Chap 3: Error Detection, Correction and Wireless Communication

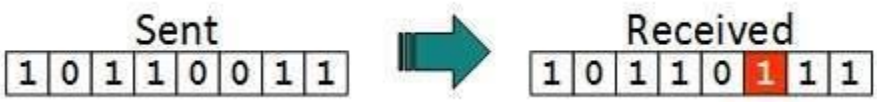
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

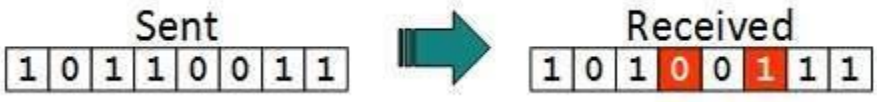
There may be three types of errors:

- **Single bit error**



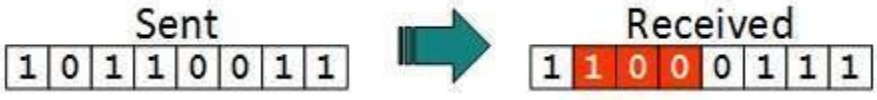
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Redundancy:

- Redundancy The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data.
- These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.
- The concept of including extra information in the transmission for error detection is a good one.
- But instead of repeating the entire data stream, a shorter group of bits may be appended to the end of each unit.
- This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.

Error Detection

Some popular techniques for error detection are:

1. Simple Parity check

2. Two-dimensional Parity check

A. VRC

B. LRC

3. Checksum

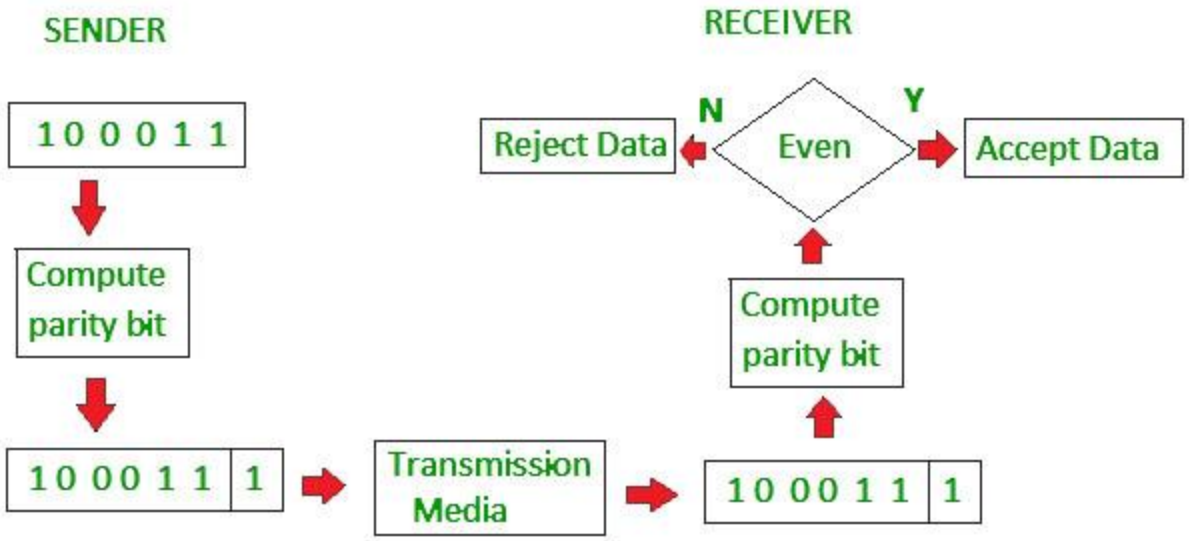
4. Cyclic redundancy check Parity Check

1. Simple Parity check

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

- 1 is added to the block if it contains odd number of 1’s, and
- 0 is added if it contains even number of 1’s

This scheme makes the total number of 1’s even, that is why it is called even parity checking.



2. Two-dimensional Parity check

Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

Original Data

10011001	11100010	00100100	10000100

Row parities

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

Column parities

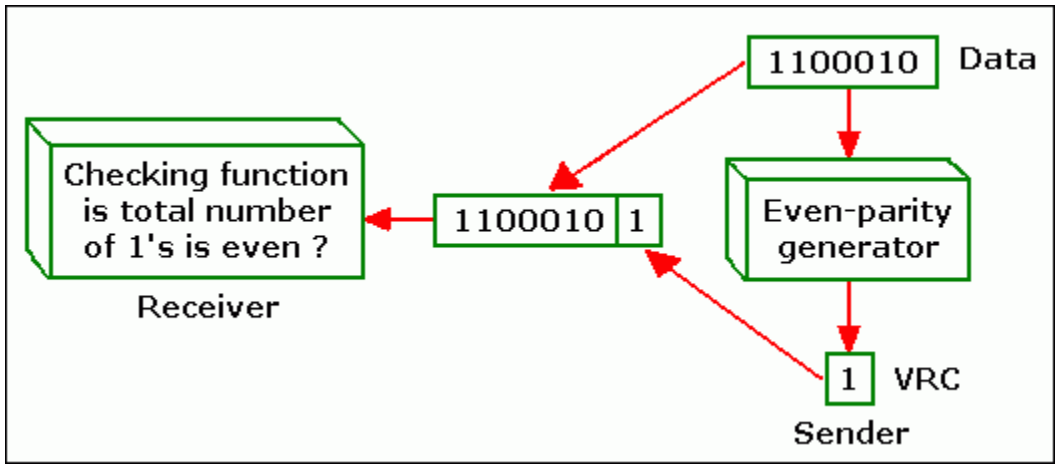
100110010	111000100	001001000	100001000	110110110

Data to be sent

A. Vertical Redundancy Check (VRC)

- Most common and inexpensive mechanism error detection which also called parity check.
- A redundant bit (parity bit) is appended to every data unit so that the total number of 1s in the unit becomes even, if there is even-parity check used.
- There are even-parity check and odd-parity check. For odd-parity check, the total number of 1s in the unit is odd.

Suppose we want to transmit the binary data unit 1100001, adding the number of 1s gives us 3, an odd number. Before transmitting, a parity generator counts the 1s and appends the parity bit (a 1 in this case) to the end. The total number of 1 becomes 4 now (even number). The system now transmits the entire appended unit across the network link.

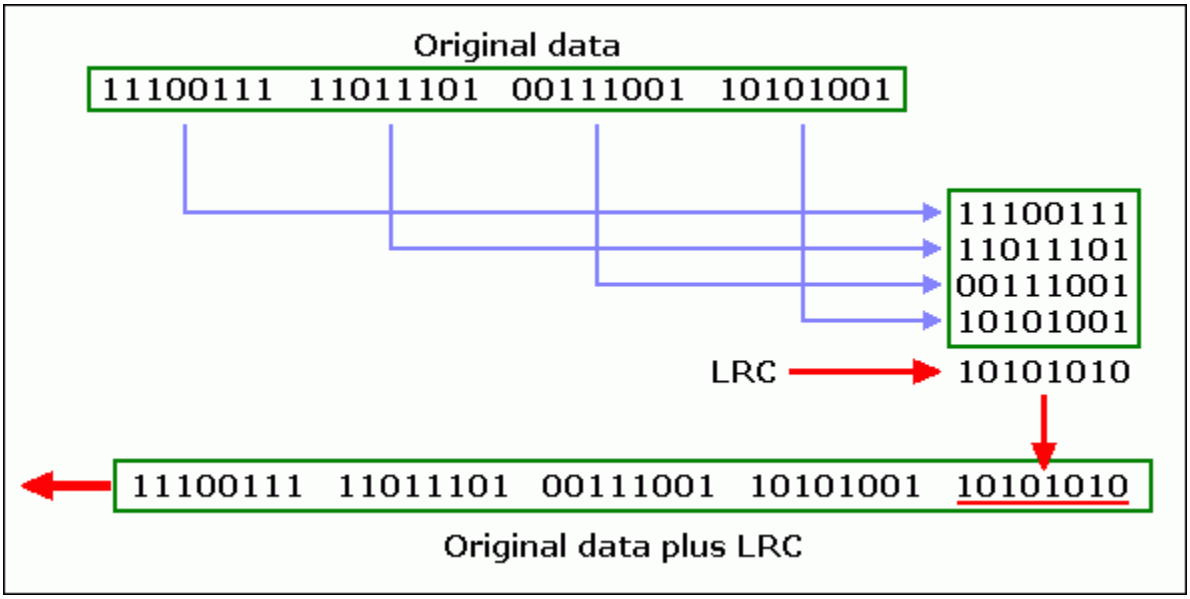


- When the data unit is reached its destination, the receiver puts all eight bits through an even-parity checking function. If the receiver sees 11100001, it counts and gets four 1s, an even number.
- But if the receiver sees 11100101, or total number of 1s is odd. The receiver knows that an error has been occurred into the data somewhere and therefore rejects the whole unit.
- For the odd-parity checking, the principle is same but the calculation is different.
- The advantages of VRC are it can detect all single-bit errors. It also can detect burst errors as long as the total number of bits changed is odd (1,3,5, etc). The same holds true for any odd number of errors.

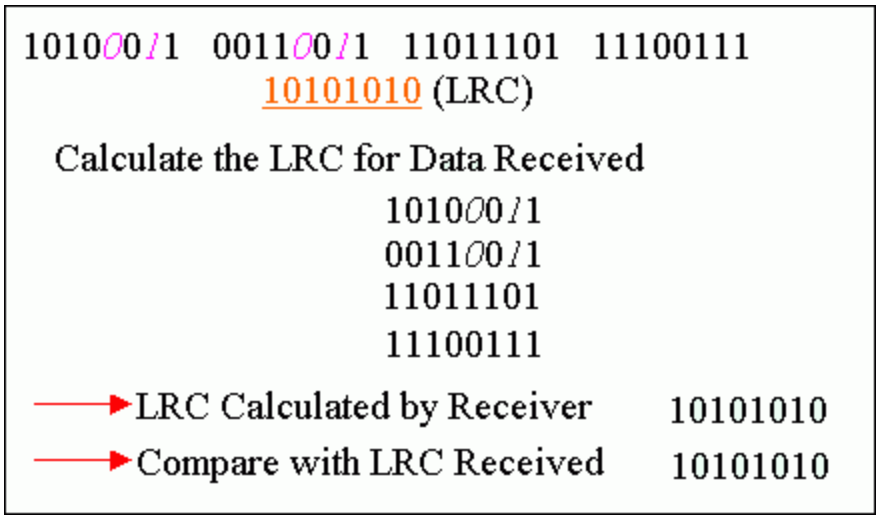
- The limitation is it cannot detect errors where the total number of bits changed is even, where the two bits of the data unit are changed. In this case, the total number of 1s is still even. The VRC checker will add them and return an even number although the data unit contains two errors. Then the unit will pass a parity check even through the data unit is damaged. The same holds true for any even number of errors.

B. Longitudinal Redundancy Check (LRC)

- In this error detection method, a block of bits is organized in a table with rows and columns. Then the parity bit for each column is calculated and a new row of eight bits, which are the parity bits for the whole block, is created. After that the new calculated parity bits are attached to the original data and sends to the receiver.



- LRC increases the likelihood of detecting burst error. An LRC of *n* bits can easily detects a burst error of *n* bits.
- However, if two bits in one data unit are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.

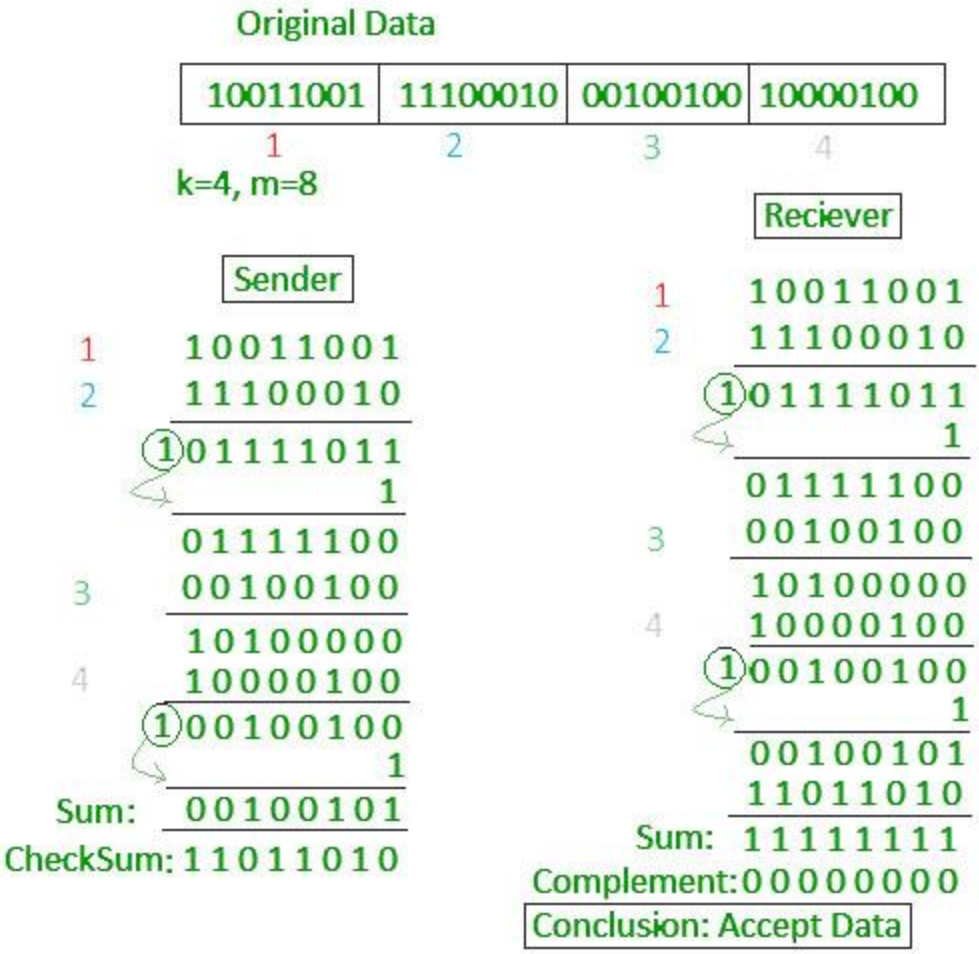


- How LRC Fail to Detect the Burst Noise

- Notice that although the 5th bit and the 7th bit for 1st and 2nd data unit have been changed but the LRC calculated by receiver is still the same as the LRC received. Thus the receiver checker cannot detect this burst error.

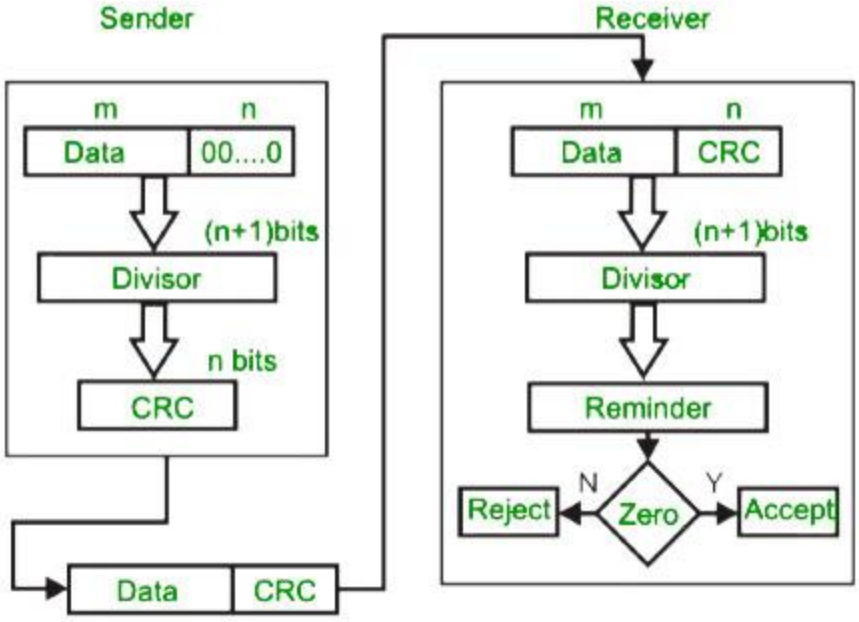
3. Checksum

- In checksum error detection scheme, the data is divided into k segments each of m bits.
- 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.

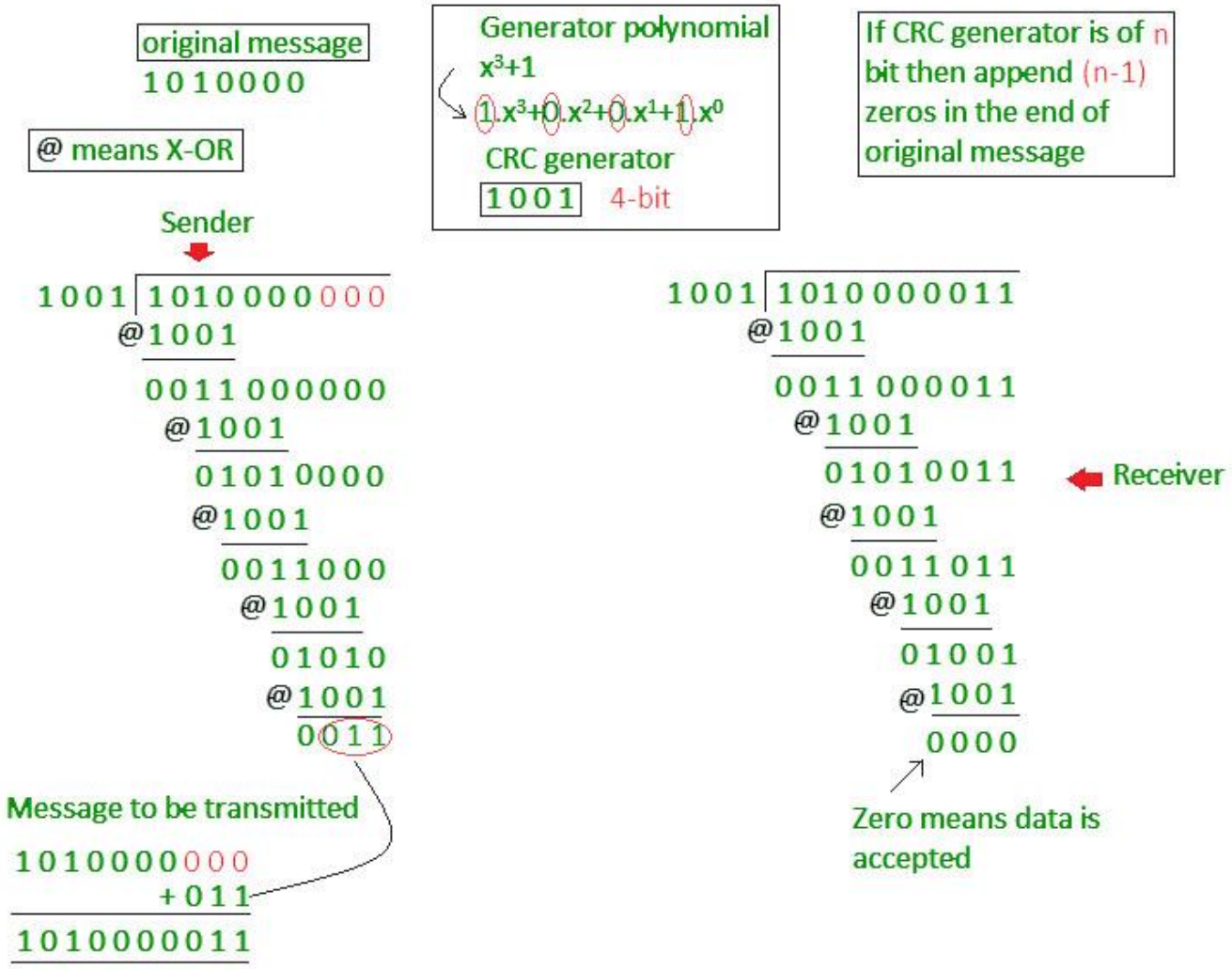


4. Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check 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.


Sender
Receiver
m
n
Data
00....0
(n+1)bits
Divisor
n bits
CRC
Data
CRC
m
n
Data
CRC
(n+1)bits
Divisor
Reminder
N
Y
Reject
Zero
Accept

Example :

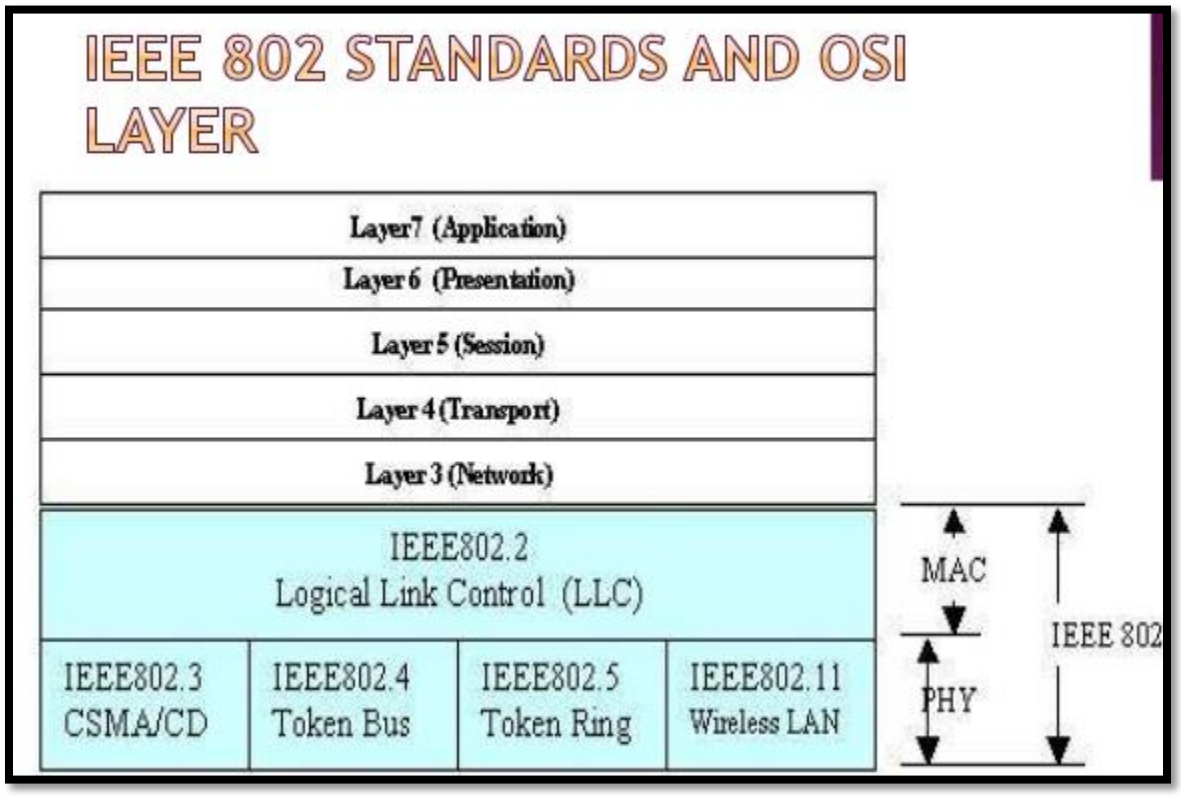


Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

IEEE 802 Standards



IEEE 802.1

IEEE 802.1 handles the architecture, security, management and internetworking of local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN) standardized by IEEE 802.

The following are key IEEE 802.1 tasks:

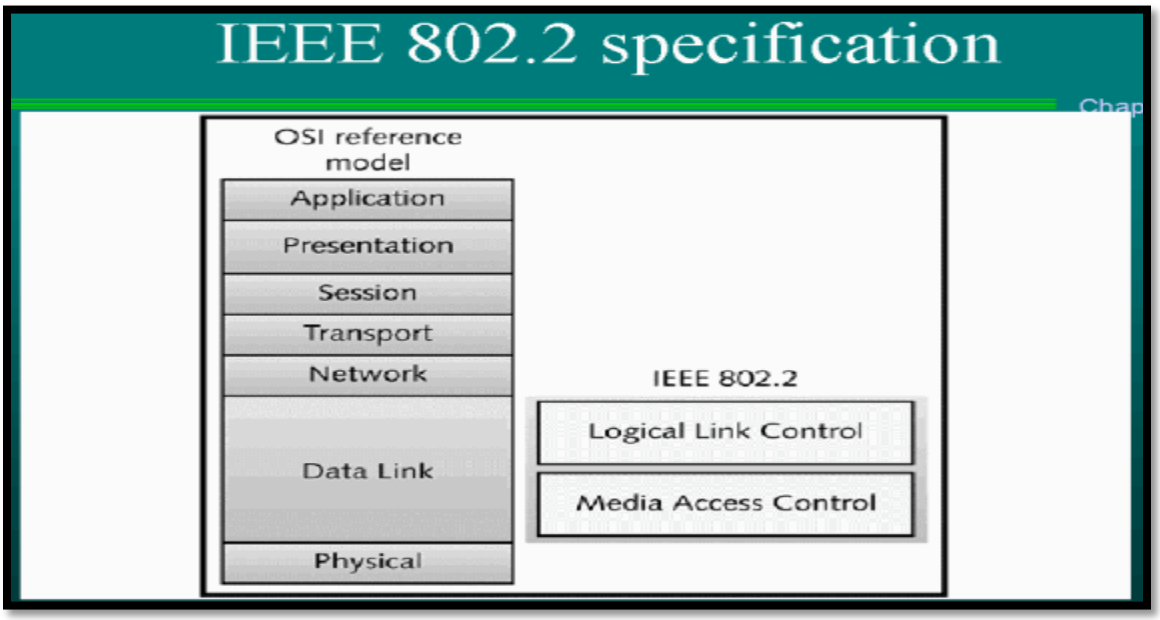
- Designs and implements standards that regulate network management practices
- Provides services, including LAN/MAN management, media access control (MAC) bridging, data encryption/encoding and network traffic management

IEEE 802.1 is comprised of four groups that focus on different standards and policies in the following areas:

- Internetworking
- Audio/video (A/V) bridging
- Data center bridging
- Security

The Internetworking group handles overall architecture, link aggregation, protocol addressing, network path identification/calculation and other technical practices and recommendations.

IEEE 802.2



802.2 Logical Link Control

- The technical definition for 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers)."
- 802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).
- Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control. The Data Link Layer wants to send some data over the network, 802.2 Logical Link Control helps make this possible. It also helps by identifying the line protocol, like NetBIOS, or Netware.
- The LLC acts like a software bus allowing multiple higher layer protocols to access one or more lower layer networks. For example, if you have a server with multiple network interface cards, the LLC will forward packers from those upper layer protocols to the appropriate network interface. This allows the upper layer protocols to not need specific knowledge of the lower layer networks in use.

Operational modes[edit]

IEEE 802.2 provides two connectionless and one connection-oriented operational modes:

- **Type 1** is an unacknowledged connectionless mode for a datagram service. It allows for sending frames
  - to a single destination (point-to-point or unicast transfer),
  - to multiple destinations on the same network (multicast),

- or to all stations of the network (broadcast).

The use of multicasts and broadcasts reduce network traffic when the same information needs to be propagated to all stations of the network. However the Type 1 service provides no guarantees regarding the order of the received frames compared to the order in which they have been sent; the sender does not even get an acknowledgment that the frames have been received.

- **Type 2** is a connection-oriented operational mode. Sequence numbering ensures that the frames received are guaranteed to be in the order they have been sent, and no frames are lost.
- **Type 3** is an acknowledged connectionless service. It supports point-to-point communication only.

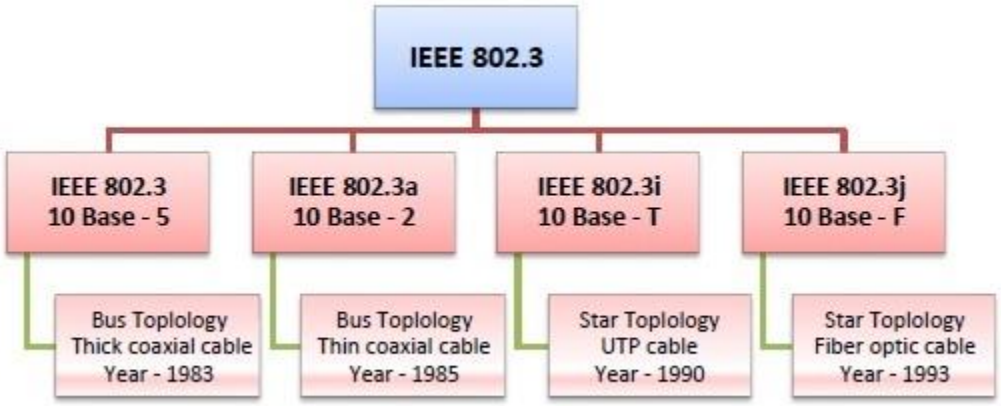
IEEE 802.3

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in MANs and even WANs. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

IEEE 802.3 Popular Versions

There are a number of versions of IEEE 802.3 protocol. The most popular ones are.

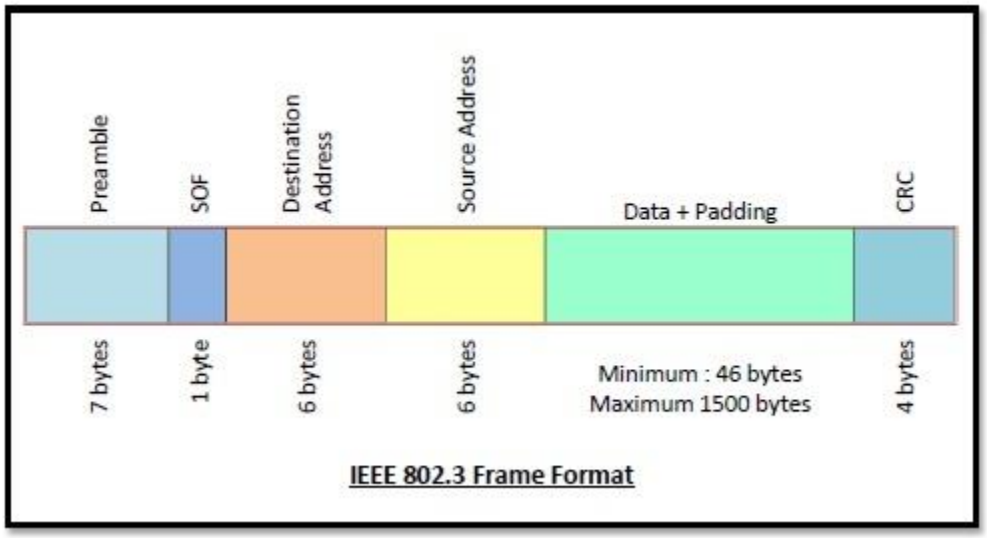
- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a**: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i**: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- **IEEE 802.3i**: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.



Frame Format of IEEE 802.3

The main fields of a frame of classic Ethernet are -

- **Preamble**: It is a 7 bytes starting field that provides alert and timing pulse for transmission.
- **Start of Frame Delimiter**: It is a 1 byte field that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address**: It is a 6 byte field containing physical address of destination stations.
- **Source Address**: It is a 6 byte field containing the physical address of the sending station.
- **Length**: It a 7 bytes field that stores the number of bytes in the data field.
- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for cyclic redundancy check. It contains the error detection information.

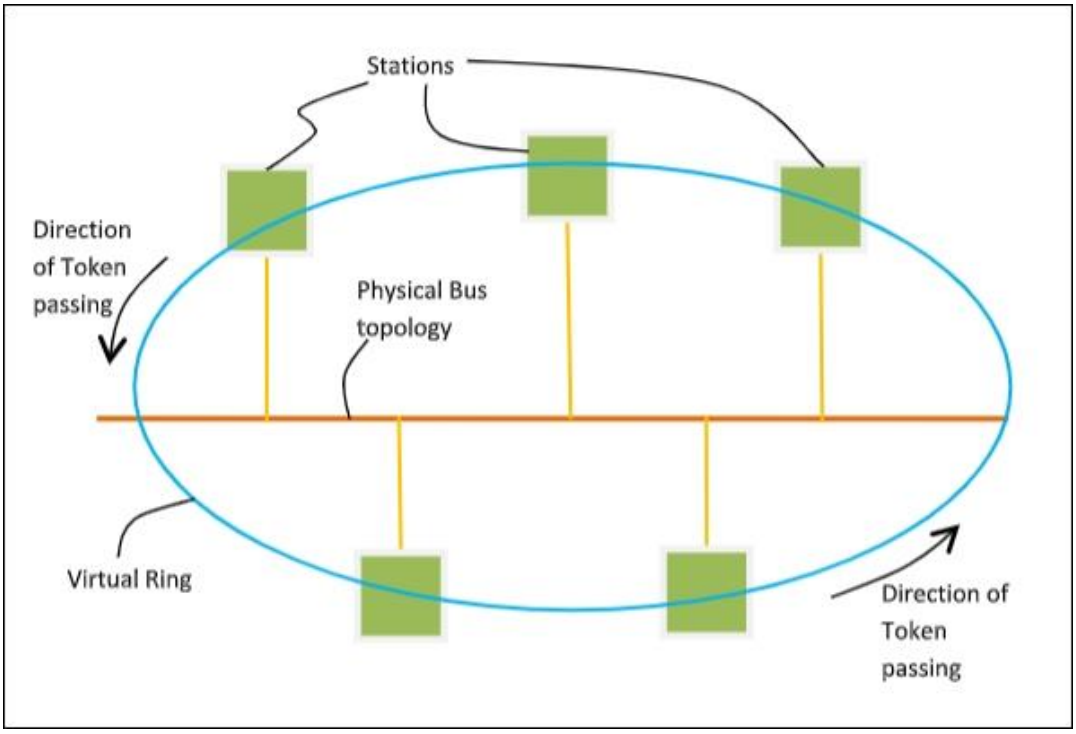


Token Bus (IEEE 802.4) Network

Token Bus (IEEE 802.4) is a standard for implementing token ring over the virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of the token bus is similar to Token Ring.

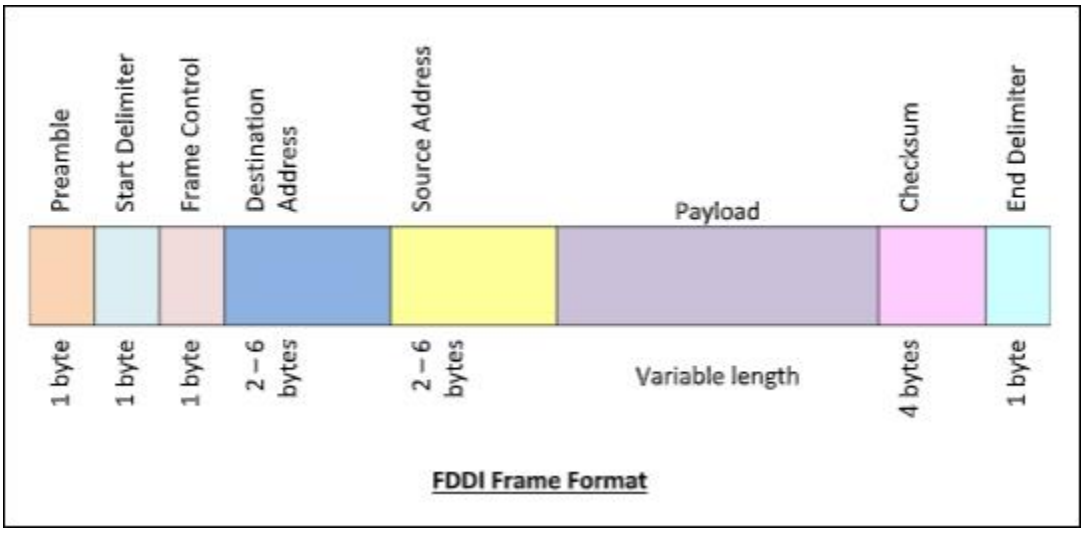
Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram −



Frame Format of Token Bus

The frame format is given by the following diagram −



The fields of a token bus frame are −

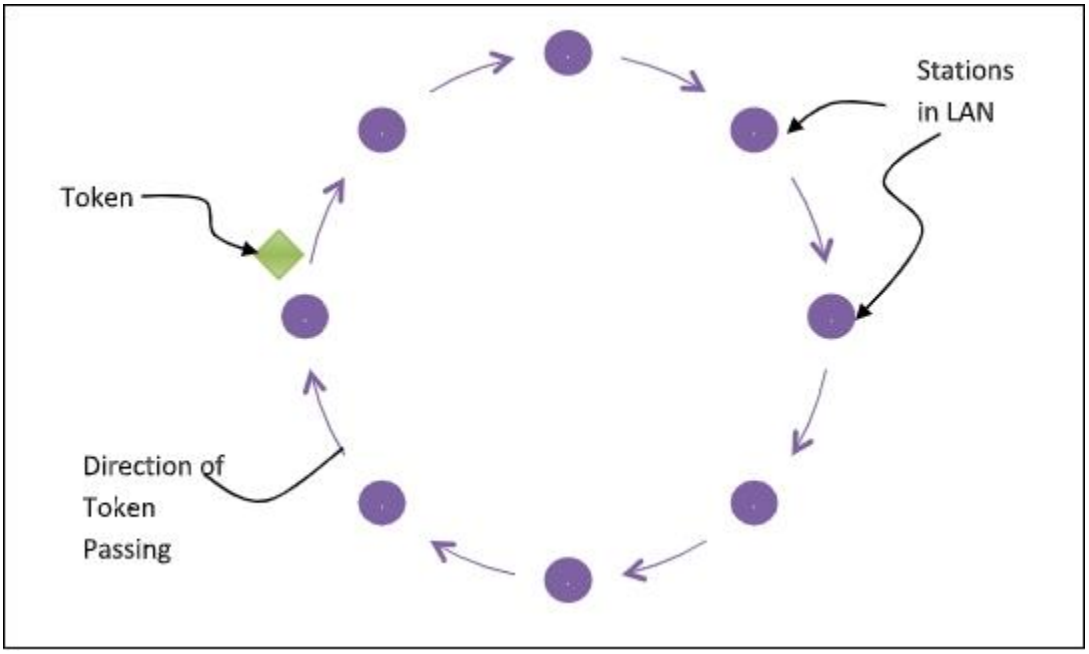
- **Preamble:** 1 byte for synchronization.
- **Start Delimiter:** 1 byte that marks the beginning of the frame.
- **Frame Control:** 1 byte that specifies whether this is a data frame or control frame.
- **Destination Address:** 2-6 bytes that specifies address of destination station.
- **Source Address:** 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.

Token Ring(IEEE 802.5)

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

Token Passing Mechanism in Token Ring

If a station has a frame to transmit when it receives a token, it sends the frame and then passes the token to the next station; otherwise it simply passes the token to the next station. Passing the token means receiving the token from the preceding station and transmitting to the successor station. The data flow is unidirectional in the direction of the token passing. In order that tokens are not circulated infinitely, they are removed from the network once their purpose is completed. This is shown in the following diagram −



Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.

Token Ring	Token Bus
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Wireless LAN : IEEE 802.11

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- **Wireless Access Pointz (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client.** − Clients are workstations, computers, laptops, printers, smartphones, etc.

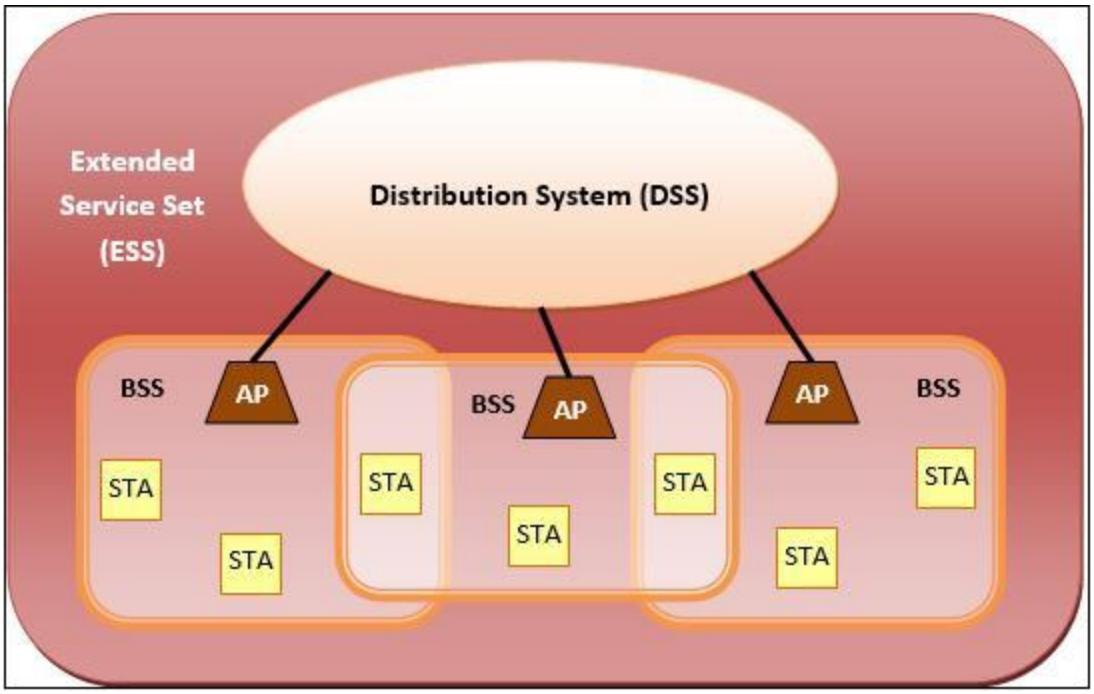
Each station has a wireless network interface controller.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- **Infrastructure BSS** − Here, the devices communicate with other devices through access points.
- **Independent BSS** − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.



Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

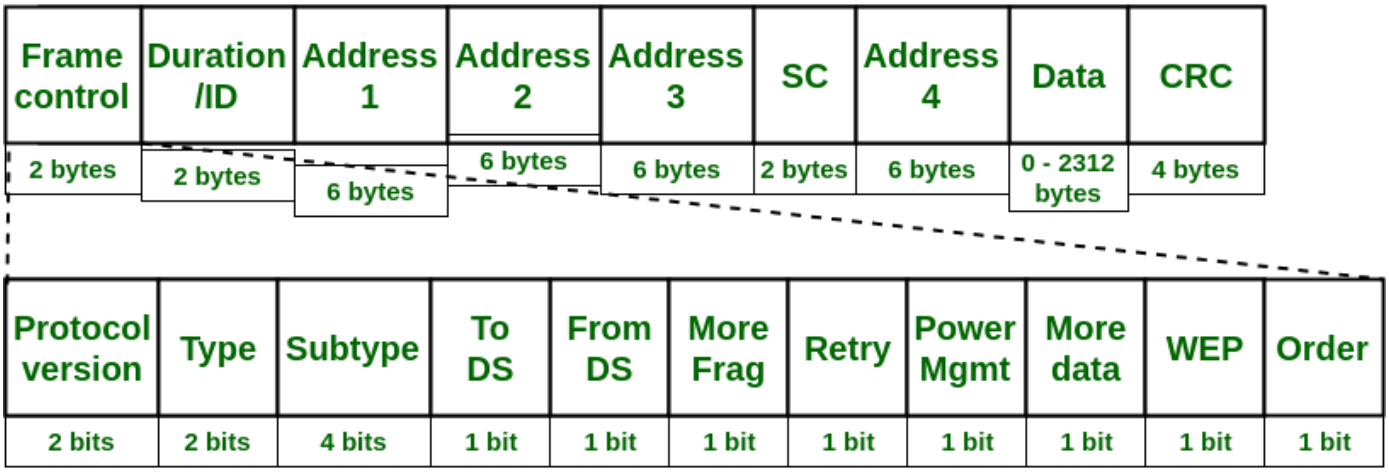
IEEE 802.11 MAC(Media Access Control) Frame

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by

MAC are the mandatory asynchronous data service and an optional time-bounded service. IEEE 802.11 defines two MAC sub-layers :-

1. **Distributed Coordination Function (DCF) –**
   DCF uses CSMA/CD as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.
2. **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.

MAC Frame:
The MAC layer frame consist of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



IEEE 802.11 MAC Frame Structure

- **Frame Control(FC) –**
  It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
  1. **Version:**
     It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
  2. **Type:**
     It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.
  3. **Subtype:**
     It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
  4. **To DS:**
     It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).

5. **From DS:**
   It is a 1 bit long field which when set indicates frame coming from DS.
6. **More frag (More fragments):**
   It is 1 bit long field which when set to 1 means frame is followed by other fragments.
7. **Retry:**
   It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
8. **Power Mgmt (Power management):**
   It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
9. **More data:**
   It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
10. **WEP:**
    It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
11. **Order:**
    It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- **Duration/ID –**
  It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).

- **Address 1 to 4 –**
  These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

- **SC (Sequence control) –**
  It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

- **Data –**
  It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).

- **CRC (Cyclic redundancy check) –**
  It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

802.11 Addressing

• There are four different addressing cases depending upon the value of *To DS And from* DS subfields of FC field.

• Each flag can be 0 or 1, resulting in 4 different situations.

1. If *To* DS = 0 and *From* DS = 0, it indicates that frame is not going to distribution system and is not coming from a distribution system. The frame is going from one station in a BSS to another.

2. If *To* DS = 0 and *From* DS = 1, it indicates that the frame is coming from a distribution system. The frame is coming from an AP and is going to a station. The address 3 contains original sender of the frame (in another BSS).

3. If *To* DS = 1 and *From* DS = 0, it indicates that the frame is going to a distribution system. The frame is going from a station to an AP. The address 3 field contains the final destination of the frame.

4. If *To* DS = 1 and *From* DS = 1,it indicates that frame is going from one AP to another AP in a wireless distributed system.

The table below specifies the addresses of all four cases.

TO DS	From DS	Address 1	Address 2	Address3	Addres 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

Bluetooth architecture: piconet and scatternet network

Bluetooth

• Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on. Bluetooth is an example of personal area network.
• Nowadays, Bluetooth technology is used for several computer and non-computer application:

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

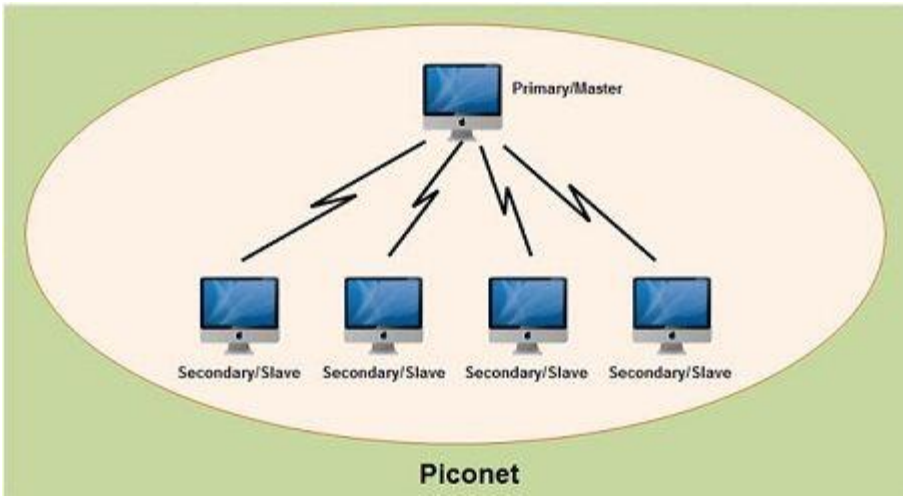
1. Piconet
2. Scattemet

1. Piconet

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

• Thus, piconet can have upto 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.



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

• In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

2. Scatternet

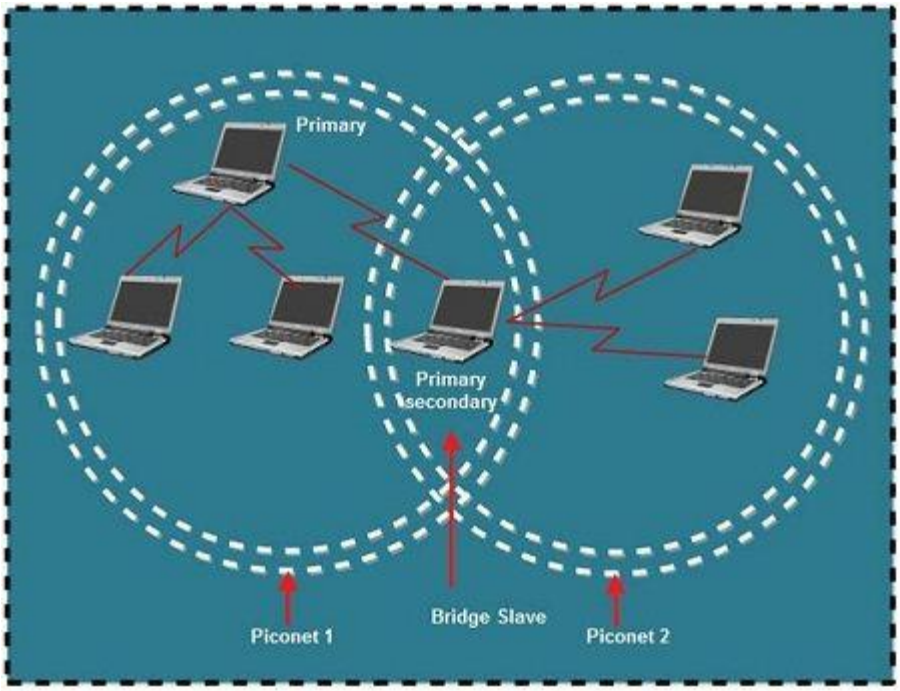
• Scattemet is formed by combining various piconets.

• 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.

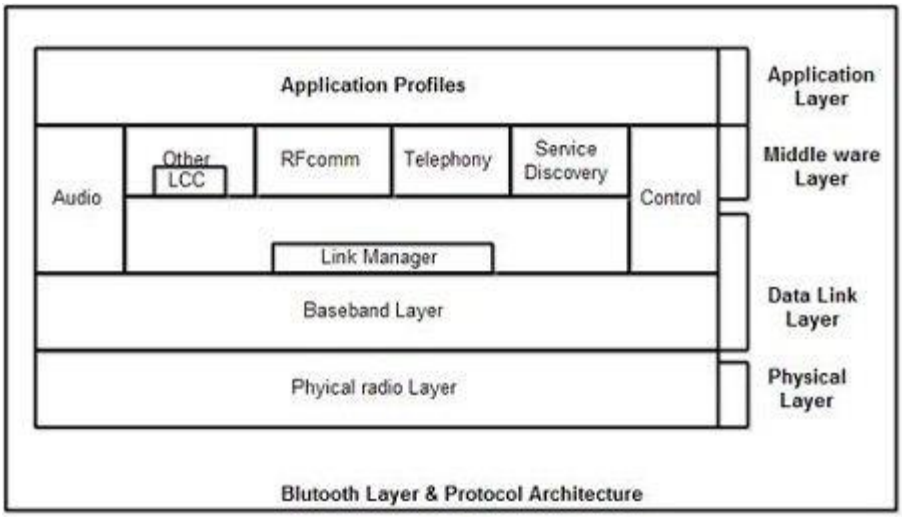


Bluetooth layers and Protocol Stack

• Bluetooth standard has many protocols that are organized into different layers.

• The layer structure of Bluetooth does not follow OS1 model, TCP/IP model or any other known model.

• The different layers and Bluetooth protocol architecture.



Radio Layer

• The Bluetooth radio layer corresponds to the physical layer of OSI model.

• It deals with ratio transmission and modulation.

• The radio layer moves data from master to slave or vice versa.

• It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.

• This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.

• Bluetooth hops 1600 times per second, i.e. each device changes its modulation frequency 1600 times per second.

• In order to change bits into a signal, it uses a version of FSK called GFSK i.e. FSK with Gaussian bandwidth filtering.

Baseband Layer

• Baseband layer is equivalent to the MAC sublayer in LANs.

• Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).

• Master and slave stations communicate with each other using time slots.

• The master in each piconet defines the time slot of 625 µsec.

• In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.

• If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5, ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.

• If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

• In Baseband layer, two types of links can be created between a master and slave. These are:

1. Asynchronous Connection-less (ACL)

• It is used for packet switched data that is available at irregular intervals.

• ACL delivers traffic on a best effort basis. Frames can be lost & may have to be retransmitted.

• A slave can have only one ACL link to its master.

• Thus ACL link is used where correct delivery is preferred over fast delivery.

• The ACL can achieve a maximum data rate of 721 kbps by using one, three or more slots.

2. Synchronous Connection Oriented (SCO)

• sco is used for real time data such as sound. It is used where fast delivery is preferred over accurate delivery.

• In an sco link, a physical link is created between the master and slave by reserving specific slots at regular intervals.

• Damaged packet; are not retransmitted over sco links.

• A slave can have three sco links with the master and can send data at 64 Kbps.

Logical Link, Control Adaptation Protocol Layer (L2CAP)

• The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN.

• The ACL link uses L2CAP for data exchange but sco channel does not use it.

• The various function of L2CAP is:

1. Segmentation and reassembly

• L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission.

• It adds extra information to define the location of frame in the original packet.

• The L2CAP reassembles the frame into packets again at the destination.

2. Multiplexing

• L2CAP performs multiplexing at sender side and demultiplexing at receiver side.

• At the sender site, it accepts data from one of the upper layer protocols frames them and deliver 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 protocol1ayer.

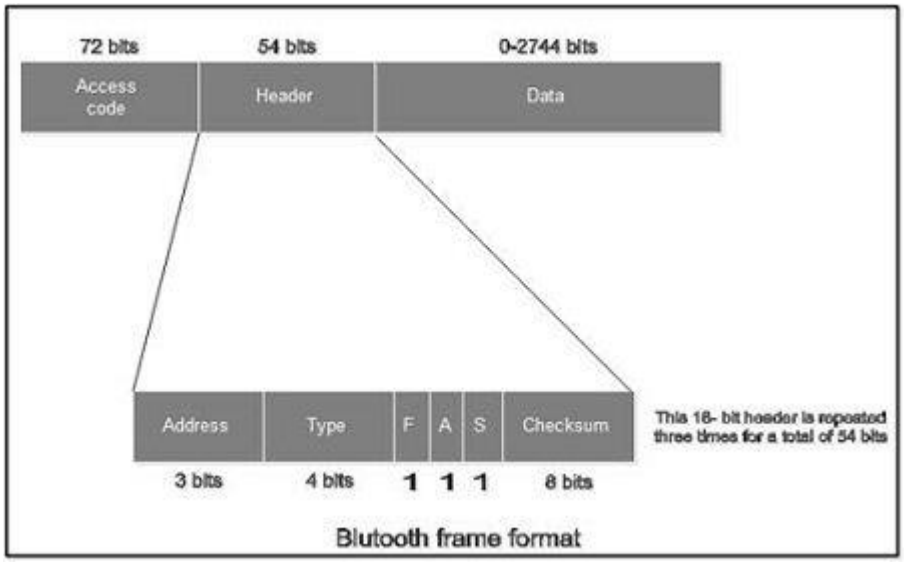
3. Quality of Service (QOS)

• L2CAP handles quality of service requirements, both when links are established and during normal operation.

• It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format

The various fields of blue tooth frame format are:



1. Access Code: It is 72 bit field that contains synchronization bits. It identifies the master.

2. Header: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following subfields:

(i) Address: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) F: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) A: This bit is used for acknowledgement.

(**v) S:** This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.

(vi) Checksum: This 8 bit field contains checksum to detect errors in header.

3. Data: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers

Mobile Generations:

The **"G"** stands for **"GENERATION"** .

While you connected to internet, the speed of your internet is depends upon the signal strength that has been shown in alphabets like 2G, 3G, 4G etc. right next to the signal bar on your home screen.

Each Generation is defined as a set of telephone **network standards** , which detail the technological implementation of a particular mobile phone system.

1G - First Generation

- This was the first generation of **cell phone technology** . The very first generation of commercial cellular network was introduced in the late 70's with fully implemented standards being established throughout the 80's. It was introduced in 1987 by Telecom (known today as Telstra), Australia received its first cellular mobile phone network utilising a 1G analog system.

- 1G is an analog technology and the phones generally had poor battery life and voice quality was large without much security, and would sometimes experience **dropped calls** . These are the analog telecommunications standards that were introduced in the 1980s and continued until being replaced by 2G digital telecommunications. The maximum speed of 1G is **2.4 Kbps** .

2G - Second Generation

- Cell phones received their first major **upgrade** when they went from 1G to 2G. The main difference between the two mobile telephone systems (1G and 2G), is that the **radio signals** used by 1G network are analog, while 2G networks are **digital** . Main motive of this generation was to provide secure and reliable communication channel. It implemented the concept of **CDMA** and **GSM** . Provided small data service like sms and mms. Second generation 2G cellular telecom networks were commercially launched on the GSM standard in Finland by Radiolinja (now part of Elisa Oyj) in 1991. 2G capabilities are achieved by allowing multiple users on a single channel via multiplexing.

- During 2G Cellular phones are used for data also along with voice. The advance in technology from 1G to 2G introduced many of the fundamental services that we still use today, such as SMS, **internal roaming** , conference calls, call hold and billing based on services e.g. charges based on long distance calls and real time billing. The max speed of 2G with General Packet Radio Service (**GPRS**) is 50 Kbps or 1 Mbps with Enhanced Data Rates for GSM Evolution (**EDGE**). Before making the major leap from 2G to 3G wireless networks, the lesser-known 2.5G and 2.75G was an interim standard that bridged the gap.

3G - Third Generation

- This generation set the standards for most of the wireless technology we have come to know and love. Web browsing, email, video downloading, picture sharing and other **Smartphone technology** were introduced in the third generation. Introduced commercially in 2001.

- The goals set out for third generation mobile communication were to facilitate greater voice and data capacity, support a wider range of applications, and increase data transmission at a **lower cost** .

- The 3G standard utilises a new technology called **UMTS** as its core network architecture - Universal Mobile Telecommunications System. This network combines aspects of the 2G network with some new technology and protocols to deliver a significantly faster data rate. Based on a set of standards used for mobile devices and mobile telecommunications use services and networks that comply with the International Mobile Telecommunications-2000 (**IMT-2000**) specifications by the International Telecommunication Union. One of requirements set by IMT-2000 was that speed should be at least 200Kbps to call it as 3G service.

- 3G has Multimedia services support along with **streaming** are more popular. In 3G, Universal access and portability across different device types are made possible (Telephones, PDA's, etc.). 3G increased the efficiency of frequency spectrum by improving how audio is **compressed** during a call, so more simultaneous calls can happen in the same frequency range. The UN's International Telecommunications Union **IMT-2000** standard requires stationary speeds of 2Mbps and mobile speeds of 384kbps for a "true" 3G. The theoretical max speed for **HSPA+** is 21.6 Mbps.

- Like 2G, 3G evolved into 3.5G and 3.75G as more features were introduced in order to bring about 4G. A 3G phone cannot communicate through a **4G network** , but newer generations of phones are practically always designed to be backward compatible, so a 4G phone can communicate through a 3G or even **2G network** .

4G - Fourth Generation

- 4G is a very different technology as compared to **3G** and was made possible practically only because of the advancements in the technology in the last 10 years. Its purpose is to provide **high speed** , high quality and high capacity to users while improving security and lower the cost of voice and data services, multimedia and internet over IP. Potential and current applications

include amended mobile web access, **IP telephony** , gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

- The key technologies that have made this possible are **MIMO** (Multiple Input Multiple Output) and **OFDM** (Orthogonal Frequency Division Multiplexing). The two important 4G standards are WiMAX (has now fizzled out) and **LTE** (has seen widespread deployment). LTE (Long Term Evolution) is a series of upgrades to existing UMTS technology and will be rolled out on Telstra's existing 1800MHz frequency band.

- The max speed of a 4G network when the device is moving is 100 Mbps or **1 Gbps** for low mobility communication like when stationary or walking, latency reduced from around 300ms to less than 100ms, and significantly lower congestion. When 4G first became available, it was simply a little faster than 3G. 4G is not the same as **4G LTE** which is very close to meeting the criteria of the standards. To download a new game or stream a TV show in HD, you can do it **without buffering** .

- Newer generations of phones are usually designed to be **backward-compatible** , so a 4G phone can communicate through a 3G or even 2G network. All carriers seem to agree that **OFDM** is one of the chief indicators that a service can be legitimately marketed as being 4G. OFDM is a type of digital modulation in which a signal is split into several narrowband channels at different frequencies.

- There are a significant amount of infrastructure changes needed to be implemented by service providers in order to supply because voice calls in **GSM** , **UMTS** and **CDMA2000** are circuit switched, so with the adoption of LTE, carriers will have to re-engineer their voice call network. And again, we have the fractional parts: **4.5G** and **4.9G** marking the transition of LTE (in the stage called LTE-Advanced Pro) getting us more MIMO, more D2D on the way to IMT-2020 and the requirements of **5G** .

5G - Fifth Generation

- 5G is a generation currently **under development** , that's intended to improve on 4G. **5G** promises significantly faster data rates, higher

connection density, much lower latency, among other improvements. Some of the plans for 5G include **device-to-device** communication, better battery consumption, and improved overall wireless coverage.

- The max speed of 5G is aimed at being as fast as **35.46 Gbps** , which is over 35 times faster than 4G.
- Key technologies to look out for: **Massive MIMO** , Millimeter Wave Mobile Communications etc. Massive MIMO, milimetre wave, small cells, **Li-Fi** all the new technologies from the previous decade could be used to give 10Gb/s to a user, with an unseen low latency, and allow connections for at least **100 billion devices** .
- Different estimations have been made for the date of commercial introduction of 5G networks. Next Generation Mobile Networks Alliance feel that 5G should be rolled out by **2020** to meet business and consumer demands.