Unit -3 Error Detection correction and Wireless communication

Error: A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

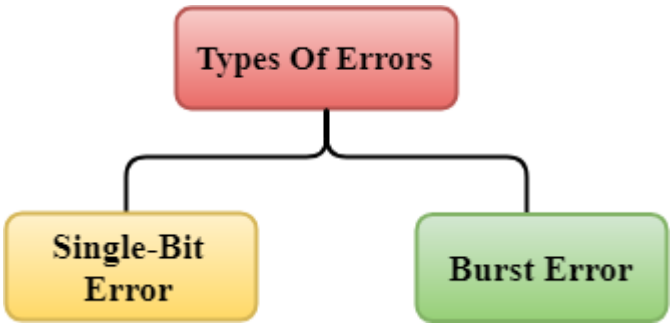
Redundancy We need to send some extra bits with our data to detect or correct the errors. (These redundant bits are added by the sender and removed by receiver. Error control mechanism may involve two possible ways:

1. Error detection: We will check if any error has occurred or not. We are not interested in the number of errors.

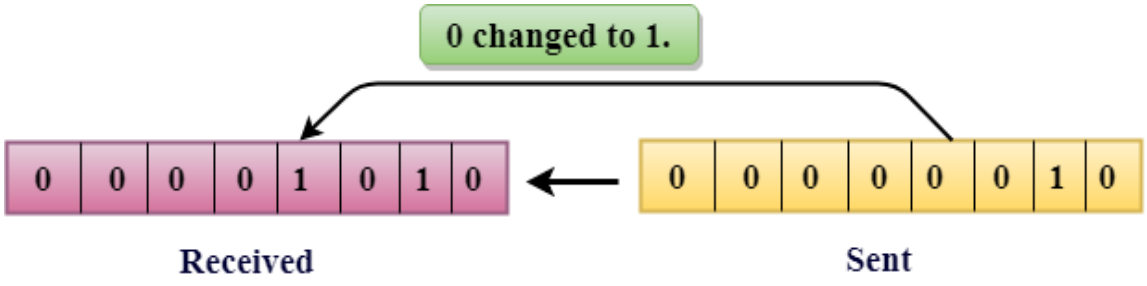
2. Error correction: We have to check exact number of bits that are corrupted and their location in the message.

Types Of Errors

Errors can be classified into two categories



Single-Bit Error: The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



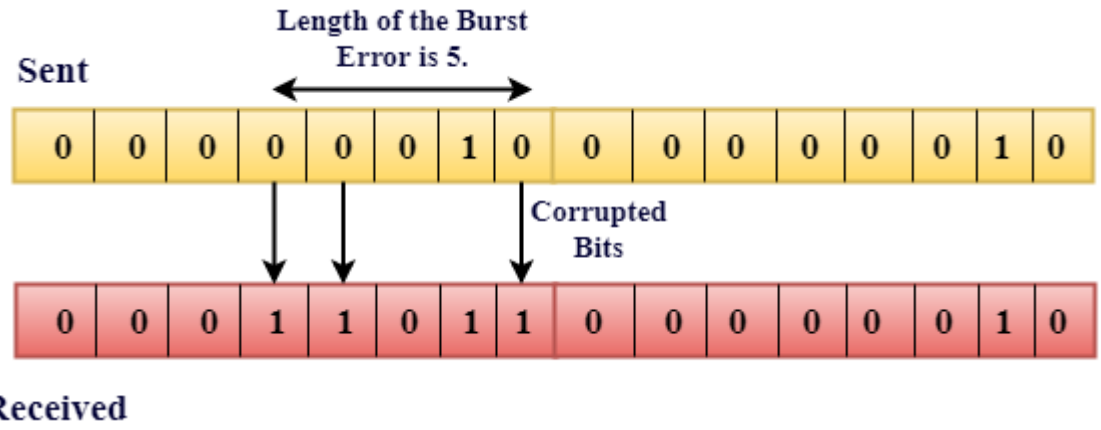
In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1. Single-Bit Error does not appear more likely in Serial Data Transmission. For example,

Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s. Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



Error Detecting Techniques:

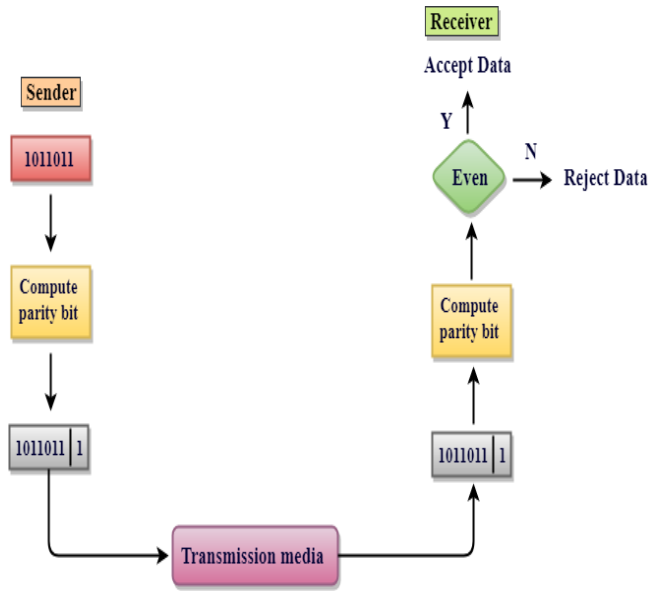
The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

- single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



Parity Check Example:

Consider the data unit to be transmitted is 1001001 and even parity is used. Then,

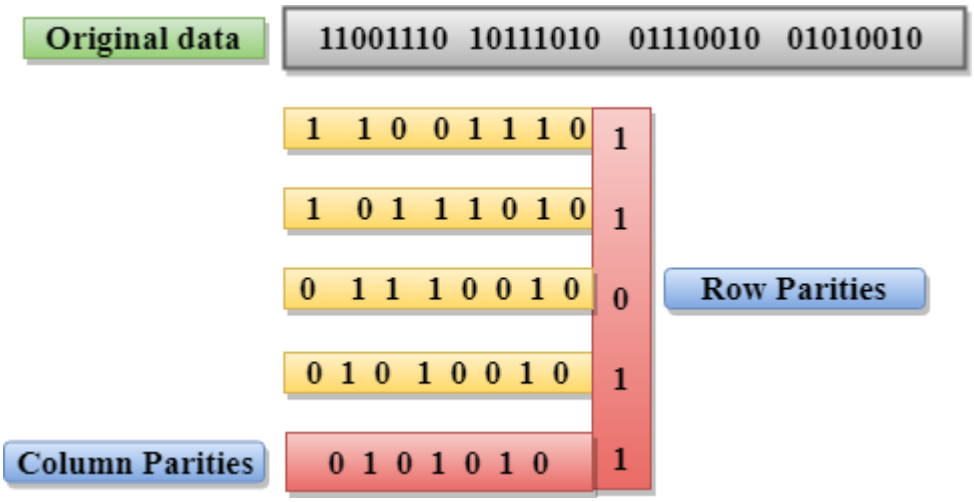
- Total number of 1's in the data unit is counted.
- Total number of 1's in the data unit = 3.
- Clearly, even parity is used and total number of 1's is odd.
- So, parity bit = 1 is added to the data unit to make total number of 1's even.
- Then, the code word 10010011 is transmitted to the receiver.

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.

Two-Dimensional Parity Check/Longitudinal Redundancy Check(LRC):

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

- if two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

A Checksum is an error detection technique based on the concept of redundancy.

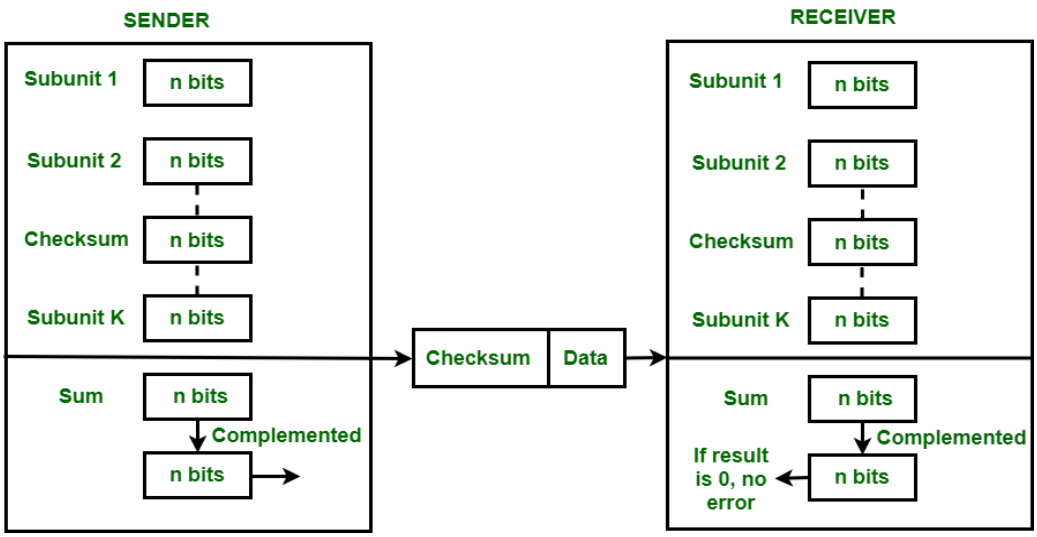
It is divided into two parts:

Checksum Generator

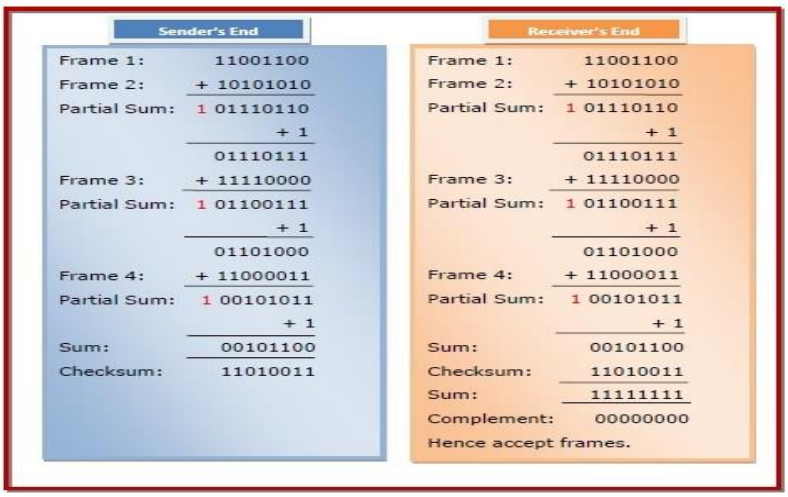
A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.



Example:



Cyclic Redundancy Check (CRC):

CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

o In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.

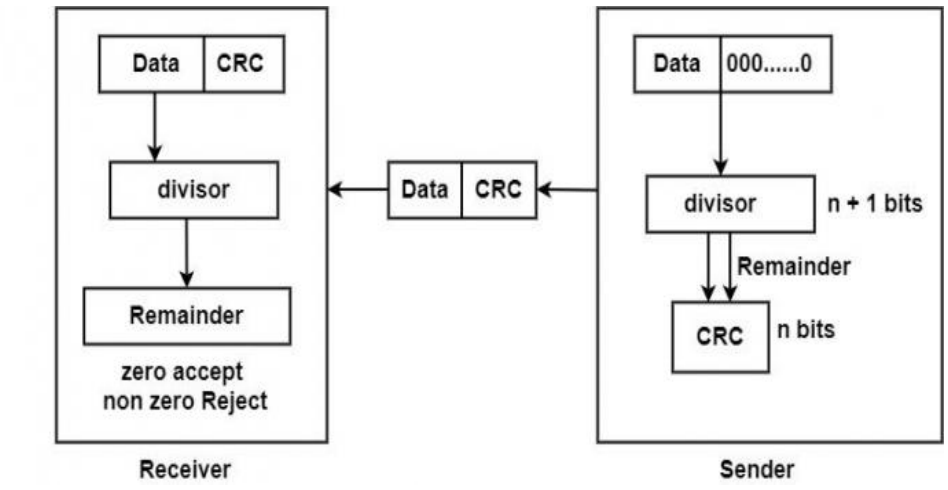
o Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

o Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

o The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.



Let's understand this concept through an example:

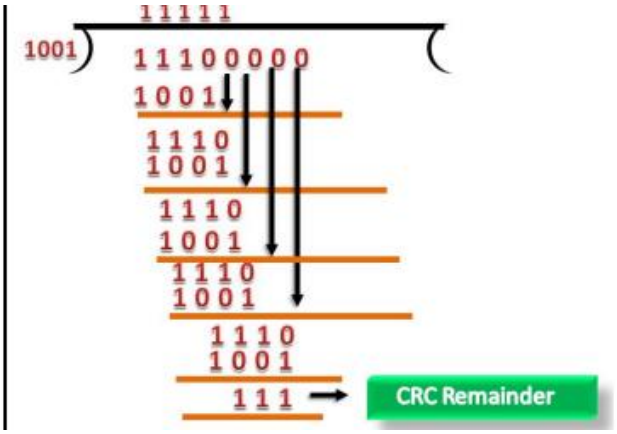
Suppose the original data is 11100 and divisor is 1001. CRC Generator o A CRC generator uses a modulo-2 division.

Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.

o Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.

o The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.

o CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



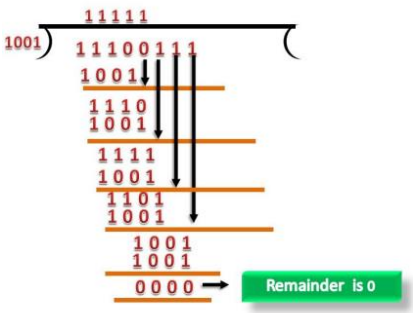
CRC Checker

o The functionality of the CRC checker is similar to the CRC generator.

o When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.

o A string is divided by the same divisor, i.e., 1001.

o In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted



Error Correction Technique:

Hamming Code:

Wireless Communication

IEEE Standards:

IEEE 802 an Institute of Electrical and Electronics Engineers (IEEE) standard set that covers the physical and data link layers of the Open Systems Interconnection (OSI) model. It defines standards and protocols for local area networks (WLAN), metropolitan area networks (MAN) and wireless networks.

A set of network standards developed by the IEEE they include:

IEEE 802.1: Standards related to network management.

IEEE 802.2: General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the logical link control (LLC) layer and the media access control (MAC) layer.

IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.

EEE 802.4: Defines the MAC layer for bus networks that use a token passing mechanism (token bus networks).

IEEE 802.5: Defines the MAC layer for token-ring networks.

IEEE 802.6: Standard for Metropolitan Area Networks (MANs).

IEEE 802.11: Wireless Network Standards, Wireless Local area network.

Wireless Local Area Network(WLAN)/ Wifi/ 802.11

- **WLAN** stands for **Wireless Local Area Network.**
- The performance of WLAN is high compared to other wireless networks.
- the coverage of WLAN is within a campus or building or that tech park. It is used in the mobile propagation of wired networks.
- The standards of WLAN are HiperLAN, Wi-Fi, and IEEE 802.11.

- the offers service to the desktop laptop, mobile application, and all the devices that work on the Internet.

802.11 Architecture:

The 802.11architecture defines two types of services:

1. Basic services set (BSS)

2. Extended Service Set (ESS)

1. Basic Services Set (BSS):

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

• The use of access point is optional.

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

• The BSS in which an access point is present is known as an infrastructure network.

2. Extend Service Set (ESS):

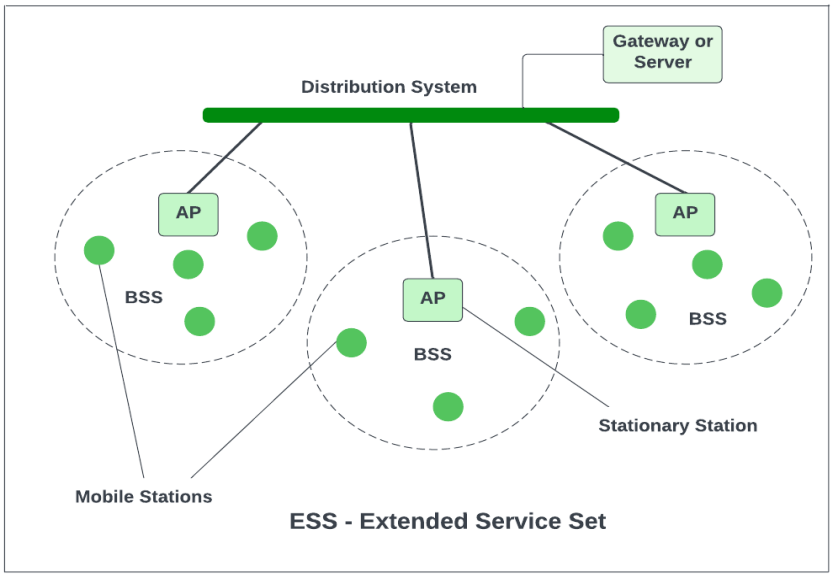
An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).

These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.

There are two types of stations in ESS:

(i) **Mobile stations**: These are normal stations inside a BSS.

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



Advantages of WLAN

1. Installation speed and simplicity.
2. Installation flexibility.
3. Reduced cost of ownership.
4. Reliability.

Disadvantages of WLAN

1. Installation speed and simplicity.
2. Installation flexibility.
3. Reduced cost of ownership.
4. Reliability.

Bluetooth:

- Bluetooth is universal for short-range wireless voice and data communication. It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances.
- This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific, and medical (ISM) band from 2.4 GHz to 2.485 GHz.
- Maximum devices that can be connected at the same time are 7. Bluetooth ranges up to 10 meters. It provides data rates up to 1 Mbps or 3 Mbps depending upon the version.

- A Bluetooth network is called a piconet and a collection of interconnected piconets is called scatternet. Bluetooth is Wireless.

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet 2. Scatternet

1. Piconet:

• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

• Thus, piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.

• There can be only one primary or master station in each piconet.

The communication between the primary and the secondary can be one-to-one or one-to-many/.

communication is between master and a slave. Salve-slave communication is not possible.

Scatternet:

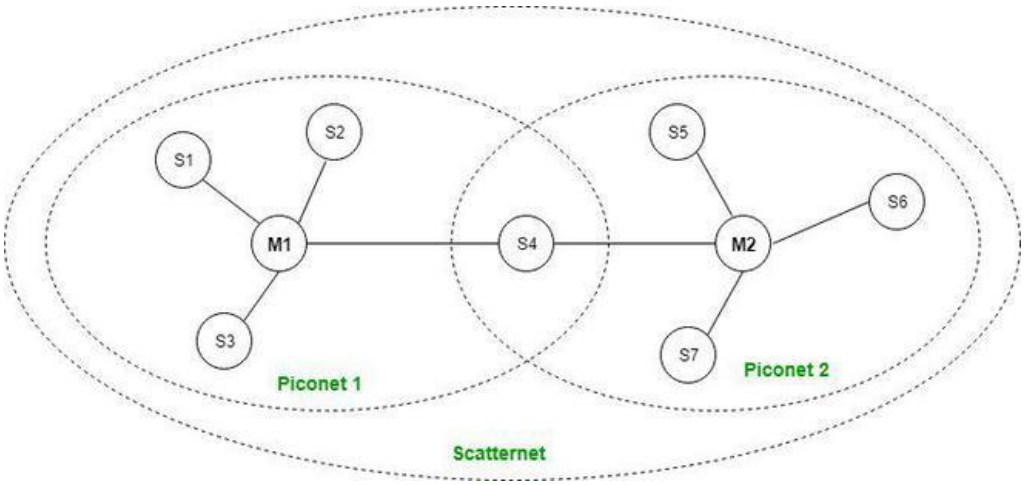
•Scattemet is formed by combining various piconets.

• A slave in one piconet can act as a master or primary in other piconet.

• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

• Thus a station can be a member of two piconets.

• A station cannot be a master in two piconets



Advantage:

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

- It can be used in laptops, and in wireless PCs, printers.
- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wirelessly to mobile phone.

Mobile generation:

1G,2G,3G,4,G,5G: Simply, the "G" stands for "GENERATION".

When connected to internet, the speed of internet depends on the signal strength that has been shown in alphabets like 2G, 3G, 4G etc. right next to the signal bar on home screen of mobile phone. Each Generation is defined as a set of telephone network standards, which detail the technological implementation of particular mobile phone system.

1G (1st Generation):

- First-time calling was introduced in mobile systems.
- It used analog signals.

- The coverage area was small.
- No roaming support between various operators.
- Low sound quality.
- Speed:- 2.4 kbps.

2G (2nd Generation) :

- Shifted from analog to digital.
- It supported voice and SMS both.
- Supported all 4 sectors of the wireless industry namely Digital cellular, Mobile Data, PCS, WLAN,
- Moderate mobile data service.
- 2G WLAN provided a high data rate & large area coverage.
- Speed:- 64 kbps.

2.5G came after 2G which used the concept of GPRS. Streaming was also introduced and mail services too. Then came 2.75G or EDGE which was faster in providing services than 2.5G. It gave faster internet speed up to 128kbps and also used edge connection.

3G (3rd Generation):

- The Internet system was improved.
- Better system and capacity.
- Offers high-speed wireless internet.
- The connection used was UMTS and WCMA.
- Speed:- 2mbps.

4G (4th Generation):

- IP-based protocols.
- LTE (Long term evaluation) was mainly for the internet.

- Vo-LTE (Voice over LTE) is for both voice and the internet.
- Freedom and flexibility to select any desired service with reasonable QoS.
- High usability.
- Supports multimedia service at a low transmission cost.
- HD Quality Streaming.
- Speed:-100mbps.

5G (5th Generation):

- It is yet to come in many countries but here are some notable points about 5G. • Higher data rates.

- Connectivity will be more fast and more secure,
- Data Latency will be reduced to a great level.
- Massive network capacity.
- It is 30 times faster than 4G.
- There would be more flexibility in the network.

Difference between VRC and LRC :

S.No.	Vertical Redundancy Check (VRC)	Longitudinal Redundancy Check (LRC)
1.	It stands for Vertical Redundancy Check.	It stands for Longitudinal Redundancy Check.
2.	In this redundant bit called parity bit is added to each data unit.	In this redundant row of bits is added to the whole block.
3.	VRC can detect single bit errors.	LRC can detect burst errors.
4.	It is also known as parity checker.	It is also known as 2-D parity checker.
5.	The advantage of using VRC is that it can checks all single bit errors but can check odd parity only in the case of change of odd bits.	The advantage of using LRC over VRC is that it can check all the burst errors.
6.	It is not capable of checking the burst error in case of change of bits is even.	If two bits in data unit is damaged and also in other data unit the same bits are damaged at same position, then it is not capable of detecting such kind of error.