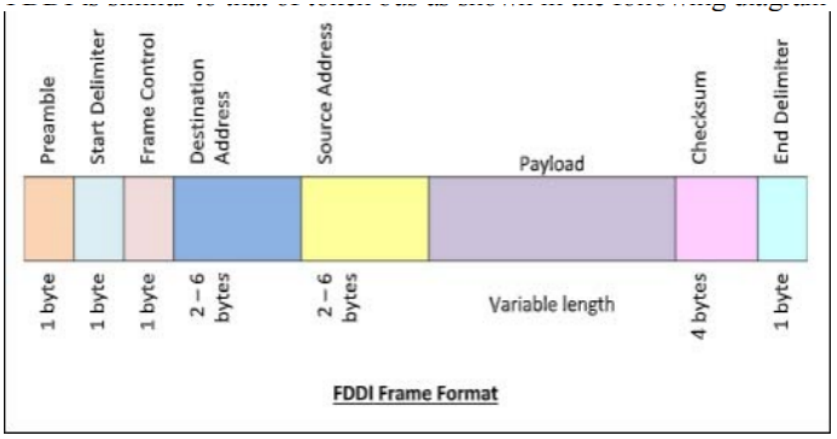
Features

- FDDI uses optical fiber as its physical medium.
- It operates in the physical and (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard
- It can also be used as a backbone for a wide area network (WAN)

The following diagram shows FDDI –



Frame Format



Preamble: 1 byte for synchronization.

Start Delimiter: 1 byte that marks the beginning of the frame.

Frame Control: 1 byte that specifies whether this is a data frame or control frame.

Destination Address: 2-6 bytes that specifies address of destination station.

Source Address: 2-6 bytes that specifies address of source station.

Payload: A variable length field that carries the data from the network layer.

Checksum: 4 bytes frame check sequence for error detection.

End Delimiter: 1 byte that marks the end of the frame.

3.8 Wireless LAN: IEEE 802.11x and Bluetooth Standards

802.11x

> IEEE 802.11 standard for defining communication over a wireless LAN (WLAN)

- 802.11, commonly known **as Wi-Fi**
- **Wi-fi is an over-the-air interface between two wireless clients**

IEEE 802.11 defines two MAC sub-layers :-

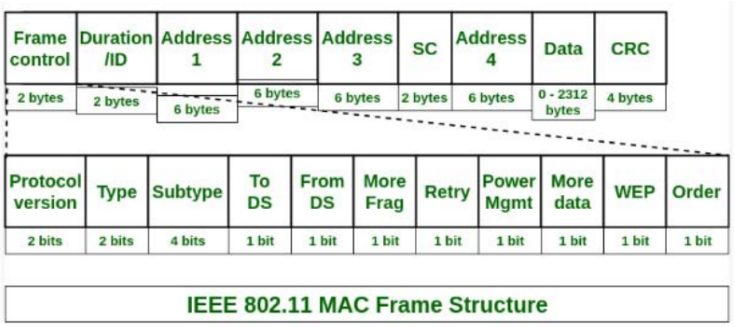
▼ **Distributed Coordination Function (DCF) –**

DCF uses CSMA/CD as access method as wireless LAN can’t implement CSMA/CD. It only offers asynchronous service.

▼ **Point Coordination Function (PCF) –**

PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

Frame Format



1. **D .** It stands for **duration** and is of 2 bytes. This field defines the duration for which the frame and its
2. **D .** It stands for **duration** and is of 2 bytes. This field defines the duration for which the frame and its acknowledgement will occupy the channel. It is also used to set the value of NA V for other stations.
3. **Addresses.** There are 4 address fields of 6 bytes length. These four addresses represent source, destination, source base station and destination base station.
4. **Sequence Control (SC).** This 2 byte field defines the sequence number of frame to be used in flow control.
5. **Frame body**. This field can be between 0 and 2312 bytes. It contains the information.
6. **Frame Check Sequence (FCS)**. This field is 4 bytes long and contains error detection sequence.

Blue Tooth

- **Personal Area Networks (PANs):**
  Bluetooth creates PANs, which are small networks connecting devices within a short distance (typically up to 10 meters).
  This allows computers to connect with peripherals like wireless keyboards, mice, headsets, or printers without wires.
- **Data transfer:**
  Bluetooth enables data transfer between devices like sharing files between a computer and a phone.
- **Internet of Things (IoT):**
  Bluetooth is a key technology in IoT for connecting various devices like sensors or wearables to a computer or a central hub within a short range.

Overall, Bluetooth acts as a useful supplement to traditional computer networks, providing a way to connect devices in close proximity for data exchange and peripheral use.

Types of Bluetooth Wireless Technology

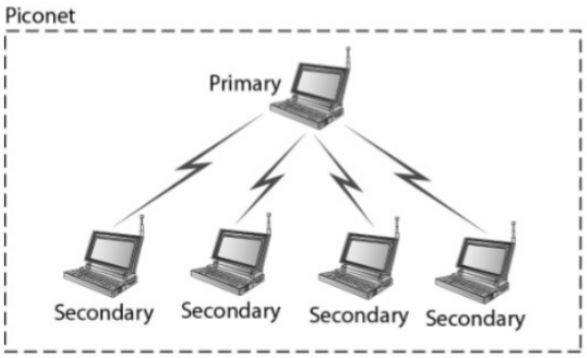
 Depending on the power consumption and range of the device, there are 3 Bluetooth Classes as:

- **Class 1:**
  - Highest power consumption (around 100 mW)
  - Longest range (up to 100 meters)
  - Less common due to higher power usage
- **Class 2:**
  - Medium power consumption (around 2.5 mW)
  - Standard range (up to 10 meters)
  - Most commonly used in devices like smartphones and laptops
- **Class 3:**
  - Lowest power consumption (around 1 mW)
  - Shortest range (up to 1 meter)
  - Least common, often used in wearable devices like headsets

---

Bluetooth defines two types of network topology:

1. **Piconet:** This is the most common Bluetooth network structure. It resembles a **star topology** with:
   - One **master device** that controls communication and data flow.
   - Up to seven **slave devices** that connect and communicate with the master device.
   - Slave devices cannot directly communicate with each other, only with the master.



---

2. **Scatternet:**

- This is a more complex network formed by connecting multiple piconets.
- It allows some devices to act as a master in one piconet and a slave in another, enabling more flexible communication between a larger number of devices.

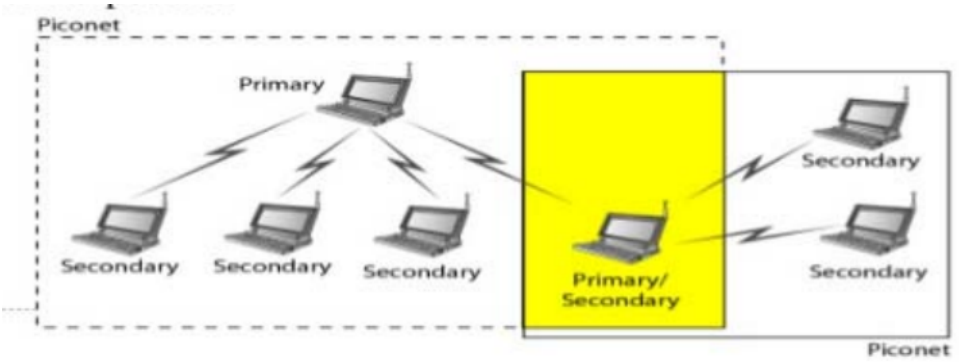


Figure : Scatternet (combine of Piconet)

Blue Tooth Link Security and Algorithm parameters

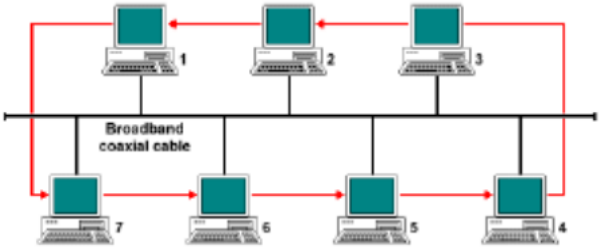
Bluetooth Link Security

- **Elements:**
  - ✓ Authentication – verify claimed identity
  - ✓ Encryption – privacy
  - ✓ Key management and usage
- **Security algorithm parameters:**
  - ✓ Unit address
  - ✓ Secret authentication key (128 bits key)
  - ✓ Secret privacy key (4-128 bits secret key)
  - ✓ Random number

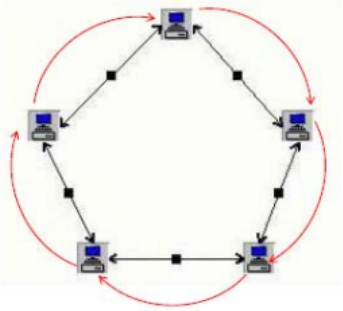
3.9 Token Bus, Token Ring and Virtual LAN

802.4 Token Bus

- Token Bus protocol use token-passing method on a bus topology.
- A special packet called a token is passed from station to station and only the token holder is permitted to transmit packets onto the LAN.
- No collisions can occur with this protocol
- When a station is done transmitting its packets, it passes the token to the "next" station
- A station can hold the token for only a certain amount of time before it must pass it on - even if it has not completed transmitting all of its data.



802.5 Token Ring



- It is another token passing access method, but for a ring topology.
- A ring topology consists of a series of individual point-to-point links that form a circle
- A token is passed from station to station in one direction around the ring, and only the station holding the token can transmit packets onto the ring.
- Data packets travel in only one direction around the ring
- When a station receives a packet addressed to it, it copies the packet and puts it back on the ring
- When the originating station receives the packet, it removes the packet.

Virtual LANs

In computer networking, a Virtual LAN (VLAN) acts like a virtualized network segment within a physical LAN. It creates a logical grouping of devices on a network, regardless of their physical location. Here's a deeper dive into VLANs:

Concept:

- A physical LAN operates on Layer 2 (Data Link Layer) of the OSI model, where devices communicate based on MAC addresses. Traditionally, all devices on a LAN can see and potentially communicate with each other's broadcasts.
- VLANs segment this broadcast domain. They logically group devices on a single physical LAN into separate broadcast domains, even if they're physically connected to the same switch.

Benefits of VLANs:

- **Improved Security:** By isolating broadcast traffic, VLANs restrict unauthorized devices from seeing sensitive data traveling on other VLANs. This enhances network security.
- **Enhanced Performance:** Broadcast traffic is limited within each VLAN, reducing congestion on the network and improving overall performance for devices within a particular VLAN.
- **Simplified Network Management:** VLANs allow for easier network administration by grouping devices based on department, function, or security needs. This simplifies tasks like troubleshooting and access control.

Implementation:

- VLANs are typically configured on network switches. Switches can be programmed to identify devices that belong to specific VLANs based on various criteria like:
  - **Port-based VLANs:** Assigning specific switch ports to VLANs.
  - **MAC address-based VLANs:** Assigning VLAN membership based on a device's MAC address.
  - **802.1X authentication:** Using a more secure method where devices need to authenticate to join a VLAN.

Applications of VLANs:

- **Departmental Segmentation:** Isolating traffic from different departments (e.g., Finance, Marketing) to improve security and network performance.
- **Guest Network:** Creating a separate VLAN for guest users to restrict their access to sensitive resources on the main network.
- **IoT Devices:** Grouping Internet of Things (IoT) devices on a dedicated VLAN for better management and security.

Overall, VLANs are a valuable tool for network administrators to create secure, efficient, and manageable network environments.

Types of VLAN

- Static VLANs are manually assigned to ports on a switch
- Static VLANs are the most common method of assigning ports to VLANs, with devices automatically assuming the VLAN membership of the port they are attached to.

- dynamic VLANs allow membership based on the MAC address of the device connected to the switch port.
- Dynamic VLANs query a database within the switch for VLAN membership and are configured using a VLAN Membership Policy Server (VMPS).
