LEARNING RESOURCE MATERIAL

ON

MOBILE COMPUTING

(For 5th Semester CSE/ IT)

Prepared by:

Nayana Patel

PTGF (CSE/IT)

UCP Engineering School, Berhampur.

NETWORKS: -

A network is a communication system that enables computer users to share computer equipment, application s/w, data/information, voice and video transmission. Networks are used to transmit information by wired or wireless (using radio waves) communication media. Communication media are cabling (coaxial cable, twisted pair cable, fiber-optic cable). Wireless commercial networks use spread spectrum technology.

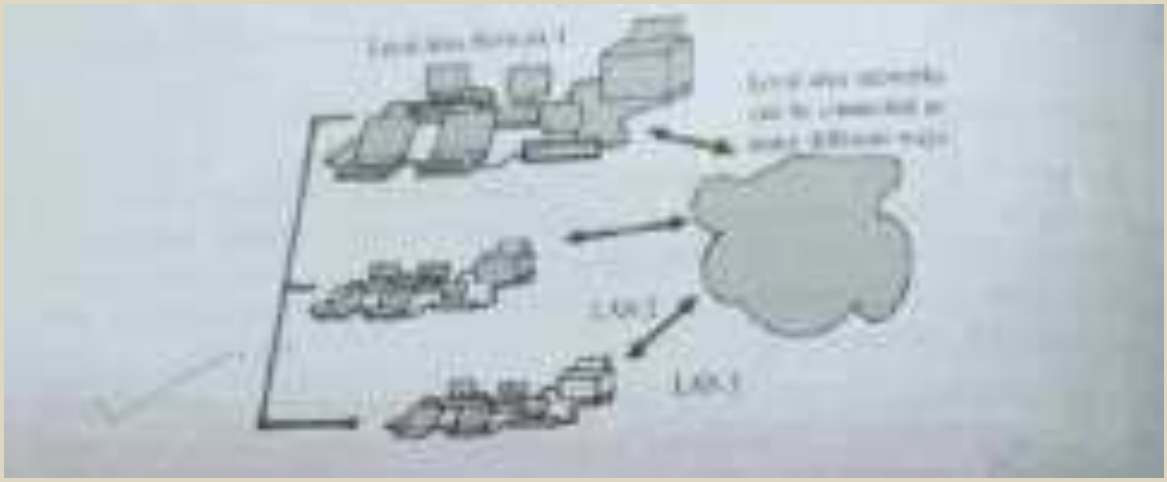
The wire-based technology was used for connection computers. This technology falls into three categories:

- Local Area Networks (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Networks (WAN)
- Personal Area Network (PAN)

I. LAN supports sharing of applications or any other resources within a small fixed boundary.

II. MAN covers the boundary of a campus or a city area and connects the LANs usually with optical fiber for data transmission.

III. WAN uses telephone circuits, leased lines and private circuits to support networking globally by using circuit and packet switching networks and protocols.



(Wired LAN)

Next is the extension of LAN i.e., WAN. Below figured out the WAN.

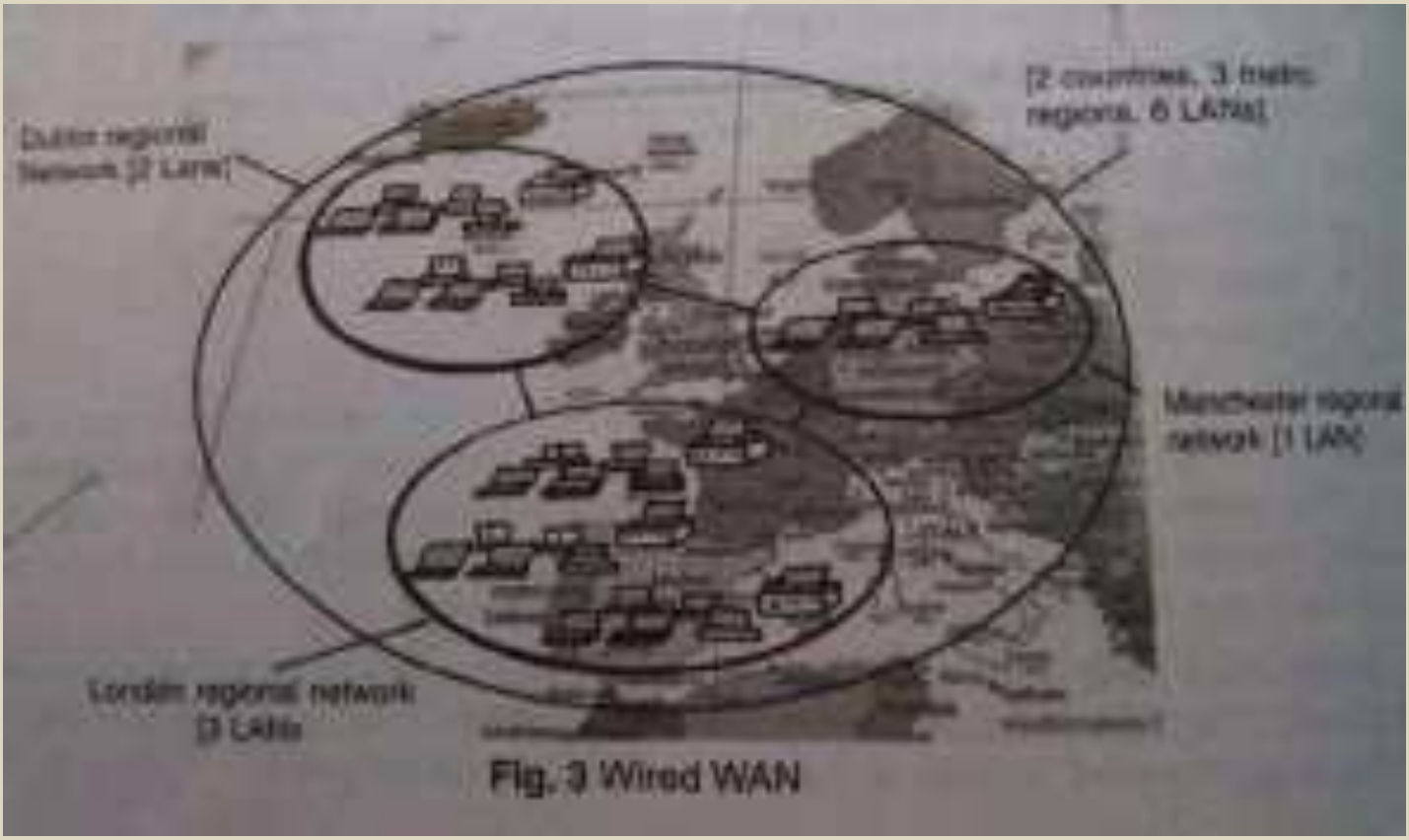


Fig. 3 Wired WAN

WIRELESS NETWORKS: -

I. Wireless network is a network of devices – computing and networking that are connected logically without wires.
II. It means it is a telecommunication network in which the devices are implemented without the use of wires.
III. Wireless telecommunication networks are implemented with information transmission system that uses electromagnetic waves, such as radio waves.
IV. The term wireless technology is generally used for mobile IT equipment.

The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling
- To avoid obstacles such as physical structures etc.
- To provide a backup communications link in case of normal network failure

- To link portable or temporary workstations
- To overcome situations where normal cabling is difficult or financially impractical
- To remotely connect mobile users or networks

Wireless communications involve:

- Radio frequency communication
- Microwave communication, for example long-range line-of-segment via highly directional antennas, or short-range communication, or
- Infrared (IR) short-range communication, for example from remote controls or via IRDA

In wireless communication, electromagnetic waves (rather than some form of wire) carry the data signals. Common examples of wireless equipment in use today include:

- **Cellular phones and pagers:** provide connectivity for portable and mobile applications, both personal and business.
- **Global Positioning System (GPS):** allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- **Cordless computer peripherals:** the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless.
- **Cordless telephone sets:** there are limited-range devices, not to be confused with cell phones.
- **Satellite television:** allows viewers in almost any location to select from hundreds of channels.

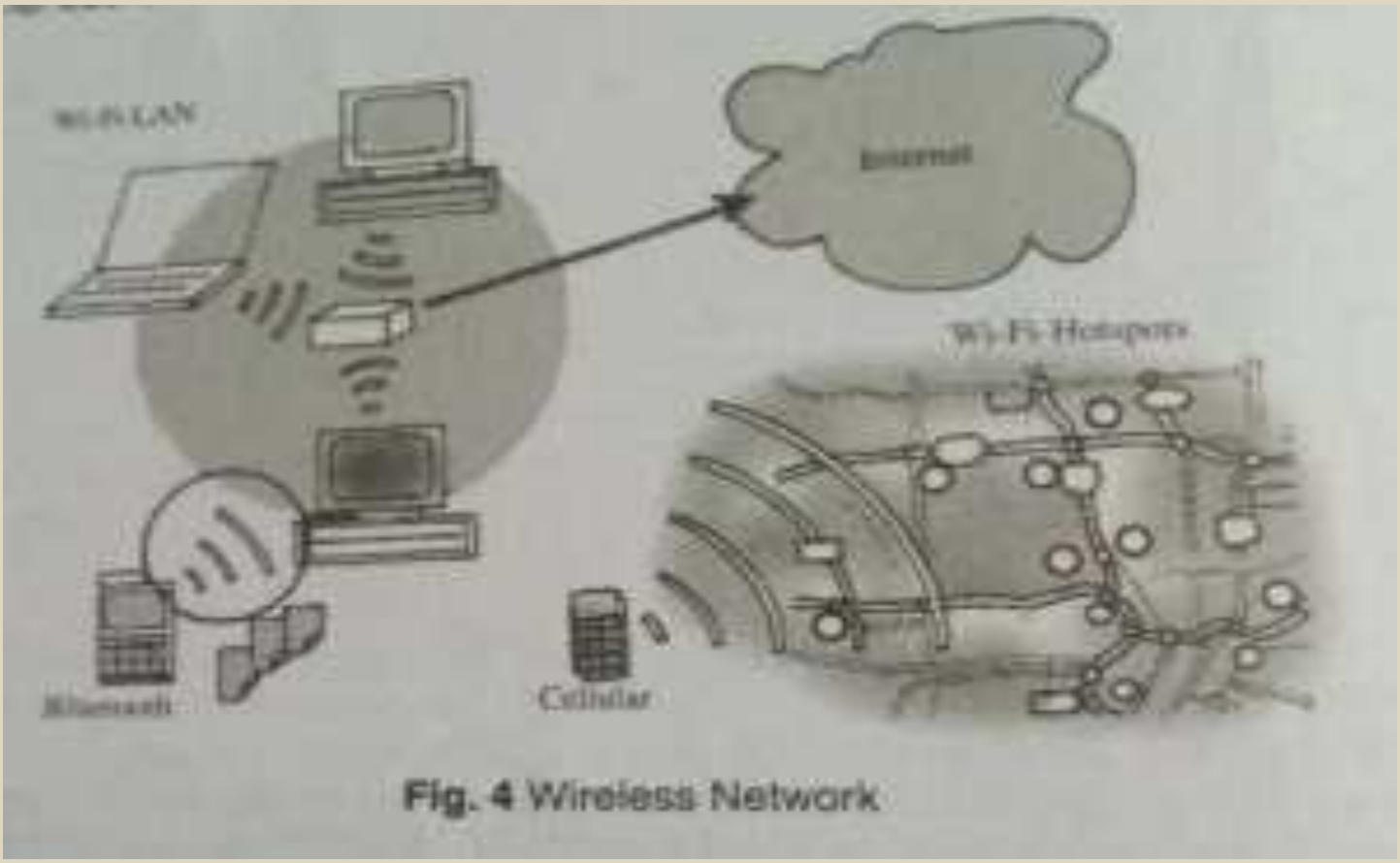


Fig. 4 Wireless Network

MOBILE COMPUTING: -

a) Mobile computing is a computing environment over physical mobility.
b) The user of a mobile computing environment is able to access the data, information or other logical objects from any device in the network while on move.
c) Mobile Computing system allows the user to perform a task from anywhere using a computing device in public (the web), corporate (business information) and personal information areas (medical record, address book etc.).

Dimensions of Mobile Computing:

It is obvious that any mobile computing system can also be stationery. It is stationery of we stop moving. Therefore, we can say that stationery systems are the subset of mobile computing systems. Here we will take a look at the dimensions which make a system mobile. These dimensions are as follows:

- Location Awareness
- Quality of Service
- Limited Device Capability
- Limited Power Supply
- Support for a wide variety of user interfaces

Location Awareness

A mobile device is not always at the same place; its place is not fixed. Maintaining the location of the user is a big challenge for the application developers. There are varieties of methods for collecting data of location of user and device.

Quality of Service

a) Using any type of network whether wired or wireless; mobility means loss of network connectivity.
b) Movement means increase in physical barriers and disconnection from network. Movement means increase in physical barriers and disconnection from network.
c) In short degradation in quality of service is the result. Stationary applications mean increased network quality of service is the result.
d) Stationary applications mean increased network quality, However the about Quality of Service in designing the mobile applications is take care.

Limited Device Storage Capability

a) We have seen that size is the biggest constraint for the mobile device; for the same reason batteries are the main resources of power for mobile devices.
b) As the user requirements increase, batteries are improving every day.
c) The power supply constraint must be balanced with the processing power, storage and size constraints.

Support for a wide variety of use interfaces

Mobile applications can also be handled from the stationary devices like PC's. the keyboard, mouse and monitor have proved to be very efficient user interfaces for such

type of applications. The other interfaces include touch pad, smaller displays, other pointing devices etc.

MOBILE COMPUTING CHARACTERISTICS: -

Mobile Computing environment supports the following characteristics:

- **User Mobility:**

→ User should be able to move from one physical location to another and use the same service without any interruption.

→ For e.g., User moves from Singapore to Germany and uses the internet to access his application the same way he uses in his office.

- **Network Mobility:**

→ User should be able to move from one network to another and use the same service.

→For e.g., User moves from London to New Delhi and uses the same GSM phone to access his application through WAP.

- **Bearer Mobility:**

→ User should be able to move from one bearer to another and use the same service.

→ For e.g., User was using a service through WAP bearer in his home network in Bangalore.

→ He moves to Chennai where WAP is not supported, he switched over to voice or SMS bearer to access the same application.

- **Device Mobility:**

→ User should be able to move from one device to another and use the same service.

→ For e.g., User could be a representative using his desktop at his office and during the day work outside his office, uses his palmtop or laptop to access the same application.

- **Session Mobility:**

→ User's session should be moved from one environment to another.

→ For e.g., User was using the service thorough CDMA network, He entered into basement are and got disconnected from the network.

→ Her there goes to his office and uses his desktop.

→ The unfinished session moves from mobile device to desktop.

- **Service Mobility:**

→ User should be able to move from one service to another. For e.g., User is writing mail.

→ For getting some information he switches over to some other application and returns back and completes his mail sending process same way users should be able to switch between applications in wireless devices.

The Mobile Computing functions can be logically divided into following major segments. The below fig. shows the segments:

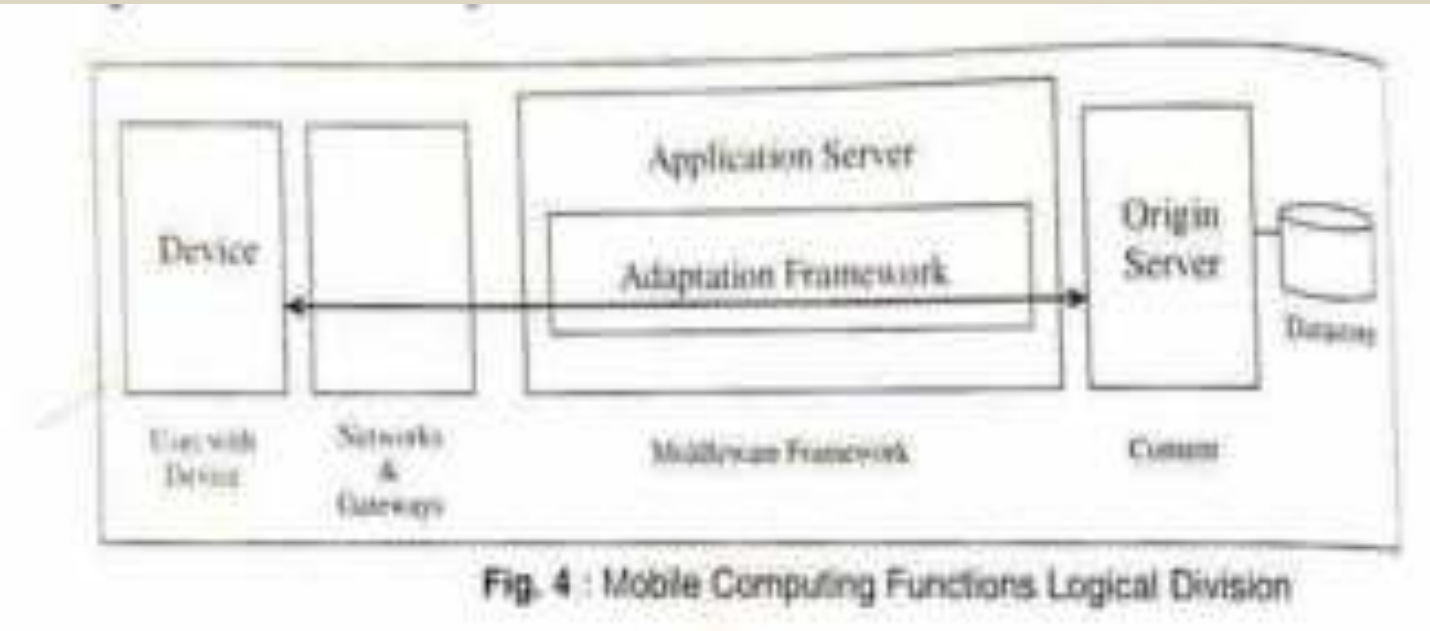


Fig. 4 : Mobile Computing Functions Logical Division

Various segments are described as below:

- **User with Device:** The used could have a fixed like desktop computer or a portable or mobile device like mobile phone.
- **Network:** Whenever a user is mobile, he will be using different networks at different places at different time.
- **Gateway:**

→ This is required to interface different transport bearers.

→ These gateways convert one specific transport bearer to another bearer.

→ For example, from a fixed phone we access the service by pressing different keys on the telephone.

→ These keys generate DTMF (Dual Tone Multi Frequency).

→ These are analog signals which are then converted into digital by IVR (Interactive Voice Response) gateway to interface with a computer application.

- **Middleware:** A s/w layer between a user application and operating system can be termed as middleware.

- **Content:** This is the place or server where originally the content is stored. This could be an application, system or even a collection of systems. This server will access the data store for reference.

APPLICATIONS OF MOBILE COMPUTING: -

The users might want available while they are on mobile include:

- Flight, directions, and traffic information
- Movie listings
- News
- Weather
- Reading email
- Retail
- Warehousing
- Healthcare
- Real Estate
- Field Service
- Field Sales
- Hospitality
- Vending

1. All the applications must provide high value with a minimum of typing. This eventually leads to location-based services.
2. Wireless coverage of lecture theatres will allow experimentation using novel teaching methods and provide better support for conferences.
3. The use of mobile devices inn offices is now fairly commonplace; however, such a diverse test-bed offers many new opportunities for experimentation.

4. Through mainly concerned with mobile systems, the project will also deploy services to homes and University residences. …we aren't always mobile.
5. There are many situations where wireless access would make life easier, including home working, database access, or just for entertainment.
6. Another aspect of the project will be to extend our previous work on context aware systems to many environments, including the home.

We already have a wireless network around the city providing tourist information. The system also allows families to keep in touch as they roam. Checking lecture times while on the move or downloading an e-book while relaxing in a café. …wireless coverage of leisure areas is also high on our list. Extending our city-wide wireless network would allow new services such as instant price comparisons and access to product information.

CLIENT-SERVER ARCHITECTURES: -

I. Client-Server architectures were the first network-based computing architectures to become commercially available.
II. Distributed computing architectures were already in existence, but the most commercial systems that allowed networking were based on centralized model.
III. In a client-server model there are two different programs residing on separate machines.
IV. One program is said to be the client and the other is said to be the server because client generates the request and the server serves the client's request.
V. In the real world there is one server and more than one client.
VI. The main aim of client-server architecture was an application of one of the basic principles in software engineering i.e. separation of concerns.
VII. In other words, the client-server architecture predetermined that the client can do more than just being hardware with no computing power.
VIII. There were many benefits of making a client more powerful.
IX. All the client interfaces were moved to client machine.
X. Another benefit is the handling of server downtime.
XI. In client-server architecture the client can give the information to the user about the server breakdown or why the server is not accessible.
XII. This is not the case with fully centralized system.

Modern client-server architecture includes database on the server side. These databases can be used by client by using some connectivity protocols.

They not only store data but also hold business logic.

The below fig. depicts client-server architecture:

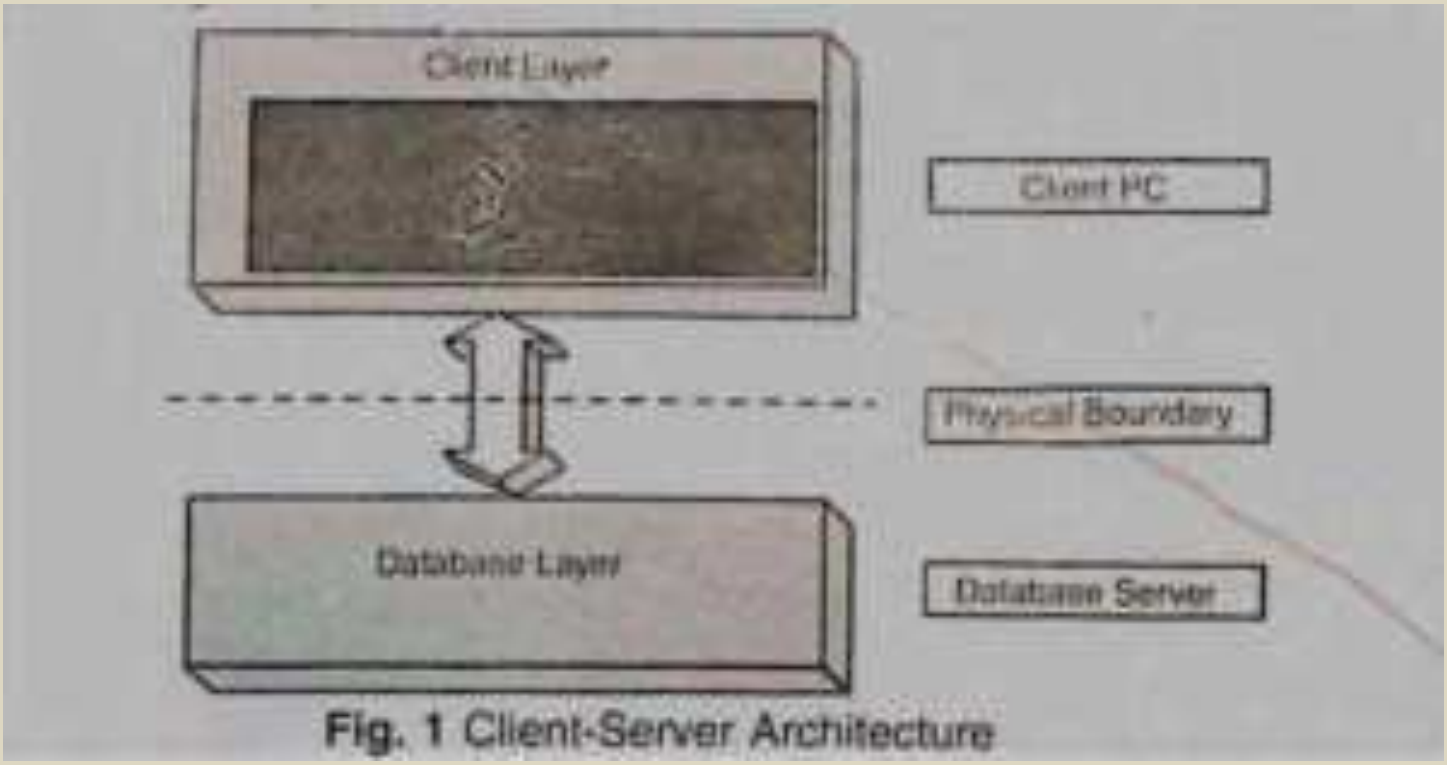


Fig. 1 Client-Server Architecture

N-TIER ARCHITECTURE: -

With the increasing use of web application, an examination of the best architecture to support web applications is suitable. Here we will be discussing tier architecture, which is the breaking down of an application into logical chunks that are called tiers. Tiers can exist on the same computer and be connected virtually or logically or on different machines.

The simplest examples of tier architecture are enumerated as 1-tier, 2-tier, and 3-tier architecture is the simplest.

1-Tier Architecture: Single tier on single user, and is the equivalent of running an application on a personal computer.

→ All the required components to run the application are located within it.

→ User interface, business logic, and data storage are all located on the same machine.

→ They are the easiest to design, but the least scalable. Because they are not part of network, they are useless for designing web applications.

2-Tier Architecture: This tier architectures supply a basic network between a client and a server.

→ For example, the basic web model is a 2-tier architecture. A web browser makes a request from a web server, which then process the request and returns the desired response, in this case, web pages. This approach improves scalability and divides the user interface from the data layers. However, it does not divide application layers so they can be utilized separately. This makes them difficult to update and not specialized. The entire application must be updated because layers aren't separated.

3-Tier Architecture: It is most commonly used to build web applications.

→ In this model, the browser acts like a client, middleware or an application server contains the business logic, and database servers handle data functions.

→ This approach separates business logic from display and data. But, it does not specialize functional layers.

→ N-tier architectures provide finer granularity, which provides more modules to choose from as the application is separated into smaller functions.

→ Usually N-tier architecture begins as a 3-tier model and is expanded. It provides finer granularity. Granularity is the ability of a system.

In this case an application, to be broken down into smaller components or granules. The finer, the granularity, the greater, the flexibility of a system. It can also be referred to as a system's modularity. Therefore, it refers to the pulling apart of an application into separate layers or finer grains. The below fig. depicts N-tier architecture:

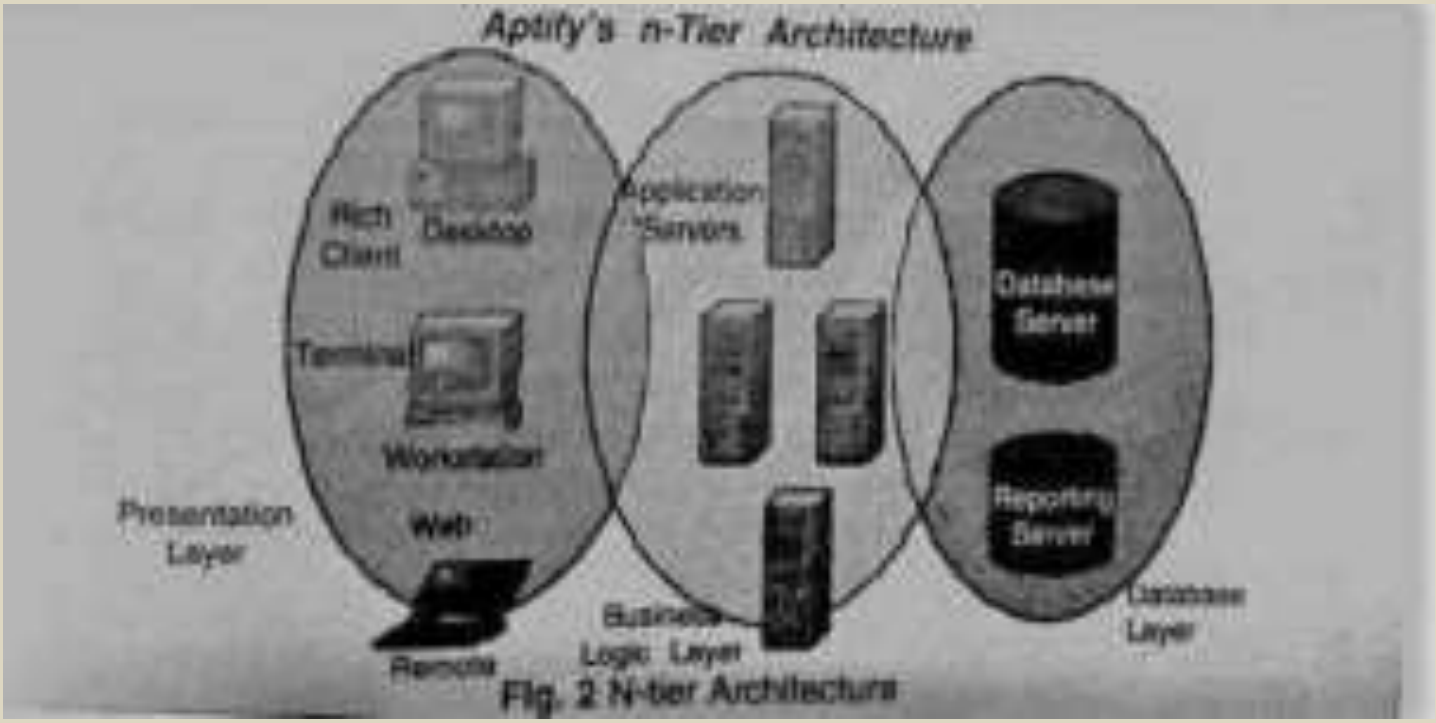


Fig. 2 N-tier Architecture

Today a large portion of the infrastructure of the WWW is based on N-tier architecture. Let us have a look at it.

N-TIER ARCHITECTURES AND THE WWW: -

The web is actually a client-server mechanism where the client and server communicate through HTTP (Hyper Text Transfer Protocol). The clients are the browsers which interpret the user interface in HTML and other client-side scripting languages for rendering interface. The servers are the Web Servers which servers the client request coming from HTTP with HTML response.

- One of the best examples of N-tier architecture in web applications is the popular shopping-cart web application.
- The client tier interacts with the user through GUIs and with the application and the application server.
- In web applications, this client tier is a web browser.
- In a shopping cart web application, the presentation tier displays information related to such services as browsing, purchasing, and shopping cart contents.

- It communicates with other tiers by outputting results to the browser/client tier and all other tiers in the network.
- This layer calls custom tags throughout the network and to other networks. It also calls database stored procedures and web services, all in the goal of providing a more sophisticated response.
- This layer glues the whole application together and allows different nodes to communicate with each other and be displayed to the user through the browser. It is located in the application server.

In N-tier architecture, the business logic tier is pulled out from the presentation tier and, as its own layer; it controls an application's functionality by performing detailed processing. For example, in our shopping cart example, this tier completes credit card authorization and calculates things like shipping costs and sales tax. The tools used to encapsulate an application's business logic into its own layer include web services, custom tags, and stored procedures.

PEER-TO-PEER ARCHITECTURE: -

N-tier architectures, with all of their benefits, do not address several dimensions of mobility. N-tier architectures require that the user be connected to the network because the servers are somewhere else on the network. The data interchange is not possible between clients. Here "let alone explore" concept totally fails.

I. Often referred to simply as peer-to-peer, or abbreviated P2P, peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities.
II. This differs from client-server Architecture where some computers are dedicated to serving the others.
III. Peer-to-peer networks are generally simpler but they usually do not offer the same performance under heavy loads.
IV. The P2P network itself relies on computing power at the ends of a connection rather than from within then network itself.
V. P2P is not only popular with home users but many small businesses have come to rely on this cost-effective solution for sharing files with co-workers and clients.

VI. P2P promotes the ease of working together when you're not physically located in the same office.

VII. In just seconds updated files and data can be shared with all participants referred to as peers and confidential files can be blocked for security.

One could view the peer-to-peer architecture as placing a server module as well as a client module as well as a client module on each computer. Thus each computer can access services from the software modules on another computer, as well as providing services to the other computer.

The below fig. depicts peer-to-peer architecture:

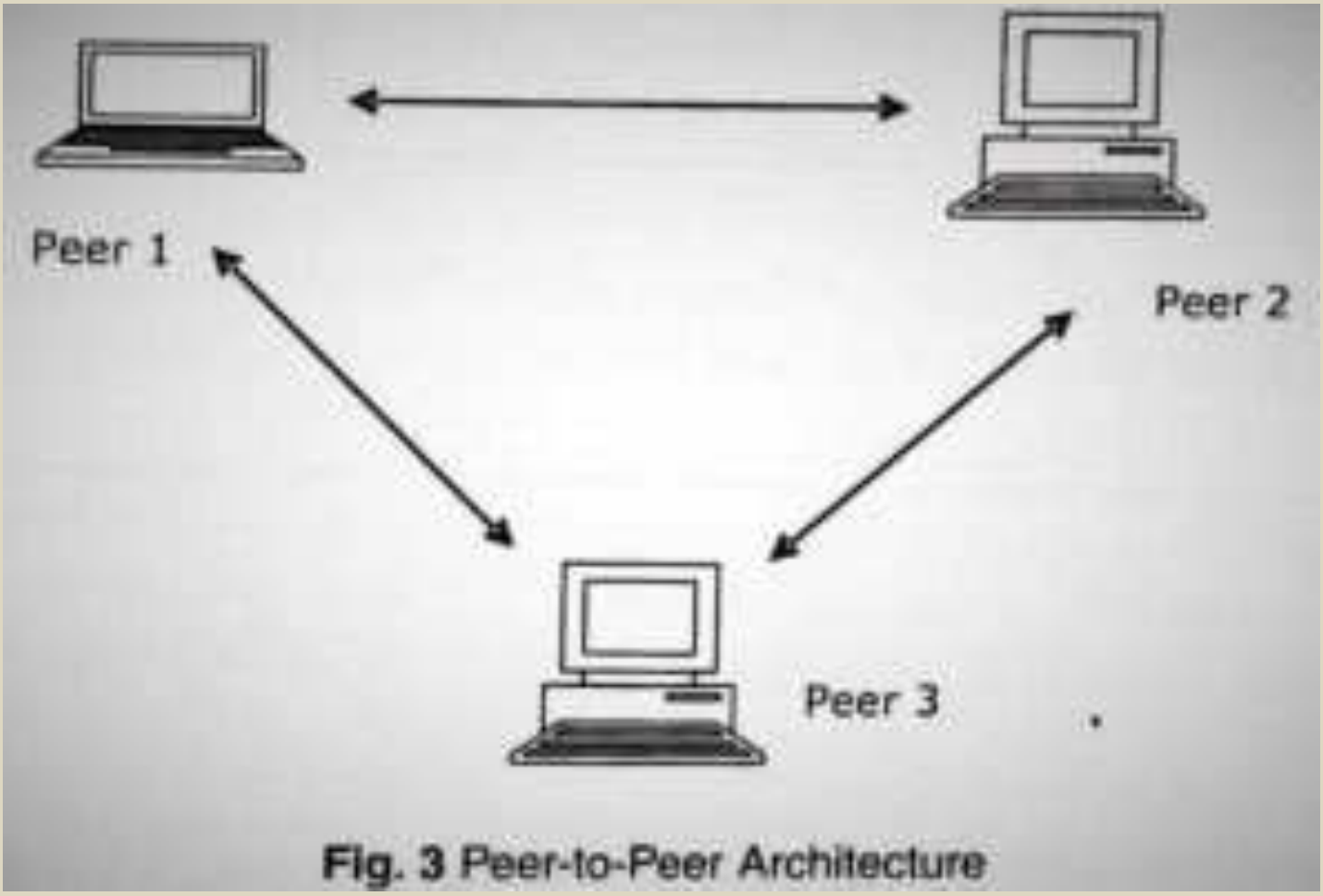


Fig. 3 Peer-to-Peer Architecture

The advantages of peer-to-peer include:

- No need for a network administrator
- Network is fast/inexpensive to setup & maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

MOBILE AGENT ARCHITECTURE: -

Mobile Agent based software systems have a totally different architecture from client-server and N-tier systems. Mobile agents have the following properties:

- They are the programs which hide data and code which are transported from client machine to remote server for execution.
- They execute asynchronously.

The term mobile agents have no relation with mobile user, mobile device or any other aspects of mobility. They are software components which move from server to server in a network while keeping the state of application intact.

Mobile age agents can manage their own life cycle. This means that we do not have to load and unload the applications manually or store many applications on the device. Hence the usage of CPU and other resources are minimized and simplified.

Introduction: -

At physical layer data is moved the form of electromagnetic signal across a transmission medium. The transmission medium works by conducting energy along a physical path. This requires the data stream of 1's & 0's to be turned into energy in the form of electromagnetic signals can be made to travel through wires. In case of wired network & can be made to travel through open space in case of wireless network.

Radio transmission (travelling) of radio waves through air can take place from different frequency bands.

Signals: -

Signals are the physical representation of the data. When users of a communication system want to exchange data, this data must be converted into signal. Before it is transmitted through a transmission medium.

→ Signals are functions of time and location.
→ Signal's parameters represent the data values.

Data can be analog or digital signals.

Analog Signals: -

→ Analog signals are continuous electrical signals that vary in time.
→ A simple analog signal is a sine wave.
→ A composite analog signal is consisting of multiple sine waves.
→ An analog signal can be classified into two types.
- Periodic Signal
- Aperiodic Signal

Fig. 1. Analog Signal

Periodic Signal:

→ A periodic signal completes a pattern within a time frame called a Period & this pattern is repeated over sub-sequent identical periods.
→ The completion of one full pattern is called a cycle.

Aperiodic Signal:

→ An Aperiodic signal changes without showing a pattern or cycle that repeats over time.

Digital Signal: -

→ Digital signals are transmission signals that carry information in a discontinuous stream of ON / OFF pulses.
→ They consist of pulses or digits with descript levels or values.
→ Digital signals have two amplitude levels called Nodes i.e., 1 or 0, HIGH or LOW, TRUE or FALSE.

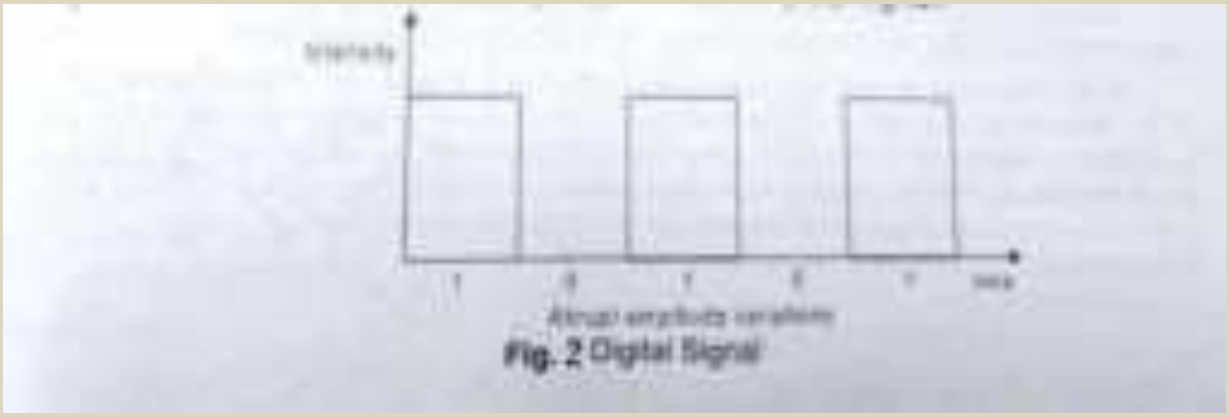


Fig. 2 Digital Signal

Digital signals can be classified into 2 types.

- Periodic Signal
- Aperiodic Signal

→ Analog signals require a transmission medium having much less bandwidth i.e., only about 4.5 MHz with a 143.2 MBPS of data rate.
→ Whereas the digital signals the transmission medium requires much high bandwidth i.e., 74.25 MHz with a data rate of 1485 MBPS.

Any digital signal has 3 parameters.

1. Amplitude
2. Frequency
3. Phase

Period & Frequency: -

→ Period refers to amount of time in seconds a signal leads to complete one cycle.
→ Frequency is the measurement of the number of occurrences of a repeated event per unit of time.

Bandwidth: -

The range of frequency that medium can pass is called its bandwidth. It is the property of a medium. It is a difference between the highest and lowest frequency that medium can pass.

Antennas: -

An antenna is also known as aerial which is a transducer i.e., designed to transmit or receive radio wave. A transducer is a device that converts energy from one form to another form for the purpose of the measurement of a physical quality or for information transfer.

Antennas are used in system such as radio & television broadcasting, point -to – point radio communication, wireless LAN, radar & space exploration. Antennas generally work in air or outer space. Antennas have practical uses for the transmission & reception of radio frequency signals, which can travel over great distances at the speed of light.

There are 2 types of antenna.

1. Omni Directional
2. Directional

Omni Directional:

Omni directional antenna radiates signal equally in all direction.

Directional:

Directional antenna radiates more in one direction than in the other direction. It means directional antennas concentrate most of its power in one direction.

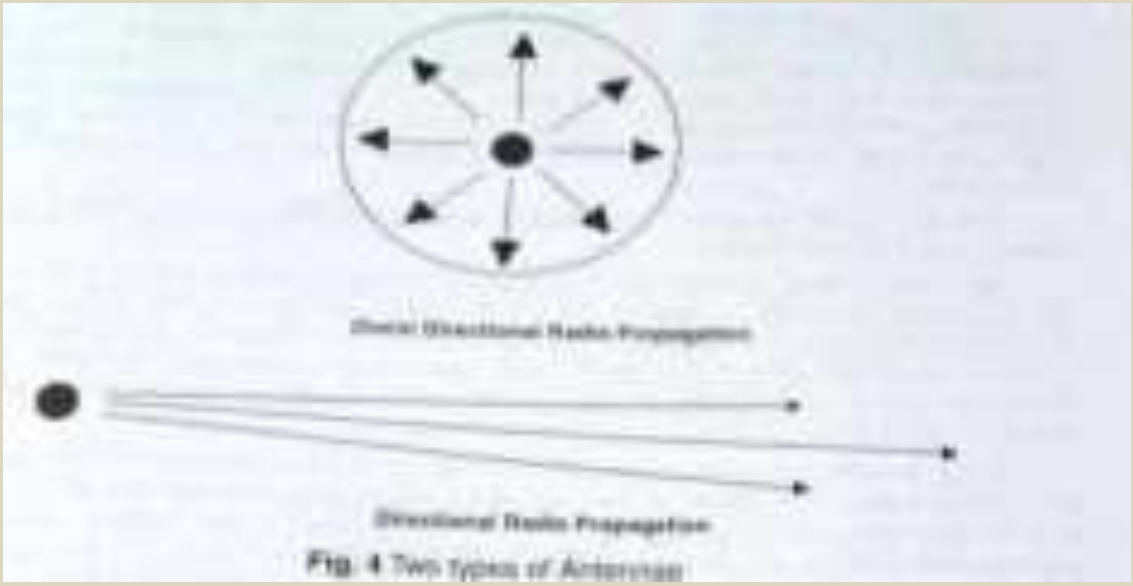


Fig. 4 Two types of Antennas

Antenna Gain: -

I. Antenna Gain is a measure of directivity.
II. It is defined as at the radio of the radiation intensity in a given direction to the radiation intensity that would be obtained if the power accepted by the antenna where radiate equally in all directions.
III. Antenna Gain is expressed in DB (Decibel). A directional antenna has more gain than Omni directional antenna. So, Omni-directional antenna is capable of transmitting signals for short distance.
IV. Wireless LANs & WANs used Omni-directional antennas & wireless used directional antennas.

Antenna Array: -

It is a two or more antenna to a common source or load to produce a specific directional radiation pattern.

Signal Propagation: -

The electromagnetic spectrum classifies electromagnetic energy according to frequency.

As shown in the figure below, the electromagnetic spectrum ranges from energy waves having extremely low frequency to energy waves having much higher frequency such as X-rays.

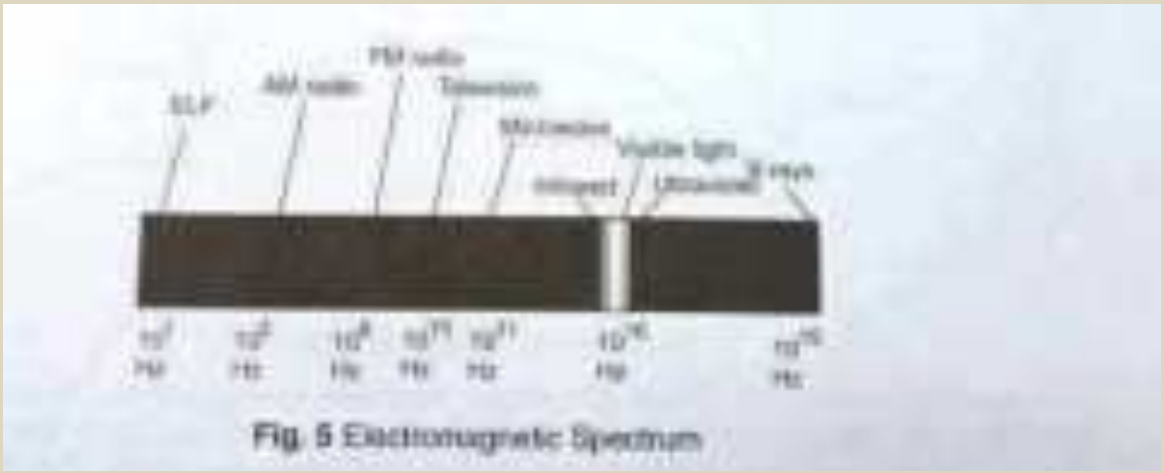


Fig. 5 Electromagnetic Spectrum

Signal propagation is nothing but travelling of signals through some medium in case of both wired or wireless networks. Transmission media is of two types.

1. Guided Media
2. Unguided Media

- In case of guided media, it is through various types of cables like Twisted Pair, Coaxial Cable, and Fiber Optical Cable.
- In case of unguided media, signals travel through air there is grounded propagation, sky propagation and line of sine propagation.
- In ground propagation, radio waves to travel through lowest part of the atmosphere, touching the earth. These low frequency signals are transmitted in all the direction.

The greater the power the greater is the distance. In sky propagation, higher frequency radio waves are transmitted upwards in the ionosphere where there reflect back to the earth.

The greater the distance low & is the power low. In line of sight very high frequency signals are transmitted in straight line from antenna to antenna.

Classification of wireless transmission: -

Wireless transmission can be divided into 3 parts.

1. Radio waves
2. Micro waves
3. Infrared waves

- Electromagnetic waves ranging in frequency between 3 KHz to 1GHz are normally called Radio Wave.
- Electromagnetic waves ranging in frequency between 1 KHz to 300 GHz are normally called Micro Wave.
- Radio waves are used for multicast communications such as radio and television system.
- Micro waves are used for unicast communications such as cellular telephone, satellite networks and wireless LANs.

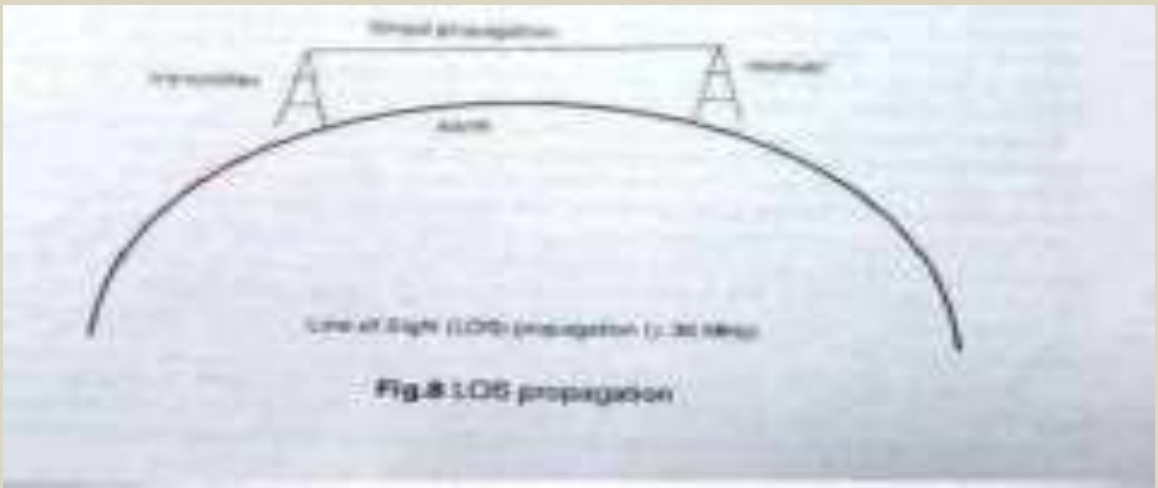


Fig.6 LOS propagation

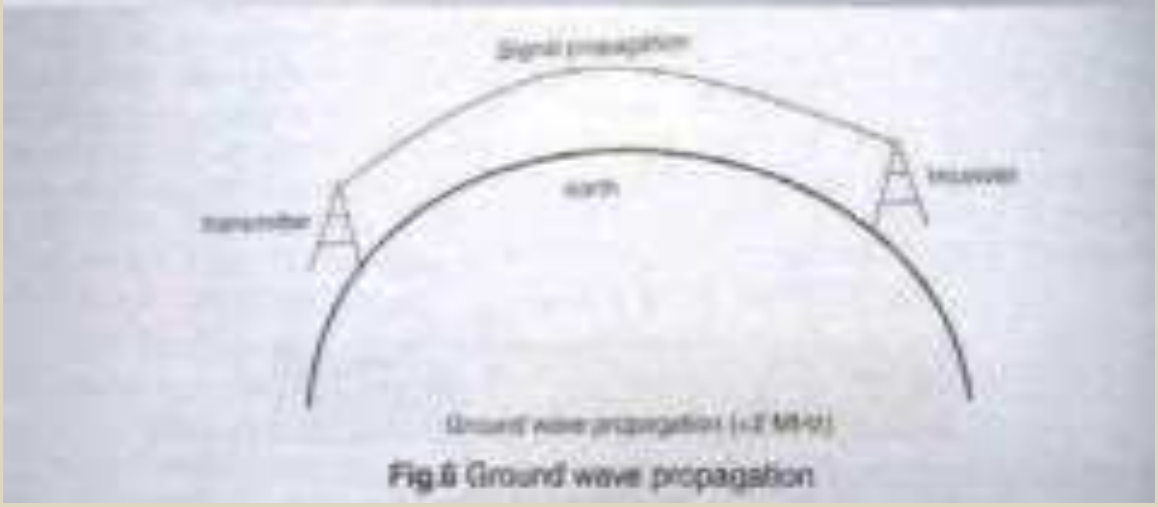


Fig.6 Ground wave propagation

Fig.6 Ground wave propagation

Multiplexing: -

I. Multiplexing provides a mechanism to share the use of a common channel by two or more devices.

II. Multiplexing is a technique for sending more than one information signal over a single common path or medium or channel.

III. So, multiplexing is named as many-to-one.
IV. It means signals for many devices can be transmitted through one transmission medium at a time or simultaneously.

Multiplexing is of 4 types.

1. Space Division Multiplexing (SDM)
2. Frequency Division Multiplexing (FDM)
3. Time Division Multiplexing (TDM)
4. Code Division Multiplexing (CDM)

1. Space Division Multiplexing: -

i. Space Division Multiplexing means division of available space, so that multiple sources can access the medium at the same time.

ii. Channels are assigned on the basis of a space but operate on same frequency.
iii. The assignment makes sure that the transmission doesn't interfere with each other as guard band in between the channel are provided.
iv. Overlap, Recovery of each of the signal is possible at the receiving end.
v. In order to prevent of overlap of the signals and to simplify filtering, each of the modulating signals is separated by a guard band, which consists of an unused portion of the available of frequency spectrum.

vi. Each user is assigned a given frequency band for all time.

2. Frequency Division Multiplexing: -

i. Frequency Division Multiplexing is a method in which each signal is allocated.
ii. A frequency slot within the overall transmission bandwidth.
iii. In other words, the total available frequency bandwidth on the transmission line is divided into frequency channel and each informational signal occupies one of the channels.
iv. The signal we have exclusive use of this frequency slots all the time i.e., each subscriber occupies his or her own slot.

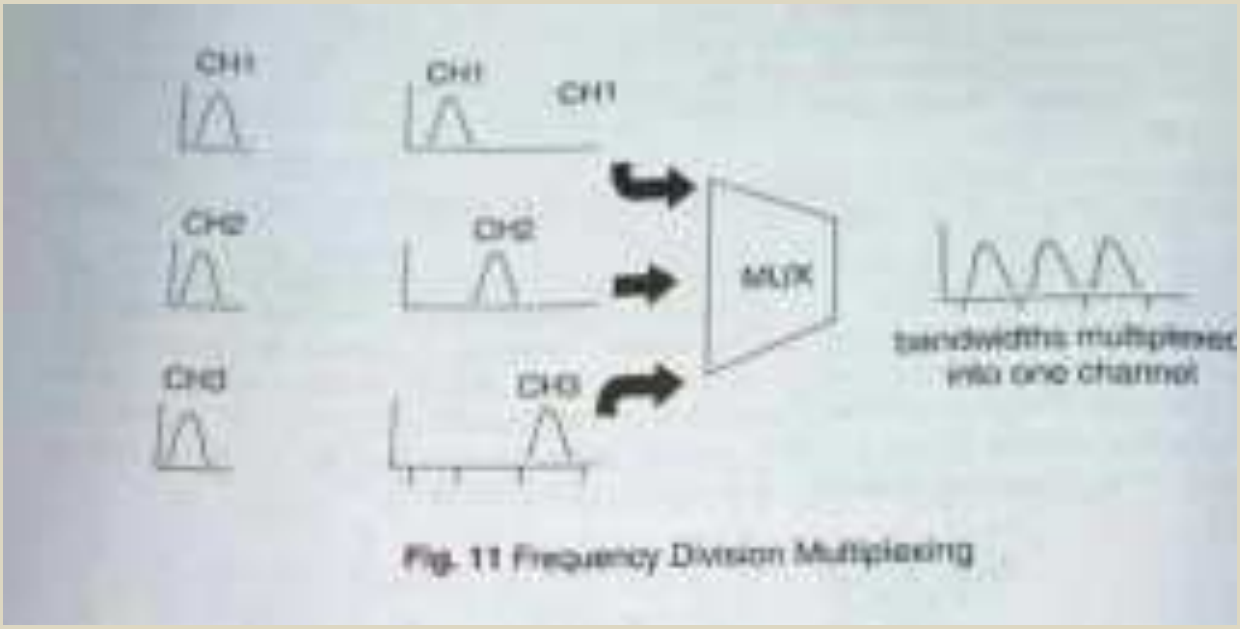


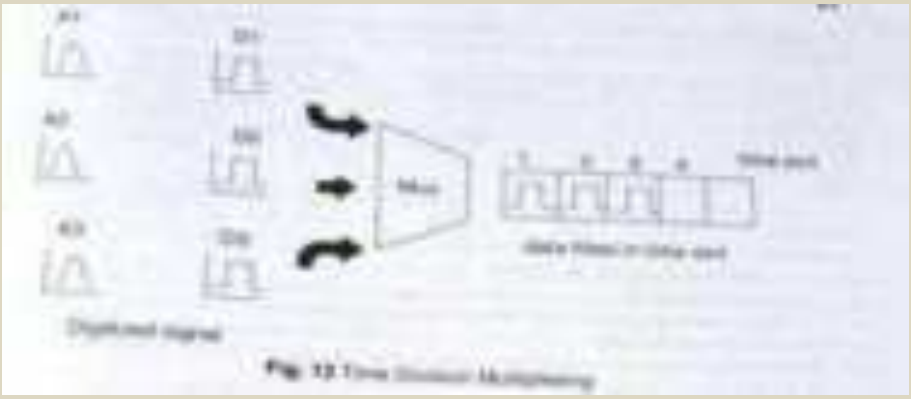
Fig. 11 Frequency Division Multiplexing

Example: Suppose a long-distance cable is available with a bandwidth allotment of 3 MHz i.e., 3000 KHz.

→ It is possible to place 1000 signal each of 3KHz wide into the long-distance channel.
→ The circuit that does, this is called as Multiplexer.
→ At the receiving end, there is a De-multiplexer, which can separate out the individual signal from the complex signals.

3. Time Division Multiplexing: -

i. Time Division Multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval or slot or slice for the transmission of each channel i.e. the channels take turn to use the link.



ii. Some kind of periodic synchronizing signal or identifier is required so that receiver can tell which channel is reached.

iii. Time Division Multiplexing becomes inefficient when traffic is less or there is no traffic; because the time slot is still allocated even when the channel has no data to transmit.

4. Code Division Multiplexing: -

i. Code Division Multiplexing is a technique in which each channel is transmits its bits as a coded channel specific sequence of pulses.

ii. It allows signals from a series of independent sources to be transmitted at the same time over the same frequency band.

iii. This is archived by using codes to spread each signal over a large common frequency band.

iv. At the receiving end, the appropriate code then used again to recover the particular signal intended for a particular user.

v. All channels each with a different code can be transmitted over the same fiber and asynchronously demultiplexed.

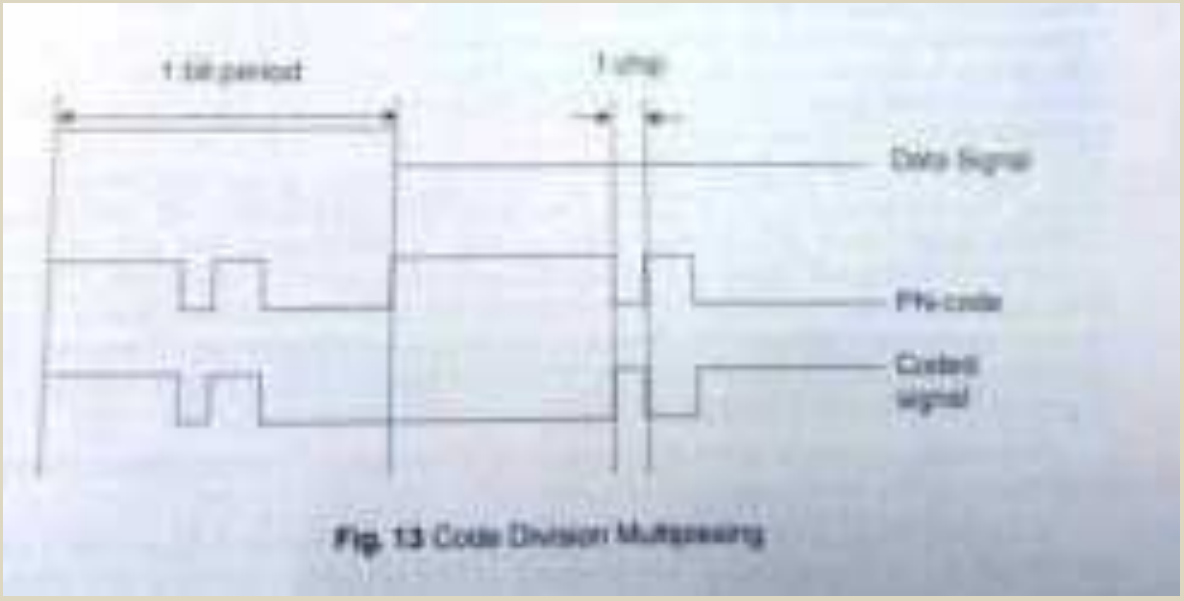


Fig. 13 Code Division Multiplexing

Characteristics of wireless communication: -

Wireless communication system can transmit either analog or digital information. Two situations may arise.

1. Transmission of analog data over analog communication system.
2. Transmission of digital data over analog communication system.

- When analog data is transmitted on transmission medium no encoding is request but when digital data is transmitted one analog transmission medium encoding is necessary.
- The circuits and devices for this communication system are complex but digital wireless communication has the following advantages.
- The digital wireless communication data is transmitted as stream of 0's and 1's so it is easier to differentiate noise signals from the informational signal.
- Reliability of digital signal can be increased by adding parameters such as checksums, error-correcting codes to ensure reliability of data.
- The transmission can take advantage of comparison by the removal of repeating patterns of 0's and 1's from data stream to conserve bandwidth.

- This transmission can be made secure by application of a encryption and authentication algorithms to ensure that 3rd party can't view or tamper with the information stream.

Modulation: -

a. Size of antenna required for wireless transmission is inversely proportional to the frequencies of the transmitted signal.
b. So, it is concluded that low frequency signal need very large antenna for their transmission.
c. Due to the properties of signal, propagating medium, very low frequency signal can't be transmitted across long distance without the loss in the signal strength.
d. So, modulation is requiring in wireless transmission by increasing the compatibility of the transmitted signal and the medium transmission.

Signal consists of two components.

1. Information Signal
2. Carrier Signal

- The transmission of any signal over same communication medium usually involves modulation of a carrier.
- Before the transmission the information signal & the carrier signal are combining and the process of combining these two signals is called **Modulation**.
- A device that performs modulation is known as a modulator and the device that performs the inverse operation of modulation is known as a **Demodulation**.
- A device that can do both operations is called as a **Modem**.

Size of antenna $\propto$ 1/f

Information signal (Low frequency signal)

Carrier Signal (High frequency signal)

A carrier is high frequency signal with which the information signal is super-imposed (combine) by a process called as a modulation.

Modulation is two types.

1. Analog Modulation
2. Digital Modulation

Analog Modulation:

Modulation of an analog signal or analog to analog conversion is the representation of analog information by an analog signal. Analog modulation is 3 types.

1. Amplitude Modulation (AM)
2. Frequency Modulation (FM)
3. Phase Modulation (PM)

Amplitude Modulation: -

In Amplitude Modulation the carrier signal is modulated so that it's amplitude varies with the changing amplitude of the modulating signal.

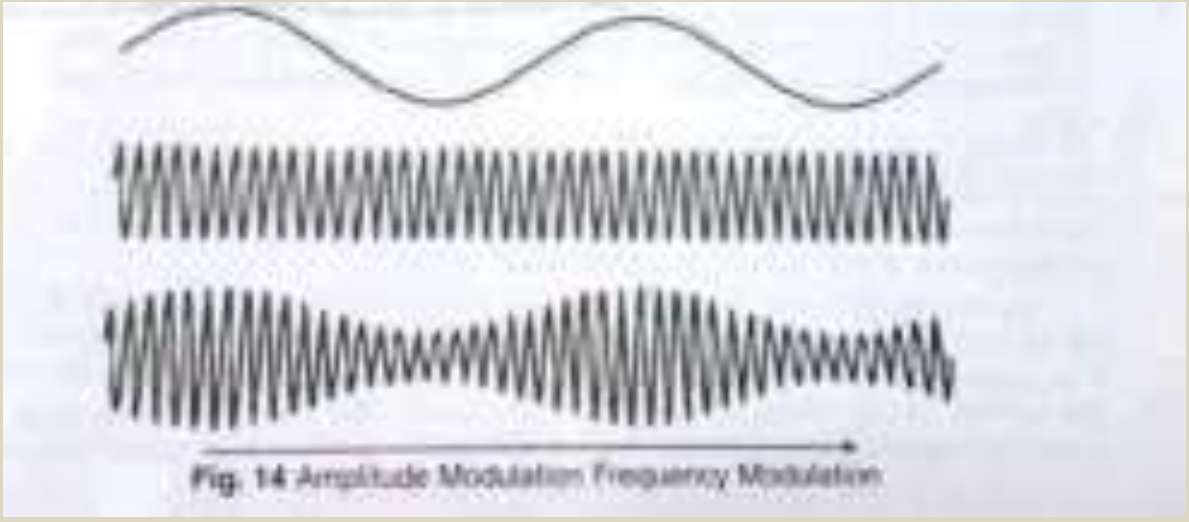


Fig. 14 Amplitude Modulation Frequency Modulation

The Frequency and Phase of the signal remains constant, only the Amplitude of the carrier signal changes to follow variation of in the information signal.

BWT = 2 * BWA

Frequency Modulation: -

In frequency modulation the Frequency of the carrier signal is modulated to follow the changing Amplitude of the modulating signal.

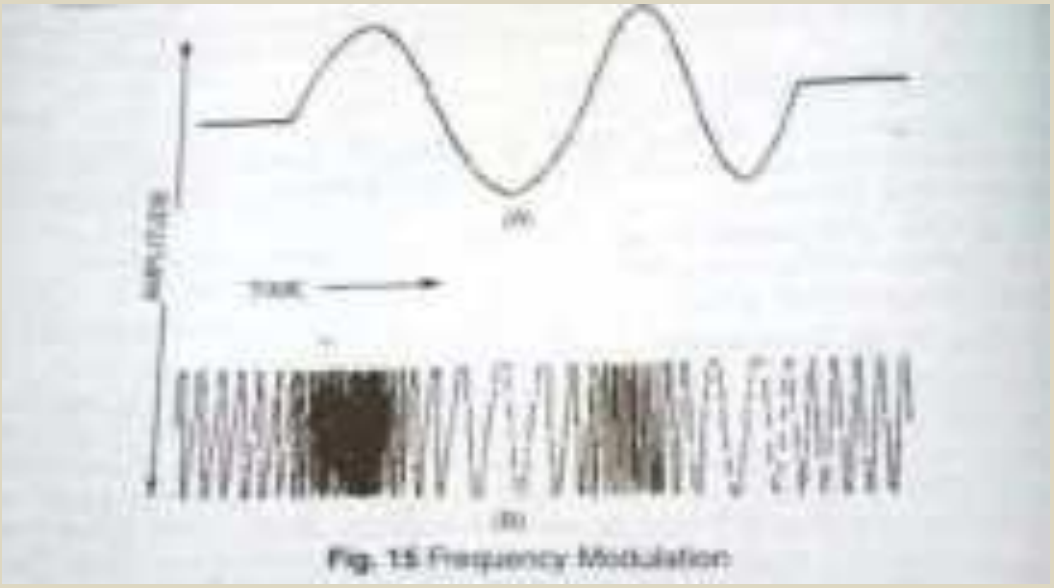


Fig. 15 Frequency Modulation

It means when there is change in the Amplitude of information signal, Frequency of the carrier signal changes but the Amplitude and Phase of the carrier signal remains constant.

The total bandwidth required for Frequency Modulation can be determined from the bandwidth of the audio signal.

BWT = 10 * BWA

Phase Modulation: -

In Phase Modulation, the phase of the carrier signal is modulating to follow the changing Amplitude of the modulating signal or information signal.

It means the Phase of the carrier signal changes only when there is change in Amplitude in the information signal, whereas the Amplitude and Frequency of the carrier signal remains constant.

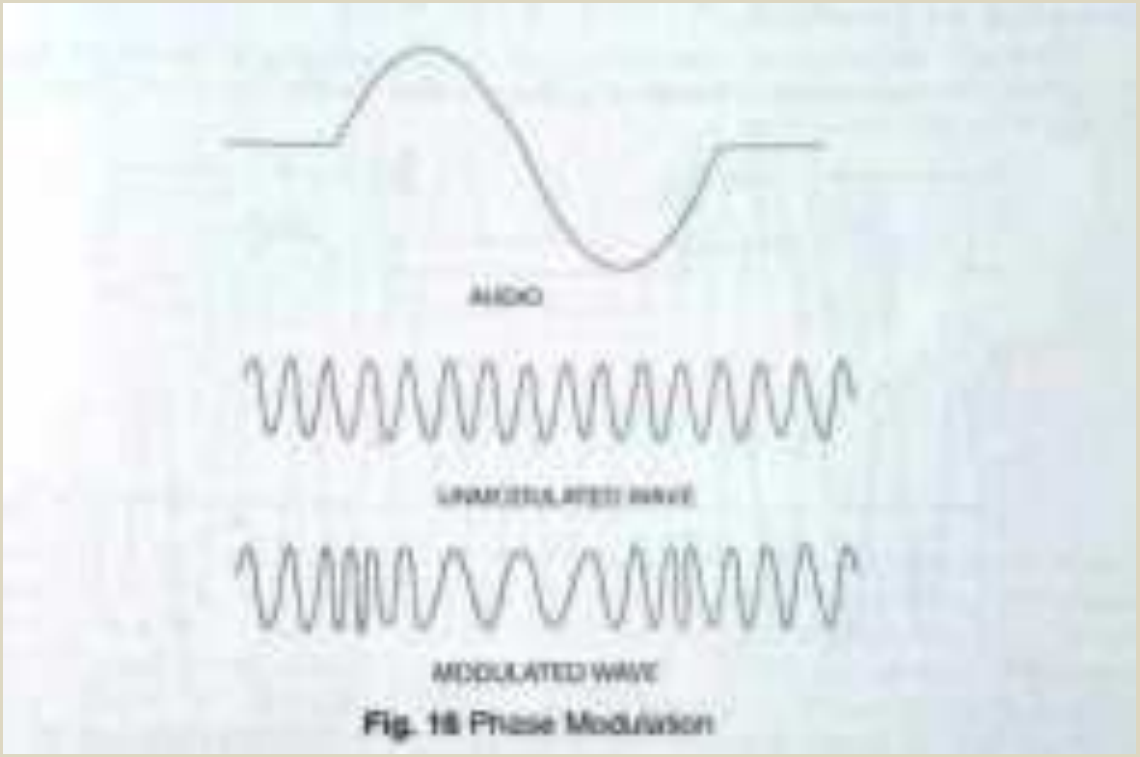


Fig. 18 Phase Modulation

Digital Modulation:

In digital modulation an analog carrier signal is modulated by a digital bit stream of either equal length signal or varying length signal.

This can be described as a form of analog to digital conversion. Digital Modulation is of 3 types.

1. Amplitude Shift Keying (ASK)
2. Frequency Shift Keying (FSK)
3. Phase Shift Keying (PSK)

Amplitude Shift Keying:

- In Amplitude Shift Keying, the strength of the carrier signal is varied to represent binary 1 or 0.

- Both frequency & phase remains constant while the Amplitude of the carrier changes.
- It means in the information signal (digital signal) when the bit is 1, the Amplitude of the carrier signal changes whereas the Frequency & Phase of the carrier signal remains unchanged.

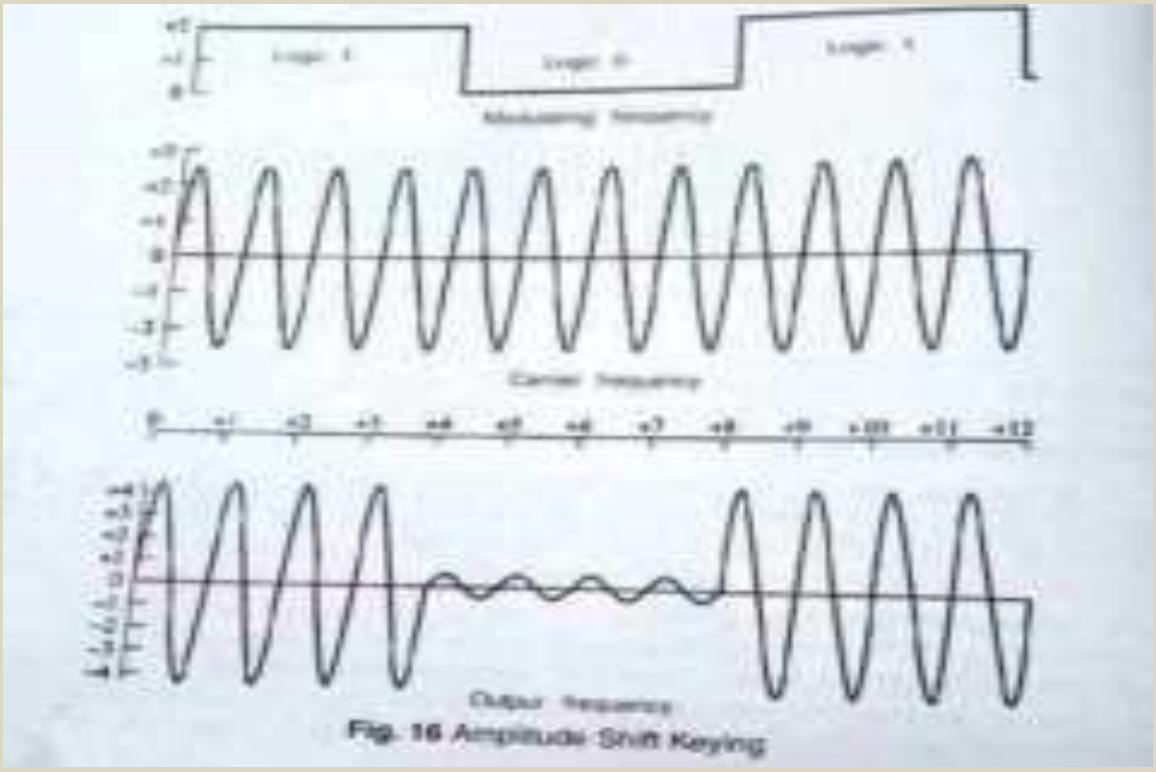
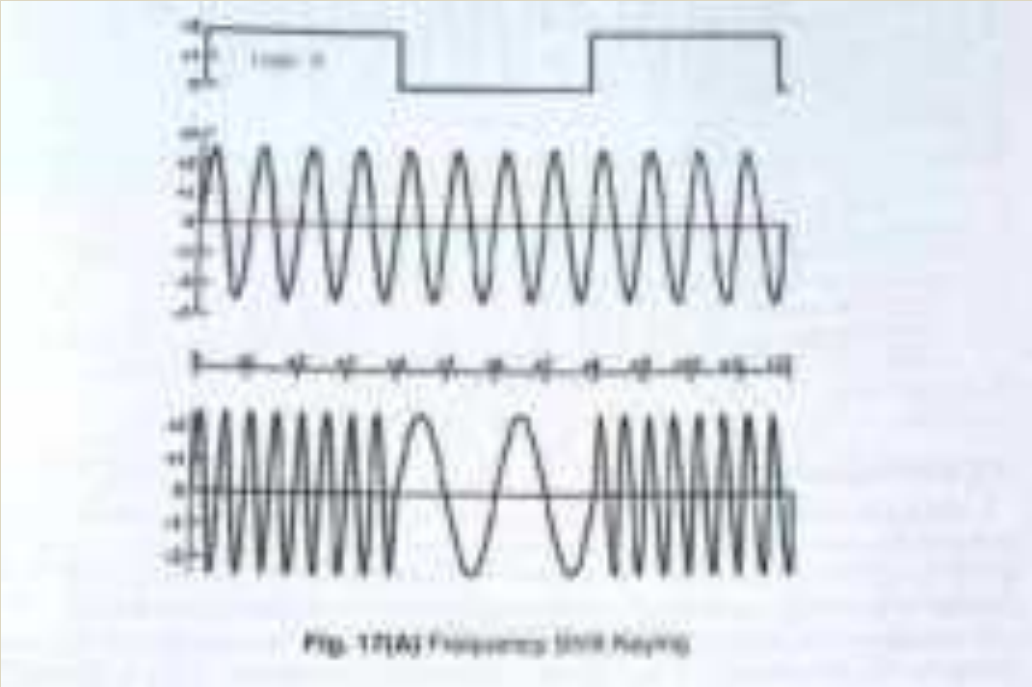


Fig. 16 Amplitude Shift Keying

- Similarly, when the bit is 0, there is no change of the Amplitude of the carrier.

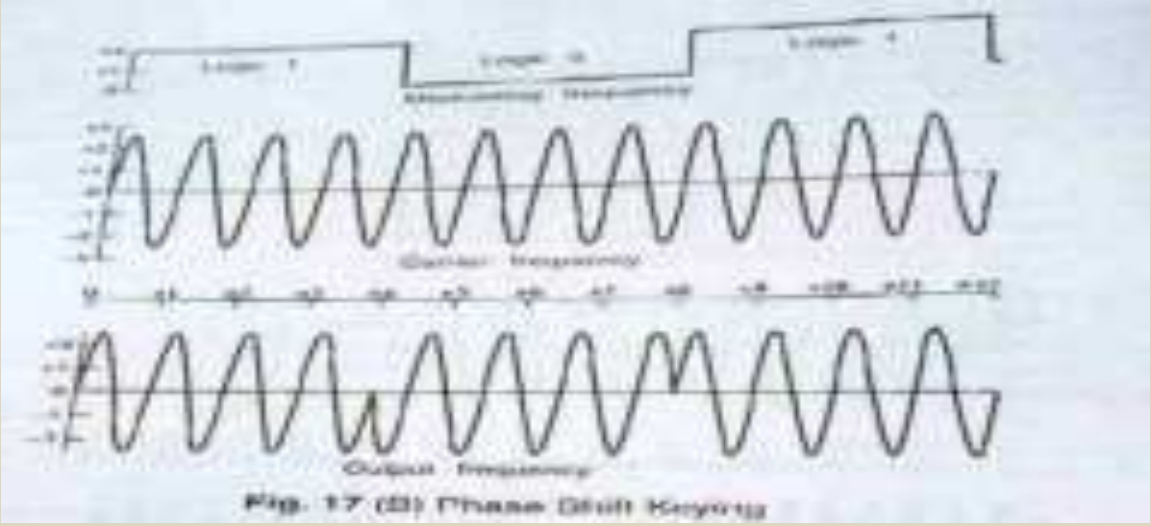
Frequency Shift Keying:

- In Frequency Shift Keying, Frequency of the carrier signal is changed when the information signal contains a binary 1 bit but there is no change in the frequency of the carrier signal if the information signal contains a binary 0 bit.
- However, the Amplitude and Phase of the carrier signal remains constant.



Phase Shift Keying:

- In Phase Shift Keying, the Phase of the carrier signal is changed if the information signal contains a binary 1 bit, but there is no change in the Phase of the carrier signal if the information signal contains a binary 0 bit.
- However, the Amplitude & Frequency of the carrier signal remains constant.



Information Signal (Digital Signal): -

Spread Spectrum: -

I. In any communication a band sometimes called as frequency band i.e. a specific range of frequency in the Radio Frequency Spectrum (RF), which is a divide among ranges from extremely low frequency to extremely high frequency.

II. Each band has a defined upper & lower frequency limit.

Designation	Frequency Band
ELF – Extremely Low Frequency	3Hz to 30 Hz
SLF – Super Low Frequency	30 Hz to 300 Hz
ULF – Ultra Low Frequency	300 Hz to 3000 Hz
VLF – Very Low Frequency	3KHz to 30KHz
LF – Low Frequency	30KHz to 300KHz
MF – Medium Frequency	300KHz to 3000KHz
HF – High Frequency	3MHz to 30 MHz
VHF – Very High Frequency	30 MHz to 300 MHz
UHF – Ultra High Frequency	300 MHz to 3000 MHz
SHF – Super High Frequency	3 GHz to 30 GHz
EHF – Extremely High Frequency	30 GHz to 300 GHz

III. Electric magnetic spectrum with largest wave-length from 10cm to 300000Meter or more are called Radio Waves.

IV. The radio spectrum is further divided into hands that are useful for specific applications.

Gamma Rays	X – Rays	Ultra Visible	Visible Light	Infrared	Micro Waves	Radio
10^{-11}	10^{-9}	10^{-7}	10^{-5}	10^{-3}	10^{-1}	10^{3}

V. Spread spectrum is an RF communication system in which the base band, signal band width is spread over a larger band width by injecting a higher frequency signal as a direct consequence.

VI. Energy used in transmitting the signal is spread over a wider bandwidth and appears as noise.
VII. The ratio in dB between the spread base band and the original signal is called Processing gain.
VIII. To apply an SS technique, simply in the corresponding SS code somewhere in the transmitting change before the antenna.
IX. That injection is called the spreading operation.
X. The effect is to diffuse the information in a large of band width.
XI. Conversely the SS code can should be removing at a point in the receiving chain before the data is retrieved.
XII. Removal of SS code is called as **Dispreading Operation**.
XIII. The effect of a dispreading operation is the formation of the information signal in its original bandwidth.

In spread spectrum, the transmission signal bandwidth is much higher than the information bandwidth. All spread spectrum system can be treated as a two steps modulation process.

Step: 1

Data to be transmitted is modulated.

Step: 2

The carrier is modulated by SS code causing it to spread over a large bandwidth.

Spread Spectrum Technique: -

Different techniques are distinguishing according to the point in the system at which a Pseudo Random Number (PRN) is inserted in the communication channel.

- In the PRN is inserted at the data level it is called as Direct Sequence Spread Spectrum (DSSS).
- In this the Pseudo Random Sequence is mixed or multiplies with the information signal giving an impression that the original data flow was hashed by the PRN.

- If the PRN acts the carrier frequency level it is called as Frequency Hopping Spread Spectrum (FHSS).
- If the PRN acts as ON/OFF get to the transmitted signal, this is called as Time Hopping Spread Spectrum (THSS).
- DSSS and FHSS can be combined to form Hybrid Spread Spectrum.

Generally, the Spread Spectrum Technique is two types.

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Spectrum (FHSS)

1. Direct Sequence Spread Spectrum: -

It is generally used to transmit digital information. Here the digital information channel is mixed with a Pseudo Random Code whose bandwidth is much greater than that of the signal itself.

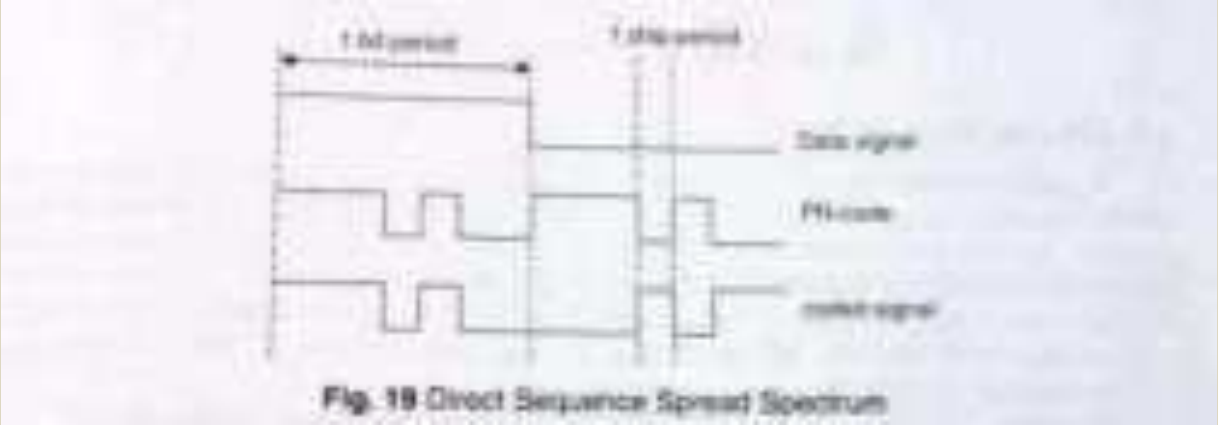


Fig. 19 Direct Sequence Spread Spectrum

In this method the PRN or Pseudo Random Code are applied directly to the entering the carrier modulator. These codes are not required to provide call security but created a uniqueness to enable call identification.

2. Frequency Hopping Spread Spectrum: -

It is a form of spreading in which the frequency of the carrier is changed many times within a fixed time period in accordance with a fixed time period in accordance with a Pseudo Random List of channels.

The signals jump from on the frequency to another within a given frequency range.

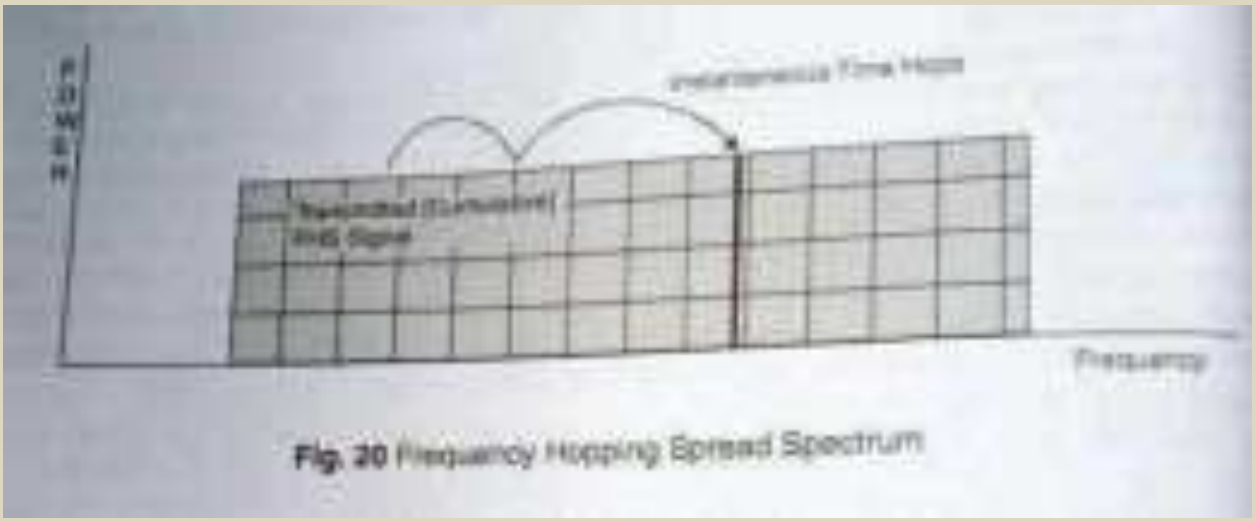


Fig. 20 Frequency Hopping Spread Spectrum

The transmitter device listens to a channel, if it detects an idle time; it transmits the data using the full channel bandwidth. If the channel is busy or full, it hopes to another channel and it repeats the process. The transmitter & receiver jump in a same manner.

The total available bandwidth is split into many channels of smaller bandwidth and guard spaces. Transmitter and receiver stay on one of these channels for a certain time period and then hope to another channel.

Cellular System: -

A cellular mobile communication system uses a large number of low power wireless transmitters to create cells in order to word properly a cellular system must verify the following two conditions.

1. The power level of transmitter within a single cell must be limited in order to reduce the interference with the transmitters or neighboring.
2. The neighboring cells can't share the same channels in order to reduce the interference the frequency must revised only a certain pattern.

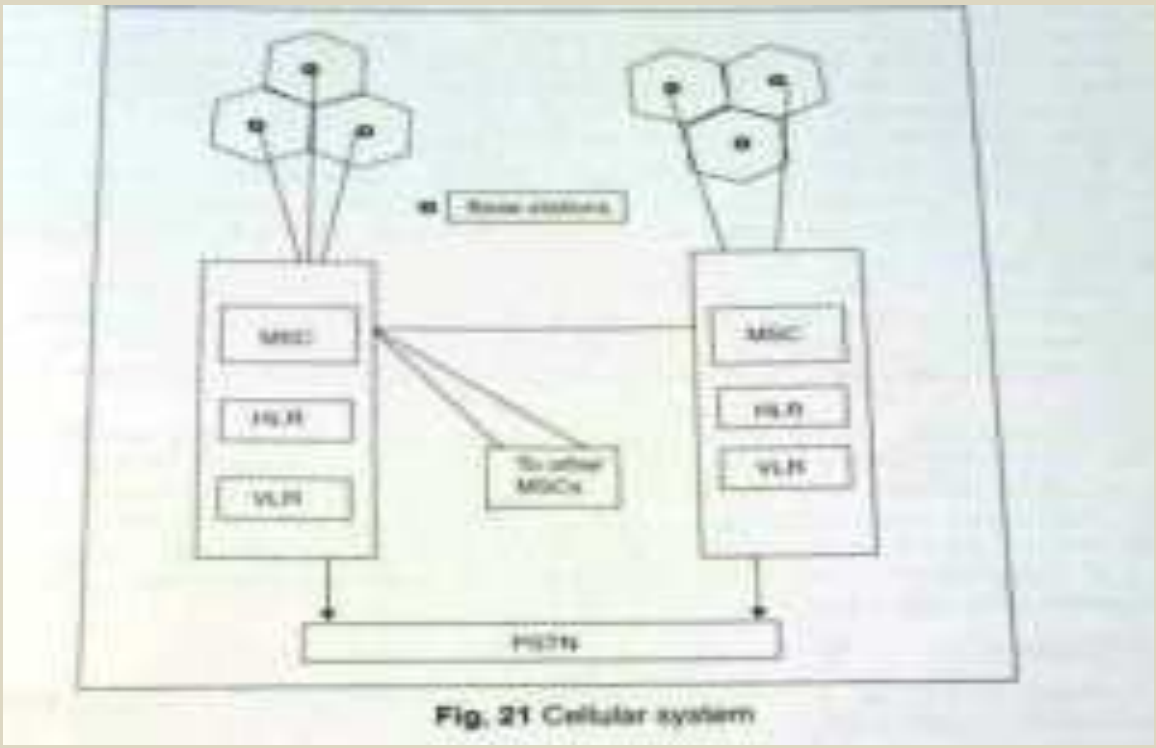


Fig. 21 Cellular system

A cellular network is a radio network made up of a number of radio cells served by a fixed transmitter known as cell site or based station. These cells are used to cover different area in order to provide radio coverage over a wider area than the area of one cell.

Cellular network has the following advantage.

→ Increase capacity
→ Reduced Power usage
→ Better coverage

The cellular system includes the following technical terms for its implementation.

1. Cells
2. Cluster
3. Frequency reuse
4. Handovers

Cells: -

- Cell is the basic geographical unit of a cellular system.
- Cells are base stations transmitting over small geographic areas that are represented as hexagons.
- Each cell size varies depending on the land-scape.
- Because of constraints imposed by natural terrain and manmade structure, the true shape of cells isn't a perfect hexagon.
- Different types of cells are used which are as follows.

1. Macro cell
2. Micro cell
3. Selective cell
4. Umbrella cell

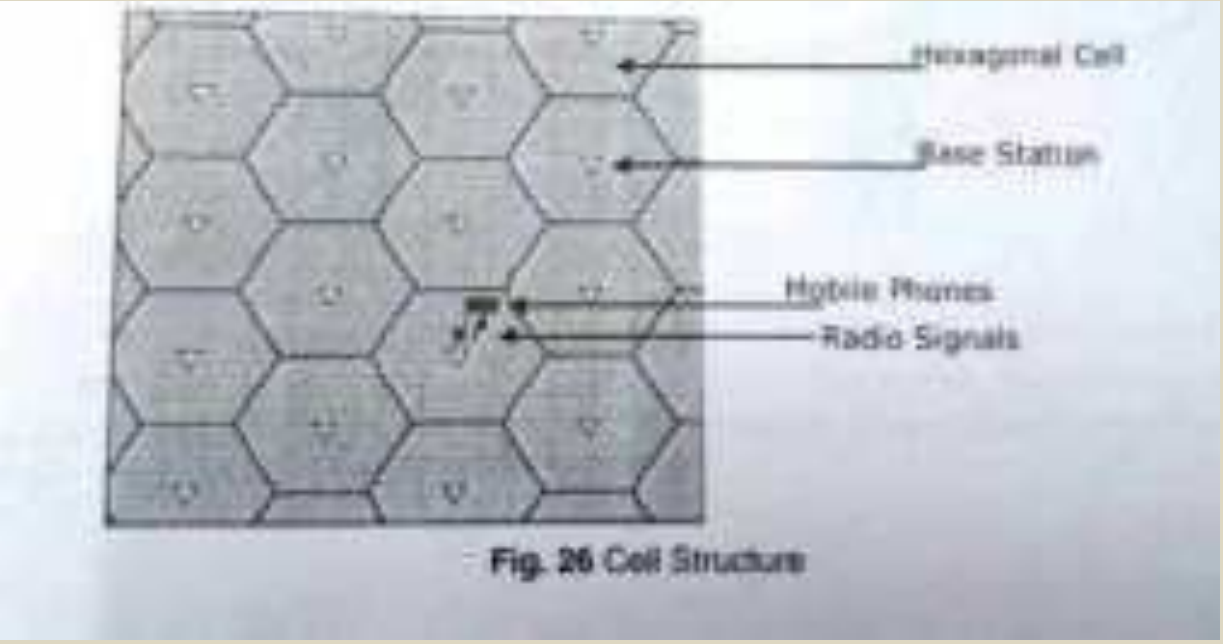


Fig. 26 Cell Structure

- A mobile communication system has a cell structure constituted by integrating macro cells & micro cells and at least one MS.
- Macro cells are large cell for remote and a sparsely populated area.
- However, micro cells are used for density populated areas.
- By splitting existing areas into smaller size cell, the available channels are increased as well as the capacitive of the cell.

Selective Cell: -

- These cells should be defined in such a way that they prove their existence.
- For example: The selective cells are the cells which are located at the entrance of a tunnel. The areas of cells need not to be of 360^{o} always.

Umbrella Cells: -

- Crossing of small cell creates and important number of handovers among different small neighboring cell.
- To solve this problem the idea of umbrella cells was introduced. An umbrella cell covers several microcells.
- The power level inside and umbrella cell is increased comparing the power level is used in the microcells to from the umbrella cell.

Cluster: -

- A cluster is a group of cells.
- No channels are reused within a cluster.
- Number of cell in a cluster play very important role as there will smaller number of cells in cluster bigger will be number of channels per cell.
- Therefore each cell's capacity will be increase.
- One thing to take care is to avoid the interface that might occur due to never in clusters.

Fig. 22 Seven Cell Cluster

Frequency reuse: -

- Because only a smaller number of radio channels frequencies are available for mobile systems, engineers have to find a way to the reuse radio channel to carry more than one conversation at a time.
- The solution the industry adapted was called frequency planning or frequency reuse.
- The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area.
- Cells are assigned a group of channels that are completely different from neighboring cells.
- The coverage area of cells is called footprint.
- The footprint is limited by a boundary, so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.

Handover: -

- The final obstacle in the development of cellular network involved the problem created when a mobile subscriber travel from one cell to another during a call.
- As adjacent area is do not used is the same radio channels a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells.
- Because dropping the call is unacceptable, the process of handoff or handover was created.
- Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as mobile crosses adjacent cells.

Introduction: -

When a number of signal sources attempt to access wireless medium simultaneously, networks encounter the problem of receiving signal from each radio carrier distinctly. This is because of the signal interference with each other when they transmitted simultaneously through the medium. Also, networks encounter the problems of signals from hidden and exposed terminals as well as near & far terminals. To overcome these problems communication system receivers extracts distinct signals from various terminal in presence of signals divided into different cells, time states, frequencies and codes.

HIDDEN/EXPOSED TERMINALS: -

This problem does not occur on a wired LAN.

Consider the scenario with three mobile phones.

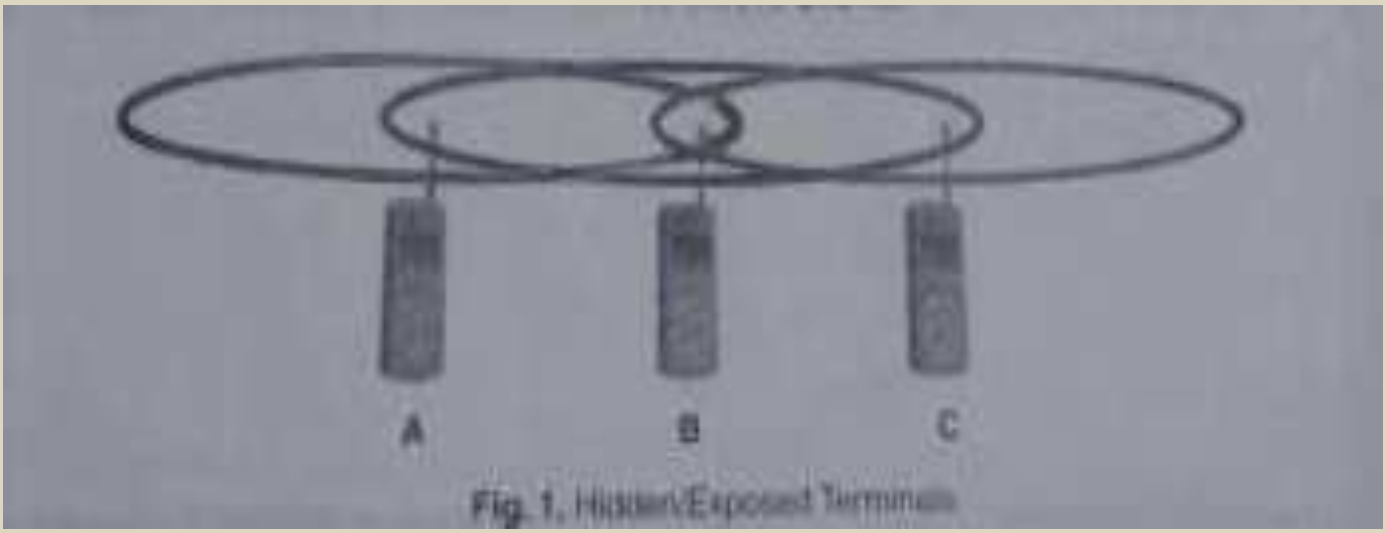


Fig. 1. Hidden/Exposed Terminals

The transmission range of A reaches B, but not C. The transmission of C reaches B, but not A. Finally, the transmission range of B reaches A and C. A can't detect C and C can't detect A.

A start sending to B, C doesn't receive this transmission. C also want send some data to B and senses the medium. Thus, C starts sending causing a collision at B. But A can't detect this collision and continues with its transmission. A is hidden for C and vice versa.

While hidden terminals cause collision, the next effect is unnecessary delay. Now, B sends something to A and C wants to send data to some other mobile phone outside

the range of A, B, and C. C senses the carrier and detects that carrier is busy. Hence, C posts pones its transmission, But as A is outside the interference range of C, waiting is not necessary. Causing a collision at B doesn't matter because the collision is too weak to propagate to A. In this situation, C is exposed to B.

Carrier Sense Multiple Access with Collision Detection CSMA/CD...

Hidden Terminal:

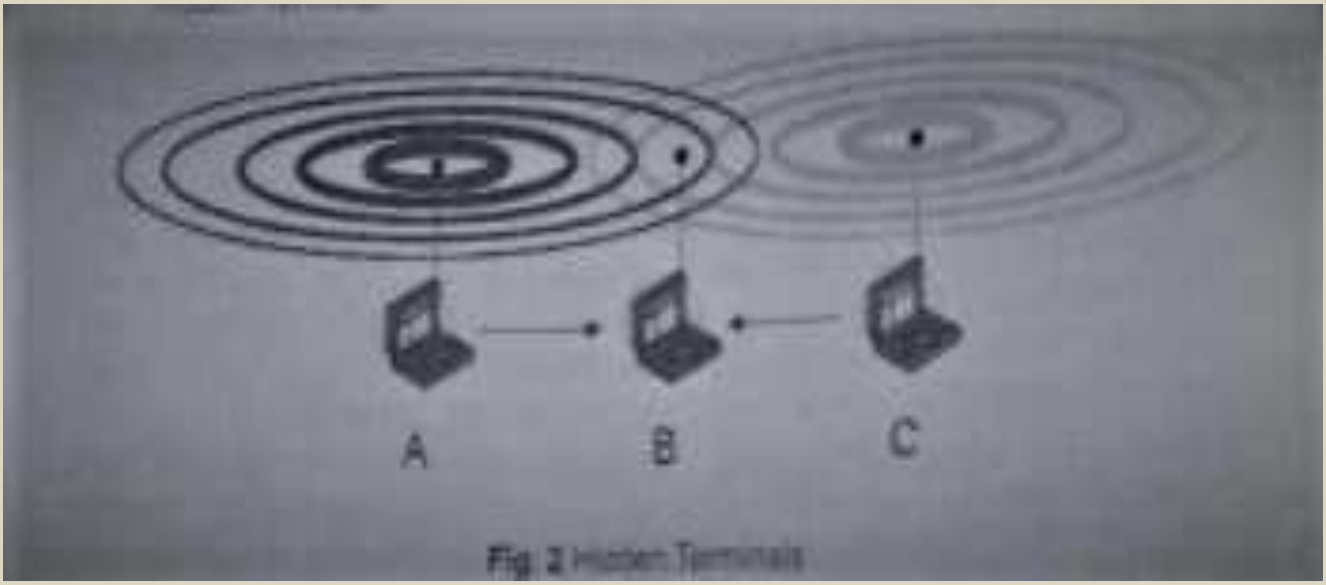


Fig. 2 Hidden Terminals

Exposed Terminal Problem:

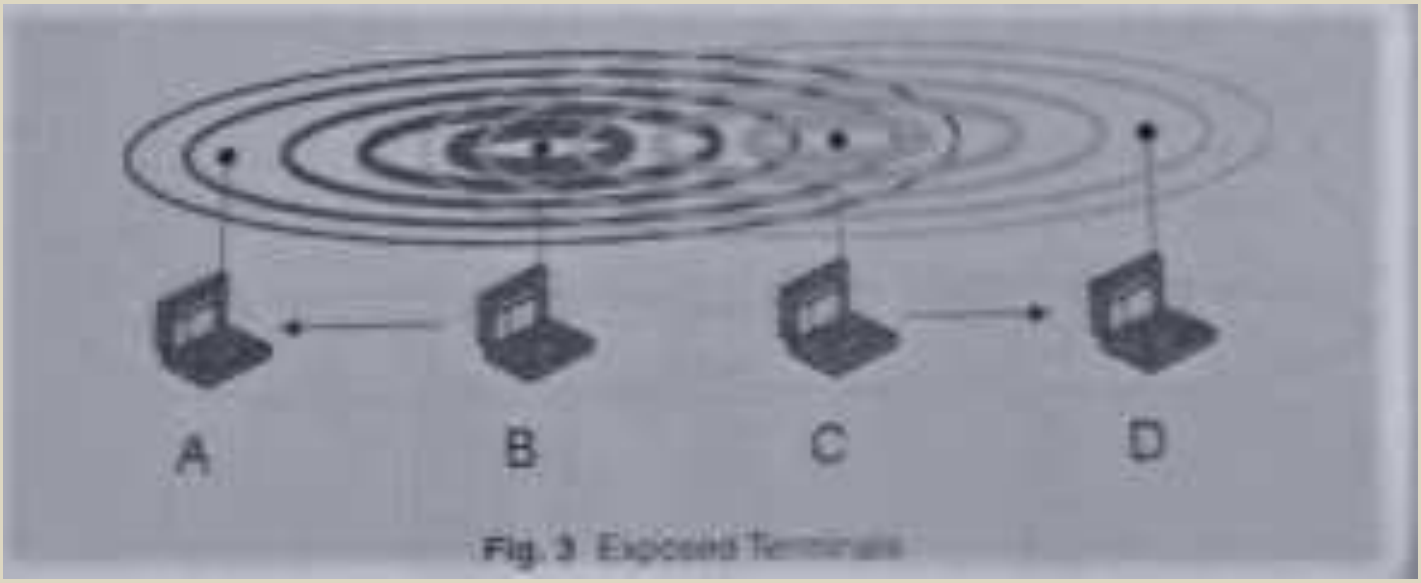


Fig. 3 Exposed Terminals

THE BASIC ACCESS METHOD: -

The basic access mechanism is carrier sense multiple access (CSMA). It is classified into 2 groups.

1) CSMA / CD (Carrier Sense Multiple Access / Collision Detecting)
2) CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance)

Problems in wireless networks: -

Signal strength decreases as the distance increases. The sender would apply CS and CD, but the collisions happen at the receiver due to a second sender. It might be the case that a sender can't hear the collision, I.e., CD doesn't work. Further, CS might not work if, e.g., a terminal is hidden. The solution is CSMA/CA.

The CSMA Protocol works as follows:

A station which wants to transmit the data senses the medium if the medium is busy, then the station will pause its transmission for some time. If the medium is sensed free then, the station is allowing the transmit.

This kind of protocol is very effective when the medium is not heavily loaded, as the allows the station. To transmit with minimum delay, there is always chance of station transmitting at the same time which may cause a collision.

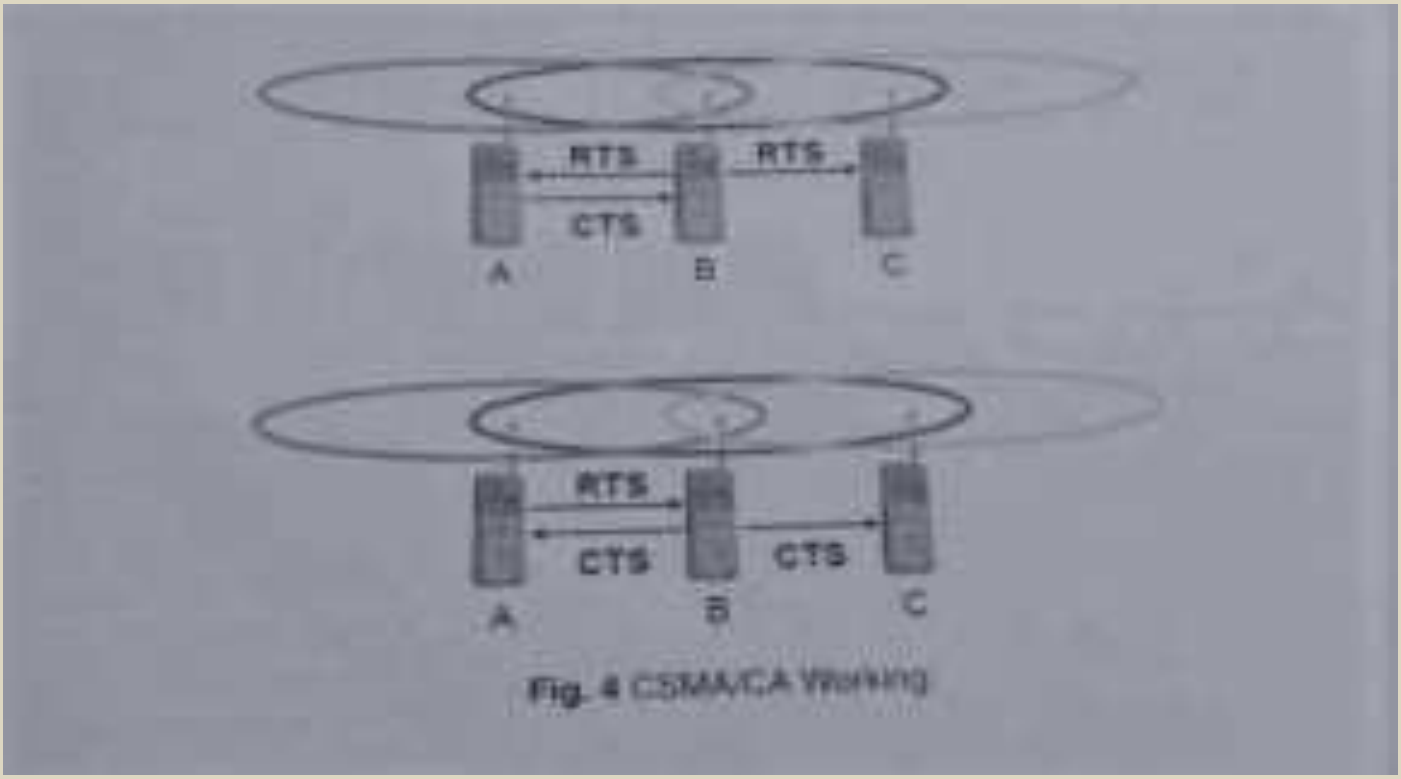


Fig. 4 CSMA/CA Working

CSMA is of 3 types.

→ One Persistent CSMA
→ Non-Persistent CSMA
→ P-Persistent CSMA

Non-Persistent CSMA:

In this method if a station waste channel is busy then it has to wait for fixed interval of time. After this time, it again checks status of the channel and if the channel is free it transmits the frame.

One-Persistent CSMA:

In this method the station which wants to transmit continuously checks the channel until it is idle (free) and then transmits immediately. The disadvantage of this method is that if two stations transmit simultaneously a collision take place.

P-Persistent CSMA:

In this method the collision and retransmission of frame is reduced in comparison to One-Persistent and Non-Persistent CSMA. In this method, all the waiting stations are not allowed to transmit simultaneously as soon as the channel is idle. A station is assumed to be transmitting with a probability P.

Example: If P = 16, then only 1 number of waiting station out of 6 stations can be allow to transmit the data.

NEAR/FAR TERMINALS: -

Consider the following scenario.

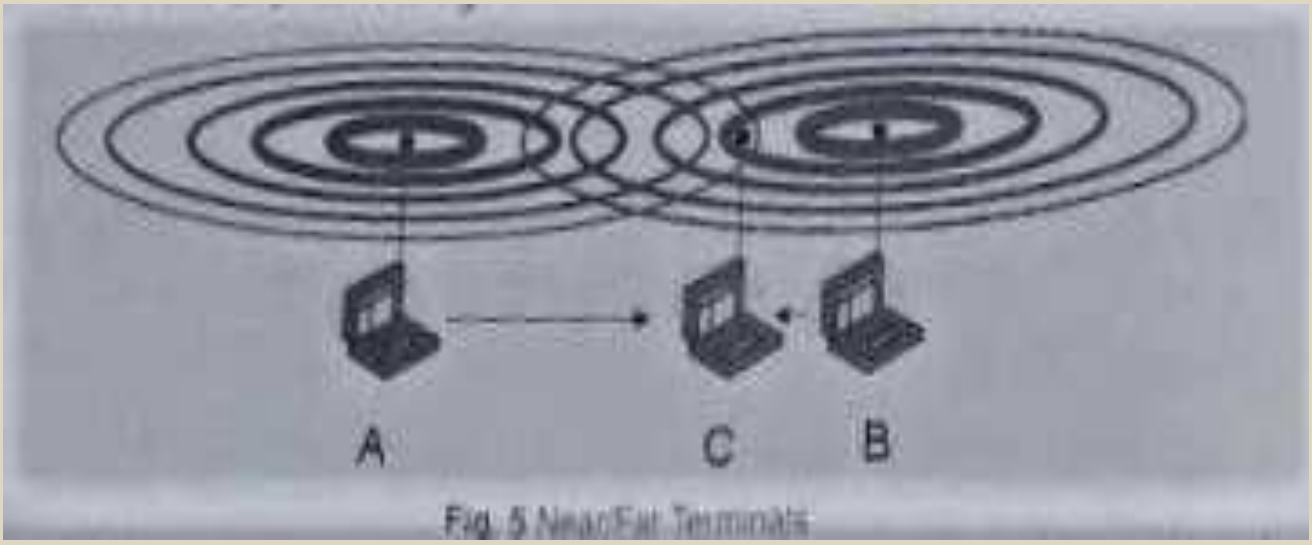


Fig. 5 Near/Far Terminals

Here A and B both are sending signals with same transmission power. As the signal strength decreases proportionally to the square of the distance. B's signal drowns out A's signal. As a result, C can't receive A's transmission.

Frequency Division Multiple Access (FDMA): -

It is one of the most common multiplexing techniques. The available frequency band is divided into channels of equal bandwidth so that each communication is carried on a different frequency. This multiplexing technique is used in all the first-generation analogue mobile networks like Advanced Mobile Phone System (AMPS) in USA and Total Access Communication System (TACS) in UK.

Each user is allocated two channels, one for uplink and another for downlink communication. No other user is allocated the same channel at the same time.

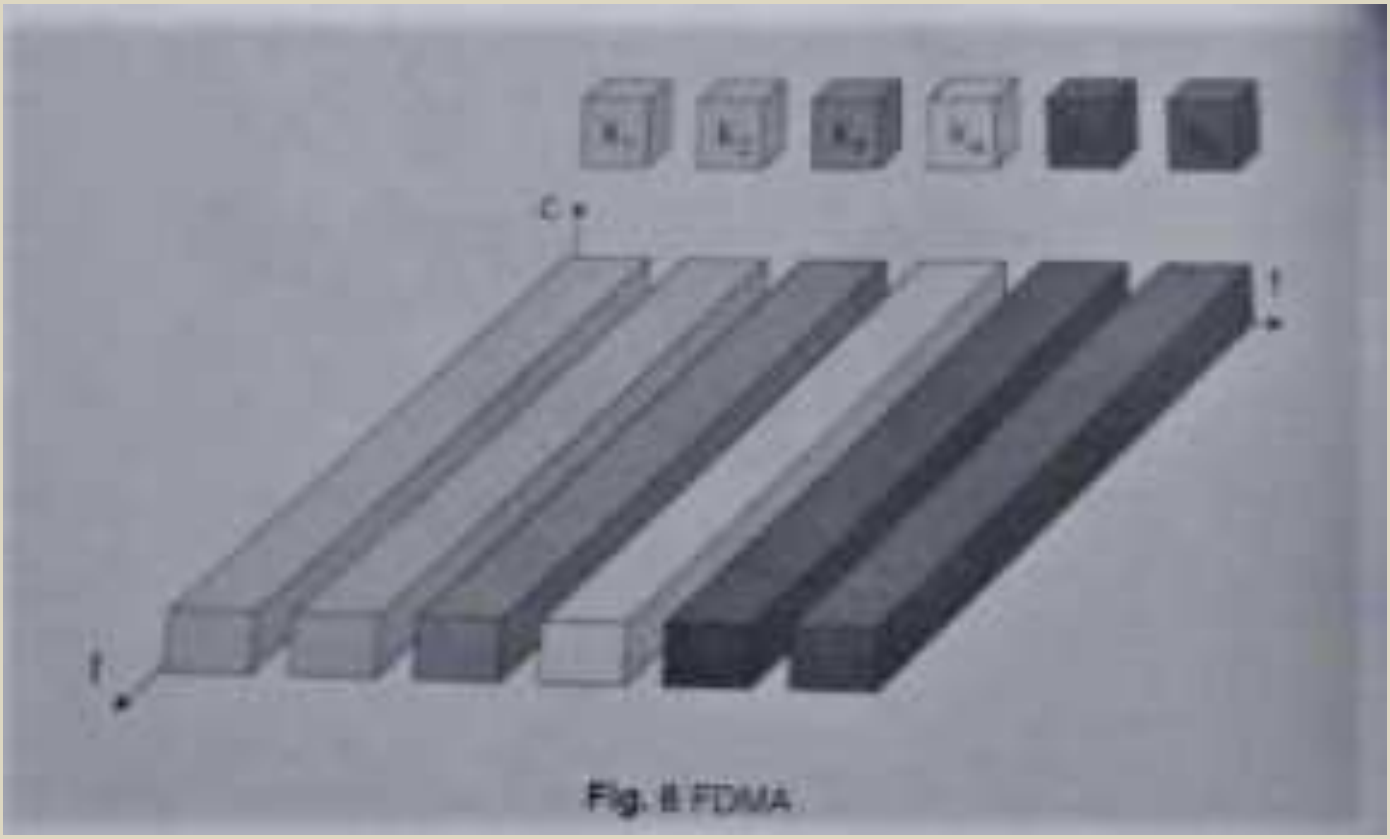
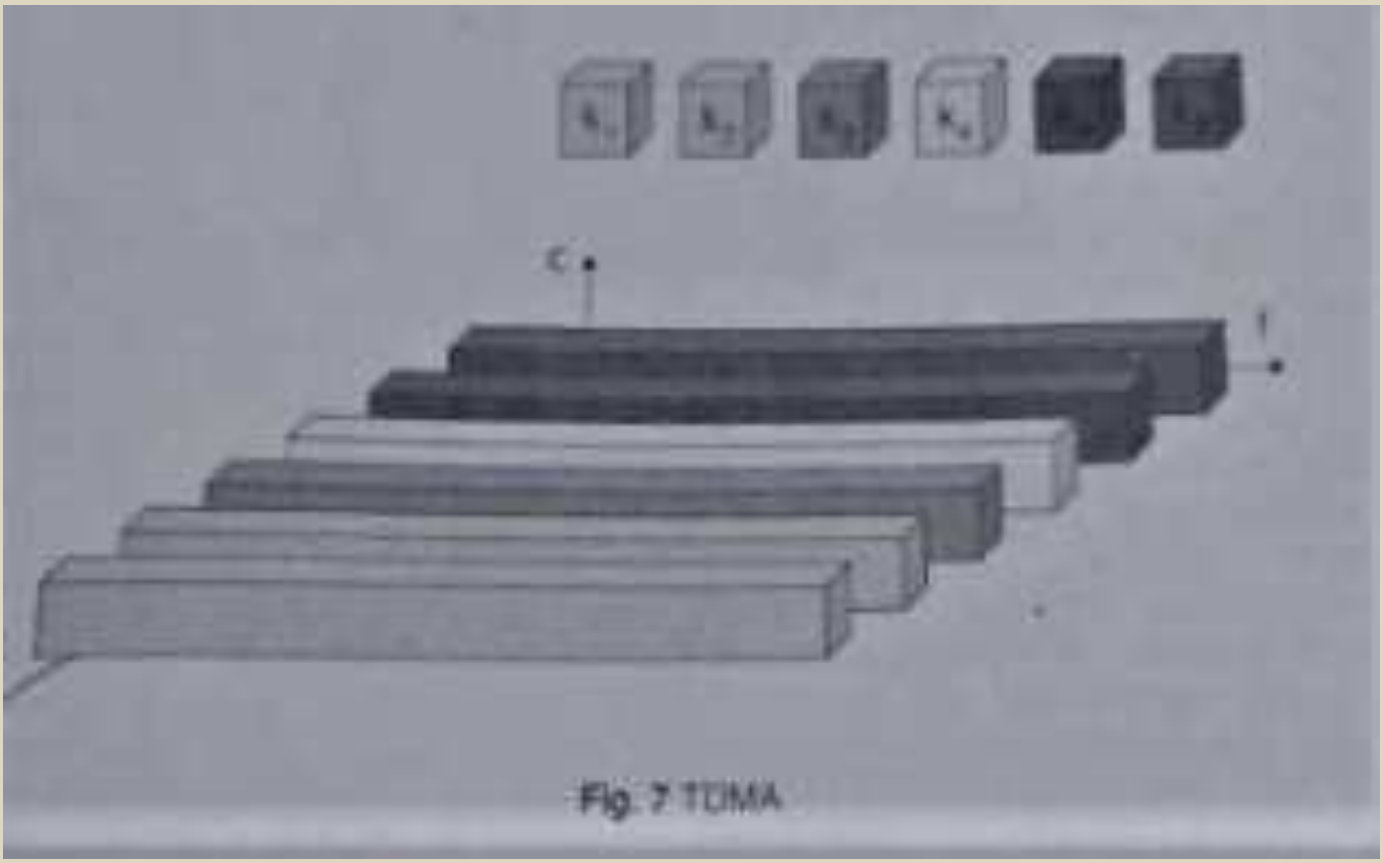


Fig. 8 FDMA

TIME DIVISION MULTIPLE ACCESS (TDMA): -

It is more expensive technique compared to FDMA as it needs proper synchronization between sender and receiver. TDMA is access method for shared medium (usually radio) networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots i.e.,

each channel is split up into time segments, and a transmitter is given exclusive use of one or more channels only during a particular time period. TDMA is used in the digital 2G cellular systems such as Global System for Mobile Communications (GSM), Personal Digital Cellular (PDC) etc. It is also used extensively in satellite systems.

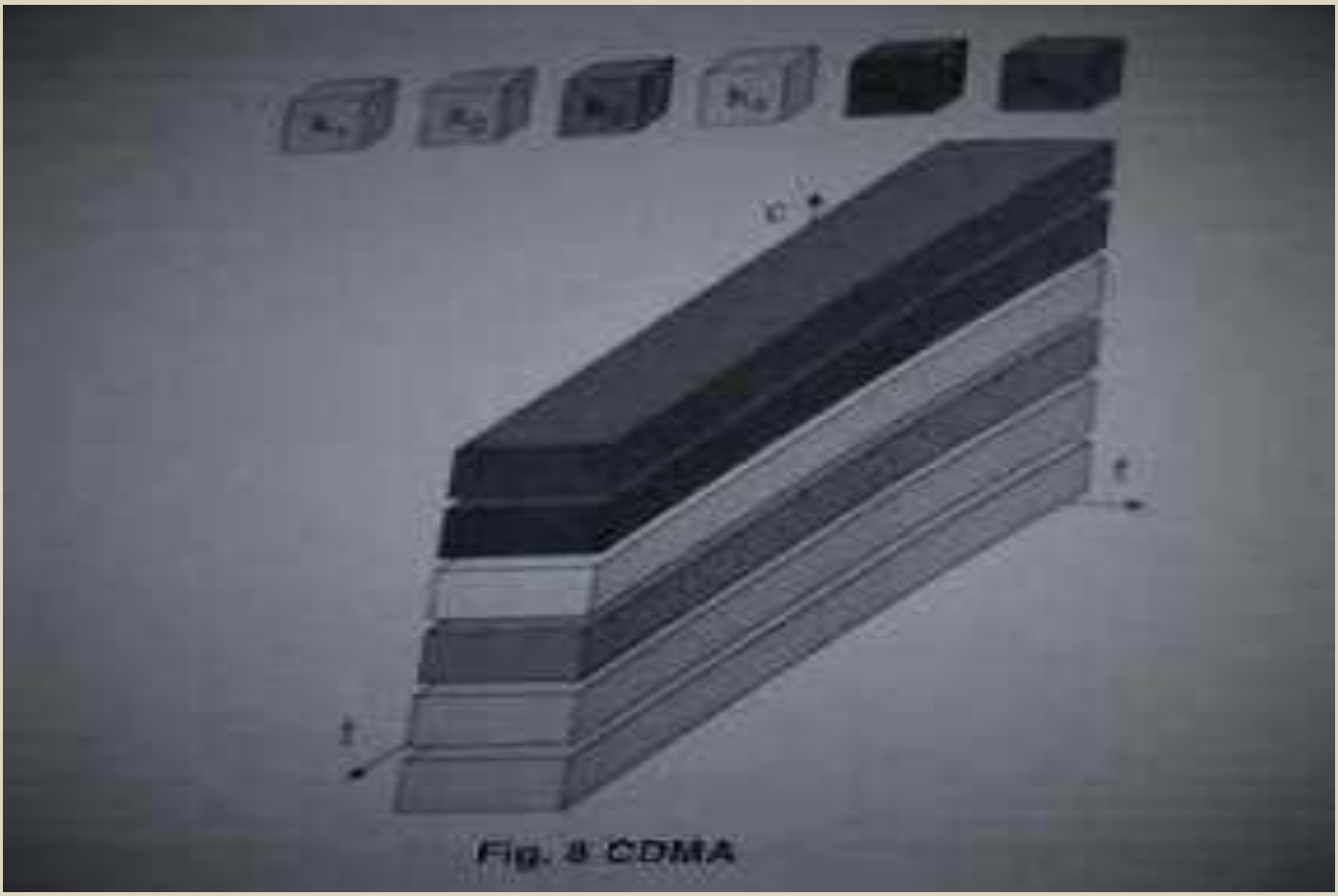


Code Division Multiple Access (CDMA): -

CDMA is a broadband system and hence functionally different from FDMA and TDMA. FDMA and TDMA transmit a strong signal in a narrow frequency band; CDMA transmits a relatively weak signal across a wide frequency band.

It goes spread spectrum technique where each subscriber uses the whole system bandwidth. Unlike TDAM and FDMA where frequency or time slot is assigned exclusively to a subscriber, in CDMA all subscribers in a cell use the same frequency and simultaneously. To separate the signals, each subscriber is assigned an orthogonal code called chip.

They are difficult to detect and jam. CDMA has been used in many communications and navigation systems, including the Global Positioning System (GPS) and in the satellite system for transportation.



Space Division Multiple Access (SDMA): -

Analog with the above access methods, space is also used effectively. This is a technique where different parts of space are used for multiplexing.

It is a technique in which a transmitter transmits the modulated signal and accesses a slot of space and another transmitter uses another slot of space such that both the signals can propagate in two separate spaces in the medium without affected each other. It is used in radio transmission and is more useful in satellite communication to optimize the use of radio spectrum by using directories properties of antenna. In SDMA, antennas are highly directional, allowing duplicate frequencies to be used at the same time for multiple surface zones on earth Precise antenna alignment is also required.

Wireless LAN & Communication: -

Wireless communication allows information exchange between two devices without the use of wires or cables. A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier to give a network connection to all users in the surrounding area. Areas may range from a single room to an entire campus. The backbone network usually uses cables with one or more wireless access point connecting the wireless user to the wired network. WLANs provide high speed data communication in small areas such as a building or an office.

WLANs transmit information by means of 3 ways. They are microwave, spread spectrum, and infrared.

Infrared: -

Infrared (IR) is electromagnetic radiation with wave length longer than visible light but shorter than radio waves. Infrared radiation is the region of the electromagnetic spread spectrum between microwaves and visible light. In infrared communication an LED transmits the infrared signal as bursts of non-visible lights. At a receiving end a photo diode detects and captures the light pulses, which are then processed to retrieve the information they contain.

Application of infrared –

1. Computers, keyboard, mouse, disk drive, printers, Headphones
2. Home security systems
3. Telephone
4. TV, VCR, CD players etc.

IR Advantage: -

- Low power requirements
- Low circuitry cost
- Simple circuitry
- Portable
- Few internationally regulatory constraints
- High noise immunity

IR Disadvantage: -

- Line of sight is required. It means transmitter and receivers must be almost directly aligned to communicate.
- Blocked by common materials such as Peoples, walks, plants etc. can blocked transmissions.
- Short range – The performance of IR communication drops off with longer distances.
- Light and weather density – Direct sunlight, rain, fog, dust, pollution can affect transmission.
- Speed, data rate transmission of infrared is lower than the wired transmission.

Radio Frequency: -

I. Radio frequency refers to that portion of the electromagnetic spectrum in which electromagnetic waves can generated by alternating current which is fed to an antenna.

II. All FM Radio station in a band of frequencies between 88 MHz and 108 MHz This band of radio spectrum is used for no other purpose but FM Radio broadcasts.

III. In the same way FM radio station can transmit a band of frequencies between 535 KHz. and 1700 KHz.

Advantages: -

- Line of sight is not required.
- Not blocked by common materials. It can penetrate most solids and pass-through walls.
- Longer range transmission.
- Not light sensitive and weather sensitive.

Disadvantages: -

- Interference communication devices using similar frequencies can interfere with transmission.
- Lack of security.

- Higher cost than infrared communication.
- Federal communication commission (FCC) licenses required for some product.
- Lower speed
- Data transmission rate is lower than were an infrared transmission.

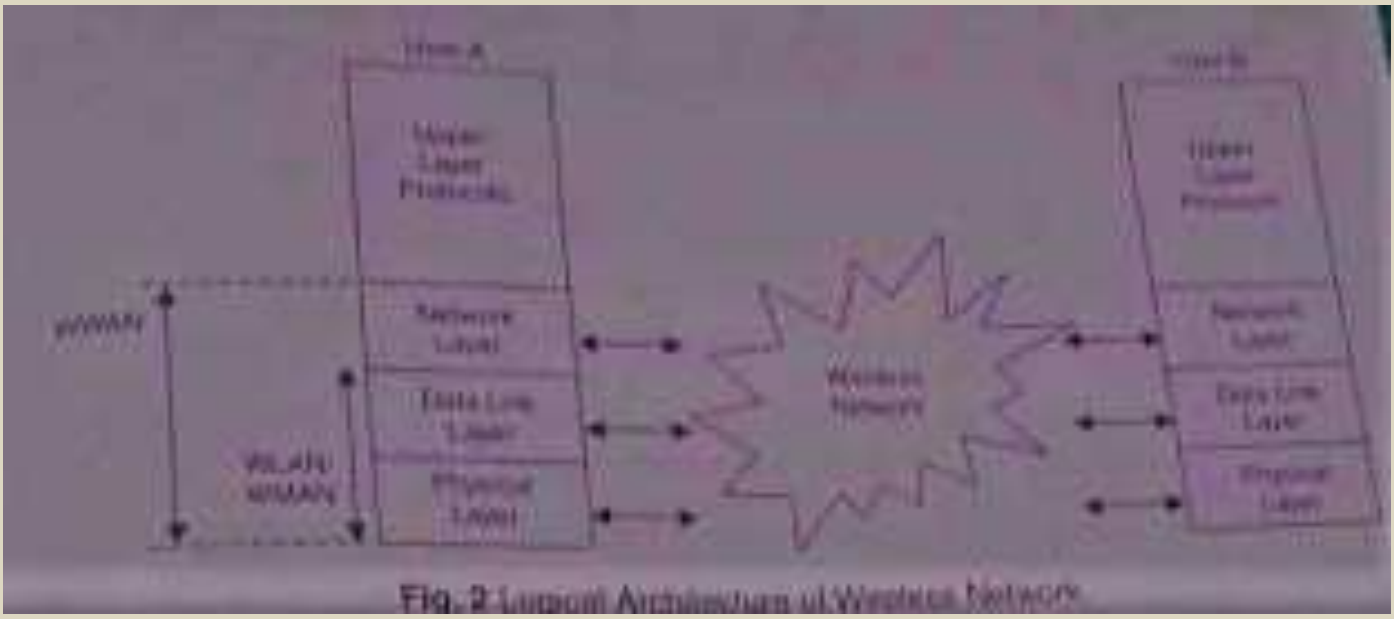
Wireless Network Architecture: -

Network performs many functions to transfer information from source to destination, they are as follows:

➔ The medium provides the path for data to flow.
➔ Medium access techniques provide the sharing of common medium.
➔ Synchronization and error control mechanisms transfers of the data properly.
➔ Routing mechanism move the data from the source to destination properly.

Logical Architecture of Wireless Network: -

Logical architecture defines the networks protocol, rules by which two entities communication. The most popular standard logical architecture is 7 layers of OSI Model. Wireless network does not concern with all 7 OSI layers. They function only within physical, datalink, and network layer.



Types of WLAN: -

There are 2 types of WLANs.

i. Ad-hoc Mode

- ➔ The Ad-hoc Mode include WLAN cell interacting without connecting the wired network i.e., without connection to an access point.
- ➔ No access point is needed and the device might connect to the internet through wired other wireless technique.
- ➔ There is no fixed infrastructure and information is forwarded in peer-to-peer mode.
- ➔ There is no administrator, no setup and no cost.
- ➔ Each node can directly communicate with another node.
- ➔ Nodes can only communicate if there reach each other physically or if other nodes forwarded the message.
- ➔ This network structure way operates in a stand-alone fashion. Each node is equipped with a wireless transmitter and receiver with appropriate antenna.

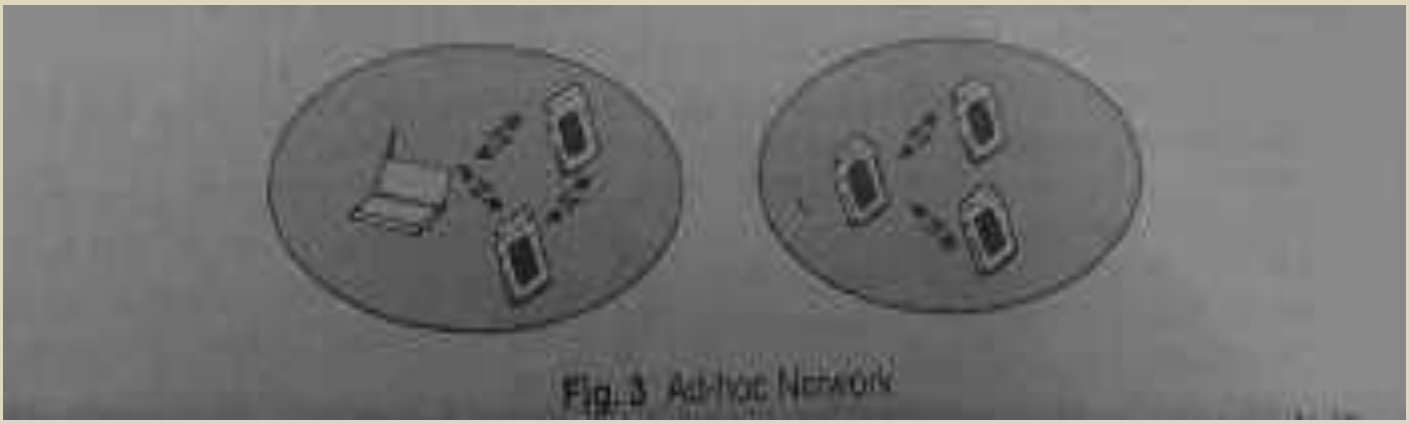


Fig. 3 Ad-hoc Network

ii. Infrastructure Mode

- ➔ The infrastructure mode includes one or several interconnected WLAN cells which are connected to a fixed network through access point.

➔ Wireless access point can be compared with an Ethernet hub or switch and is used to allow computer or other devices with wireless cards to participate in a network.

➔ All communication occurs through access points.

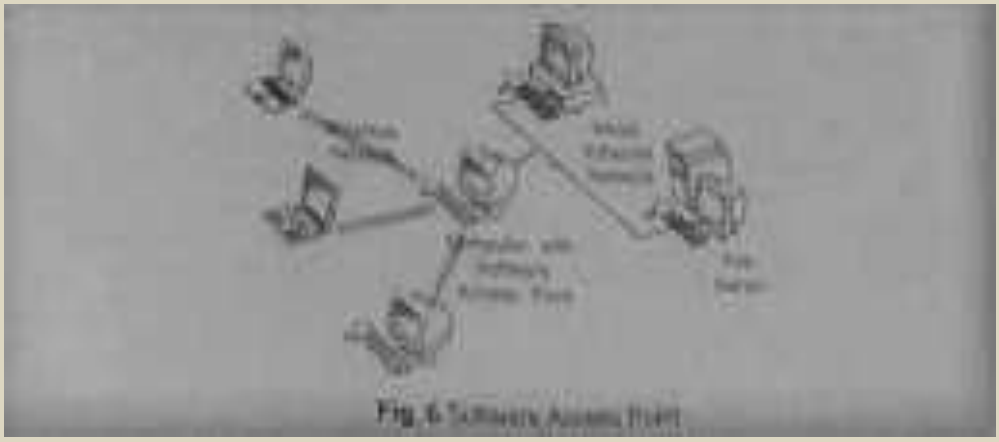
➔ In this network communication takes places only between the wireless node and the access point and not directly between the wireless node. Access points acts as a bridge.

➔ Access points with a fixed network can connect several wireless networks to from a larger network beyond the actual radio coverage.

There are 2 types of access points: -

i. **Hardware Access Point:**
Example – Maybe a hub, router with antenna, bridges

ii. **Software Access Point:**
It runs on a computer equipped with a wireless network interface card.



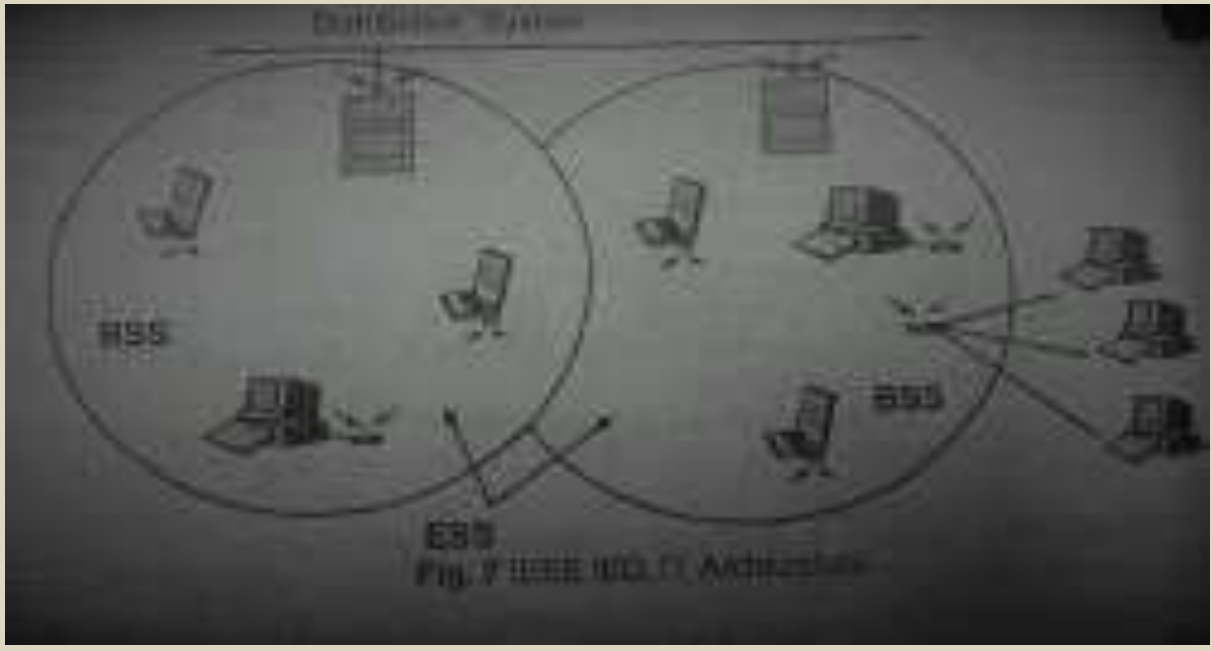
IEEE 802.11: –

- IEEE adopted the first standard for WLANs. As the standards no indicates this standard belongs to the group of 802.
- X LAN standards – this means that standard specifies the physical and medium access layer adapted to the special requirements of wireless but offers the same interface as the others.
- The primary objective of this standard was the specification of simple and robust of WLAN which offers time bounded an asynchronous service.
- IEEE 802 community was formed to setup standard for LAN domain.
- These specifications define an over the air interface between wireless client and a based station or access point or between two or more wireless client.
- IEEE 802.11 is known as Wi-Fi. Wi-Fi came into existence because of a decision in 1985 by the federal communication commission to open several bands of the wireless spectrum for use without a government license.

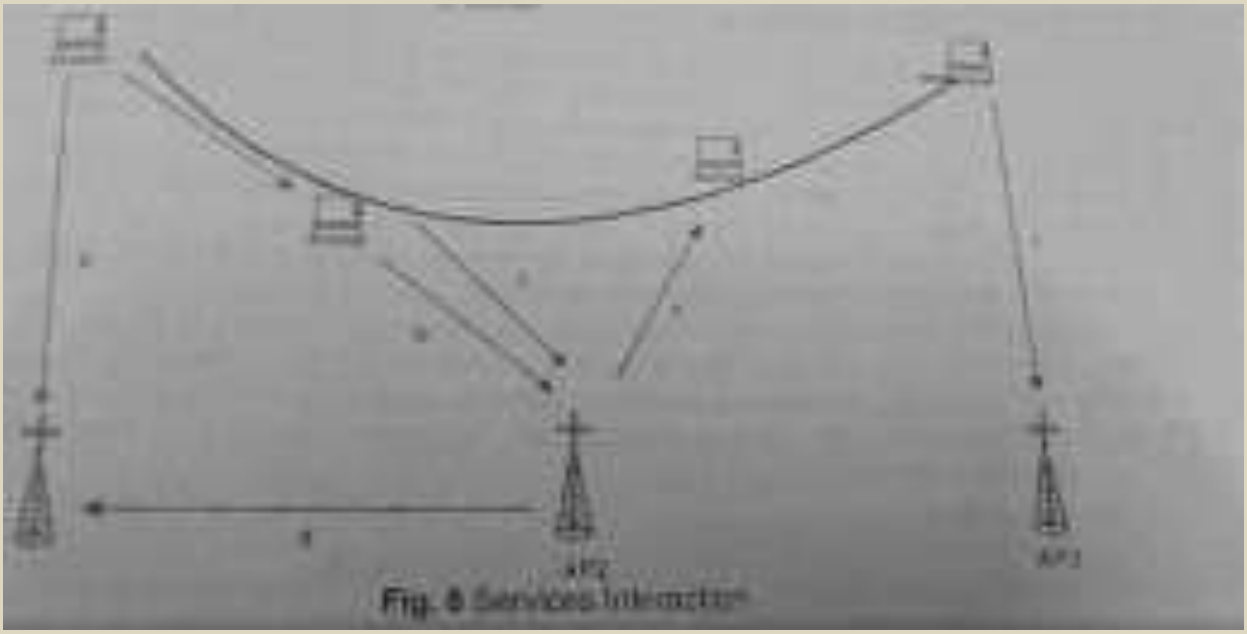
IEEE 802.11 Architecture: -

- The IEEE 802.11 standard permits devices to establish either peer to peer networks or networks based on fixed access points with which mobile nodes can communicate so this standard defines two basic network topologies.

i. The infrastructure mode network
ii. Ad-hoc mode network



- Infrastructure is meant to extend the range of the wired LAN to wireless nodes that useful of other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN.
- A cell is the area covered by an AP & is called BSS (Basic Service Set). The whole interconnected wireless LAN including different cell, their access point & the distribution system is called ESS (Extended Service Set).
- A wireless LAN environment has wireless client stations that use radio modems to communicate to an AP.



- The client station is generally equipped with a wireless network interface card (NIC) that consist of the radio transceivers and the logic to interact with the client machine and software.
- An AP consist of a radio transceiver on one side and a bridge to the wired backbone on the other side.
- Access points are connected through some kinds of backbone called distributed system (DS).
- All communication between the client system and between clients and the wired network go through the AP.

The various components used in IEEE 802.11 Architecture as follows:

- ❖ Station is the component that connects to the wireless medium.

- A BSS is a set of station that communicate with an another. When all the station in the BSS is MS and there is no connection to a wired network, the BSS is called independent BSS.
- When a BSS includes an access point the BSS is called infrastructure BSS.
- When there is an Access Point (AP) and if one MS in the BSS want to communicate with another MS, the communication is sent first to the AP and then from the AP to the other MS.
- An ESS is set of infrastructure BSS where the APs communicate among themselves to forward traffic from one BSS to another and to help the movement of MS from one BSS to another.
- DS is a mechanism by which one AP communicates which another to exchange frames for stations in their BSSs, forward frames to follow MS from one BSS to another and exchange frames with wired network.

Problems of IEEE 802.11 –

- The main problem of IEEE 802.11 and the range.
- If a group of system share the same key for an extended period and one system key is stolen then the whole group will face the difficulty.

Initialization Vector (IV):

- IV is the 24 bits in length and is displayed in plain text form.
- The RC4 encryption key length is 40 bit which can easily be cracked.

Other standards of IEEE 802.11 –

IEEE 802.11 a –

It transmits at 5 GHz and sends data up to 54MBps using orthogonal frequency division multiplexing.

IEEE 802.11 b –

It transmits at 2.4 GHz and send data up to 11 MBPS using direct sequence spread spectrum modulation.

IEEE 802.11 g –

It is similar to IEEE 802.11 a.

IEEE 802.11 x –

It is used with IEEE 802.11 b and IEEE 802.11 a. It uses a central authentication server to authenticate each user on the network.

IEEE 802.11 I –

It provides encryption in wireless transmission. It is requiring new encryption key protocols as temporal key integrity protocol (TKIP) and Advance Encryption Standard (AES).

MAC Layer: -

- ➔ When the transmission medium share there should be method to control access to the medium at any movement of time.
- ➔ To prevent the collision on the network, there should be method for medium access control. This method defines the procedure a computer follows when it needs to send frames.
- ➔ The medium access control (MAC) is a sub layer of datalink layer.
- ➔ This layer defines who can use the network medium when multiple computers are trying to access it simultaneously.
- ➔ Most de3cissions for accessing the wireless medium are made in MAC layer.
- ➔ It establishes a reliable point to point connection between different devices over a wireless medium.

For example –

I. CSMA/CD are taken passing for Ethernet.
II. MAC layer is used for reliable data delivery and provides central access to the share wireless medium and protect the data that it delivers.
III. The IEEE 802.11 uses a MAC layer known as CSMA/CA. In CSMA/CA a wireless mode that wants to transmit perform the following steps.
IV. Listen on the desired channel.
V. If the channel is idle it sends a packet.
VI. If the channel is busy it waits until the transmission is completed and then it waits for a random period of time.

VII. If the channel is still idle then the station transmits it packet otherwise it repeats the step 3 process.

VIII. To improve the efficiency some extra features are added.

IX. The receiver has to send a positive acknowledgement (ACK) after receiving.

a) MAC level retransmission

b) Fragmentation

Security: -

In wireless world every bit is in air so security is the major issue. 3 basic security services defined by IEEE for the wireless LAN environment are as follows –

I. Authentication

- IEEE 802.11 defines 2 means to validate wireless users attempting to gain access to a wired network i.e., open system authentication, and shared key authentication.
- Shared key authentication is based on cryptography whereas open system authentication is not based on cryptography whereas open system authentication is not based on cryptography.
- The open system authentication cryptography is not truly authenticated as the access point accepts.
- The MS without verifying the identity of the station.

II. Confidentially

- IEEE 802.11 standard supports privacy with cryptography techniques for the wireless interface.
- Wired Equivalent Privacy (WEP) cryptography technique for confidentiality also uses RC4 symmetric key, stream cipher symmetric algorithm generates a Pseudo Random data exchange.
- The key stream is simply added modulo 2 (EX-OR operation) to data to be transmitted.

III. Integrity

- The IEEE 802.11 also outlines a means to provide the data integrity for messages transmitted between wireless clients and access points.
- This security service was designed to reject any messages that had been changed in the middle.
- This technique uses a simple encrypted cyclic redundancy check approach so was to maintained the integrity of the data.

Synchronization: -

I. Synchronization is the process of stations in a BSS getting in step with each other, so that reliable communication is possible.
II. Mobile nodes need to maintain synchronization.
III. The MAC provides the synchronization mechanism to allow support of physical layers that make use of frequency hopping or other time-based mechanisms were the parameter of physical layer change with time.
IV. It is archived by all the stations updating their clocks according to access point clocks.
V. The access point transmits periodic frame called beacon. Time between two intervals is called the beacon interval.
VI. Beacon contains the value of access point clock at the movement of transmission.
VII. This is the time when physical transmission actually happens and not when the packet is not actually put in the queue for transmission.

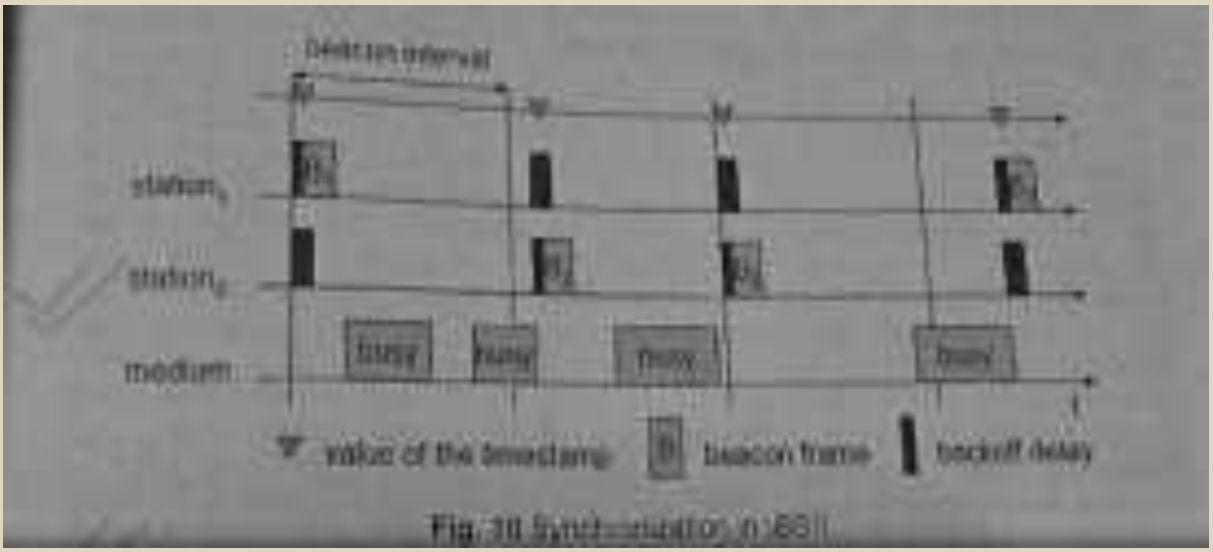
VIII. Time stamp is 64-bit value of the station's timer at that time a frame was transmitted.

IX. The receiving station check the value of their clocks at the movement the signal is received and correct it to keep synchronized with the clock of access point (AP).

X. This prevents clock drifting time synchronization in an independent.

IBSS: -

- In an IBSS, timer synchronization mechanism is completely distributed among the mobile stations of the BSS.
- The MS that starts the BSS will begin by resetting it timer to zero and transmitting beacon, choosing a beacon period, each station will attempt to send a beacon after the target beacon transmission time (IBTT) arrives.
- The stations back off for a random time to send a beacon.
- In this random time if a station hears a beacon, it cancels it transmission.
- Timer synchronization in an infrastructure.



BSS: -

- In an infrastructure, BSS the AP is responsible for transmitting a beacon frame periodically.
- The beacon period is included as part of the information in the beacon frame in order to inform stations receiving the beacon when to expect the next beacon.

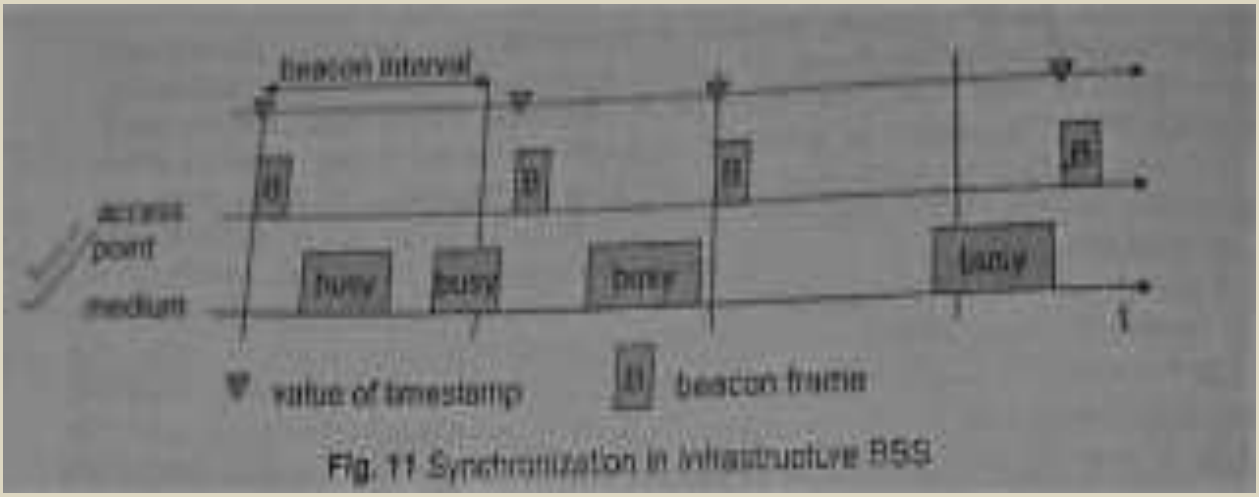


Fig. 11 Synchronization in Infrastructure BSS

- The synchronization function in this case is very simple.
- A MS will update its timer with the value of the timer it receives from the AP in the beacon frame, modified by any processing time required to perform the update operation.

Power Management: -

I. In case of wireless LAN battery power is to be same.
II. Power saving enables station to go into sleep mode without losing information.
III. The access point maintains an updated record of all the station in power saving mode.
IV. Access point buffers the packet which are for these stations until either the station request for these packets or until the change their operation mode.
V. Station must wakeup periodically to receive becomes and buffered data.

Power Management in an Independent BSS: -

I. In an independent BSS, power management is a fully distributed process, managed by the individual MS.
II. Power management consist of 2 parts i.e., the functions of the station entering a low power operating mode and the functions of the station that desired to communicate with the station.
III. For a station to enter a low power operating state, a state where it has turned off of the receiver and transmitter to conserve power.

IV. The station must successfully complete a data frame handshake with another station with the power management bit set in the frame header.

Power Management in an Infrastructure BSS: -

a) In an infrastructure BSS, the power management mechanism is centralized in the AP.
b) This power management mechanism allows much greater power saving for MS than the mechanism used in the independent BSS.
c) This is so because the AP consume all of the builder of buffering data frame for power saving station and delivering them when the station request, allowing the MS to remain in their power saving state for much longer periods.

Roaming: -

a) It is the process of moving from one cell to another cell without losing connection.
b) A client can switch between access points while physically moving or because of load balancing between access point.
c) Client is not restricted to being stationary.
d) Usually this is completely transparent to the user, they are not aware that a different access point is being used from area to area.

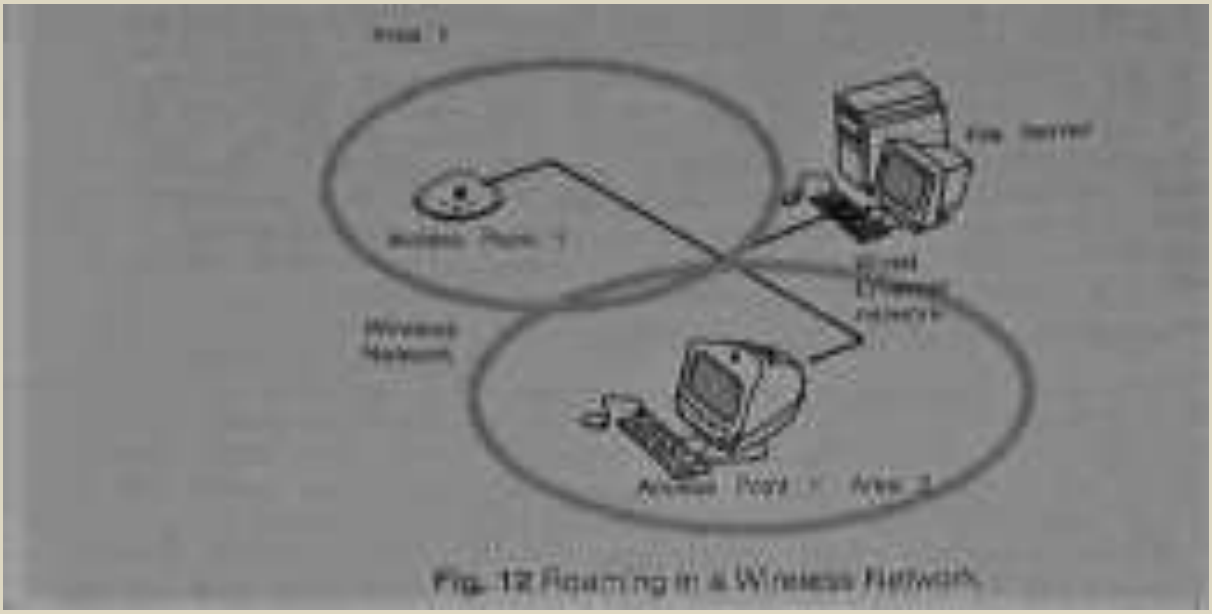
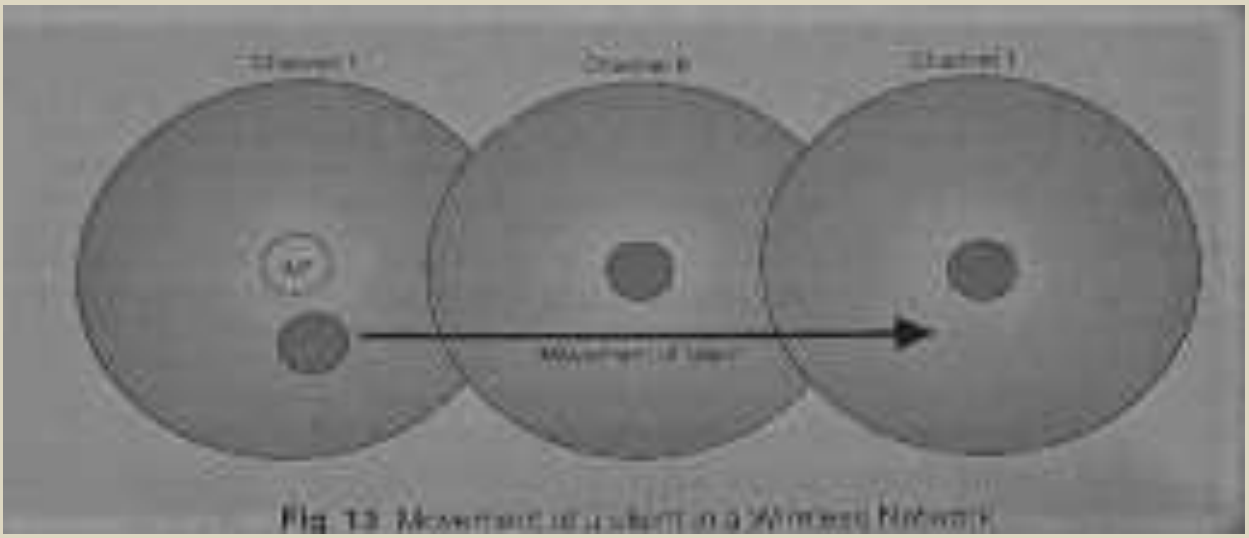


Fig. 12 Roaming in a Wireless Network

e) As the client physically gets closer to another access point, the signal strength from the other will increase.
f) At one point the signal strengths of the two will equal then the other will have the strongest signal and the client should be come to the next AP.



Bluetooth: -

- It is an emerging technology and the global initiative taken by erosion, IVM, INTEL, NOKIA, TOSHIVA. To set a standard for cable free connective between mobile phones, mobile, PCs, handheld computers and other peripherals.
- They group are called special interest group (SIG) that content two market leaders in mobile telephony, to in laptop computing and one in digital signal processor technology.
- Bluetooth uses short range radio links in the 2.4 GHz instrumentation scientific and medical (ISM) free band frequency.

Bluetooth communication type: -

I. Piconet:

- Bluetooth devices can interact with one or more other Bluetooth devices in several different ways.
- The simplest method is when only two devices are involved and these devices acts as the master and the other device acts as a slave.
- This ad-hoc network is called as a Piconet.

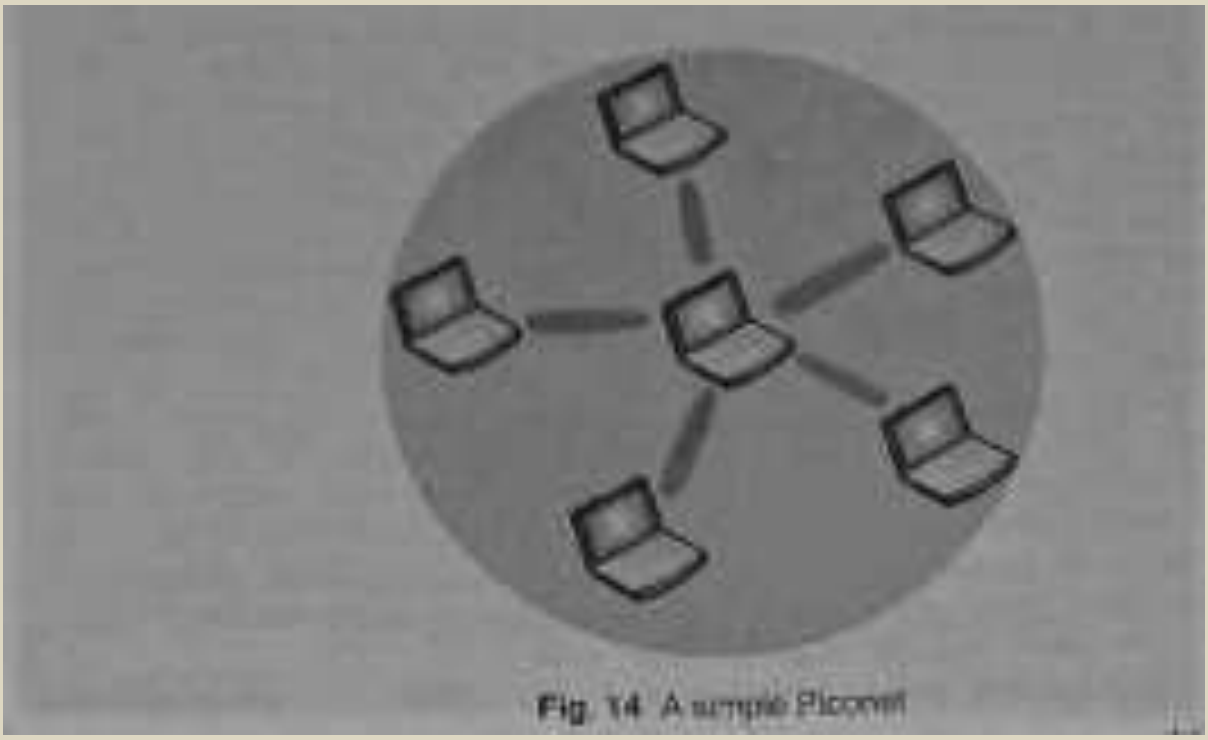
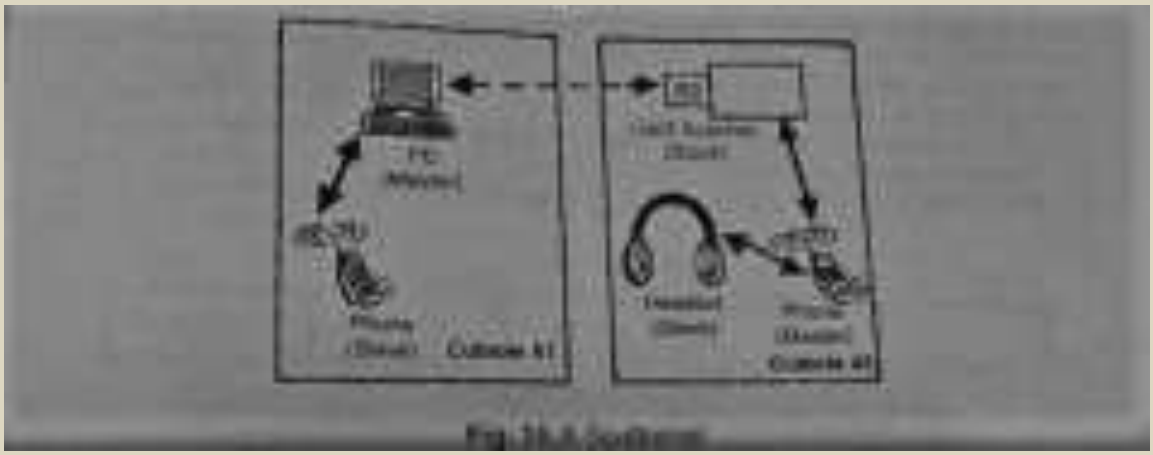


Fig. 14 A simple Piconet

- A piconet is any such Bluetooth network with one master and one or more slave.
- In case of multiple slaves, the communication topology is point to multipoint topology.
- In this case channel or the bandwidth is shared among all the device in the Piconet.
- The device initiating the connection usually becomes the master however the master provides the synchronization of the FHSC communication between the devices.

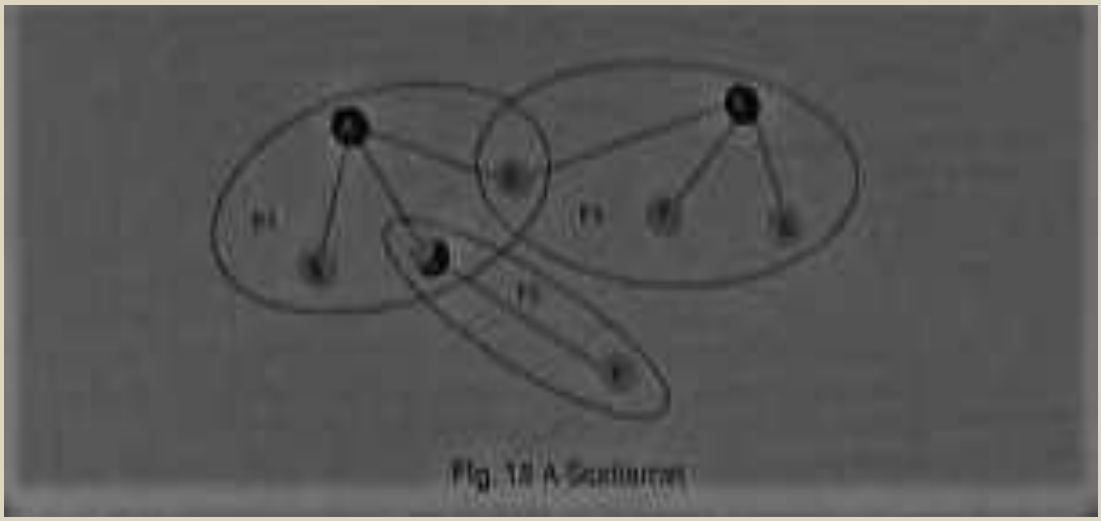
II. Scatternet:

- As with Piconet where multiple Bluetooth devices are able to connect with each other in an ad-hoc manner, the same way multiple Piconets join together for a larger network known as Scatternet.



- Here Bluetooth devices must have point to multipoint capability in order to communicate in a Scatternet.
- Several Piconet can be connected to each other through one Scatternet.
- A single Bluetooth device may participate as a slave in several Piconets but can only be a master in one Piconet.

As shown in the figure below, a Scatternet consist of 3 separate Piconets P1, P2, P3. Each Piconet is controlled by a separate master (devices A, C, E) and contents one more slave. It should be noted that the device C which connects P1, and P2 is a slave in one Piconet P1 and master in another Piconet P2.



III. Links type between master and slave:

For example: one might have a Piconet consisting of the mobile phone and the PC and one's while the person neighboring while may have a Piconet consisting of a mobile phone, headset, business card scanner.

- Slave in one piconet can participate in another Piconet as either a master or a slave this is done through time division multiplexing.

Links type between master and slave: -

- The following two types of links can be established between the master and slave.

➔ Synchronous connection oriented (SCO)
➔ Asynchronous connection less (ACL)

SCO Link –

This link is a point-to-point link between a master and a single slave in the Piconet. The master maintains the SCO link by using he reserved slots at a regular interval.

As the SCO link reserves slots it can be considered as a circuit switched connection between master and slave.

The SCO link typically supports time bounded information such as the voice.

The master can support into three SCO links to the same slave or two different slaves.

A slave can support into 3 SCO links from the same master or two SCO links if the links away from different master. SCO packets are be retransmitted.

ACL Link –

The ACL link is a point-to-multipoint link between the master and all the slave participating on the Piconet.ACL links are used for carrying asynchronous data.

The ACL link provides a packet switched connection between the master and all active slaves participating in the Piconet.

In this case, the master can establish an ACL link on a per slot basis to any slave.

IV. Straight transition:

The following diagram shows a state diagram showing the different stated used in the Bluetooth link controller. There are two major states.

- ➔ Stand-by
- ➔ Connection

In addition to these two states there are 7 sub-states.

I. Page
II. Page Scan
III. Inquire
IV. Inquire Scan
V. Master Response
VI. Slave Response
VII. Inquire Response

The sub-states are temporary states that are used to add new slaves to a Piconet. To move from one state to another, either commands from the Bluetooth link manager are used or internal signals the link containers are used.

In a connected state, the device is a member of the Piconet. On the other hand, when a device is not associated in any Piconet, or participate in no action it is said to be in the standby state. The standby state is the default operation state for the Bluetooth device.

V. Packet format:

The data on the Piconet channel is the transmitted in the form of channel. Each packet consists of 3 entities.

Access Code – That is 72 bits field.

Header – That is 54 bits field.

Payload or Data – That is 0 to 2745 bits.

Definition: -

The idea of anywhere, anytime, by anything and anyone (or '4A's) networking each at the core of the new emerging technology referred to as ubiquitous. Networking ubiquitous is a Latin word whose meaning is being everywhere, especially at the same time.

Objective of ubiquitous technique:

The 4 main objectives are as follows –

1. Freed from networking constraints concerning capacity, location and different link ups.
2. Freed form the constraints of terminal limitation.
3. Freed from constraints of limited service and contained.
4. Freed form the constraints of network links.

Scenarios of Mobile Communication: -

The mobile industry has seen explosive growth in number of subscribers particularly over the past few years. However, while usage is measured in terms of the number of wireless minutes increasing, the price per minute for this service is decreasing.

This means that Average Revenue Per User (ARPU) is decreasing. The mobile industry is addressing the followed challenges in mobile communication.

a) By adding new services on new user experiences for which mobile subscribers are willing in pay.
b) By reducing operating expenses (ROF)

At the top of the list is the wireline infrastructure that mobile operators have to maintain regardless of whether they own lease line.

There are two primary eco-system i9n the wireless industry:

a) Global Systems for Mobile Communication (GSM)
b) Code Division Multiple Access (CDMA)

Mobile Communication Generations: 1G to 3G-

- Standard bodies such as 3GPP (GSM), and 3GPP2 (for CDMA networks) are actively involved in driving the development of the next generation of wireless system.
- The high-level objective is to create highspeed broadband and IP – based mobile system featuring networks to networks interconnection feature or service transparency, Global Roaming and seamless services independent of location.

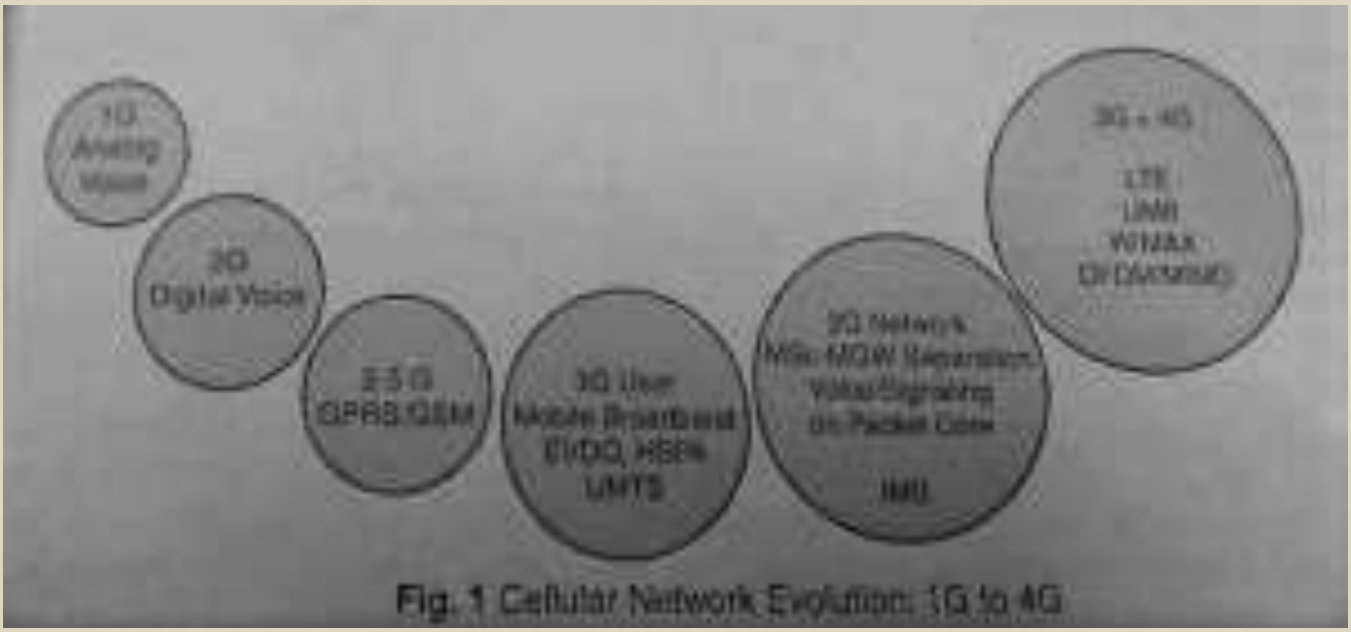
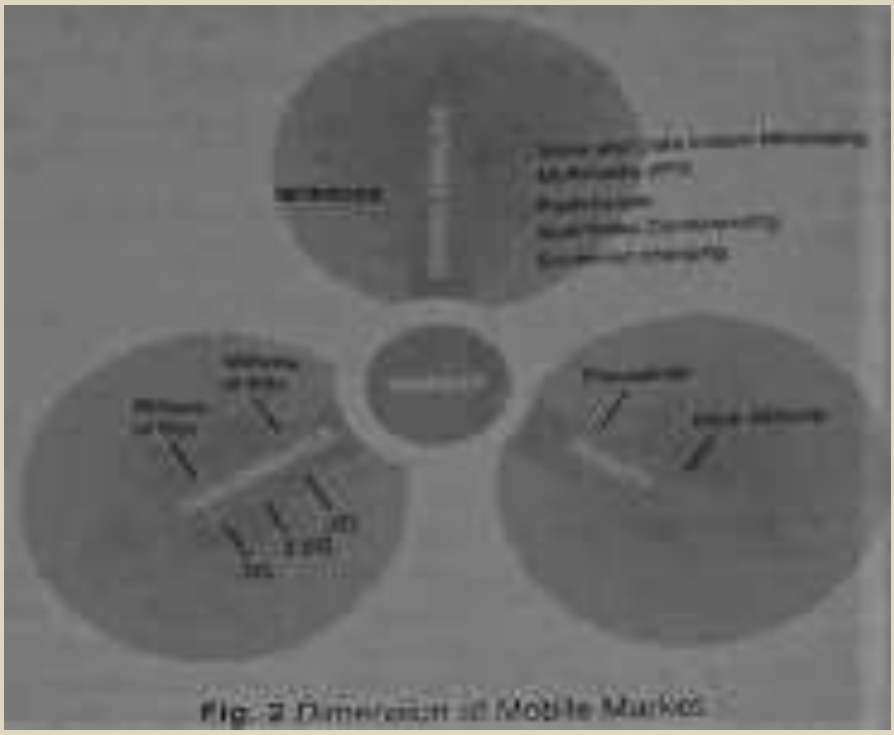


Fig. 1 Cellular Network Evolution: 1G to 4G

- 3G mobile systems are defined by International Telecommunication Union (ITU) whose specification is IMTS – 2000 (International Mobile Telecommunication System 2000).
- It is a radio and network access specification.
- 3G is the successor of 2G. 2G is the successor of 1G which is the original analogue mobile system.
- GSM is the most pre-domanial choice for 2G deployments.
- Though voice remains the primary method of mobile communication, a new generation of wireless technology is now offering highspeed data and multimedia capabilities.

3rd Generation Mobile Communication Network: -

- Cellular communication service begins with 1G services i.e., delivery of voice from one mobile phone to another.
- Next to 1G the 2G communication service increase3s.
- The service including the data transfer as well as other services initiated one by one.



- But the 3G networks enables a lot of services which ranges from audio or video conferencing, internet application, chatting and much more service. So, user interaction with mobile not limited to talk but mobile become equipment to shared feeling with others.
- As the use of mobile is increasing 3G pushes the growth of mobile market in the direction to increase the services quality of services and generating more revenue.
- 3G operators purpose broadband services such as internet connection, video telephony clip download or television on a mobile phone.
- Universal Mobile Telecommunication System (UMTS) is a third generation of mobile communication system that provides a range of broadband services to the world of wireless and mobile communication.
- The UMITS delivers a low-cost mobile communication at data rate of up to 2Mbps.

- It also includes the global roaming capability of second-generation GSM/ GPRS networks and provides new enhanced capability.
- The UMTS is designed to deliver pictures graphics, video communication and other multimedia information, as well as voice and data to mobile wireless subscriber.

Objectives: -

1. High transmission rates using circuit switched and packet switched connection.
2. High spectral efficiency and overall cost improvement.
3. Definition of common radio interfaces for multiple environments.
4. Portability of services in various environment (indoor, outdoor, sub-urban, urban, rural etc.) this service portability is also known as Virtual Home Environment concept.

UMTS Services: -

The UMTS provides supports for both voice and data service. The following data rates are target for UMTS.

1. 144 kbps: Satellite and rural outdoor.
2. 384 kbps: Urban outdoor
3. 2084 kbps: Indoor and low range outdoor.

Data services provide different Quality of Service (QoS) Parameter for data transfer. UMTS networks services uses quality of service classes the following 4 types of traffic.

1. Conversational Class: voice, video telephony, video gaming
2. Streaming Class: multimedia, video and demand, webcast
3. Interactive class: web browsing, network gaming; database access.
4. Background Class: E-mail, SMS, file downloading.

The UMTS supports the following service categories and application.

1. Internet Access
2. Internet or Intranet Access
3. Customized Information of Entertainment
4. Multimedia Messaging
5. Location Based Services

UMTS Specifications and Management: -

In order to create and manage system as complicated as UMTS of WCDMA, it is necessary to develop and maintenance a large number of documents and specifications for UMTS. These are now managed by a group known as 3GPP i.e., 3 Generations Partnership Program.

UMTS Architecture: -

A UMTS network is logically divided into 2 parts which are referred to with the generic terms core network and a Generic Radio Access Network (GRAN). The core network reuses several elements already present in GPRS and GSM networks and consist of two overlapping domains.

1. Circuit Switched Domain (CS)
2. Packed Switched Domain (PS)

CS Domain is made up of those entities which allocate dedicated resources for user traffic and control signals when the connections are establish and release them when the sessions finish.

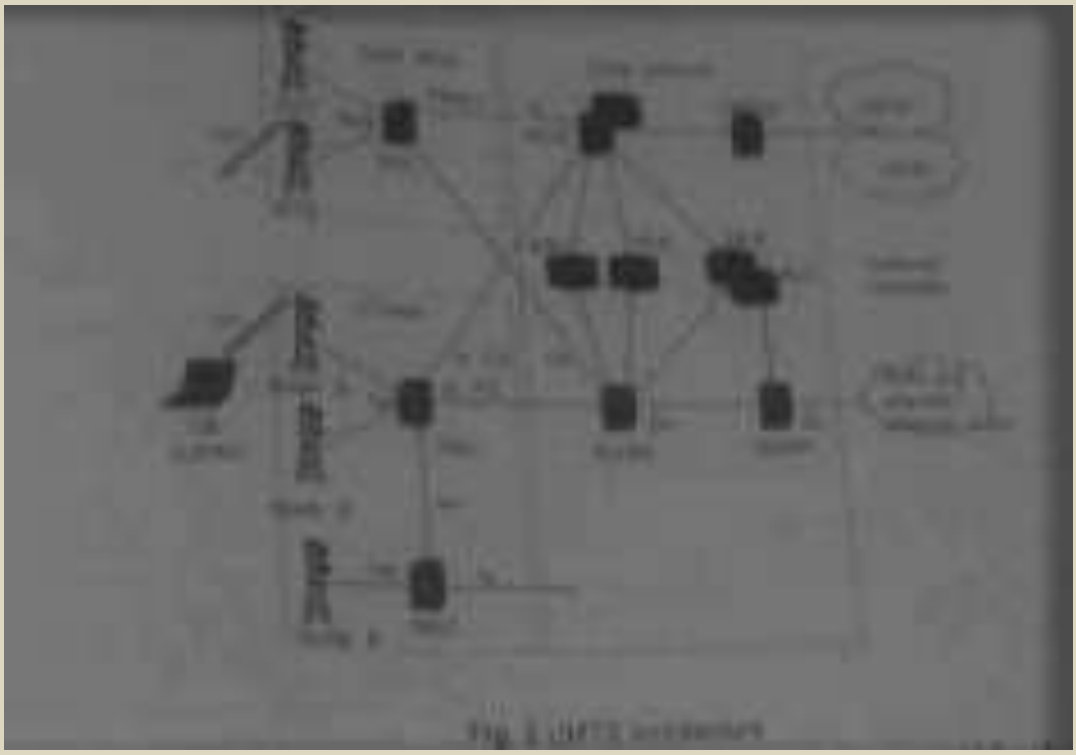
Generally, voice calls are always handled by the components belonging to CS Domain.

- The entities in the PS Domain transport user data in the form of autonomous packet, which are routed independently of each other.
- This method overcomes the limitations of 2G networks to transmit data efficiently.
- It is through the core network that the user can setup as connection to and from external packet data networks, Public Switched Telecommunication Network (PSTN) and other wireless networks.

- The UMTS Terrestrial Radio Access Network (UTRAN) is UMTS implementation of the GRAN concept.

  Some of the functions performed by its component are as follows:

1. Management of Radio Resources
2. Power Control both in downlink and uplink direction
3. Handover Management and Allocation of Challenge for Transmission



The components used in UMTS Architecture:

1. Radio Network Controller (RNC)
2. Mobile Services Switched Centre (MSSC)
3. Home Location Register (HLR)
4. Visitor Location Register (VLR)
5. Equipment Identify Register (EIR)
6. Authentication Center (AUC)
7. Service GPRS Support Node (SGSN)
8. Gateway GPRS Support Node (GGSN)
9. Base Transmission Station (BTS)

Introduction to Mobile IP: -

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identify by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved without user interference. Roaming from a wired network to a wireless network or WAN is also done with ease.

A data connection between two end points through TCP/IP Network requires a source IP address, source ICP Port and target IP address with a target TCP port. The combination of one IP address of host system combined with the TCP port as the identification of the service becomes a point of attachment for an end point. TCP Port Number is application specific and remains constant. IP address is network specific and varies from network to network. TP addresses is assigned to a host from a set of addresses assigned to a host. This structure works well as long as the client is static and is using a desktop computer.

Now a consider that the user has mobile and he is using his laptop. As the user moves, the point of attachment will change from one network to another resulting in the change of IP address. This change will terminate the connection. Therefore, the question is how to maintain the mobility during a live connection. The technology that does so is called Mobile IP. Mobile IP is most often found in wireless one environment where the users need to carry their mobile devices across multiple LANs with different IP address.

Working Principle of Mobile IP: -

Internet protocol routes the packets from a source end point to a destination end point through a various router. An IP address of a host can be considered to be a combination of network address (MSB 24 bits) and the node address (LSB 8 bits).

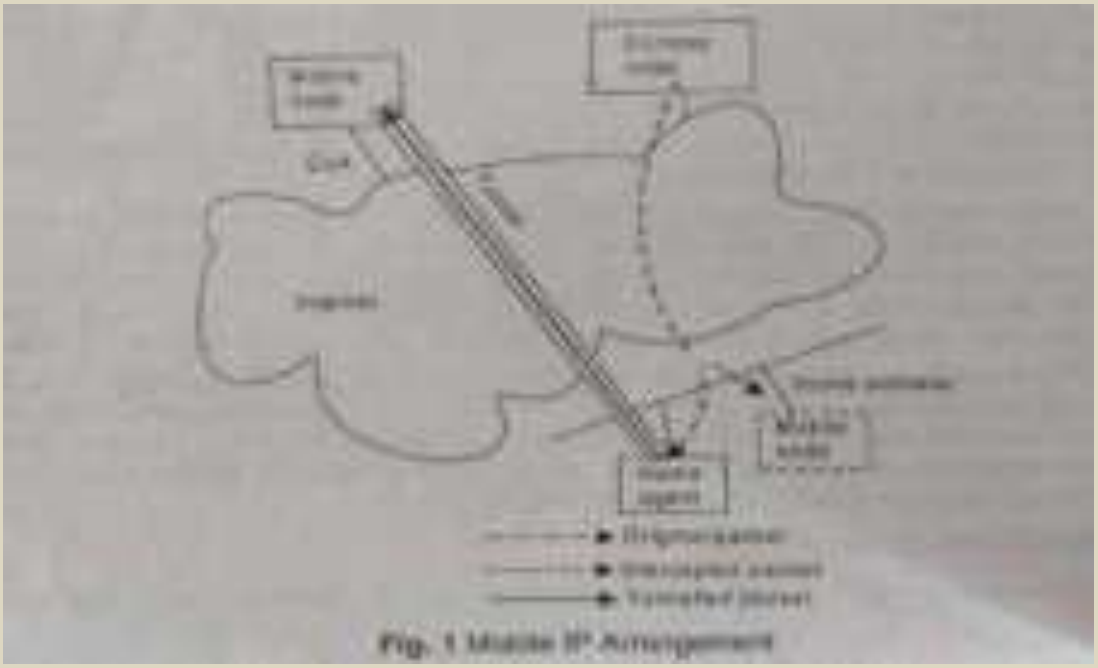
Later assume a C class IP address 203.197.175.123 to be of the mail server. The first 24 bits 203.197.175 is class address of the network and the last 8 bits containing 123 is the address of the host. The network portion of an IP address is used by the routers to deliver the packet to the last router in the chain to which

target computer is achieved. This last router then uses the host portion i.e., 123 of the IP address to deliver the IP packet to the destination computer.

A TCP connection is identified by 4 identities that content the IP address and port number of the sender end point and the IP address and Port number of the receiving end point to ensure that the connection is not terminated while the user is moving, it is important that all of these identities remain constant. Ports are application specific and generally constant. However, the IP address change from network to network.

To solve this problem mode, IP allows the mobile node to use two IP address these IP addresses ae home address and care of address. The home address is static and known to everybody as the identity of the host. The care of address changes every time a new attachment is made. This is mobile nodes location specific address. When the mobile node is roaming and is attached to a foreign network, the home agent receives all the packets for the mobile node and arrange to forward them to the mobile nodes current point of attachment. The node i.e., responsible for forwarding and managing the transparency is called home agent.

Whenever the mobile node moves it registers its new care of address with its home agent. The home agent forwards that packet to the foreign network using the care of address which is the destination IP address. This new header encapsulates the original packet causing the mobile node home address to have no impact on the encapsulated packets routing this phenomenon is called **Tunneling**.



Internet protocol version 4 is the first version protocol used for internet application. It is a data-oriented protocol to be used on a packet switched internet work. It doesn't guaranty delivery.

Mobile IP Entities: -

1. **Mobile Node (MN):**
   It is a node that can change the point of connection to the network without changing its IP address and maintain reachability using its home agent.

2. **Home Agent (HA):**
   A router on the home link that maintains registration of mobile nodes that are away from home and the different address that they are currently using. If the mobile node is away from home, it registers its current address with the home

agent which tunnels data sent to the mobile home node current address on IPv6 networks and forwards tunned data send by the mobile node.

3. **Foreign Agent (FA):**
   It is a system of current foreign network of the MN; typically, a router. It is the default router for the MN.

4. **Care of Address (CoA):**
   An address used by a MN while it is attached to a foreign link. A mobile node can be assigned with multiple care of addresses, however only one care of address is registered as the primary care of address with the mobile nodes home agent. The association of as home address with a care of address for a mobile node is known as binding.

5. **Corresponded Nodes (CN):**
   A node that communicates with MN, it doesn't have to be mobile IP capable.

6. **Home Address (HA):**
   An address assigned to the mobile node when it is attached to the home link and through which the mobile node is always reachable, regardless of its location on an IPv6 network. If the mobile node is attached to the home link mobile IPv6 processed are not used and communication occurs normally. If the MN is away from home, packet address to the MN home address are inters pended by the home agent and tunneled to MNs current location on an IPv6 network. Because the MN is always assigned the home address it is always logically connected to the home link.

7. **Home Link (HL):**
   The link that is assigned to the home, subnet prefix, which the MN obtains its home address. The home resides on the home link.

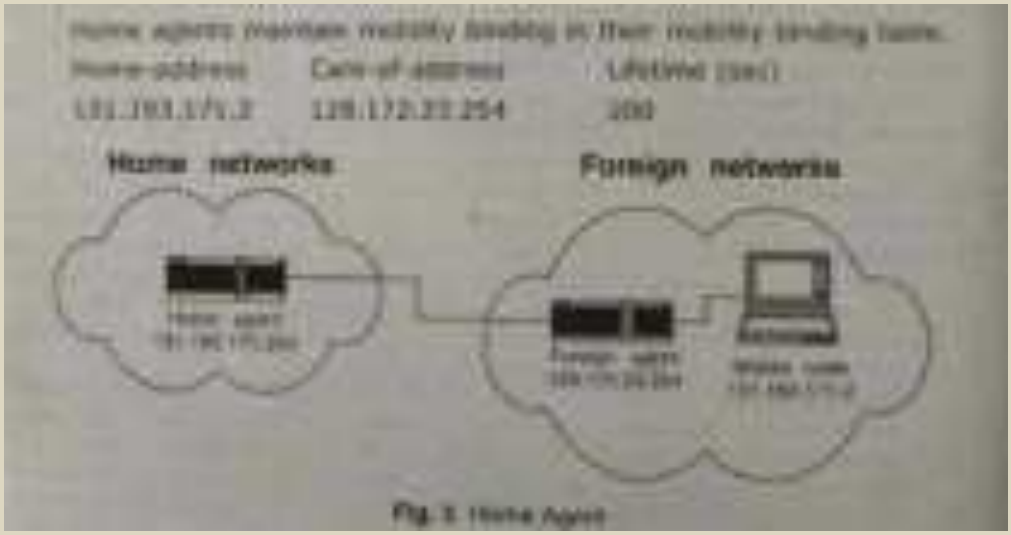
8. **Foreign Link (FL):**
   A link that is not the MNs home link.

Mobility Agents

Fig. 2 Mobility Agents

Home Agent

Home agents maintain mobility binding in their mobility binding table.



Foreign Agent

Foreign agent maintains visitor table which contain all mobile nodes currently visiting table.

Home Address	Home Agent Address	Media Address	Lifetime Guarantee
131.193.171.2	131.193.171.254	00-00-E2-30-39-18	200

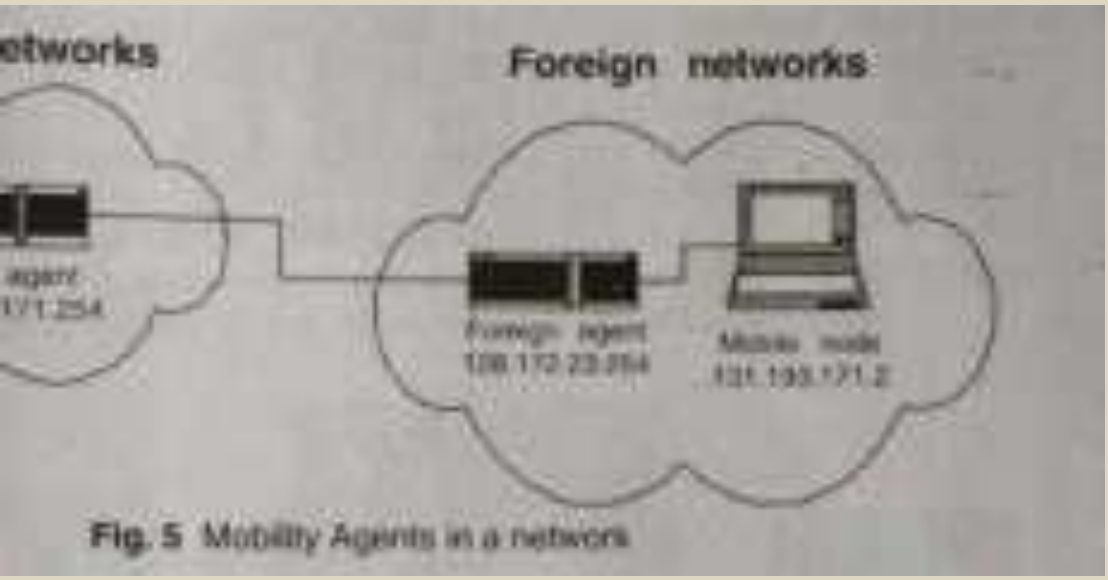


Fig. 5 Mobility Agents in a network

Components of Mobile IP: -

There are 3 components available in Mobile IP.

1) **Discovering the care of address:**
   Mobile node uses discovering procedure to identify perspective home and foreign agent.

2) Registering the care of address:

Mobile node uses an authenticated registration procedure to inform home agent of its care of address.

3) Tunneling the care of address:

Used to forward IP datagrams from a home address to a care of address.

Mobile IPv6 Features: -

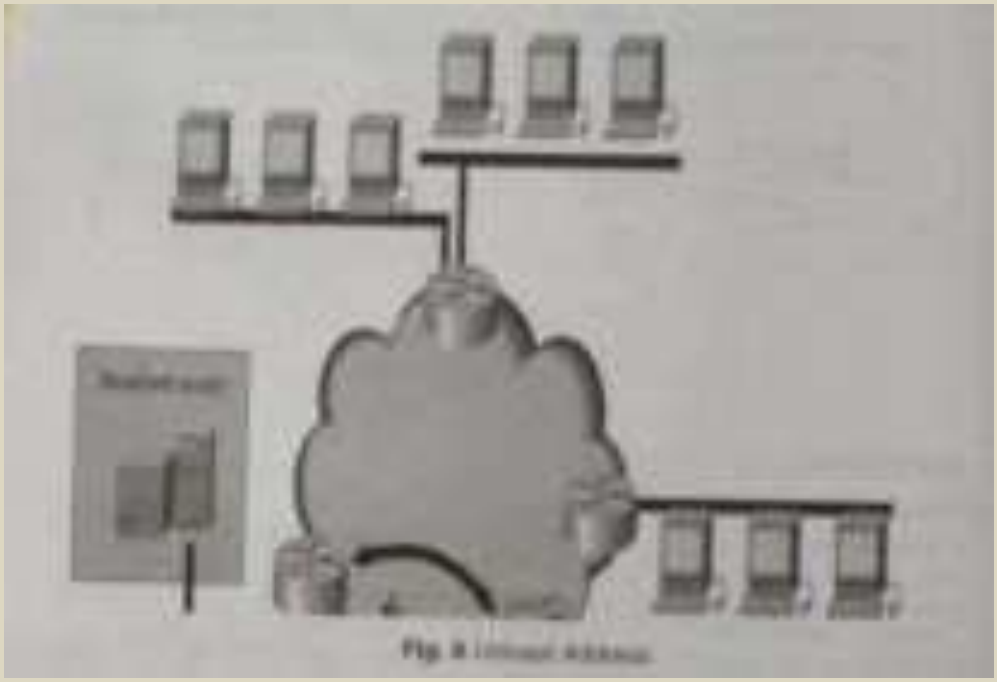
1. Larger address space i.e., unique global address for each device.
2. Scalable: It can run over multiple media i.e., wireless LAN, ethernet, 3G.
3. Autoconfiguration Capabilities: i.e., plug and play.
4. Fixed Header Format
5. Router Headers
6. Security Extensions
7. Any cast addresses
8. Encapsulation: It provides authentication and encryption.
9. Quality of Services and Flow Levels: Efficient routing for real time application.
10. Elimination of triangle routing for Mobile IP.
11. All nodes can handle binding.

Mobile IPv6 Address Type: -

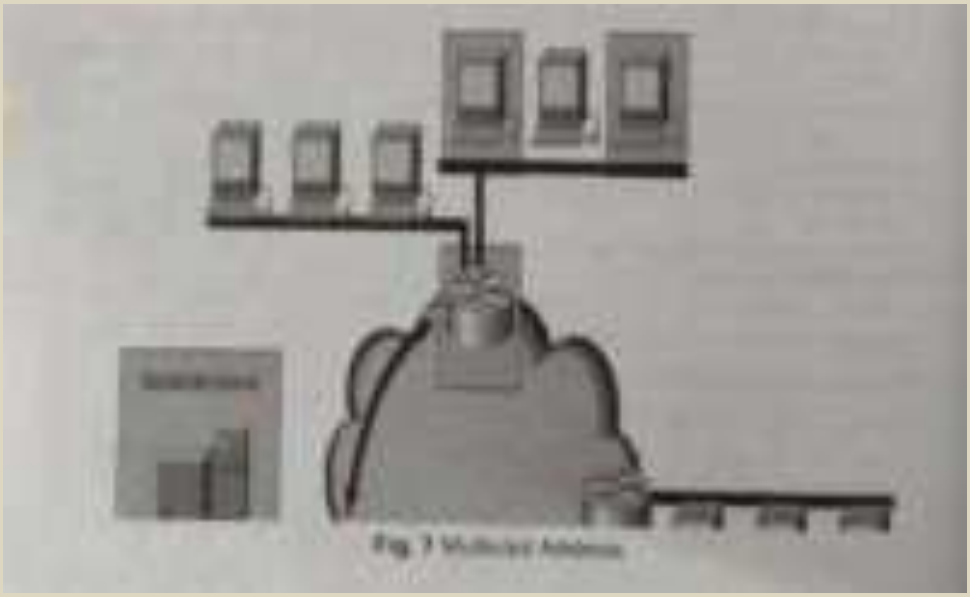
There are 3 types of addresses used by Mobile IPv6.

1. **Unicast:**

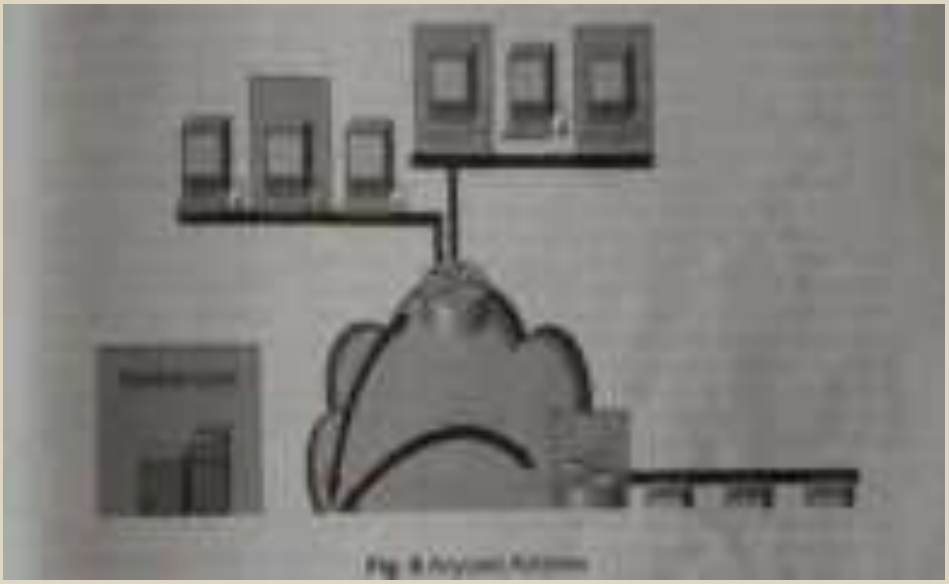
It is a communication between a single host and a single receiver. A unicast address defines a single interface. A packet send to a unicast address is delivered to that specific computer.



2. **Multicast:**
   It is a communication between a single host and a multiple receiver. These addresses are used to define a set of interfaces that typically belong to different nodes instead of just one node. When a packet is sent to a multicast address, the protocol delivers the packet to all interfaces identified by that address.



3. **Anycast:**
   It is a communication between a single sender and a list of addresses. These addresses are also assigned to more than one interface belonging to different nodes. However, a packet send to anycast address is delivered to just one of the member interfaces; typically, the nearest according to the routing protocols idea of the distance.



MOBILE IP V4 & V6 COMPARED

	Mobile IPv4	**Mobile IPv6**
Routing	Optimal Routing only if MN in the Home Network. (Otherwise, non-efficient "Triangle"-Routing)	Optimal Routing is generally possible if CN knows the Care-of Address
Bottlenecks	HA is a possible bottle neck, because all traffic to the MN is processed by it.	HA load is essentially reduced, because CNs can just directly communicate with MNs.
Security	Authentication is mandatory only for registration and then only between HA and MN	Authentication and encryption are possible anywhere, because they are supported by IPv6
Robustness	Used FAs/ Has must not be off-line	Short-time failure/re-configuration of HA is masked thanks to Automatic Home Agent Discovery. IPv6 is essentially simpler to upgrade.

Performance	No good performance due to IPv4-limitations and non-optimal Routing	Mobile IPv6 Essentially better due to characteristics of IPv6 (uniform Headers, less overheads) and optimal Routing

Mobile IP Operation: -

A Mobile Node (MN)listens for agent advertisement and then initiates registration. If the responding agent is the home agent, the mobile IP isn't necessary. After receiving a registration request from a mobile node, the home agent acknowledge and the registration is completed. Registration happens as often as mobile node changes network. Home Agent (HA) intercepts all packets destined for MN. This is simple unless sending application is on or near the same network as the MN. There is a specific lifetime for service before a MN must re-register. There is also a de-registration process with HA if an MN returns home. HA then encapsulates all packets addressed to MN and forwards them to FA. FA decapsulates all packets addressed to MN and forwards them via hardware address (learned as part of registration process). Note that the MN can perform FA functions if it acquires an IP address e.g., Via DHCP. Bidirectional communications require tunneling in each direction.

World Wide Web: -

The WWW architecture provides a very flexible and powerful programming model. Applications and content are represented in standard data formats and are browsed by applications known as Web Browser. The web browser is a network application i.e., it sends requests for named data objects to a network server and the network server responds with the data encoded using the standard formats.

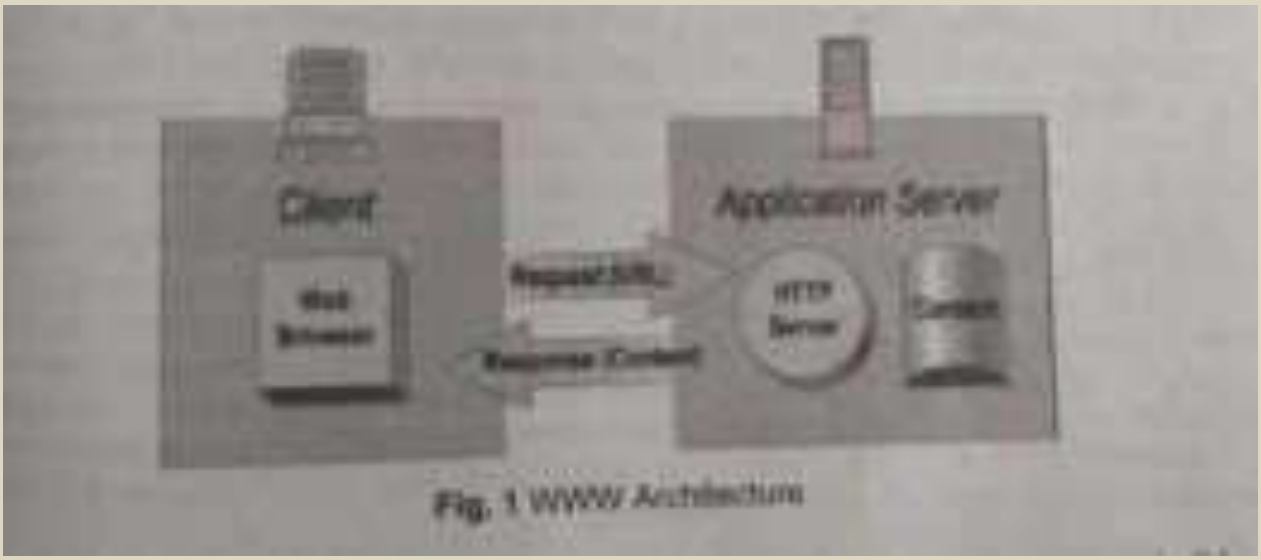


Fig. 1 WWW Architecture

The WWW standard specified many of the mechanisms necessary to build a general-purpose application environment including

1. **Standard Naming Model –** All servers and content on the WWW are named with internet standard URL.
2. **Content Typing –** All content on WWW is given a specific type there by allowing web browsers to correctly process the content based on its type.
3. **Standard Content Formats –** All web browsers support a set of standard content formats. They include the HTML, Scripting Languages (like JavaScript), and a large number of other formats.
4. **Standard Protocols –** Standard networking protocols allow any web browser to communicate with any web server. The most commonly used protocol on the WWW is the HTTP, operating on the TCP/IP protocol suit.

Wireless Application Protocol (WAP): -

WAP is an open international standard for applications that use wireless communications. It enables easy, fast delivery of required informatio0n and services to mobile users with Wireless Terminals with limited displays and data transfer capabilities. It is a specification for a set of communication protocols to standardize the way in which cellular devices use internet access.

WAP is HTTP/HTML adjusted to small devices. It consists of a network architecture, a protocol stack and a WML (Wireless Markup Language).

Need of WAP: -

Having the performance and data transfer capabilities of the common desktop computer in mind, the web designers constructed the internet technology for devices as powerful as those computers. Handheld wireless devices have less powerful CPUs or low battery life, less memory, restricted power consumption, smaller displays and different input devices can provide the better performance and better data transfer capabilities as compare to desktop computers.

Benefits of WAP: -

1. It is device independent.
2. It is network independent.
3. WAP utilizes Standard Internet Markup Language (SIML) technology.
4. Optimizing the content and air-linked protocols
5. The WML UI components map well onto existing mobile phone UI.
6. No re-education of the end users

Examples of WAP used for –

1. Checking train table information
2. Ticket purchase
3. Flight check-in
4. Checking weather conditions
5. Looking up stock values

6. Looking up phone numbers
7. Looking up addresses
8. Looking up sport results

WAP Architecture: -

3 main components are available in the WAP architecture.

(i) WAP Client
(ii) WAP Proxy/ WAP Gateway
(iii) Application Servers

WAP utilizes proxy technology to optimize and enhance the connection between wireless domain and
WWW.

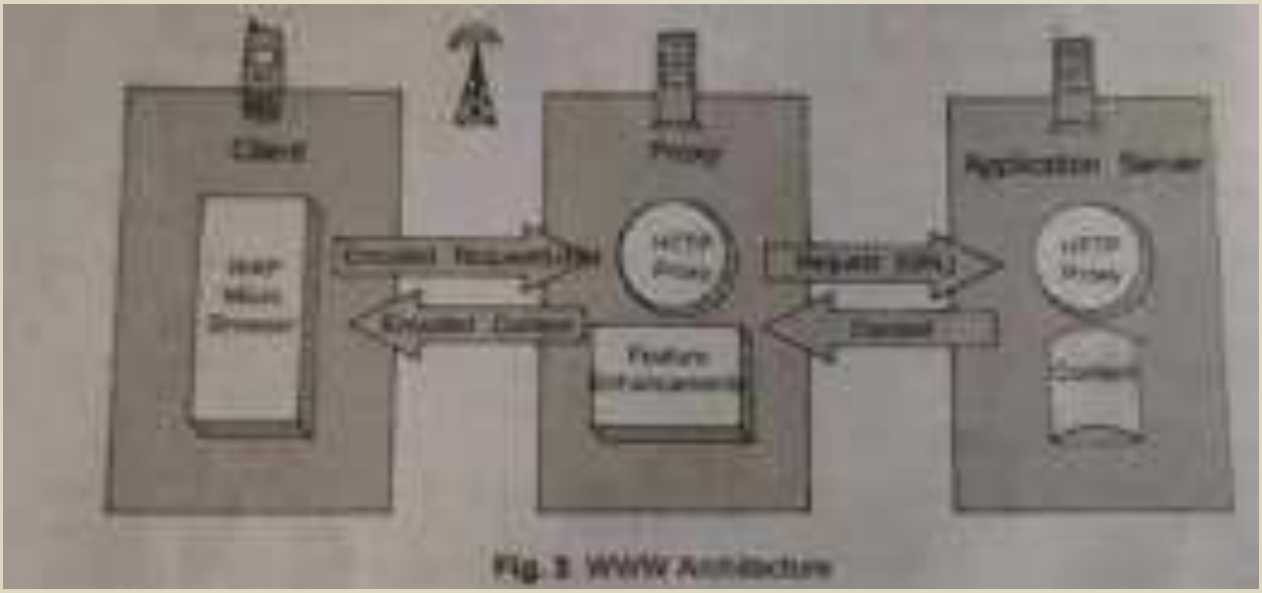


Fig. 3 WWW Architecture

WAP Proxy provides various functions including

a) **Protocol Gateway –** It translates request from a wireless protocol stack to the WWW protocols. Also performs DNS (Domain Name Server) look-up.
b) **Content encodes and decodes –** Translates WAP content into a compact format due to slow underling wireless link and vice versa.

c) **User Agent profile management –** Enable personalization and customization of the device.
d) **Catching Proxy –** Improves perceived performance and network utilization by maintaining a cache of frequently accessed resources.

WAP Client primarily includes wireless phones, PDAs, and Pagers. It contains a user agent or a micro browser that allows the user to manage UI similar to a web browser on a desktop computer.

Application servers consisting of 3 tires:

1. **Web Server –** It understands HTTP protocols and response to HTTP requests from the clients.
2. **Application Server –** It encodes elements like personalization, commerce, security and data persistence logic, etc.
3. **Database Server –** used for persistence storage of application data.

<u>WAP Protocols</u>: -

I. **Physical and Datalink Layer:** In WAP, point-to-point protocols are used over one or more OTA bearer protocols.

II. **Network Layer:** IP is the Network layer of choice in WAP. However, not all wireless networks are capable of transmitting IP. Some uses SMS or other non-packet network protocols.

III. **Wireless Transport Layer Security:** All the communication from the mobile phone to internet passes through the WAP Gateway. The communication between the mobile phone and this WAP Gateway has to be secured. The SSL (Secure Socket Layer) or TLS protocol can't be used for this purpose because of the constraints over the mobile phone. A mobile phone has very limited bandwidth, memory, computational power, and battery power and can't perform heavy computations. So, WTLS is used in place of SSL/TLS. WTLS provides the following features:
    - Data integrity
    - Privacy
    - Authentication
    - Denial of service protection

Wireless Transaction Layer Protocols (WTP): -

Because wireless connectivity introduces a variety of irregularity problems; WTP specifies a set of transaction semantics to be implemented to provide so called reliable and unreliable messaging between the client and the WAP Gateway. It provides 3 different kinds of transaction services. Such as:

- Unreliable one way
- Reliable one way
- Reliable two-way communication

Wireless Session Protocol (WSP): -

WSP provides a consistent interface between two session services it establishes a reliable session from client to server and closes it in a proper manner. In addition, data exchange is performed using compact encoding method also it suspends and resumes the session. It offers both connection oriented or connectionless services. The connectionless service is most suitable for where applications don't need reliable delivery of data and don't care about confirmation. The connection-oriented session services include services from session management to session rescue.

Wireless Application Environment (WAE): -

The Wireless Application Environment (WAE) is the top-most level in the WAP architecture. It is based on WWW and Mobile Telephony technologies, the aim of WAE is to provide the software manufacturers, hardware vendors or service providers an interoperable environment on which they can build applications and services which, in turn, can be used in a wide variety of wireless devices. WAE includes the micro-browser that contains functionality for using not only WML and WML Script as previously stated, but also Wireless Telephony Application, namely (WTA and WTAI) - telephony services and programming interfaces as well as content formats including well-defined data formats, images, phone book records and calendar information.

WAP PUSH Architecture: -

The WAP PUSH Framework allows information to be send to a client device without user action. In a client – server model, a client requests for a service or information from a server. The server then responds to this request by providing information back to the client. This is call as PULL technology. Here, the client pulls the information from the server.

In addition to this technology WAP provides other technology called PUSH technology. It is also based on client-server model, but there is no explicit request originated by the client. The server transmits its content before the client's request.

In short, PULL transactions are always initiated by client while PUSH transactions are always initiated by server. PUSH technology is helpful to implement alerts and notifications. PUSH saves resources.

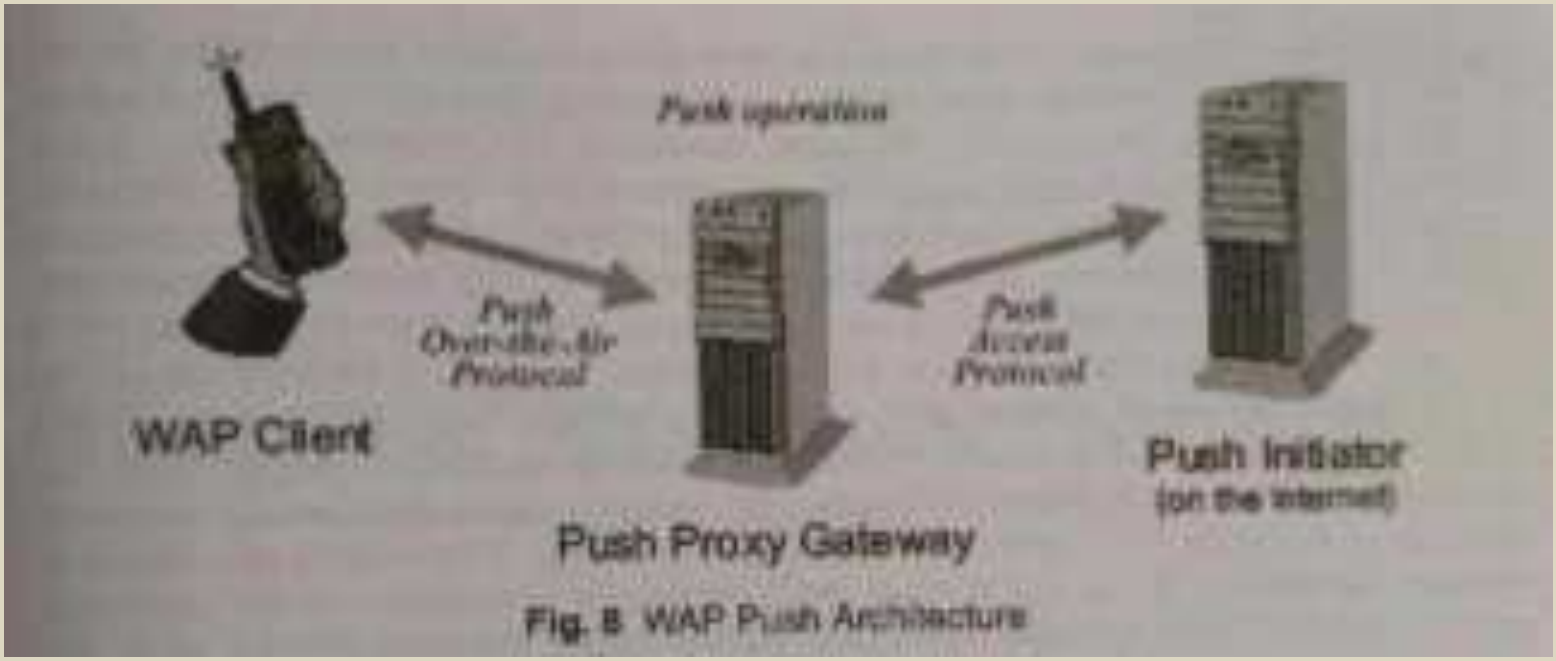


Fig. 8 WAP Push Architecture

PUSH Framework can be explained as follows:

The PUSH content is originated in a server in the internet that needs to be delivered to a mobile phone. The PUSH Initiator (PI) contacts the PUSH Proxy Gateway (PPG) from the

internet site and delivers content to the destination client. The PPG then forwards the content to the mobile network to be delivered to destination client OTA.

The Internet side PPG protocol is called the PUSH Access Control. The WAP side PPG protocol is called OTA Protocol.

PUSH – PULL Based Data Acquisition

3 types of browsing contents can be pushed to a WAP micro browser.

(i) Service Indication (SI)
(ii) Service Loading (SL)
(iii) Cache Operation (CO)

PUSH SI provides the ability to PUSH content to users to notify them about E-mail messages awaiting retrieval, News Headlines, Commercial Offers and so on.

PUSH SL provides the ability to PUSH some contents to the WAP device without user explicit request.

PUSH CO provides a means for invalidating objects stored in the WAP device cache memory.

I Mode: -

It is the packet-based service for mobile phones offered by Japan's one of the wireless technologies. It was first introduced in 1999 which was world's first i-Phone (smart phone) for web browsing. The I Mode wireless data service offers color and video over many phones. Its mobile computing service enables users to do Telephone Banking, make Airline Reservation, Conduct Stock Transaction, Send and Receive E-mails, and have access to the internet.

WAP 2.X: -

The WAP 1.X architecture consisting of the origin server, gateway, and user terminal environment (mobile sets). The server could be a WAP or HTTP server. The Gateway translated the protocol layer and application information.

In contrast to this, WAP 2.X architecture consisting of 4 components.

1. Application Environment
2. Protocol Frameworks
3. Security Services
4. Service Discovery

The WAP 2.X architecture doesn't have strict divisions between the server, gateway, and user terminal environments.

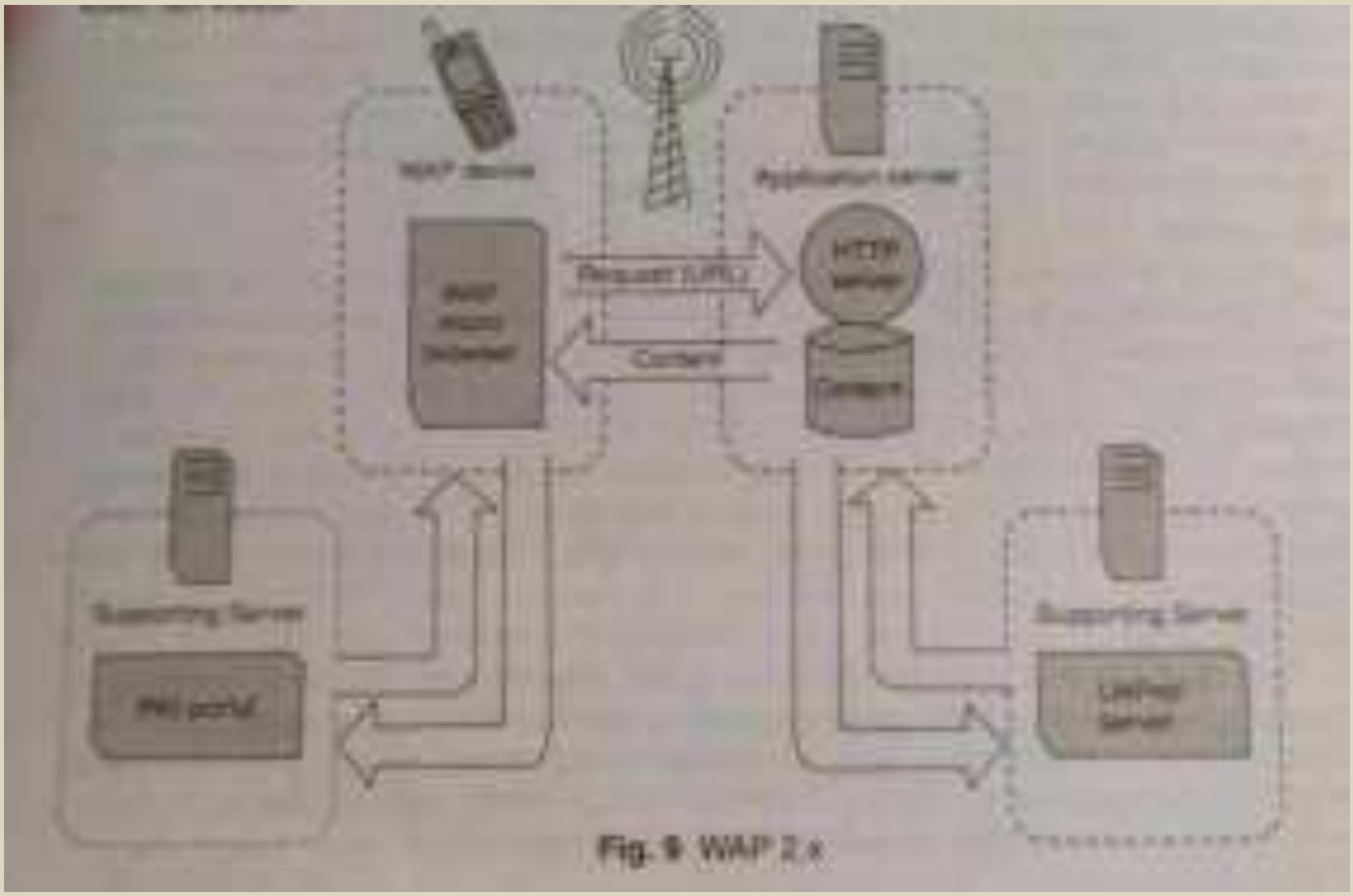


Fig. 9 WAP 2.x

First generation wireless devices communicated only voice signals. Voice only communication is referred as 1G. Thereafter voice transmission carried data. Second generation devices (2G) communicate voice as well as data signals. 2G services came into market in year 1988 and provided data rates up to 14.4kbps. The enhancements of 2G came as 2.5G and 2.5G+. They supported data rates up to 100kbps. The third-generation mobile devices (3G) communicate at much higher rates and support voice, data and multimedia streams. 3G supports data rates of 2Mbps or higher for short distances and 384kbps for long distance transmissions. High data rates in 3G devices enable transfer of video clips supporting faster multimedia communication.

GLOBAL SYSTEM FOR MOBILE COMMUNICATION (GSM): -

GSM is a globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that would formulate specifications for a European mobile cellular radio system operating at 900 MHz.

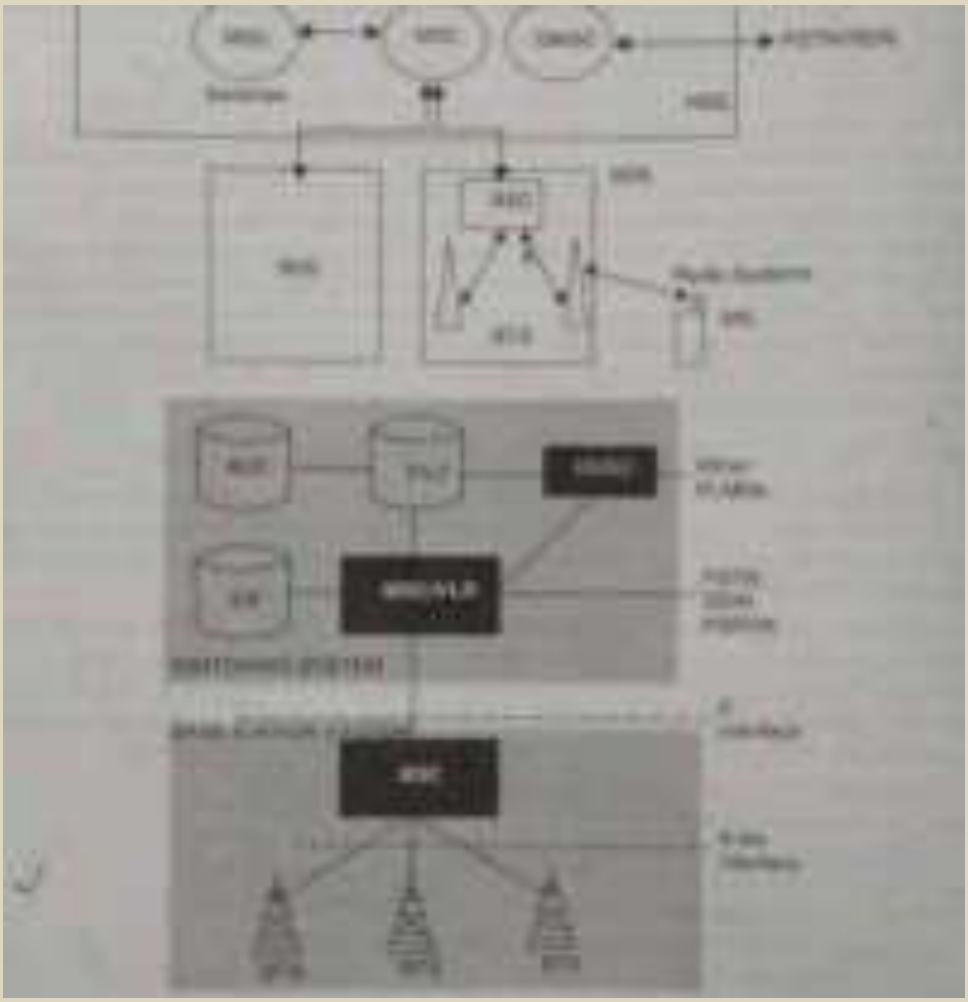
GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but don't address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to but equipment from different suppliers. The proposed GSM system had to meet certain business objectives:

- Support for international roaming
- Good speech quality
- Ability to support handheld devices
- Low service cost
- Use of spectrum efficiently
- Support for a range of new services and facilities
- ISDN compatibility

In a short, GSM became global. Depending on locally available frequency bands, different air interfaces were defined. These are 900 MHz, 1800 MHz and 1900 MHz. GSM uses a combination of FDMA and TDMA access techniques. The GSM system has an allocation of 50MHz.

GSM Architecture: -

Below given figure illustrates the architecture of GSM network.



MS: Mobile Station

BTS: Base Transceiver Station

BSC: Base Station Controller

MSC: Mobile Service Switching Center

GMSC: Gateway Mobile Services Switching Center

EIR: Equipment Identity Register

VLR: Visitor Location Register

HLR: Home Location Register

AuC: Authentication Center

NSS: Network Sub System

PSTN: Public Switched Telecomm Network

ISDN: Integrated Services Digital Network

OMC: Operations and Management Center

The GSM network is divided into four major systems: The *Mobile station (MS)*, the *Switching System (SS)*, and the *Base Station Subsystem (BSS)*, and the *Operation and Support System (OSS)*.

The MS is carried by the subscriber; the BSS controls the radio link with the Mobile Station. The NSS, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. The MS and the BSS communicates across the Um interface, also known as the air interface or radio link. The BSS communication with the Mobile Service Switching Center across the A interface.

GSM Components: -

- **Mobile Station (MS)-** The MS consists of the physical equipment or *Mobile Equipment (ME)*, such as the radio transceiver, display and digital signal processors, and a smart card called the *Subscriber Identity Module (SIM)*. The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. A smart card usually is the size of a credit card. To use it just plug it into the instrument. SIM and ME are collectively called *Mobile Terminal (MT)*. By inserting the SIM into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services. The ME is uniquely identified by the *International Mobile Subscriber Identity (IMSI)*, identifying the subscriber, a secret key for authentication, and other user information. The IMEI and the IMSI are independent, thereby providing personal mobility. The IMSI is a unique non-dialable number allocated to each mobile subscriber in the GSM system that identifies the subscriber and his or her subscription within the GSM network.

- **The IMSI is made up of three parts-** The *Mobile Country Code (MCC)* consisting of three digits, the *Mobile Network Code (MNC)* consisting of two digits, and the *Mobile Subscriber Identity Number (MSIN)* with up to 10 digits. The SIM is protected by a *personal Identification Number (PIN)*, which is between four to eight digits in the length. The PIN is initially loaded by the network operator at the subscription time. This PIN can be deactivated or changed by the user. To use the MS, the user is asked to enter the PIN. If the number is not correctly entered in the three connective attempts, the SIM is blocked and MS can't be used. To unblock the SIM, the user is asked to enter the eight-digit PIN *Unblocking Key (PUK)*. A SIM contains the subscriber-related information, including the PIN and PUK codes. The subscriber-related data also include a list of abbreviated and customized short dialing number; short message received when the subscriber is not present, and the names of the preferred networks to provide service and so on. The ME contains the non-customer-related hardware and software specific to the radio interface. When the SIM is removed from an MS, the remaining ME can't be used for reaching the service, except for emergency calls.
- **Switching System (SS) or Network and Switching Subsystem (NSS)-** The central component is of NSS is MSC. The NSS consists of MSC, HLR, VLR, and AuC. NSS acts like a normal switching node for mobile subscribers of the same network (connection between mobile phone to mobile phone within the same network). It acts as a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone). It acts like normal switching node for ISDN. It supports the switching functions, subscriber profiles, and mobility management. Various components are described as below:
- **HLR:** It is the database, which stores the information of subscribers belonging to the covering area of MSC. There is logically one HLR per GSM network, although it may be implemented as a distributed database. The current location of MS is usually maintained by the HLR and VLR. When an MS moves from the home system. The VLR then informs the MS's HLR of its current location. The AuC is used in the security data management for the authentication of subscriber. The AuC may be co-located with the HLR. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The current location of the mobile is in the form of a Mobile Station Roaming Number (MSRN), which is a regular ISDN number used to route a call to the MSC where the mobile is currently located.
- **VLR:** The VLR can be considered as temporary copy of selected information stored in HLR of the mobile subscribers that are currently located in a given MSC serving area, but whose Home Location Register (HLR) is elsewhere. This information is necessary for

call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each entity can be implemented as an independent unit but all manufacturers implement the VLR as an integral part of MSC so that the geographical area controlled by the MSC corresponds to that controlled by VLR. The MSC contains no information about particular mobile stations; this information is stored in the location registers. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to ask the HLR each time.

- **AuC:** The AuC is responsible for the authentication of subscriber. The AuC may be co-located with the HLR. It verifies the user's identity and ensures the confidentiality of each call. The AuC protects different types of fraud found in today's cellular world. It is a database, which is protected and stores a copy of the secret key stored in each subscriber's SIM card. These data help to verify the user's identity.
- **EIR:** The EIR is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its IMEI. It prevents calls from stolen, unauthorized, or defective mobile stations. The AuC and EIR are implemented as stand-alone nodes or as a combined AuC/ EIR node. The EIR is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its IMEI. An IMEI is marked as invalid if it has been reported stolen or isn't type approved.
- **Base Station Subsystem:** All radio-related functions are performed in the BSS, which consists of Base Station Controllers (BSC) and the Base Transceiver Stations (BTS). BSC – The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency power levels in BTSs. A number of BSC is served by an MSC. The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTS is controlled by a BSC.
- **Operation and Support System (OSS):** OSS controls and monitors the GSM system. The Operations and Maintenance Center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the OSS. The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

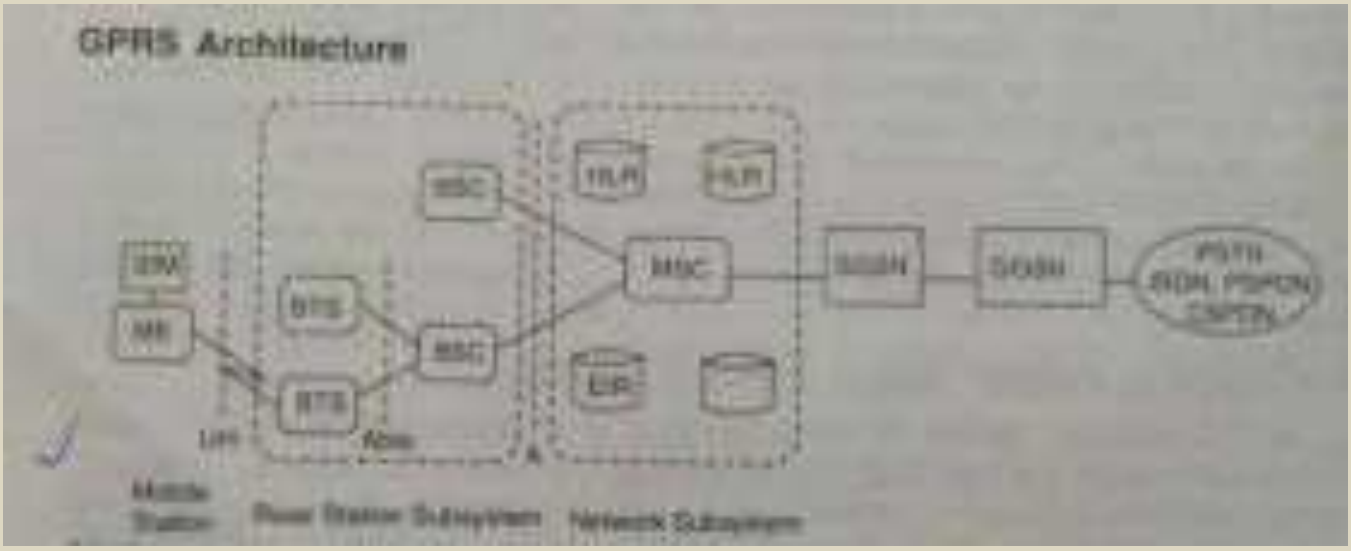
GENERAL PACKET RADIO SERVICE (GPRS): -

GPRS (General Packet Radio Service) is a packet-based communication service for mobile devices that allows data to be send and received across a mobile telephone network. GPRS is a step towards 3G and is often referred to as 2.5G. The GPRS network is an "always on", private network for data. It used the existing GSM network to transmit and receive data to and from GPRS mobile devices. Private IP address are dynamically assigned within the network to mobile devices. However, Access Point Names (APN's) provide a gateway route to other networks such as the Internet, WAP services or private corporation networks. Firewalls typically reside at the APN to isolate the public and private networks. IP address allocated to mobile GPRS devices are therefore not addressable from outside the GPRS network (e.g. from the Internet) without specialized services or infrastructure.

The two key benefits of GPRS are better use of radio and network resources and completely transparent IP support. GPRS optimizes the use of network and radio resources. It uses radio resources only when there is data to be sent or occupy the network when a payload is being transferred, and so is well adapters to the very busty nature of data applications. Another important feature of GPRS is that it provides immediate connectivity and high throughput. GPRS will enable Internet applications, from web browsing to chat, location-based applications, e-commerce etc. over the mobile network. Other new applications for GPRS, include file transfer and the ability to remotely access and control house appliances and machines.

In addition, GPRS allows improved quality of data services in terms of reliability response time, and features supported. GPRS offers up to ~ 171.2 Kbps, depending on the network availability, channel coding scheme and client capability. This increase in speed with respect to GSM is achieved by using more than one timeslot of the TDMA frame. Due to the packet switched characteristics the allocation of the available timeslots may vary from one instant to the next (e.g. it may have 8 timeslots at one time and 4 later on).

To use GPRS, users specifically need a mobile phone or terminal that supports GPRS, a subscription to a mobile telephone network that supports GPRS and the use of GPRS must be enabled for that user. GPRS will allow network operators to implement an IP-based core architecture for data applications, which will continue to be used and expanded upon for 3G services for integrated voice and data applications. In addition, GPRS will provide a testing and development area for new services and applications, which will also be used in the development of 3G services.



- **SIM:** Subscriber Identity Module
- **MSC:** Mobile Services Switching Center
- **HLR:** Home Location Register
- **BTS:** Base Transceiver Station
- **AuC:** Authentication Center
- **BSC:** Base Station Controller
- **ME:** Mobile Equipment
- **EIR:** Equipment Identity Register
- **VLR:** Visitor Location Register

GPRS Applications: -

- Chat
- Textual and Visual Information
- Still & Moving Images
- Web Browsing
- Document sharing/ Collaborate working
- Audio
- Email, File Transfer…

IS-95: -

Interim Standard 95 (IS-95) is the first CDMA-based digital cellular standard. The brand name for IS-95 is cdmaOne. It is a 2G Mobile Telecommunications Standard that uses CDMA, a multiple access scheme for digital radio, to send voice, data and signaling data (such as a dialed telephone number) between mobile telephone and cell sites.

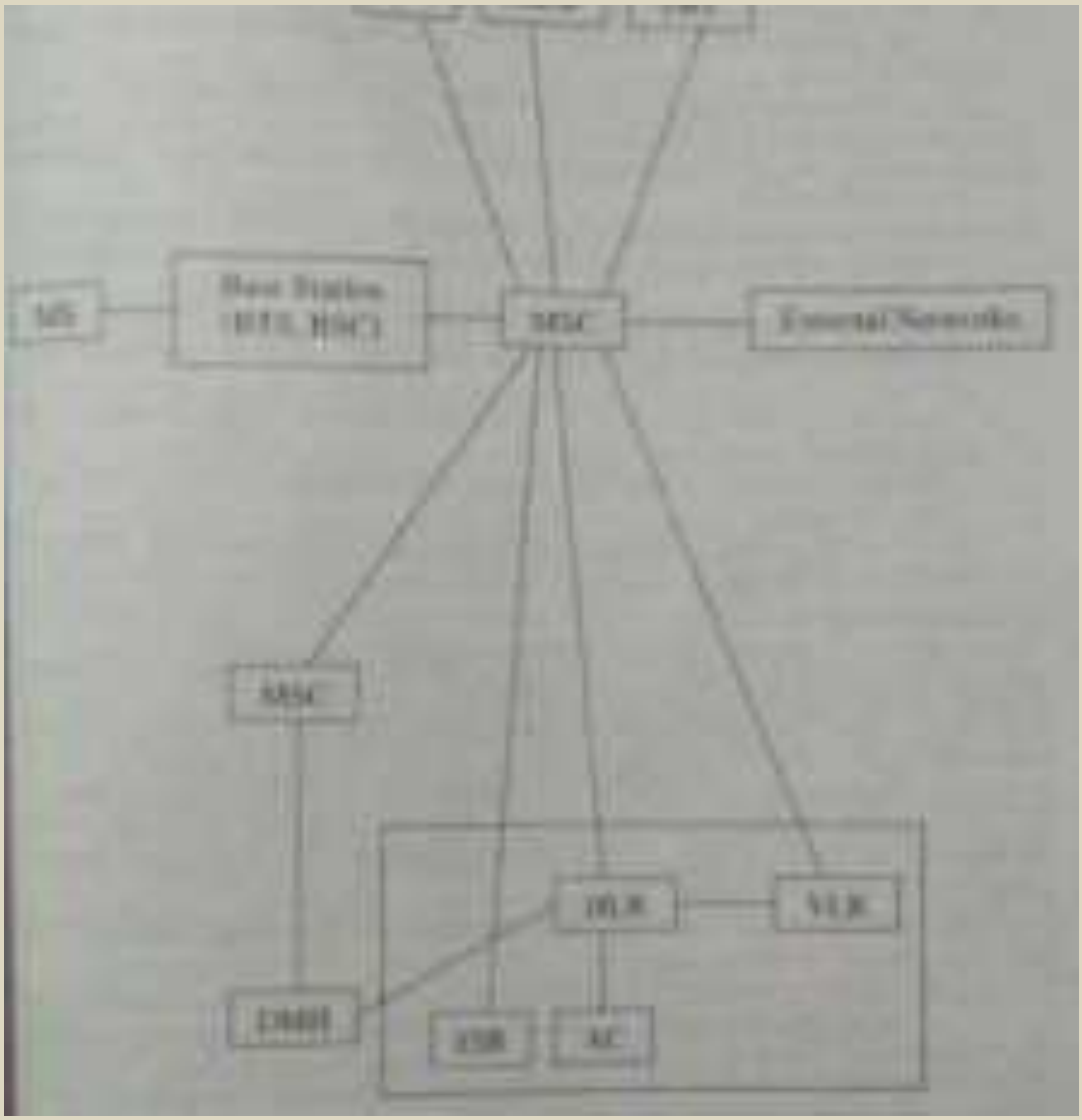
CDMA is a digital radio system that transmits streams of bits (PN Sequences). CDMA permits several radios to share the same frequencies. Unlike TDMA, a competing system used in 2G GSM, all radios can be active all the time, because network capacity doesn't directly limit the number of active radios. Since larger numbers of phones can be served by smaller numbers of cell sites, CDMA-based standards have a significant economic advantage over TDMA-based standards, or the oldest cellular standards that used frequency-division multiplexing.

Each user is identified by a different spreading code. Energy received over multipath channels can be resolved to avoid cancellation of waves. Transmissions are asynchronous on the uplink, but synchronous on the downlink. Power control is needed to mitigate near-far problems.

In a commercial cellular system, we need to increase the transmission power when the mobile user moves away and reduce the power when the user comes nearer to the base station.

IS-95 Architecture:

Network components within IS-95 architecture are almost similar to GSM architecture. The following figure illustrates the architecture:



The main compoents of IS-95 are as follows:

- **Mobile Station (MS):** This is the mobile phgone instrument with the user. This mobile station can be a stand alone device or other devices like fax machines etc.
- **Base Station (BS):** It connects to the MSC. BS is a system between the MS and the MSC. The BS is divided into BTS and BSC.
- **Mobile Switching Center (MSC):** It is equivalent to the telephone exchange of a fixed network. The MSC is an automatic system that interchange of a fixed network. The MSC is an automatic system that interfaces the user trafficfrom the wireless network with the wired network. It plays many roles like originating MSC, servingMSC, terminating MSC, visited MSC etc.
- **Home Location Register (HLR):** It is the functional unit which manages mobile subscribers by managing their details. One HLR can also serve multiple MSCs.
- **Data Message Handler (DMH):** It is responsible for collating billing data.

- **Visited Location Register (VLR):** It is linked to one or more MSCs. It is the functional unit that dynamically stores subscriber information obtained from respective HLR.
- **Authentication Center (AC):** It manages the authentication process of subscribers. It may be located within an HLR or MSC or it may be independent of both.
- **Equipment Identity Register (EIR):** It keeps the record of mobile devices and provides on need. It may be located with MSC or may be independent of it.
- **Operation System (OS):** It is responsible for overall management of wireless network.
- **Internetworking Function (IWF):** It enables to communicate the MSC with other networks.
- **External Networks:** These are other communicaton networks. They can be PSTN, ISDN, etc.

CDMA 2000: -

CDMA 2000 is the 3G version of IS-95. It builds on the inherent advantages of CDMA technologies and introduces other enhancements, such as Orthogonal Frequency Division Multiplexing (OFDM and OFDMA), advanced control and signaling mechanisms, improved interference management techniques, end-to-end Quality of Service (QoS), and new antenna techniques such as Multiple Inputs Multiple Outputs (MIMO) and Space Division Multiple Access (SDMA) to increase data throughput rates and quality of service, while significantly improving network capacity and reducing delivery cost. There are many attributes of CDMA which are of great benefit to the cellular system:

• **Soft handoff:-** Since every cell uses the same radio frequency band, the only difference between user channels is the spreading code sequences. Therefore, there is no jump from one frequency to another frequency when a user moves between cells. The mobile terminal receives the same signal in one cell as it does in the next, and thus there is no harsh transition from one receiving mode to another. Two or more neighboring base stations can receive the signal of a particular user, because they all use the same channel. Moreover, two base stations can simultaneously transmit to the same user terminals. The mobile receiver can resolve the two signals separately and combine them. This feature is called *soft handoff*.

• **Soft capacity or graceful degradation:-** In theory, it does not matter whether the spectrum is divided into frequencies, time slots, or codes, the capacity provided from these three multiple access schemes is the same. However, in CDMA, all the users in all cells share one radio channel and are separated by codes. Therefore, an additional user may be added by sacrificing

somewhat the link quality, with the effect that voice quality is just slightly degraded compared to that of the normal N-channel cell. Thus, degradation of performance with an increasing number of simultaneous users is 'graceful" in CDMA systems, versus the hard limits placed on FDMA and TDMA systems.

- **Multipath tolerance:-** When a signal is spread over a wide bandwidth, a frequency selective fade will corrupt only a small portion of the signal's power spectrum, while passing the remaining spectrum pure. As a result, upon despreading there is a better probability that the signal can be recovered correctly.
- **Leading performance:-** CDMA2000 performance in terms of data-speeds, voice capacity and latencies continue to outperform in commercial de-ployments other comparable technologies.
- **Efficient use of spectrum:-** CDMA2000 technologies offer the highest voice capacity and data throughput using the least amount of spectrum, lower-ing the cost of delivery for operators and delivering superior customer experience for the end users.
- **Support for advanced mobile services:-** CDMA2000 enables the delivery of a broad range of advanced services, such as high-performance VoIP, push-to-talk, video telephony, multimedia messaging, multicasting and multi-playing online gaming with richly rendered 3D graphics.
- **All-IP:-** CDMA2000 technologies are compatible with IP and ready to sup-port network convergence. Today, CDMA2000 operators that have de-ployed IP-based services enjoy more flexibility and higher bandwidth effi-ciencies, which translate into greater control and significant cost savings.
- **Devices selection:-** CDMA2000 offers the broadest selection of devices and has a significant cost advantage compared to other 3G technologies to meet the diverse market needs around the world.
- **Seamless evolution path:-** CDMA2000 has a solid and long-term evolution path which is built on the principle of backward and forward compatibility, in-band migration, and support of hybrid network configurations.
- **Flexibility:-** CDMA2000 systems have been designed for urban as well as remote rural areas for fixed wireless, wireless local loop (WLL), limited mobility and full mobilility applications in multiple spectrum bands, including 450 MHz, 800 MHz, 1700 MHz, 1900Mhz and 2100 MHz .

WIDEBAND CODE DIVISION MULTIPLE ACCESS (WCDMA)

WCDMA is a wideband spread-spectrum 3G mobile telecommunication air interface that utilizes code division multiple access (or CDMA the general multiplexing scheme not to be confused with CDMA the standard). It provides , simultaneous support for a wide range of services with different characteristics on a common 5MHz carrier.

The term WCDMA also refers to one of the International Telecommunications Union's IMT-2000 standards, a type of 3G cellular network. WCDMA is the technology behind the 3G UMTS standard and is closely allied with the 2G GSM standard. It provides new service capabilities, increased network capacity and reduced cost for voice and data services.

WIRELESS SENSOR NETWORK

A wireless sensor network is a wireless network consisting of spatially distributed devices using sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communication devices, a small microcontroller, and an energy source, usually a battery. The size of a single sensor node can vary from shoebox-sized nodes to devices of the size of grain of dust. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station).

The below fig. depicts Typical Multihop Wireless Sensor Network Architecture.

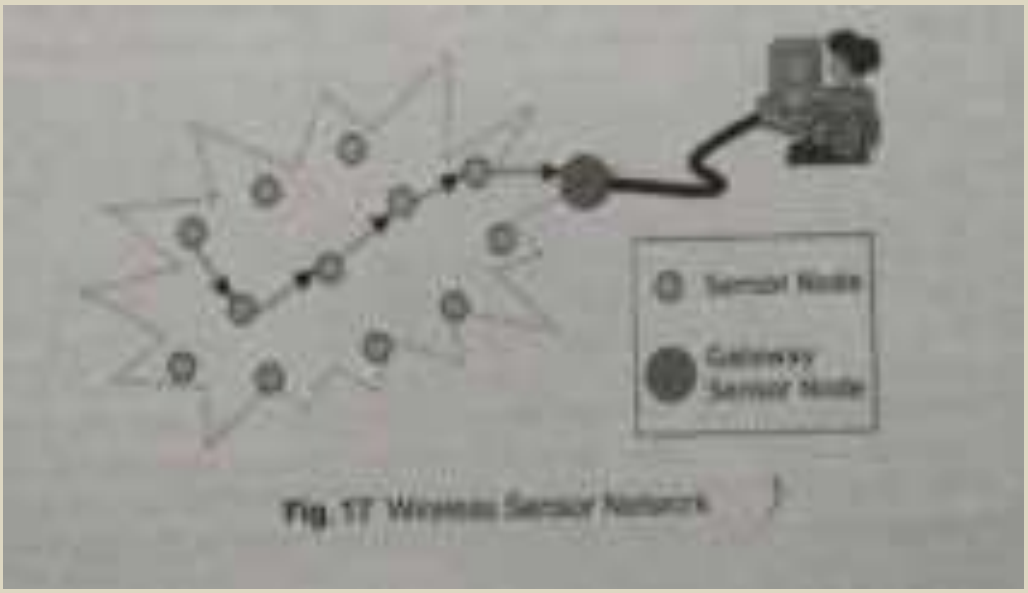


Fig. 17 Wireless Sensor Network

SHORT MESSAGE SERVICES (SMS): -

Introduction:

SMS is the delivery of alphanumeric messages to mobile phones over wireless networks. It is not a wireless communication technology. It is a value-added service which operates on long range wireless networks. SMS provides a connectionless transfer of messages with low capacity and low time performance. It is most important form of data communication. It can be sent from any mobile device to any destination as a message, an email or some other form of electronic message. The features which make SMS functionally different from other data communication technologies is that it can be delivered to the destination whether or not the voice service is in user and it is asynchronous messaging service in its operation. In other words, as active mobile handset is able to receive or submit a short message at any time, independent of whether or not a voice or data call is in progress. SMS also guarantees delivery of the short message by the network. Temporary failures are identified, and the short message is stored in the network until the destination becomes available.

SMS doesn't require usage of one type of wireless network over other. It can be implemented on the network which is available. Because of its pervasive nature it is used as a text-based application layer transport protocol.

SMS is a service for sending messages of up to 160 characters (224 characters if using a 5-bit mode) to mobile phones that use Global System for Mobile (GSM) communication. It can be sent to digital phones from a Web site equipped with PC Link or from one digital phone to another. Typical uses of SMS include:

- Notifying a mobile phone owner of a voicemail message
- Notifying a salesperson of an inquiry and contact to call
- Notifying a doctor of a patient with an emergency problem
- Notifying a service person of the time and place of their next call
- Notifying a driver of the address of the next pickup

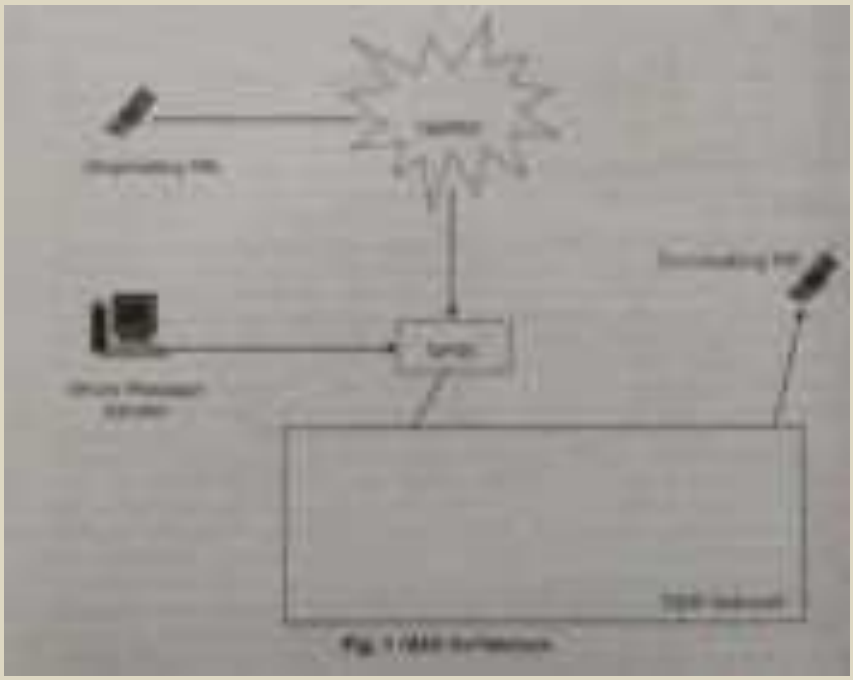
An SMS gateway is a Web site that lets you enter an SMS message to someone within the cell served by that gateway or that acts as an international gateway for users with roaming capability.

Two types of GSM SMS have been defined. They are:

- **Cell Broadcast:** It is a service which delivers short messages to all users in a given area at regular intervals.
- **Point-to-Point Service:** It is a service which sends short messages to a particular user.

SMS Architecture: -

The basic network architecture is shown below:



Legend:

- **SMS GMSC:** SMS Gateway MSC
- **IWMSC:** Internetworking MSC
- **SMSC:** Short Message Service Center
- **MSC:** Mobile Switching Center
- **BSS:** Base Station System
- **MS:** Mobile Station

In the above shown architecture, the short message is first sent to SMSC from the message sender. The message sender can be MS or paging input device. The SMSC is connected to

the GSM network through a specific GSM MSC called the *SMS Gateway MSC (SMS GMSC)*. The SMSC may connect to several GSM networks. The SMS GMSC locates the current MSC of the message receiver and forwards the message to that MSC.

SMS also eliminates the need for separate devices for messaging since services can be integrated into a single wireless device – the mobile terminal

MULTIMEDIA MESSAGE SERVICES (MMS): -

If you've ever sent or received text messages, you'll know how useful the so-called Short Messaging Service (SMS) can be. Because most current mobile phones use narrowband GSM channels, the amount of data you can send at any one time is very limited – up to 160 characters to overcome some of the limitations, users resort to abbreviated 'SMS speak' "R U OK" (Are you OK?) and "C U L8ER" (See you later!) etc. Fun, but not very satisfactory for social communication. Imagine if, instead, you could write as much text as you liked, format it, add creative type faces and drawings, drop in animated images, include full-color photos, a bit of music or a voice clip, even a short video of you and your mates on holiday.

MMS is a store and forward messaging service that allows mobile subscribers to exchange multimedia messages with other mobile subscribers. MMS uses GPRS, so you must have GPRS in your network and be allowed to use it. As such it can be seen as an evolution of SMS, with MMS supporting the transmission of additional media types:

- Text
- Picture
- Audio
- Video
- Combinations of the above

MMS is an important emerging service, which allows the sending of multiple media in a single message, and the ability to send a message to multiple recipients.

The originator can easily create a Multimedia Message, either using a built in or accessory camera, or can use images and sounds stored previously in the phone (and possibly downloaded from a web site).

Even if the recipient phone is not switched on, the Multimedia Message will be stored and send to the recipient as soon as they switch on their phone. In a non-roaming case, it is

expected that the subscriber will allow a Multimedia Message to be downloaded automatically to their phone and then they would be notified and could see the Multimedia Message immediately.

A number of Multimedia Messages can be stored in the user's handset and reviewed or forwarded at a later date. Each Multimedia Message contains a number of pages (think of a PowerPoint slide show as an analogy). On each page, there can be one image and one set of text. An audio file can slow be attached. The time that each "page" is displayed can be specified, so the user experience is somewhat like a slide show.

Working Principle of MMS:

Depending upon the operator, a typical example of how an MMS message can be sent and received between two compatible MMS phones is detailed below:

STEP 1: Using an MMS compatible phone, take a photo.

STEP 2: Use your phone to personalize the message by adding text, sound clip or your own voice.

STEP 3: Send the MMS message.

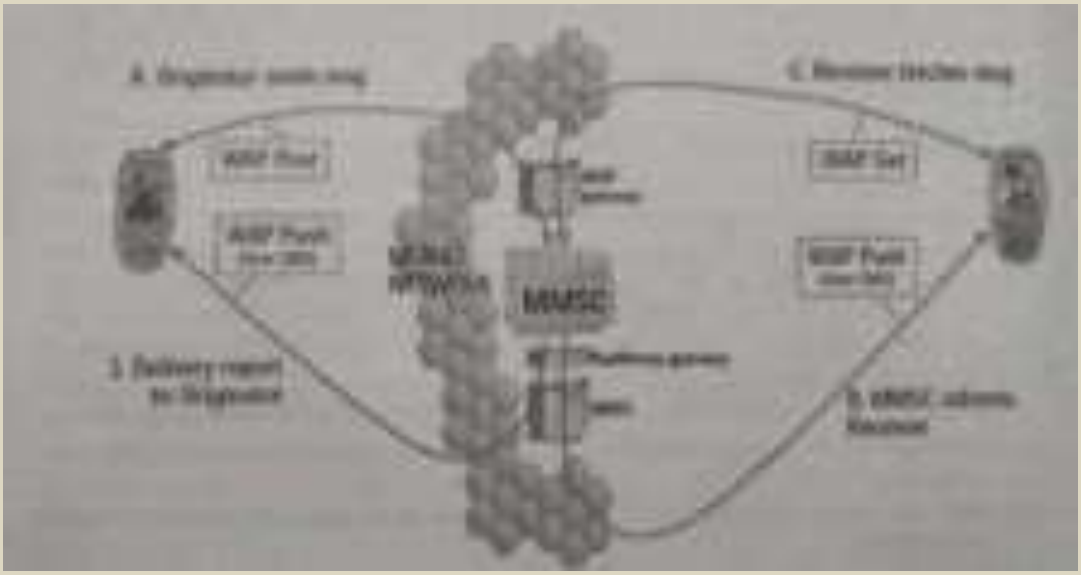
Main Components of MMS Architecture: -

MMS operates like SMS; in the sense that it is a person-to-person service with an operator controlled central message storage, management and relay center which also provides the sender with confirmation that the message has been received. The MMS center (MMSC) however needs to be more flexible than the SMS Center (SMSC) in order to cope with the variety of different message type and the need to convert message formats according to the capabilities of the receiving terminals.

The industry has defined 4 key functional elements MMSC product:

1. **MMS Relay –** The engine which transcodes and delivers the message to mobile subscribers.

2. **MMS Server –** It provides the storage mechanism in the Store and Forward MMS Architecture.
3. **MMS User Agent –** An application server providing users the ability to view, create, send, edit, delete, and manage their multimedia messages.
4. **MMS User Databases –** It contains records of user profiles, subscription of data, etc.



The Nokia MMS Center