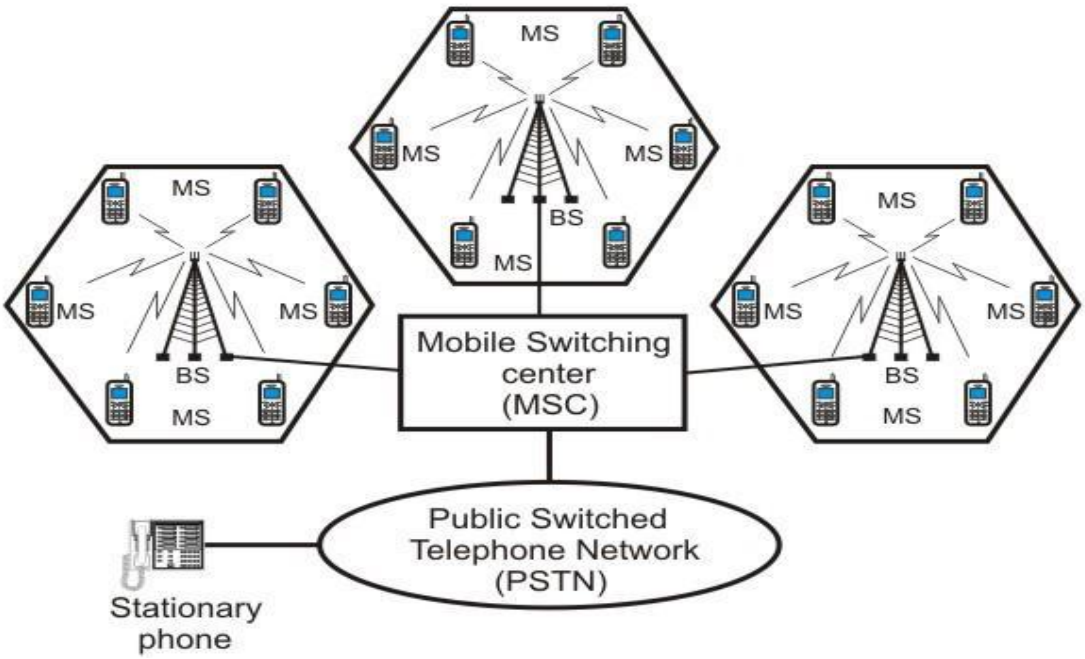
Cellular Telephone Systems

A cellular radio system provides standard telephone service by two-way radio at remote locations. Cellular radios or telephones were originally installed in cars or trucks, but today most are handheld models. Cellular telephones permit users to link up with the standard telephone system, which permits calls to any part of the world.

The Bell Telephone Company division of AT&T developed the cellular radio system during the 1970s and fully implemented it during the early 1980s. Today, cellular radio telephone service is available worldwide. The original U.S. cell phone system, known as the advanced mobile phone system, or AMPS, was based on analog FM radio technologies. AMPS has gradually been phased out and replaced by second-generation (2G), third-generation (3G), and fourth-generation (4G) digital cell phone systems.

The cellular telephone systems comprises of the following basic components which is shown in fig below:



1)Mobile Station

A mobile station (MS) comprises all user equipment and software needed for communication with a mobile network. The term refers to the

global system connected to the mobile network, i.e. a mobile phone or mobile computer connected using a mobile broadband adapter.

2)Base Station/Base Transceiver Station(BS/BTS)

It is a fixed station in cellular systems used for radio communication with mobile stations. It consists of channels, receivers and transmitters Hence it is also known as Base Transceiver Station(BTS).Base station will be located at the center of a coverage region.

3)Cell

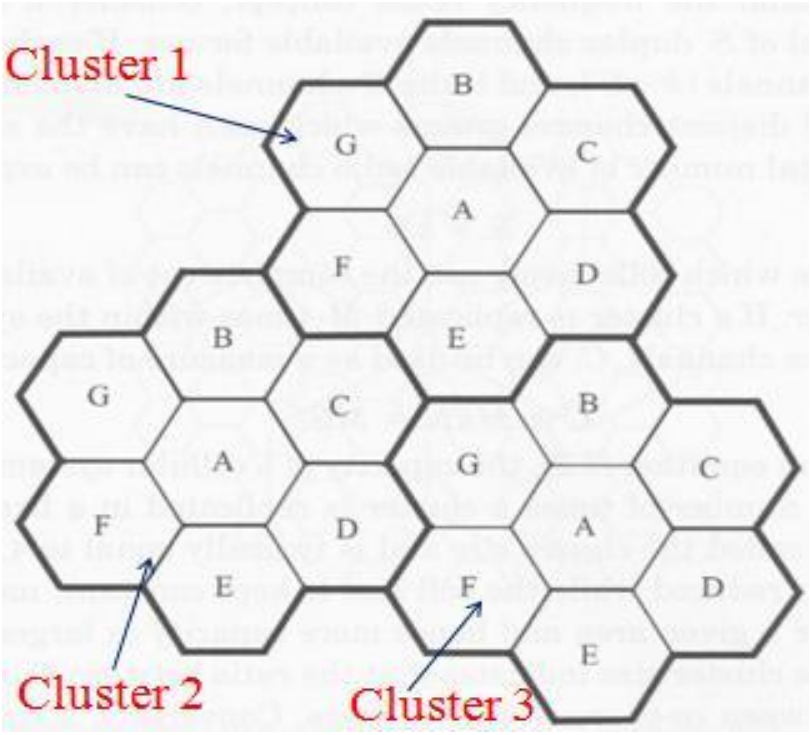
A cell is the geographic area that is covered by a single base station in a cellular network.

4)Mobile Switching Center(MSC):

A mobile switching center, is a switching office that connects mobile users to other mobile networks, the public switched telephone network and other mobile users within the same network.

The basic concept behind the cellular radio system is that rather than serving a given geographic area with a single transmitter and receiver, the system divides the service area into many smaller areas known as cells. .The typical cell covers only several square miles and contains its own receiver and low-power transmitter. The coverage of a cell depends upon the density (number) of users in a given area. High population areas uses smaller cells where as low population area is served by fewer and larger cells.Channels (frequencies) used in one cell can be reused in another cell some distance away, which allows communication using a limited number of radio frequencies.The concept of reuse allows a fixed number of channels to serve an arbitrarily large number of users. A cluster is a group of cells and no channels are reused within a cluster.

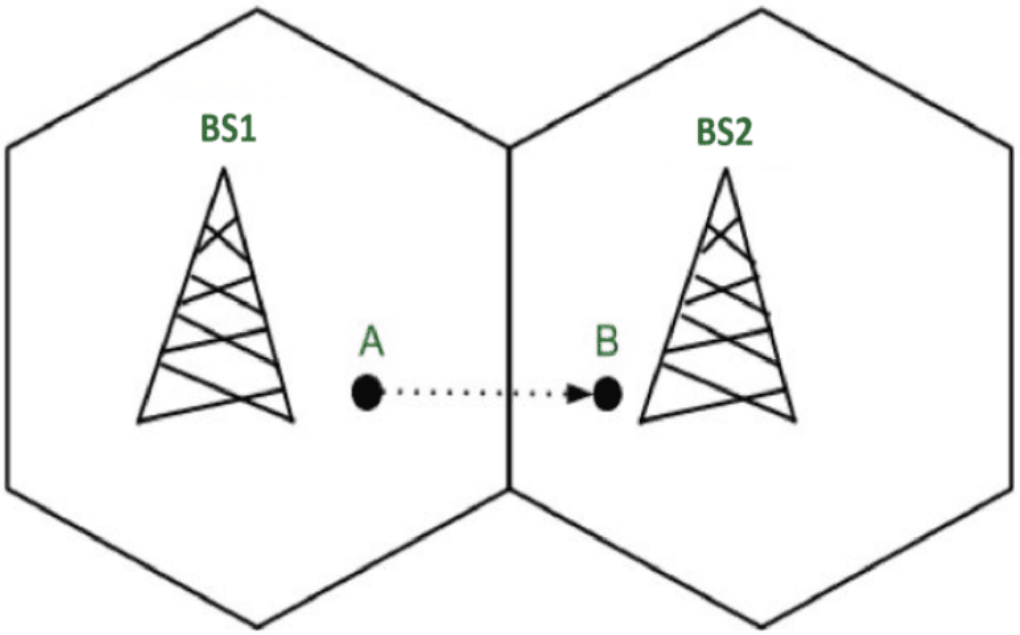
Frequency reuse is the process in which the same set of frequencies (channels) can be allocated to more than one cell, provided the cells are separated by sufficient distance. The figure shows a geographic cellular radio coverage area containing three groups of cells called clusters. Each cluster has seven cells in it, and all cells are assigned the same number of full-duplex cellular telephone channels. Cells with the same letter use the same set of channel frequencies. A, B, C, D, E, F and G denote the seven sets of frequencies.



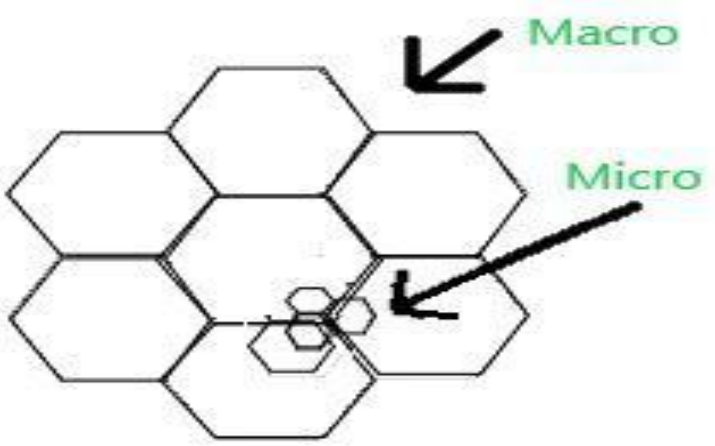
Co Channel Interference(CCI):
With frequency reuse many cells at a distance will be using the same frequency bands within a given area. These cells are called co channels.There is a possibility of interference between them since they are operating at same frequency, the interference between them is called as co channel interference.

Adjacent Channel Interference(ACI):
This occurs from channels in adjacent neighbouring cells.This is worse in small cell clusters.Adjacent channel interference results from imperfect filters in receivers that allows nearby frequencies to enter the mobile unit.It can be observed when an adjacent channel is transmitting and the mobile unit is receiving at an adjacent frequency.

Handoff/ Hand over:
In cellular telecommunications, the terms handover or handoff refers to the process of transferring an ongoing call or data connectivity from one Base Station to another Base Station. When a mobile moves into a different cell while the conversation is in progress then the MSC (Mobile Switching Centre) transfers the call to a new channel belonging to the new Base Station as shown in fig below



Cell Splitting:
Cell Splitting is the process of subdividing a cell into smaller cells each with its own Base Station. On splitting, new cells with smaller radius are added called microcells. Each new cell created is independent and has reduced antenna height and transmitter power. The creation of new smaller cells increases the capacity of the system as a whole. Cell Splitting increases the frequency reuse factor. A higher frequency reuse factor increases the capacity of the cellular system in Cell Splitting.



Cell Sectoring:
In cell sectoring, each cell is subdivided into radial sectors with directional BS antennas in order to improve the performance of the system in order to combat the interference caused by co-channels. This is a highly prevalent method that is utilized in macro cellular systems.

In actual practice, a number of sectored antennas are mounted on a single microwave tower that is situated in the middle of the cell, and a following number of antennas are installed to cover the entire 360-degree area of the cell.

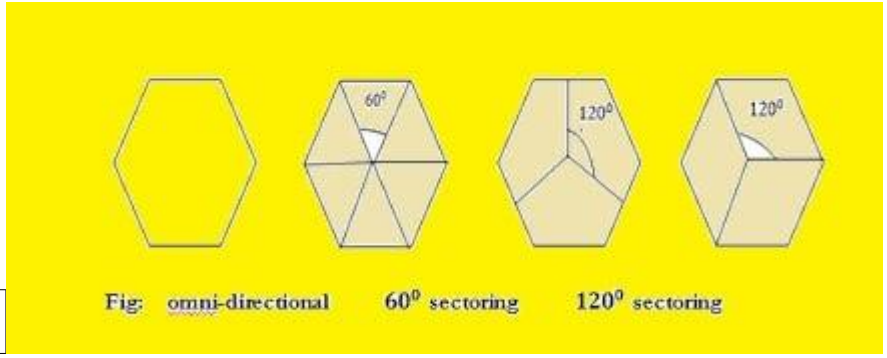


Fig: omni-directional 60^0 sectoring 120^0 sectoring

Advanced Mobile Phone System (AMPS)

Cellular telephone began as a relatively simple two-way analog communications system using frequency modulation (FM) for voice and frequency-shift keying (FSK) for transporting control and signaling information. The most recent cellular telephone systems use higher-level digital modulation schemes for conveying both voice and control information. In addition, the Federal Communications Commission (FCC) has recently assigned new frequency bands for cellular telephone.

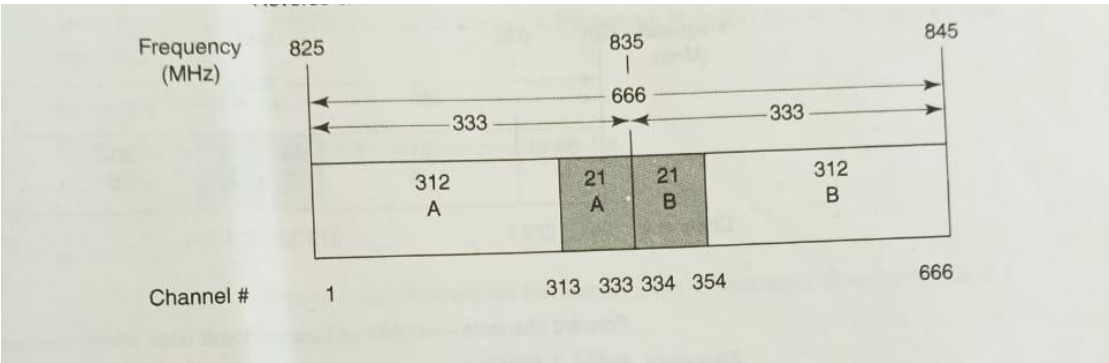
In 1971, Bell Telephone Laboratories in Murry Hill, New Jersey, proposed the cellular telephone concept as the Advanced Mobile Telephone System (AMPS).The cellular plan called for using many low-profile, low-power cell-site transceivers linked through a central computer-controlled switching and control center.

AMPS is a standard cellular telephone service (CTS) initially placed into operation on October 13, 1983, by Illinois Bell that incorporated several large cell areas to cover approximately 2100 square miles in the Chicago area. The original system used omnidirectional antennas to minimize initial equipment costs and employed low-power (7-watt) transmitters in both base stations and mobile units.The AMPS system uses a seven-cell reuse pattern with provisions for cell splitting and sectoring to increase channel capacity when needed.

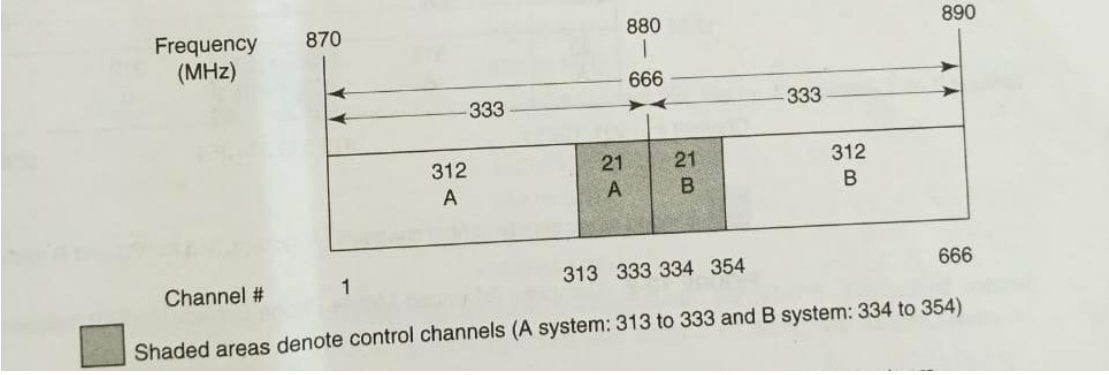
AMPS Frequency Allocation:

In 1980, the FCC decided to allocate two common carriers per cellular service area.Subsequently, two frequency allocation plans emerged-system A and system B-each with its own group of channels that shared the allocated frequency spectrum. System A is defined for the non-wire line companies (ie.,cellular telephone companies) and system B for existing wireline companies (i.e., local telephone companies). The FCC initially assigned the AMPS system a 40-MHz frequency band consisting of 666 two-way channels per service area with 30-kHz spacing between adjacent channels which is shown in fig below:

Reverse Channels:



Forward Channels:

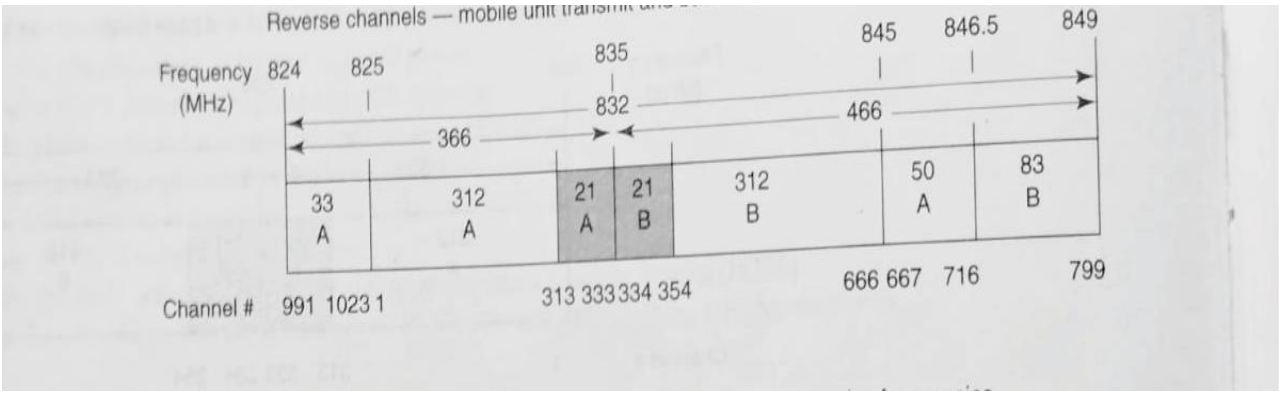


The A channels are designated 1 to 333, and the B channels are designated 334 to 666. For mobile units, channel 1 has a transmit frequency of 825.03 MHz, and channel 666 has a transmit frequency of 844.98 MHz. For base stations, channel 1 has a transmit frequency of 870.03 MHz, and channel 666 has a transmit frequency of 889.98 MHz. Simultaneous transmission in both directions is a transmission mode called full duplex (FDX) or simply duplexing. Frequency-division

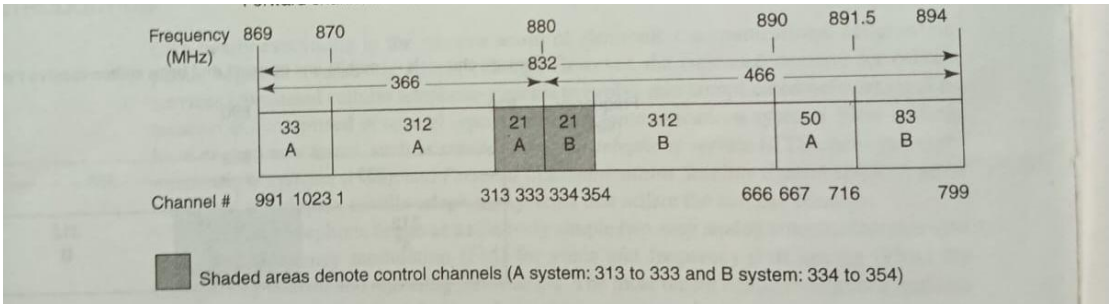
duplexing (FDD) is used with AMPS and occurs when two distinct frequency bands are provided to each user. In FDD, each duplex channel actually consists of two simplex (one-way) channels (base station to mobile and mobile to base station). A special device called a duplexer is used in each mobile unit and base station to allow simultaneous transmission and reception on duplex channels.The receiver for each channel operates 45 MHz above the transmit frequency. Consequently, every two- way AMPS radio channel consists of a pair of simplex channels separated by 45 MHz.

In 1989, the FCC added an additional 10-MHz frequency spectrum to the original 40-MHz band, which increased the number of simplex channels by 166 for a total of 832 (416 full duplex). The additional frequencies are called the expanded spectrum and include channels 667 to 799 and 991 to 1023. The complete AMPS frequency assignment is shown in Figure below

Reverse Channels:



Forward Channels:



33 of the new channels were added below the original frequency spectrum and that the remaining 133 were added above the original

frequency spectrum. With AMPS, a maximum of 128 channels could be used in each cell.

The mobile unit's transmit carrier frequency in MHz for any channel is calculated as follows:

$f_t = 0.03\ N + 825$ for $1 \leq N \leq 866$

$f_t = 0.03(N-1023) + 825$ for $990 \leq N \leq 1023$

where f_t= transmit carrier frequency (MHz)

N= channel number

The mobile unit's receive carrier frequency is obtained by simply adding 45 MHz to the transmit frequency i.e.,

$f_r = f_t + 45$ MHz

The base station's transmit frequency for any channel is simply the mobile unit's receive frequency, and the base station's receive frequency is simply the mobile unit's transmit frequency.

For example, channel 3 has transmit frequency of

$f_t = (0.03 \times 3) + 825 = 825.90$MHz

And receiver frequency of

$f_r = 825.90 + 45 = 870.90$MHz

Frequency Division Multiple Access(FDMA):

Standard cellular telephone subscribers access the AMPS system using a technique called frequency-division multiple accessing (FDMA). Multiple access is a situation in which two or more users wish to simultaneously communicate with each other using the same propagation channel.With FDMA, transmissions are separated in the frequency domain-each channel is allocated a carrier frequency and channel bandwidth within the total system frequency spectrum. Subscribers are assigned a pair of voice channels (forward and reverse) for the duration of their call. Once assigned a voice channel, a subscriber is the only mobile unit using that channel within a given cell. Simultaneous transmissions from multiple subscribers can occur at the same time without interfering with one another because their transmissions are on different channels and occupy different frequency bands.

AMPS Identification Codes:

The AMPS system uses several identification codes for each mobile unit. The mobile identification number (MIN) is a 34-bit binary code, which is the programmed handset phone number used to call

the subscriber. This programmed identifier is associated with the subscriber and is stored in erasable non-volatile memory in the handset. The second identifier is the electronic serial number (ESN), which is a manufactured characteristic of the mobile unit. This identifier is permanent and associated with the physical equipment. It is 32 bits in length, with the first 8 bits identifying the manufacturer. The third identification code is four bit station class mark (SCM), which specifies the maximum radiated power for the unit. The system identifier (SID) is a 15-bit binary code issued by the FCC to an operating company when it issues a license to provide AMPS cellular service to an area. Local operating companies assign a two-bit digital color code (DCC) and a supervisory audio tone (SAT) to each of their base stations to help the mobile units distinguish one base station from a neighbouring base station.

AMPS Control Channels:

Control channels are used in cellular telephone systems to enable mobile units to communicate with the cellular network through base stations and are used for call origination, call termination, and to obtain system information. With AMPS system, voice channels are analog FM, while control channels are digital and employ FSK. Base stations broadcast on the forward control channel (FCC) and listen on the reverse control channel (RCC). All AMPS base stations continuously transmit FSK data on the FCC so that idle cellular telephones can maintain a lock on the strongest FCC regardless of their location. A subscriber's unit must be locked on an FCC before it can originate or receive calls.

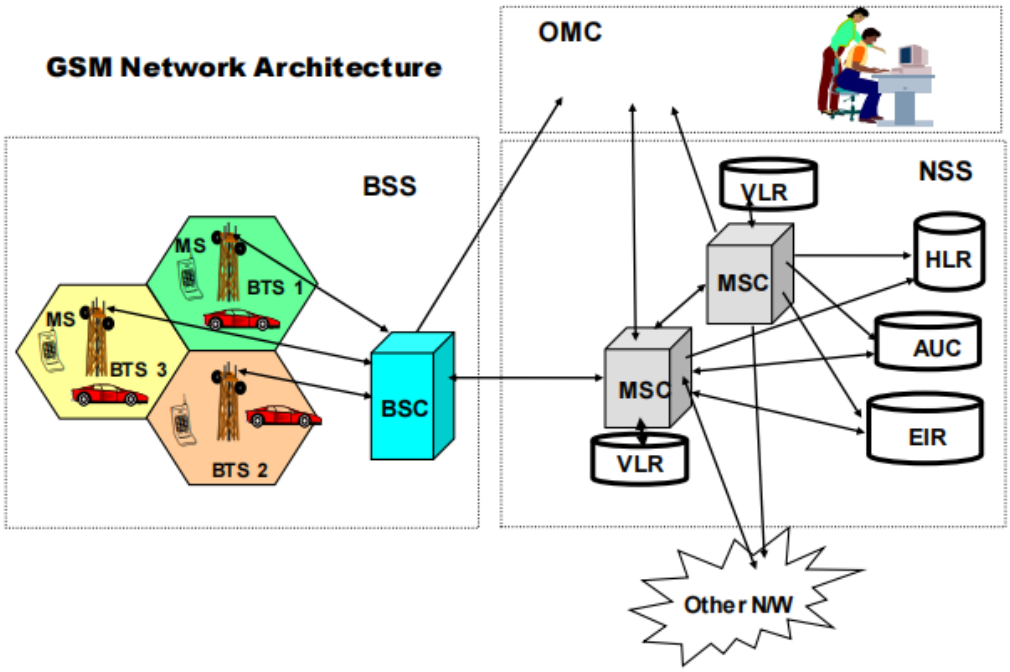
Global System for Mobile Communication(GSM)

GSM or Global System for Mobile Communications is the most popular wireless cellular communication technique, used for public communication. The GSM standard was developed for setting protocols for second generation (2G) digital cellular networks.

In the Europe and Asia, the GSM operates in 900 to 1800 MHz frequency range, whereas in United States and other American countries, it operates in the 850 to 1900 MHz frequency range. It uses the digital air interface wherein the analog signals are converted to digital signals before transmission. The transmission speed is 270 Kbps.

It was first implemented in Finland in December 1991. By the mid-2010s, it became a global standard for mobile communications achieving over 90% market share, and operating in over 193 countries and territories.

The GSM architecture consists of three major interconnected subsystems that interact with themselves and with users through certain network interface. The subsystems are Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operational Support Subsystem (OSS). Mobile Station (MS) is also a subsystem but it is considered as a part of BSS.



Interfaces:

Um Interface: The air interface between the mobile station (MS) and the BTS.

Abis Interface: Connects the BTS and the BSC, allowing for communication and control between these components.

A Interface: Connects the BSC to the Mobile Switching Center (MSC), facilitating communication between the BSS and the core network.

Network Switching Subsystem:

The NSS is responsible for performing call processing and subscriber related functions. The switching system includes the following functional units:

Home location register (HLR):
It is a database used for storage and management of subscriptions. HLR stores permanent data about subscribers, including a subscribers service profile, location information and activity status. When an individual buys a subscription from the service provider, he or she is registered in the HLR of that operator.

Visitor location register (VLR):
It is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. VLR is always integrated with the MSC. When a MS 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 needs to make a call, VLR will be having all the information needed for call setup.

Authentication center (AUC): A unit called the AUC provides authentication and encryption parameters that verify the users identity and ensure the confidentiality of each call.

Equipment Identify Register (EIR):
EIR is a database that stores the IMEI numbers for all registered mobile equipment(ME) units.The IMEI (International Mobile Equipment Identity) is a unique 17 or 15 digit code used to identify an individual mobile station to a GSM network. The IMEI number provides an important function; it uniquely identifies a specific mobile phone being used on a mobile network. The IMEI is a useful tool to prevent a stolen handset from accessing a network and being used to place calls. Mobile phone owners who have their phones stolen can contact their mobile network provider and ask them disable a phone using its IMEI number. The EIR uniquely identifies all the registered MEs.
There are three classes of ME that are stored in the database and each group has different characteristics.
• White List: contains those IMEIs that are known to have been assigned to valid MS's. This is the category of genuine equipment.
• Black List: contains IMEIs of mobiles that have been reported stolen.
• Gray List: contains IMEIs of mobiles that have problems (for example, faulty software and wrong make of the equipment).

Mobile Switching Center(MSC):
A Mobile Switching Center (MSC) is a core part of the GSM/CDMA network system. It acts as a control center of a Network Switching Subsystem (NSS). The MSC connects calls between subscribers by switching the digital voice packets between network paths.The MSC is

stationed between the base station and the Public Switched Telephone Network (PTSN). All mobile communications are routed from the base station through the MSC. The MSC is responsible for handling voice calls and SMS including other services like FAX. The MSC initiates call setup between subscribers and is also responsible for real time prepaid billing and account monitoring. The MSC is responsible for inter BSC handovers between Base Station Controllers and inter MSC handover between mobile switching centers.

Base Station Subsystem(BSS):
The GSM Base Station Subsystem (BSS) is a crucial component of the GSM architecture. It is responsible for communication between mobile devices and the network.BSS manages voice and data traffic between the mobile devices and the network.It handles signaling for call setup, maintenance, and termination.It locates and alerts mobile devices for incoming calls or messages.It ensures that all components of the network are synchronized for efficient communication.

The BSS consists of two main parts:BTS(Base Transceive Station) and BSC(Base Station Controller)

Base Transceiver Station (BTS):
The BTS is the equipment that handles the radio communication with mobile devices. A BTS is a network component that serves one cell and is controlled by a BSC. BTS is typically able to handle three to five radio carries, carrying between 24 to 40 simultaneous communications. Reducing the BTS volume is important to keeping down the cost of the cell sites. The primary responsibility of the BTS is to transmit and receive radio signals from a mobile unit over the air interface. To perform this function effectively, the signals are encoded, encrypted, multiplexed, modulated, and then fed to the antenna system at the cell site. In order to keep the mobile station synchronized, BTS broadcasts frequency and time synchronization signals. Similarly, the received signal from the mobile is decoded, decrypted, and equalized for channel impairments. Uplink radio channel(reverse channel) measurement is made by the BTS and corresponding downlink measurements(forward channel) made by MS.

Base Station Controller (BSC):
The BSC is connected to the MSC on one side and to the BTS on the other. The BSC performs the Radio Resource (RR) management for the cells under its control. It assigns and release frequencies and time slots for all MSs in its own area through the BTSs. The BSC performs the inter cell handover for MSs moving among the BTSs in its control. The

BSC controls the power transmission of both BTSs and MSs in its area. The BSC provides the time and frequency synchronization reference signals which is further broadcast by its BTSs. The BSC also measures the time delay of received MS signals relative to the BTS clock. If the received MS signal is not centered in its assigned time slot at the BTS, The BSC can direct the BTS to notify the MS to advance the timing such that proper synchronization takes place.

MOBILE STATION(MS):
The wireless mobile telephone used by the subscriber is called the MS (Mobile Station). MS includes radio equipment and the man machine interface that a user needs, in order to access the services provided by the GSM MS can be installed in vehicles or can be portable or hand-held. The MS may include provisions for data communication as well as voice.

The primary functions of MS are to transmit and receive voice and data over the air interface of the GSM system. MS performs the signal processing function of digitizing, encoding, error protecting, encrypting, and modulating the transmitted signals. It also performs the inverse functions on the received signals from the BS.

The MS continuously monitors the power level and signal quality received on the forward channel, by reading strength of the signals received from its current BTS and the six surrounding BTSs. The MS sends this information to the BTS & BSC to facilitate the network to take decision on handover

Subscriber Identity Module (SIM) Card
The SIM is a removable smart card bearing a unique identification number. At the very beginning of the service, GSM subscribers are provided with a SIM card. The subscriber is identified in the system when the user inserts the SIM card in the mobile equipment. This provides an enormous amount of flexibility to the subscribers since they can now use the SIM in the mobile equipments, as the SIM card is portable between Mobile Equipment (ME) units. The user only needs to
take his smart card on a trip. He can then rent a ME unit at the destination, even in another country, and insert his own SIM. Any calls he makes will be charged to his home GSM account. Also, the GSM system will be able to reach him at the ME unit he is currently using. The SIM contains an integrated circuit chip with a microprocessor, random access memory (RAM), and read only memory (ROM).

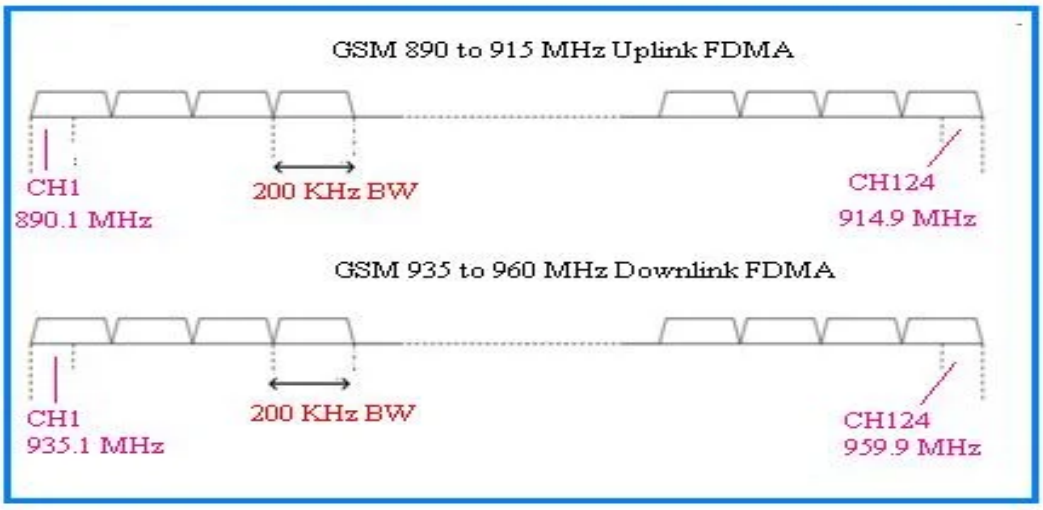
Operation Maintenance Center (OMC):

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 operation and support system (OSS).
OMC is used to monitor and maintain the performance of each Mobile Station (MS), Base Station (BS), Base Station Controller (BSC) and Mobile Switching Center (MSC) within a GSM system. The OMC has three main functions which are:
1)To maintain all telecommunications hardware and network operations with a particular market.
2)Manage all charging and billing procedures.
3)Manage all mobile equipment in the system.
The OMC is dedicated to each of these tasks and has provisions for adjusting all base station parameters and billing procedures, as well as for providing system operators with the ability to determine the performance and integrity of each piece of subscriber equipment in the system.

Global System for Mobile Communications (GSM) uses a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA).

Frequency Division Multiple Access (FDMA):

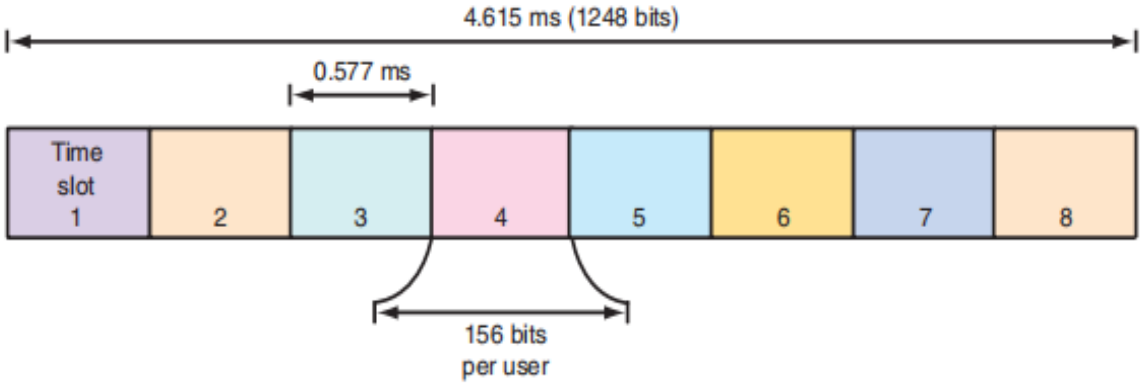
In GSM, large frequency band (25 MHz) is divided into smaller frequency bands (200 KHz) known as channels. Moreover separate frequency bands are allocated for uplink (890 to 915 MHz) and downlink (935 to 960 MHz) as shown in the figure below



Total of 124 channels are available with each having 200KHz bandwidth in each direction (uplink and downlink). For communication between users and Base station, one dedicated frequency is used for uplink and one for downlink. Hence simultaneous transmissions are possible in GSM. This process is known as FDMA (Frequency Division Multiple Access).

Time Division Multiple Access: It involves allotting same frequency channel to different subscribers by dividing the frequency band into multiple time slots. Each user gets his/her own time slot allowing multiple stations to share same transmission space.

For GSM, each sub divided channel is divided into different time slots using TDMA technique. Each TDMA frame lasts for 4.164 milliseconds (ms) and contains 8 time slots. Hence eight users can communicate with single frequency channel.Each time slot or a physical channel within this frame lasts for 577 microseconds and data is transmitted in the time slot in form of bursts as shown in fig below



Services provided by GSM:
GSM offers three basic types of services:
1. Telephony services or teleservices
2. Data services or bearer services
3. Supplementary services

Data services or bearer services:
A variety of data services are offered by GSM.
1) GSM users can send and receive data at rate upto 9600bps
2) Provides access to users on Plain Old telephone System(POTS), ISDN, Packet Switched Public Data Networks and Circuit Switched Networks using variety of access methods and protocols such as x.25 and x.35
3) As GSM is a digital network, a modem is not required between the users and GSM network but a modem is required inside the GSM network to interwork with POTS.

4) GSM supports FAX services.
5) Bidirectional SMS service, the messages are transported in a store and forward fashion.SMS can be sent on point to point and cell broadcast mode(traffic and news updates)

Telephony services or teleservices:
The most basic teleservice supported by GSM is telephony. As with all other comunications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency service provider is notified by dialing three digits 911. GSM teleservice also provides video text and tele text transmission

Supplementary Services:
Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include

1. Call hold
2. Call waiting
3. Call forwarding

4. Call barring: Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.

5. Calling Line Identification: This service displays the telephone number of the calling party on the screen.

6. Connected Line Identification: This service is provided to give the calling party the telephone number of the person to whom they are connected. This may seem strange since the person making the call should know the number they dialled, but there are situations (such as forwardings) where the number connected is not the number dialed.

7. Multiparty communications:The multiparty service allows a mobile subscriber to establish a multiparty conversation that is, a simultaneous conversation between three or more subscribers to setup a conference call.

8. Closed user group: This service is provided on GSM to enable groups of subscribers to only call each other. This type of services are being offered with special discount and is limited only to those members who wish to talk to each other.

9. Advice of Charge: This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those Service Providers who wish to offer rental services to subscribers without their own Subscriber Identity Module (SIM) can also utilize this service in a slightly different form.These data calls is provided on the basis of time measurements.
10.Operator determined call barring: Restriction of certain features from individual subscribers by operator.

Code Division Multiple Access(CDMA)

CDMA (Code Division Multiple Access) and WCDMA (Wideband Code Division Multiple Access) are two widely used wireless transmission facilities in the mobile telecommunications industry. CDMA is a digital cellular technology that uses a spread spectrum in enabling many people access one and the same channel all at once. Every user is assigned a code and the signals from all the users are sent in a manner that the signals having same code at the receiving end is distinguished and separated. WCDMA extends from CDMA and is a 3G technology that provides a faster data connection and capacity as compared to CDMA.

CDMA stands for Code Division Multiple Access and serves as a wireless standard applied in the telecommunication industry. It enables several people to work on a single channel by assigning every channel a code. In contrast to FDMA and TDMA, CDMA doesn't divide the accessible frequencies into a number of channels or time slots respectively, but all users can send signals at once on the same frequency. CDMA uses spread spectrum, lower level modulation of signals, due to this data signal occupies more bandwidth than necessary for transmission. CDMA technology was used in most of the wireless communication systems including the 2G. (eg:-IS-95), 3G (eg:- cdma2000).

Two commonly used techniques for spreading the spectrum are frequency hopping and direct sequencing. Both of these techniques are characteristic of transmissions over a bandwidth much wider than that normally used in narrowband FDMA/TDMA cellular telephone systems, such as AMPS and GSM

Frequency hopping(FH):

Frequency-hopping spread spectrum was first used by the military to ensure reliable antijam and to secure communications in a battlefield environment. The fundamental concept of frequency hopping is to break a message into fixed-size blocks of data with each block transmitted in

sequence except on a different carrier frequency. With frequency hopping, a pseudorandom code is used to generate a unique frequency-hopping sequence. The sequence in which the frequencies are selected must be known by both the transmitter and the receiver prior to the beginning of the transmission. The transmitter sends one block on a radio-frequency carrier and then switches (hops) to the next frequency in the sequence and so on. After reception of a block of data on one frequency, the receiver switches to the next frequency in the sequence. Each transmitter in the system has a different hopping sequence to prevent one subscriber from interfering with transmissions from other subscribers using the same radio channel frequency.

Direct sequence spread spectrum(DSSS):

In direct-sequence systems, a high bit rate pseudorandom code is added to a low-bit-rate information signal to generate a high bit rate pseudorandom signal closely resembling noise that contains both the original data signal and the pseudo random code. Again, before successful transmission, the pseudo random code must be known to both the transmitter and the intended receiver. When a receiver detects a direct-sequence transmission, it simply subtracts the pseudo random signal from the composite receive signal to extract the information data. In CDMA cellular telephone systems, the total radio-frequency bandwidth is divided into a few broadband radio channels that have a much higher bandwidth than the digitized voice signal. The digitized voice signal is added to the generated high-bit-rate signal and transmitted in such a way that it occupies the entire broadband radio channel. Adding a high-bit-rate pseudorandom signal to the voice information makes the signal more dominant and less susceptible to interference, allowing lower- power transmission and, hence, a lower number of transmitters and less expensive receivers

PN Codes Used in CDMA:

• CDMA system uses three types of PN code.

1. Walsh code
2. Long PN code
3. Short PN code

Walsh code: Walsh codes are set of orthogonal codes which are made up of +1 or-1 which allows multiple users share the same frequency channel without causing interference.The length of Walsh code is typically a power of 2 corresponding to the number of users that can be accommodated. In CDMA systems, Walsh codes are used for spreading

the signals of different users in which each user is assigned a unique Walsh code .The users data signal is multiplied by this code spreading the signal over a wide bandwidth.The spreading signal is then transmitted over the channel. Since the codes are orthogonal, receivers can distinguish between different users. At the receiver end, the received signal is multiplied by the same Walsh code that was used for spreading.This operation is called despreading.These codes are simple to generate and implement in hardware or software. In IS-95 CDMA, 64 Walsh codes are used per base station. This enables to create 64 separate channels per base stations (i.e. a base station can handle maximum 64 unique users at a given time).Actually in IS-95, out of the 64 available Walsh codes, Walsh code 0 is reserved for pilot channel, 1 to 7 are assigned for synch channel and paging channels and the remaining 8-63 are assigned for users (traffic channel) in the downlink(forward channel).

Long PN Code:
Long codes run at 1.2288 Mb/s and are 2^{42}-1 bits long (created using a 42 bits Linear Feedback Shift Register). It takes approx 41.2 days to repeat a long code at this rate. It is used for both encryption and spreading. Encryption is achieved by using a mask called Long Code mask which is a created using a 64-bit authentication key called A-key (assigned by CAVE protocol) and Electronic Serial Number (ESN – assigned each user based on the mobile number). The Long code changes each time a new connection is created

Short PN Code:
The Short code is PN sequence that is 2^{15}-1 bits in length.This code is used for final spreading of the signal and is transmitted as a reference known as the Pilot Carrier by the base station. The same short code is used by all the base stations.Base stations are differentiated from one another by offsetting their transmission of this code in time.This time offset is called as a PN Offset.Mobile units initially search until they synchronize with a pilot code transmitted by a base station.The base station then conveys timing information to the mobile.

CDMA Channel and Frequency Allocations`

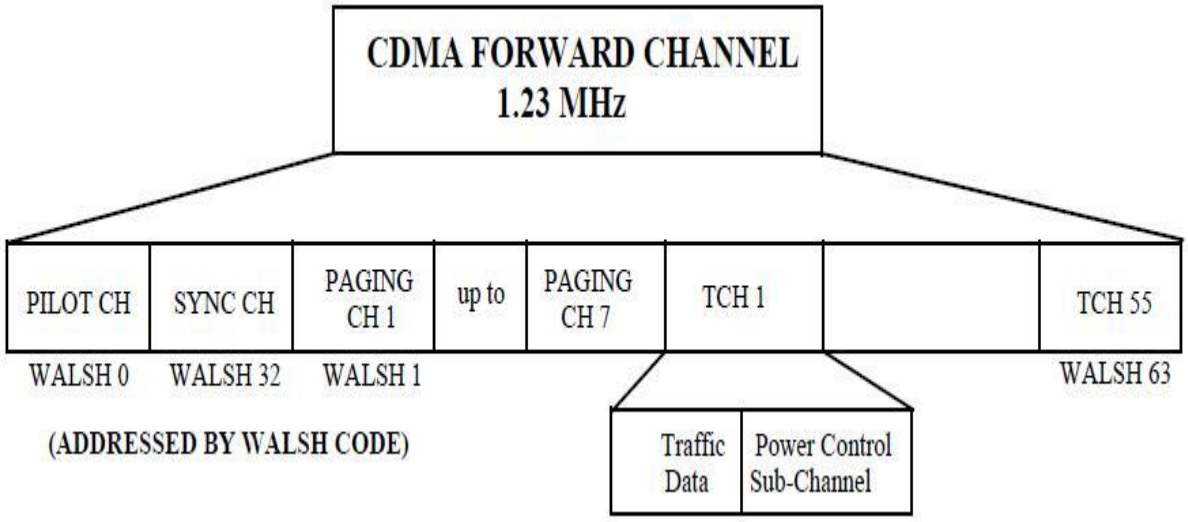
Forward CDMA Channel

CDMA forward channel uses same frequency spectrum as AMPS i.e. 869-894 MHz. Each IS-95 channel is allocated a 1.25-MHz frequency spectrum for each one-way CDMA communications channel. A single

CDMA radio channel takes up the same bandwidth as approximately 42 30-kHz AMPS voice channels.Each CDMA channel is 1.23 MHz wide with a 1.25 MHz frequency separation between adjacent carriers, producing a 200-kHz guard band between CDMA channels

The following PN Codes are used in forward CDMA channel
1) Walsh codes for differentiating users
2) Long PN Codes for identifying Base Stations
3) Short PN Codes for data scrambling

Forward CDMA channel is divided into 64 code channels using 64 Walsh codes as the chip sequence. The forward code channels are grouped into paging(1...7), Forward traffic (1...55), Pilot (1) and Sync(1) channel. Any unused forward channel is used as traffic channels.



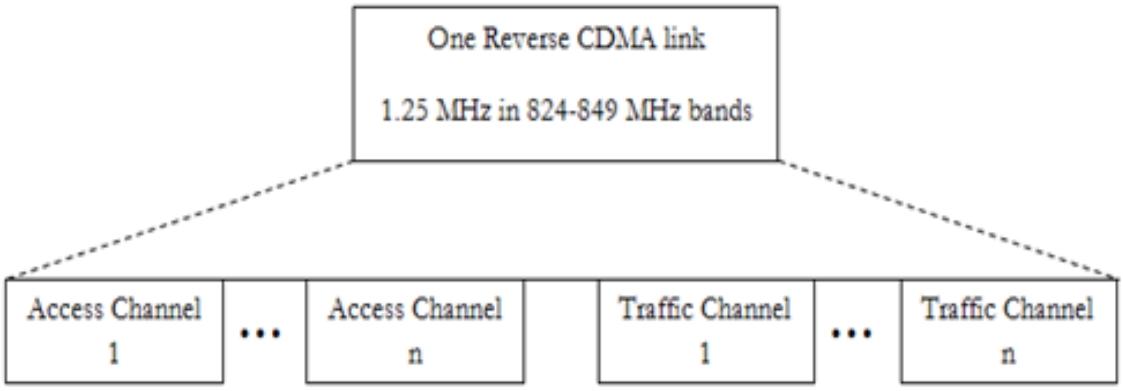
Pilot Channel − It is a reference channel which the mobile sta tion uses for synchronization with the base station's timing and and spreading code phase.It helps the mobile align its receiver with correct PN code phase . It is transmitted at all times by each base station on each active CDMA frequency. Each mobile station tracks this signal continuously and uses the pilot signal to monitor and adjust the power needed in order to transmit back to the base station. CDMA system relies heavily on power control.The users which are closer to the base station must transmit at lower power, those at far away must use a higher power. This has to be decided by some kind of a control channel and pilot channel is used to do that.

Synchronization(Sync) Channel- The BTS constantly transmits over the sync channel so that the mobile can synchronize with the base station. Synchronization is of most importance, it provides the mobile with the system time and the identification number of the cell site so it's primarily used for time synchronization. The mobile ignores the sync channel after it is synchronized.

Paging Channel(PCH)- The primary purpose is to send out pages, that is, notifications of incoming calls, to the mobile stations. The base station uses them to transmit system overhead information and mobile station-specific messages. CDMA uses up to 7 paging channels. The paging channel transmits overhead information such as commands and pages to the mobile. The paging channel also sends commands and traffic channel assignment during call setup. It may also be used to inform a mobile, which is already involved in a call to get ready to switch to a traffic channel owned by neighbouring cell,whose coverage area this mobile has entered. Such handoff direction messages are always conveyed using the paging channel. These channels are also used to initiate outgoing calls.

Traffic Channels(TCH)-These channels are used to pass incoming voice traffic from the base station to the mobiles. CDMA uses between 55 and 61 forward traffic channels to send both voice and overhead control data during a call. Additionally commands to the mobile about whether to increase or decrease its transmitted power are embedded within the voice traffic and are retrieved and executed by the mobile.Power control measures are sent by base station every 1.25ms.If the received signal is low, 0 is sent over power control sub channel instructing the mobile station to increase its mean output power level. If mobile's power level is high, 1 is sent to indicate that the mobile station should decrease the power level. A minimum of 55 Forward Traffic Channels are generally supported by a cell or sector.

Reverse CDMA Channel:
The Reverse CDMA channel is the mobile-to-cell direction of communication or the uplink path. The reverse link uses two types of channels to transmit voice and control data to the base station. The types of reverse link channels are Access channel and Traffic channel.



IS-95 Reverse Channel

The following PN Codes are used in reverse CDMA channel
1) Walsh codes for modulation(spreading)
2) Long PN Codes for identifying Mobile Stations
3) Short PN Codes for signal robustness

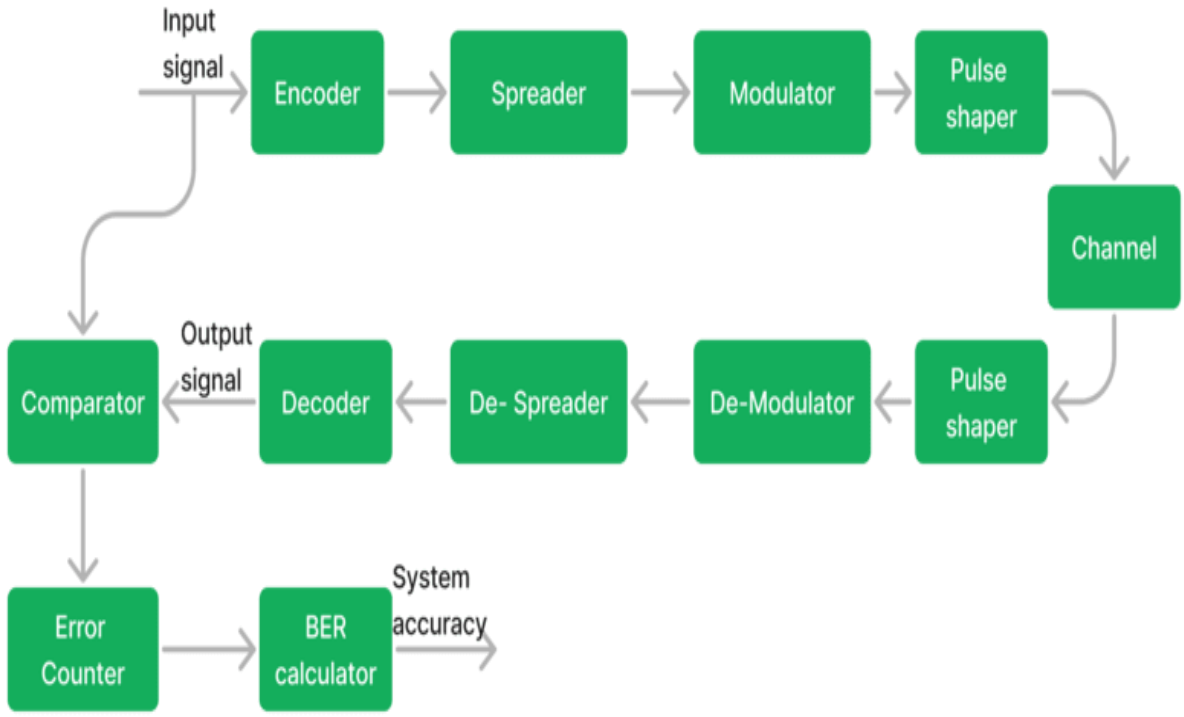
Access Channel
The mobile uses the access channel when not assigned to a traffic channel. The mobile uses the access channels to originate calls, to determine what paging channels it should monitor, respond to pages and to re register with a new network or system when the mobile has roamed outside its parent network

Traffic Channel:
The reverse link traffic channel is used only when there is a call. The reverse traffic channel transmits voice data to the BTS, it also transmits the overhead control information during the call.The mobile goes to access mode if there is a call initiated; go to the traffic mode and then go back to the idle mode once the voice communication is over. The maximum data rate per channel is 14.4 kbps.

Wideband Code Division Multiple Access(WCDMA)

Wideband Code Division Multiple Access (WCDMA) is a type of cellular technology that was developed as a third-generation (3G) mobile communications standard. It is based on the Code Division Multiple Access (CDMA) technologies that were developed in the 1980s, but it uses a wider frequency band and provides higher data rates than previous versions of CDMA.WCDMA was developed by the Third Generation

Partnership Project (3GPP), a collaboration between several telecommunications standards organizations. The first version of the WCDMA standard was released in 1998, and it was later adopted by many mobile network operators around the world as a way to provide high-speed data services to their customers.
The block diagram of WCDMA is shown in fig below:



Input signal: The input signal consists of various forms of digital data, including voice, text, and video.

Encoder/ Decoder: For encoding and decoding purposes WCDMA uses same techniques as that are used in CDMA i.e., Convolution or Turbo encoding and decoding techniques.

Spreader/ Despreader: WCDMA uses spreading techniques such as OVSF (Orthogonal variable spreading factor) codes and scrambling codes and the Despreader works the same as that in CDMA
.
Modulator/ Demodulator: Advanced modulation techniques used in WCDMA are QPSK, 16- QAM(Quadrature Amplitude Modulation), 64-QAM and demodulation techniques used are enhanced rake receiver.

Pulse Shaper: At transmitter, it uses root-raised cosine filter to determine signal bandwidth and to minimize their ISI(Inter Symbol Interference), ensures the signal is undistorted during transmission. At receiver it uses same filter to reduce ISI.

Comparator: The comparator synchronizes the received and decoded signal with the transmitted signal leads to identifying errors and assessing the transmitter's accuracy.

Error Counter: It Increments the counter for each error identified by the comparator by providing a measure for signal transmission quality and accuracy.

Bit Error Rate (BER): The BER is calculated as

BER = Number of erroneous bits received / Total number of bits transmitted

It is used to measure the effectiveness of the communication system and helps to maintain low error rates for higher data integrity.

Advantages of WCDMA

1) Higher data rates and capacity due to wider bandwidth channels and advanced modulation techniques.
2) Spectral efficiency and network performance is enhanced for better utilization of resources.
3) Support for multimedia applications such as video streaming and online gaming with improved quality.
4) Seamless handover between cells for uninterrupted connectivity during mobility.
5) Global standard for 3G networks which ensures interoperability and roaming across different regions.

Disadvantages of WCDMA

1) Higher deployment and maintenance costs compared to older technologies.
2) Limited compatibility with devices designed for other cellular technologies.
3) Spectral efficiency still may lag behind newer technologies like LTE or 5G.
4) Vulnerable to interference that impacts the performance in crowded spectrum environments.

5) Data speeds may not match those of technologies that are optimized for high-speed data.

Applications of WCDMA

1) Used in Mobile telephony for providing voice and data services with faster speeds and better quality.
2) It Supports video streaming, online gaming, and mobile internet browsing.
3) Used in IoT devices for wide coverage and remote monitoring.
4) Essential for public safety and emergency services which ensures reliable communication during crises.
5) Facilitating machine to machine connections for various purposes such as asset tracking and telemetry.

Wireless LAN

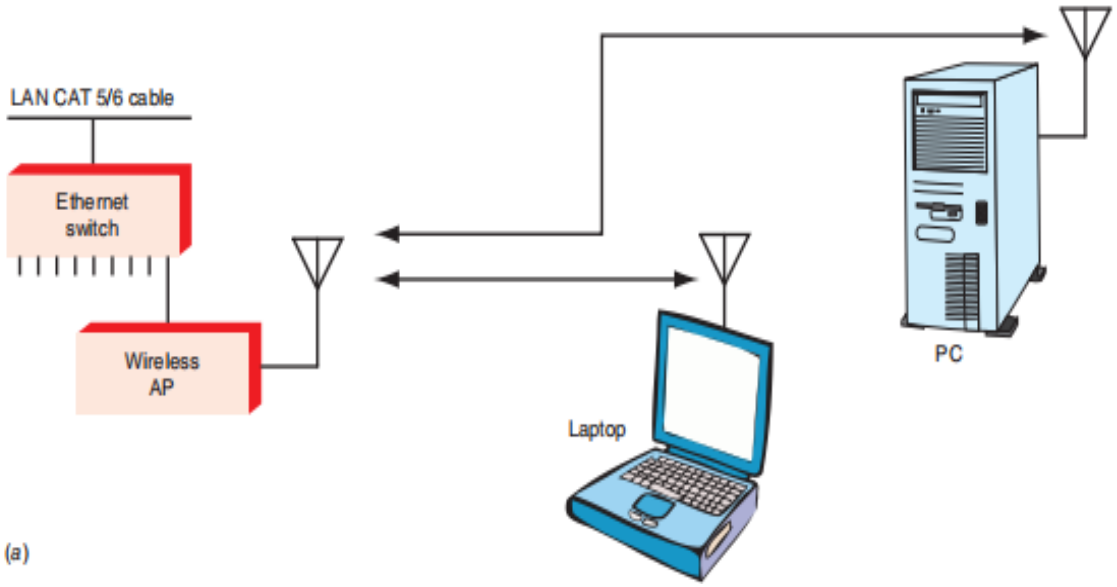
Wireless LANs are more commonly referred to by their trade name Wi-Fi. The terms Wi-Fi, WLAN, and 802.11 are used interchangeability in this text. Local-area networks (LANs) within a company, government agency, hospital, or other organization typically use CAT5 or CAT6 unshielded twisted pair as the transport medium. However, more and more, wireless extensions to these LANs are becoming popular as are entirely wireless LANs. Low-cost wireless modems installed in personal computers and laptops make this possible.

What makes the wireless LAN so appealing is that it offers flexibility, convenience and lower costs. To add a node to an existing wired LAN, the main problem is the new wiring. If such wiring is not in place already, it is time-consuming and expensive to pull cables through walls and ceilings and to install connectors. Moving computers within a building because of office reconfiguration is a huge problem and expense unless existing wiring can be reused. By using a wireless extension such problems essentially disappear. Any computer can be located at any new point quickly and easily at no additional cost. As long as the computer is within the range of the AP, the connection is automatic. Wireless is a great way to expand an existing network.

Wireless LANs also serve our continuing need to be more mobile in our jobs and activities. The cell phone has given us freedom to maintain

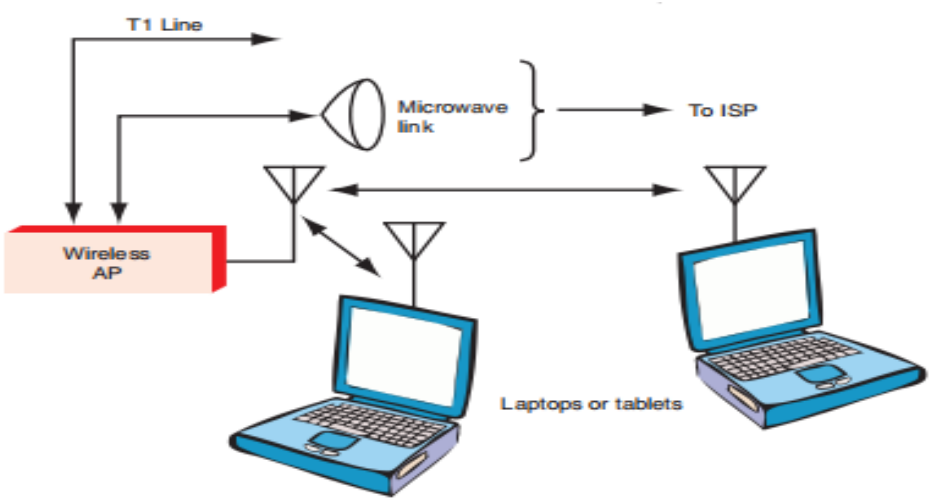
communications anywhere, at any time, and virtually in any place. The wireless LAN also gives us that same portability for our computers, mainly laptops. Within an organization, a user can take her or his laptop to the conference room for a meeting, to a colleague's office, or to the cafeteria for lunch. And with all the available hot spots, we can use our laptops almost anywhere, especially while we are traveling.

Three common configurations are shown in fig below. Fig.(a) shows a wireless access point (AP) is connected to an existing wired LAN, usually through an Ethernet switch.



The Ethernet Device connects multiple wired devices using LAN cables (CAT 5/6). It acts as a central hub for the wired network.The Wireless Access Point(AP) converts the wired network signal to a wireless signal so wireless devices (like laptops) can connect.It is connected to the Ethernet switch via LAN cable.The Ethernet switch and AP together allow integration of wired and wireless parts of the network.This setup is common in offices, schools, and homes to provide flexible network access.The wireless devices connects to the wireless AP using Wi-Fi.They can communicate with other devices in the network (both wired and wireless) through the AP.

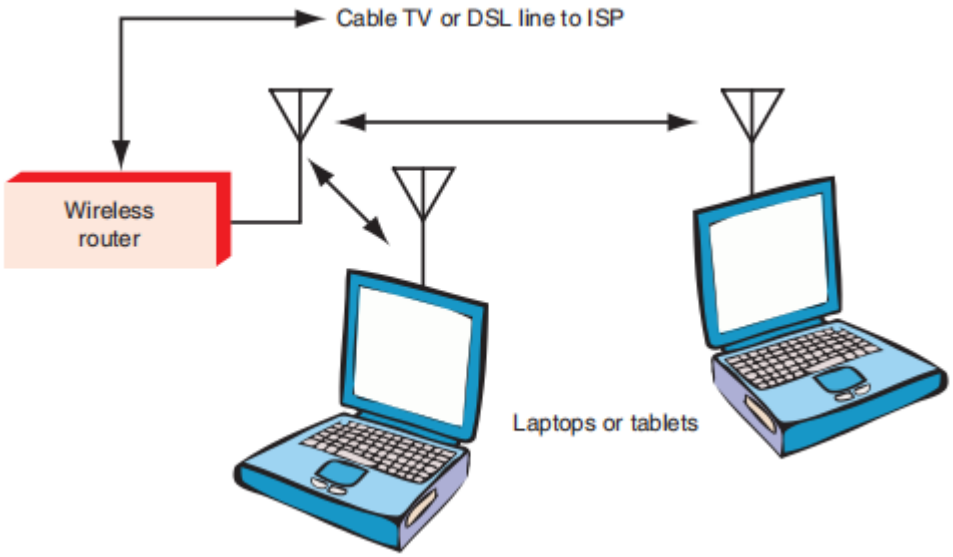
Another popular configuration is shown in Fig.(b) below.



(b)

Here the AP is connected to the main LAN or more commonly to an Internet service provider (ISP) by way of a long-range interconnection such as a hardwired T1 or T3 line, fiber connection, or a microwave relay link. A T1 line is a high-speed digital communication line that is used to carry data, voice, or internet traffic between networks — often used by businesses or network providers.A microwave link is a high-frequency wireless communication system that transmits data using microwave signals (radio waves in the range of 1 GHz – 40 GHz).It is often used when laying cables is difficult or expensive, such as between distant buildings or across rough terrain.

Another growing use of wireless LANs is in the implementation of home Networks shown in fig© below.



As more and more families become users of multiple PCs, tablets, and smart phones, there is a need to interconnect each device to a broadband Internet connection such as a DSL or cable TV line. It allows each user to

access e-mail or the Internet or to share a common peripheral such as a printer. Most homeowners do not want to wire their homes with CAT5/6 cable at great expense. Installing a wireless LAN is fast, easy, and very inexpensive these days. A special box called a residential gateway or wireless router connects to the cable TV or DSL and serves as the access point. This gateway or router uses a software approach called network address translation (NAT) to make it appear as if each networked PC has its own Internet address, when in reality only the one associated with the incoming broadband line is used.

Hardware of Wireless LAN's:

The hardware devices in a wireless LAN are the access point or the gateway/router and the radio modems in the PCs. The access point is just a box containing a transceiver that interfaces to an existing LAN by way of CAT5/6 wiring. It typically gets its dc operating power via the twisted-pair cabling, because the dc supply voltage is superimposed on the data. The AP is usually mounted high on a wall or ceiling to give good coverage to a specific area. The antenna may be built into the box or may be a separate array that gives directionality to the AP to ensure coverage of a desired area and minimum interference to other nearby WLANs. In a home network, the gateway or router is designed to attach to the DSL or cable TV modem with CAT5/6 cable. It often attaches to one of the PCs in the home network by cable. The other PCs link to the gateway/router wirelessly.

The radio modems for each PC take many forms. All are transceivers with an accompanying antenna. The transceivers are usually a single chip in most of the newer systems. In the older systems, the modem is contained on a plug-in card for the PC. Today, it is more common to have the radio modem built into the PC motherboard. For laptops and tablets, the modem is built in, so no special installation is needed.

Wireless LAN Standards

Over the years, a number of wireless LAN methods have been developed, tested, and abandoned. One standard has emerged as the most flexible, affordable, and reliable. Known as the IEEE 802.11 standard, it is available in multiple forms for different needs.
The different versions of IEEE 802.11 standard is
1) IEEE 802.11a
2) IEEE 802.11b
3) IEEE 802.11g

4) IEEE 802.11n
5) IEEE 802.11ac
6) IEEE 802.11ad

IEEE 802.11b:
The earliest useful and most widely adopted version of the 802.11 standard is 802.11b. It operates in 14 channels in the 2.4-GHz unlicensed ISM band spaced 5MHz apart. This band extends from 2.4 to 2.4835 GHz for a total bandwidth of 83.5 MHz. However, each channel is 22 MHz wide so that the channels overlap. Any given AP uses one of these channels.The center frequencies of each channel are given below:

Channel No	**Center Frequency,GHz**
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

The access method is direct sequence spread spectrum (DSSS) so that multiple signals may share the same band. Channel assignments are critical in facilities where multiple WLANs exist, so that interference is minimized.The 802.11b standard specifies a maximum data rate to 11 Mbps upto a maximum range of 100ft. This rate is achieved only under the most favorable path conditions such as minimum range and minimum noise. Increasing range or noise causes the rate to automatically drop off to 5.5, 2, or 1 Mbps. This helps ensure a reliable connection despite the lower speed. At the 1- and 2-Mbps rates, the serial data signal is XORed with an 11-bit code called the Barker code to produce the DSSS signal. This particular bit sequence has unique properties that make it easy to receive and decode. The Barker sequence is 10110011000. Each serial

data bit is XORed with this code. For modulation, 1 Mbps is achieved with DBPSK. For 2 Mbps, the modulation is DQPSK.

To achieve its faster rates of 5.5 and 11 Mbps, a different form of coding called complementary code keying (CCK) is used. The serial data signal is then modified by using one of 64 eight-bit codes to represent 6 bits of the serial data signal. The bit coded bits are the chips. The modulation is differential quadrature phase-shift keying (DQPSK). The use of CCK greatly improves the performance of the signal under noise and multipath conditions because the unique codes have properties that make them easier to identify and decode under adverse conditions.

As conditions degrade between AP and the wireless node due to increased distance, noise, or number of obstacles, the transceiver automatically readjusts to the changing conditions by adjusting the data rate downward, first to 5.5 Mbps also using DQPSK/CCK, then to 2 Mbps using DQPSK alone and then to 1 Mbps using DBPSK.

IEEE 802.11a:
The 802.11a standard was developed next. It uses the unlicensed 5-GHz band. There are three authorized segments: 5.15 to 5.25 GHz with 50-mW maximum power, 5.25 to 5.35 GHz with 250-mW maximum power, and 5.725 to 5.825 GHz at a maximum of 1 W of power. Each of these bands is divided into multiple nonoverlapping 20-MHz-wide channels. Each channel is designed to carry an OFDM signal made up of 52 subcarriers, 48 for data and the other 4 for error correction codes. Each of the subcarriers is about 300 kHz wide.

As with the 802.11b standard, the 802.11a version supports a wide range of data rates. The fastest is 54 Mbps upto a range of 50ft. Other backoff rates usually include 48, 36, 24, 18, 12, 9, and 6 Mbps. Each uses a different modulation scheme. For 6 Mbps, BPSK is used. For 12 Mbps, QPSK is used. For the higher rates, QAM is used; 16-QAM gives 24 Mbps, while 64-QAM is used to achieve 54 Mbps. The standard provides for backoff data rates as the link conditions deteriorate due to increased range, noise, or multipath interference.

The key advantage of the 802.11a standard is that the frequency band is much less used than the busy 2.4-GHz band, which contains microwave ovens, cordless phones, Bluetooth wireless, and a number of other services, all of which can cause interference at one time or another, thereby producing interference that can block communications or

at least decrease the range and data rate. With fewer interfering signals in the 5-GHz band, there is less interference and greater reliability.

The downside of this standard is its shorter range. As frequency of operation increases, the given transmission range typically decreases. Indoor operation greatly reduces range because 5-GHz signals are more easily absorbed and reflected than 2.4-GHz signals. With 802.11a, the maximum range is about 50 ft at the maximum data rate.

IEEE 802.11g:

The 802.11g standard was an attempt to extend the data rate within the popular 2.4-GHz band. Using OFDM, this standard provides for a maximum data rate of 54 Mbps at 100 ft indoors. As with the 802.11a standard, there are lower backoff rates of 48, 36, 24,18,12,11,9,6,5.5,2 and 1Mbps as the communications path degrades. The 802.11g standard also accommodates the 802.11b standards and so is fully backward-compatible. An 802.11b transceiver can talk to an 802.11g AP but at the lower data rate. An 802.11g transceiver can also talk to an 802.11b AP but also at the lower data rate.

Data Rate(Mbps)	**Transmission type**	**Modulation scheme**
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK
12	OFDM	QPSK
11	DSSS	CCK
9	OFDM	BPSK
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

IEEE 802.11n:
The 802.11n version was developed to further increase the data rate. It also uses both the 2.4-GHz and 5-GHz bands and OFDM. A primary feature of this standard is the use of multiple-input multiple-output (MIMO) antenna systems to improve reliability of the link. APs for 802.11n use two or more transmit antennas and three or more receive antennas. The wireless nodes use a similar arrangement. In each case, multiple transceivers are required for the AP and the node. This arrangement permits a data rate in the 100- to 600-Mbps range at a distance up to 100 ft. MIMO systems greatly mitigate multipath problems and help extend the range and reliability of the wireless link.

In all these standards, the carrier sense multiple access with collision avoidance (CSMA/CA) access method is used to minimize conflicts among those wireless nodes seeking access to the AP. Each transceiver listens before it transmits on a channel. If the channel is occupied, the transceiver waits a random period before attempting to transmit again. This process continues until the channel is free for transmission
.
11n Wi-Fi dominates the wireless LAN space today, as it is commonly available in all smart phones, tablets, and laptops. And it is the wireless technology of all hot spots and access points, including the millions of home wireless routers. It is increasingly embedded in consumer electronic equipment. It is also backward-compatible with previous standards, allowing 802.11a/g equipment to be used.

IEEE 802.11ac:

One of the newest versions of the standard is 802.11ac. 11ac uses the 5-GHz ISM band only, for minimum interference and maximum available bandwidth. Furthermore, it continues the use of MIMO and OFDM. However, some key changes boost the theoretical data rate above 3 Gbps depending on modulation, channel bandwidth, and MIMO configuration.

The primary changes are 80- and 160-MHz-wide channels in addition to the usual 40-MHz channel. As the bandwidth increases, so do the number of OFDM subcarriers, to a maximum of 512 at 160-MHz bandwidth. OFDM also adds 256QAM, which further boosts data rate. Finally, it defines a greater number of MIMO versions with a maximum of an 8x8 configuration. The standard also supports coexistence and compatibility with previous 11a and 11n devices.

IEEE 802.11ad:

Another version of Wi-Fi is 802.11ad. 11ad uses the 60-GHz ISM band. It is backward-compatible with all previous versions, including 11a/b/g/n/ac, as the media access control (MAC) layers of the protocol are similar. The 11ad version is also known by its trade name WiGig.

WiGi uses the unlicensed ISM 60-GHz band from 57 to 64 GHz. The technology divides this into four 2.16-GHz-wide bands. The primary modulation scheme is OFDM, which can support a data rate up to 7 Gbps, making it one of the fastest wireless technologies available. The standard also defines a single-carrier mode that uses less power; this is a better fit for some portable handheld devices. The single-carrier mode can deliver a data rate up to 4.6 Gbps. Both speeds permit transmission of uncompressed video.

The WiGig specification also provides security in the form of the Advanced Encryption Standard (AES).Because of the small antenna size at 60 GHz, gain antennas are normally used to boost signal power and range. The maximum typical range is 10 meters. WiGig products use on-chip phased array antennas that can provide beamforming.

PANs and Bluetooth

A personal area network (PAN) connects electronic devices within a user's immediate area. The size of a PAN ranges from a few centimeters to a few meters. One of the most common real-world examples of a PAN is the connection between a Bluetooth earpiece and a smartphone. PANs can also connect laptops, tablets, printers, keyboards, and other computerized devices.

PAN network connections can either be wired or wireless. Wired connection methods include USB and FireWire; wireless connection methods include Bluetooth (the most common), WiFi and Zigbee.

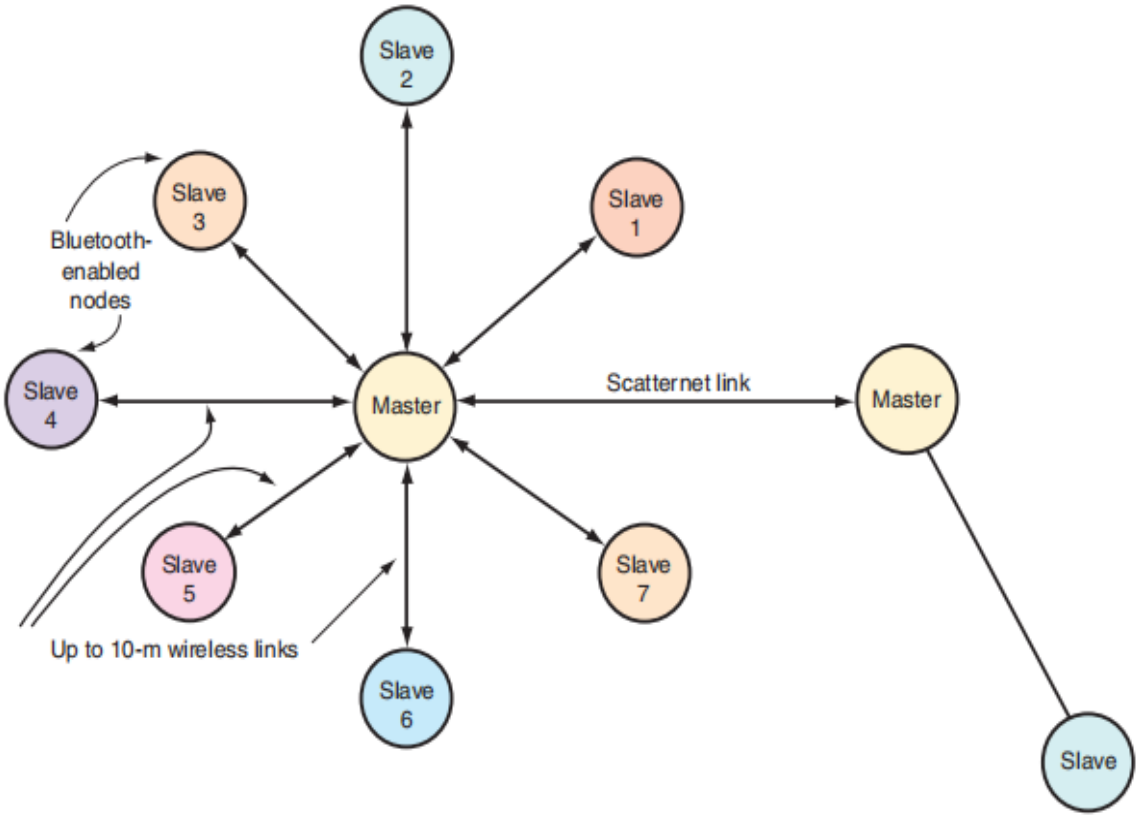
While devices within a PAN can exchange data with each other, PANs typically do not include a router and thus do not connect to the Internet directly. A device within a PAN, however, can be connected to a PC having internet connection that then connects the device to the Internet. For instance, a desktop computer, a wireless mouse, and wireless headphones can all be connected to each other, but only the computer can connect directly to the Internet.

A wireless personal area network (WPAN) is a group of devices connected without the use of wires or cables. Today, most PANs for everyday use are wireless. WPANs use close-range wireless connectivity protocols such as Bluetooth.The most popular wireless PAN system is Bluetooth, a standard developed by the cell phone company Ericsson for use as a cable replacement. The objective was to provide hands-free cell phone operation by eliminating the cable connecting a cell phone to a headset.

Bluetooth is a digital radio standard that uses frequency-hopping spread spectrum (FHSS) in the unlicensed 2.4-GHz ISM band. It hops over 79 frequencies spaced 1 MHz apart from 2.402 to 2.480 GHz. The hop rate is 1600 hops per second. The dwell time on each frequency, therefore, is 1/1600 = 625 μs. During this time, digital data is transmitted. The total data rate is 1 Mbps, but some of that is overhead (headers, error detection and correction, etc.)The data, which may be voice or any other digitized information, is put into packets and transmitted sequentially in as many as five time slots. The serial data signal is Gaussian-filtered, and then FSK is used for modulation. The frequency shift between binary 0 and 1 is ±160 kHz.

Three levels of transmission power have been defined, depending upon the application. For short distances up to 10 m, class 3 power at 0 dBm (1 mW) is used. For longer distances or more robust operation in an environment with obstacles and noise, the higher-power class 2 can be used with 4 dBm or 2.5 mW. Maximum Bluetooth range is about 100 m and is achieved with class 1 power of 20 dBm or 100 mW.

Bluetooth is set up so that the wireless transceiver constantly sends out a search signal and then listens for other nearby, similarly equipped Bluetooth devices. If another device comes into range, the two Bluetooth devices automatically interconnect and exchange data. These devices form what is called a piconet, the linking of one Bluetooth device that serves as a master controller to up to seven other Bluetooth slave devices. Once the PAN has been established, the nodes can exchange information with one another. Bluetooth devices can also link to other piconets to establish larger scatternets as shown in fig below



Another version 2.0 of Bluetooth is called Enhanced Data Rate (EDR). It has all the features described earlier but increases the overall data rate to 3 Mbps. The 3-Mbps rate includes all the headers and other overhead. The raw data rate is three times the 723 kbps rate mentioned earlier for a net rate of more than 2.1 Mbps. The new protocol still transmits at 1 Mbps using GFSK for accessing and recognizing inputs to establish a link and for the protocol headers. However, it uses different modulation method to achieve the higher data rate in the data payload.

A gross data rate of 2.1 Mbps is achieved by using a form of QPSK called DQPSK.To reach the 3-Mbps rate, an eight-phase differential phase-shift keying (8DPSK) modulation scheme is used.

The most recent version of Bluetooth is 4.0. It incorporates all the previous features of Bluetooth but adds Bluetooth Low Energy (BLE), a low-power variation of the original Bluetooth standard. Bluetooth BLE is also called Bluetooth Smart. Smart uses a different set of technical and radio techniques to ensure very low power consumption.Bluetooth Low Energy still operates in the same ISM (industrial-scientific-medical) license-free 2.4- to 2.483-GHz frequency band as standard Bluetooth. However, it uses a different frequency-hopping spread spectrum (FHSS) scheme. Standard Bluetooth hops at a rate of 1600 hops per second over

79 channels 1-MHz wide. BLE FHSS uses 40 channels 2-MHz wide to ensure greater reliability over longer distances. Standard Bluetooth offers gross data rates of 1, 2, or 3 Mbps. BLE's maximum rate is 1 Mbps with a net throughput of 260 Kbps. GFSK modulation is used

Other features of BLE are a power output of 0 dBm (1 mW) and a typical maximum range of 50 meters. Security is 128-bit AES. Link reliability is improved with the use of an adaptive frequency-hopping technique that avoids interference, a 24-bit CRC, and a 32-bit Message Integrity Check. A key point is that BLE is not compatible with standard Bluetooth, and it is a separate radio on standard Bluetooth 4.0 chips. If such interoperability is desirable, it could be implemented with a dual-mode device. This is an integrated circuit that contains both a standard Bluetooth radio and a BLE radio, where each can operate separately but not at the same time. They can share an antenna. It is also available as a separate device for low-power-only applications.

Apple, Google, Android, and Microsoft (Windows 8) provide software support for the Bluetooth standards. That expedites connectivity with devices such as smart phones, tablets and laptops.An interesting Bluetooth application is Apple's iBeacon wireless location service. It uses Bluetooth Low Energy (BLE) to implement beacons to send out a message that defines their location to nearby BLE smartphones.

A Bluetooth beacon is a small and wireless battery-powered radio transmitter that uses BLE as it
s transmission protocol. This mini-radio transmission device can be "discovered" and seen by all BLE scanners within a certain radius. The Bluetooth beacon, however, cannot "see" anyone back. Beacon technology doesn't require an internet connection and acts as a broadcaster within a short-range radius. The receiving device, such as a BLE enabled smartphone, often acts as an intermediary device that uses the information from the beacon to do something with it. The transmission distance is typically around 10-30 meters for interior spaces.The beacon pulses out a signal that is then received and acknowledged. The beacon then sends out a desired message to the phone. The most mentioned application is ads for retail stores and restaurants. In a mall or other shopping area, you would automatically receive sales notices or menu selections once you are in range of the store and if you have the appropriate iBeacon app.

The main applications for Bluetooth are cordless headsets for cell phones and hands-free voice systems in cars and trucks. It is also the main

connection between smartphones and the accessory smart watches. Bluetooth is also used in other wearables such as those for medical or fi tness monitoring. Other uses include wireless human interface devices (HIDs) such as keyboards, mice, and game controllers. Any wireless connection over a short distance that is within the data rate capability of Bluetooth is a potential application.The Bluetooth standard is maintained by the Bluetooth Special Interest Group (SIG) and supported by more than 2000 manufacturers. Bluetooth was also originally standardized by the IEEE as 802.15.1, but the standard is maintained by the Bluetooth SIG.

ZigBee and Mesh Wireless Networks

ZigBee is the commercial name for another PAN network technology based on the IEEE 802.15.4 wireless standard. Like Bluetooth, it is a short-range technology with networking capability. It was designed primarily for commercial, industrial, and home monitoring and control applications.The 802.15.4 standard defines the air interface, which is the physical layer (PHY or layer 1 of the OSI standard) and the media access control (MAC or layer 2) of the system. The ZigBee Alliance, an organization of chip, software, and equipment vendors of ZigBee products, specifies additional higher levels of layers including networking and security.ZigBee is designed to operate in the license-free spectrum available in the world.There are three basic bands and versions. Transmission is by packets with a maximum size of 128 bytes, 104 of which is data.As for range, it varies considerably with the application and the environment. Using 2.4 GHz, the typical maximum indoor range is about 30 m. Zigbee takes 3 Seconds to join a network

Frequency Band	Number of Channels	Modulation	Max. Data Rate, Kbps
868 MHz (Europe)	1	DSSS/BPSK	20
915 MHz	1	DSSS/BPSK	40
2.4 GHz	16	DSSS/O-QPSK	250

All Zigbee devices have two different addresses, a 64-bit and a 16-bit address.

64-bit device addresses

The 64-bit address is a device address which is unique to each physical device. It is sometimes also called the MAC address or extended address and is assigned during the manufacturing process. The first three bytes of the 64-bit address is a Organizationally Unique Identifier (OUI) assigned to the manufacturer by the IEEE.

16-bit device addresses
A device receives a 16-bit address when it joins a Zigbee network. For this reason, the 16-bit address is also called the network address. The 16-bit address of 0x0000 is reserved for the coordinator. All other devices receive a randomly generated address from the router or coordinator device that allows the join. The 16-bit address can change when an address conflict is detected where two devices are found to have the same 16-bit address or when a device leaves the network and later joins (it can receive a different address)

All Zigbee transmissions are sent using the source and destination 16-bit addresses. The routing tables on Zigbee devices also use 16-bit addresses to determine how to route data packets through the network. However, since the 16-bit address is not static, it is not a reliable way to identify a device.
To solve this problem, the 64-bit destination address is often included in data transmissions to guarantee data is delivered to the correct destination.

ZigBee network defines three different device types: coordinator, router, and end devices
ZigBee Coordinator(ZC):

Each ZigBee network must have one coordinator. A coordinator has the following characteristics:
1. It selects the channel and PAN ID (both 64-bit and 16-bit) to start the network.
2. It can allow routers and end devices to join the network.
3. It can assist in routing data.
4. It can not sleep. It has to be always awake.

ZigBeeRouter(ZR):

A router has the following characteristics:

1. It must join a ZigBee network before it can transmit, receive or route data.
2. After joining, it can allow routers and end devices to join the network.

3. After joining, it can route data.
4. It ca not sleep. It has to be always awake.

ZigBee End Device(ZED):

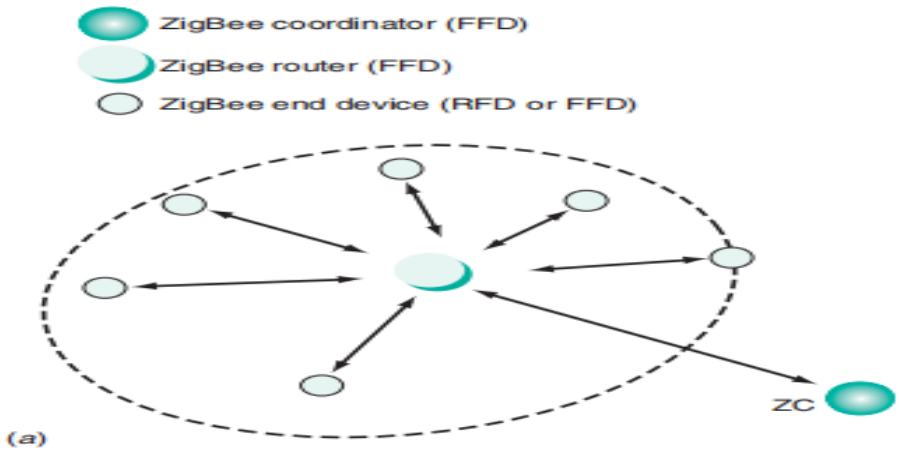
An End Device has the following characteristics:

1. It must join a ZigBee network before it can transmit or receive data.
2. It can not allow devices to join the network.
3. It must always transmit and receive RF data through its parent.
4. It cannot route data.
5. It can sleep.

In ZigBee networks, the coordinator must select a PAN ID (64-bit and 16-bit) and channel to start a network. After that, it behaves essentially like a router. The coordinator and routers can allow other router devices to join the network and route data.

After an end device joins , it must be able to transmit or receive RF data through that router or coordinator. The router or coordinator that allowed the end device to join becomes its parent. Since the end device can sleep, the parent must be able to buffer or retain incoming data packets destined for the end device until it is able to wake up and receive the data.

The ZigBee standard supports three topologies: star, mesh, and cluster tree. The most commonly used are the star and mesh, illustrated in Fig below



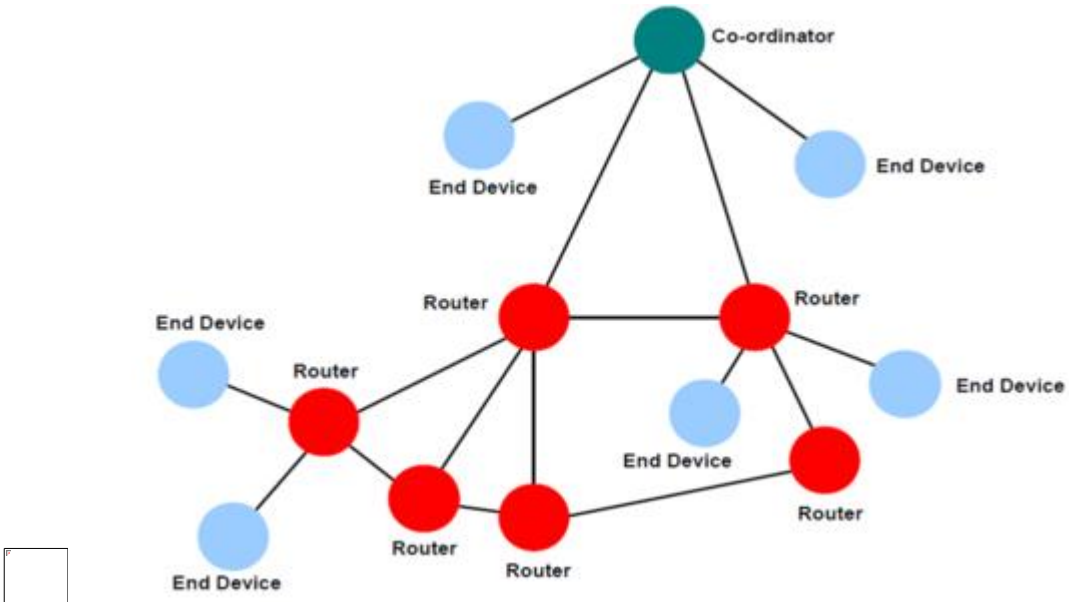


Fig: Most common ZigBee topologies (a) Star (b) Mesh

These network topologies are made up of three types of ZigBee nodes: a ZigBee coordinator (ZC), a ZigBee router (ZR), and ZigBee end device (ZED). The ZC initiates a network formation. There is only one ZC per network. The ZR serves as monitor or control device that observes a sensor or initiates off/on operations on some end device. It also serves as a router as it can receive data from other nodes and retransmit it to other nodes. The ZED is simply an end monitor or control device that only receives data or transmits it. It does not repeat or route. The ZC and ZR nodes are called full-function devices (FFDs), and the ZED is known as a reduced-function device (RFD). An FFD can perform all the tasks that are defined by the ZigBee standard, and it operates in the full set of the IEEE 802.15.4 MAC layer. An RFD performs only a limited number of tasks.

The star configuration in Fig.(a) is the most common, where a centrally located ZR accepts data from or distributes control data to other ZRs or ZEDs. The central ZR then communicates back to the ZC, which serves as the master controller for the system

In the **mesh topology**, most of the nodes are ZRs, which can serve as monitor and control points but also can repeat or route data to and from other nodes. The value of the mesh topology is that it can greatly extend the range of the network. If a node lacks the power or position to reach the desired node, it can transmit its data through adjacent nodes that pass along the data until the desired location is reached. While the maximum

range between nodes may be only 30 m or less, the range is multiplied by passing data from node to node over a much longer range and wider area.

An additional feature of the **mesh topology** is network reliability or robustness. If one node is disabled, data can still be routed through other nodes over alternate paths. With redundant paths back to the ZC, a ZigBee mesh ensures that data reaches its destination regardless of unfavorable conditions. Many critical applications require this level of reliability.

As for applications, ZigBee can address a wide range of wireless needs.

Home Automation

a. Security Systems
b. Meter Reading Systems
c. Light Control Systems
d. HVAC(Heating Ventilation and Air Conditioning) Systems

Consumer Electronics

a. Gaming Consoles
b. Wireless Mouse
c. Wireless Remote Controls

Industrial Automation

a) Asset Management
b) Personnel Tracking
c) Livestock Tracking

Healthcare

a) Hotel Room Access
b) Fire Extinguishers

WiMAX and Wireless Metropolitan-Area Networks

WMAN is a wireless metropolitan area network that can cover a whole city. It is larger than WLAN (wireless local area network) and smaller than WWAN (wireless wide area network). WMAN is managed by any private organization or government agencies. Wireless MAN is accessed by only authorized users. It can cover a distance of 30 miles(50km). WMAN can establish a network between different buildings or university campuses within the city.The wireless network established in WMAN is also known as IEEE 802.16

There are two types of wireless MAN:-

1. Back haul
2. Last mile

Back haul is an enterprise type of network which is cellular. It can use WI-FI hotspots as well. In back haul, we use fixed wireless that can save thousands of dollars per year. A DSL(Digital Subcriber Line) can be used for back haul but wireless connection is 10 times faster than normal fiber optics connection. For connecting two locations we use point to point wireless connection or private multi-point wireless connection.

Last mile connection is used to create a network for a temporary period. It is used to make a network in some construction buildings and is alternative to DSL broadband and cable modem. The last mile is a low cost and has quick installation.

WMAN Technologies:

1. WiMAX (Wireless Interoperable Metropolitan Area Exchange)
2. LMDS (Local Multipoint Distributed Service)

WiMAX (Worldwide Interoperability for Microwave Access)

The wireless contender for metropolitan-area networking known as WiMAX is the wireless system defined by the IEEE 802.16 standard. It was developed to provide a wireless alternative to consumers for broadband Internet connections.The primary standard is known as IEEE 802.16-2004 or 802.16d. Its primary applications will fit into two basic categories: point-to-point (P2P) or point-to-multipoint (PMP). The P2P mode is for applications requiring the transfer of data between two points. Common examples are cell site backhaul from a base station to the switching office or Wi-Fi hot spot interconnections to the ISP. Both of these applications typically rely on hardwired T1 or T3 connections, which are very expensive. A wireless backhaul link is far less expensive, easier to install.

The PMP mode is a broadcast mode from a central base station to multiple surrounding nodes. In this mode, WiMAX serves as a Wireless Internet Service Provider(WISP) for homes or businesses. In both modes, the service is assumed to be fixed; i.e., none of the nodes are mobile.

WiMAX was designed to operate anywhere in the 2- to 6-GHz range wherever appropriate spectrum is available. The spectrum may be

licensed or unlicensed depending upon its location and the host country. The most common bands are 2.3, 2.5, and 5.8 GHz in the United States and 3.5 GHz in Europe, Asia, and Canada.WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure.

The maximum data rate is 75 Mbps, but that is usually divided up among a large number of users. Speed is set by bandwidth, which can be anything from 1.75 to 20 MHz. The WISP will allocate bandwidth and speed to users based on their needs and charge accordingly. The maximum range of a single base station is about 30 mi(50 km form the Base Station), although in a practical system, one base station will usually only cover a range of 2 to 10 km (3.2 to 6 mi). Frequency-division duplexing (FDD) is supported by the standard.

WiMAX uses a 256-carrier OFDM system.. Reflections from buildings and other structures cause multipath problems that can stop a transmission. Trees and houses can absorb the signal, making reception poor or nonexistent. Yet OFDM helps to lessen these problems. The modulation method of each OFDM channel is selected automatically depending upon the range, noise, and data rate. The standard supports BPSK, QPSK, 16-QAM, 64-QAM, and 256-QAM. BPSK would be selected for longer range and lower speeds; 64-QAM or 256-QAM would be selected for shorter ranges to give higher speeds.

Infrared Wireless

Infrared radiation (IR), sometimes referred to simply as infrared, is a region of the electromagnetic radiation spectrum where wavelengths range from about 700 nanometers (nm) to 1 millimeter (mm).

Infrared waves are longer than visible light waves but shorter than radio waves. Correspondingly, the frequencies of IR are higher than microwave frequencies but lower than visible light frequencies, ranging from about 300 gigahertz to 400 terahertz (THz).Infrared light is invisible to the human eye, but heat sensors can detect longer infrared waves. Infrared shares some characteristics with visible light. Like visible light, infrared light can be focused, reflected and polarized.Infrared is commonly separated into near-, mid- and far-infrared.

Near-IR: The near-IR band contains the range of wavelengths closest to the red end of the visible light spectrum. Near-IR consists of wavelengths that range from 700 nanometers (nm) to 1,300 nm, or 0.7 microns to 1.3 microns. Its frequency ranges from about 215 THz to 400 THz. This group consists of the shortest wavelengths and longest frequencies, and it produces the least heat.

Mid-IR: The intermediate IR band, also called the mid-IR band, covers wavelengths that range from 1,300 nm to 3,000 nm, or 1.3 microns to 3 microns. Frequencies range from 20 THz to 215 THz.

Far-IR: Wavelengths in the far-IR band, which are closest to microwaves, extend from 3,000 nm to 1 mm, or 3 microns to 1,000 microns. Frequencies range from 0.3 THz to 20 THz. This group consists of the longest wavelengths and shortest frequencies, and it produces the most heat.

There are two communication modes in infrared viz. point to point communication and diffuse communication.
• In point to point communication, both transmitter and receiver infrared devices should be placed in line of sight of each other i.e., there should not be any obstacles (e.g. walls) in between them.
• In diffuse communication, transmitter and receiver need not be in straight line of sight.The transmitted IR signal reaches the receiver by reflecting or bouncing the transmitted signal from surfaces like wall, ceilings etc.

Infrared Data Association, or IrDA in short, is a group of device manufacturers that developed a standard for transmitting data via infrared (IR) light waves. It provides specifications for the complete set of protocols for wireless IR communication.Some of the protocols used by IrDA includeIrDA Data Object Exchange (IrDA-OBEX),
IrLAP (Link Access Protocol), IrLMP (Link Management Protocol)
TinyTP (Transport Protocol), NEC(National Electrical Code)

IR Communication Basics:

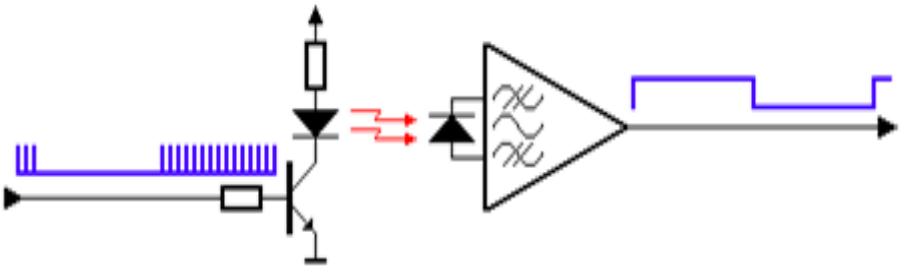


Fig: Circuits inside the remote control (RC)(Left Side Circuit) and the TV Receiver (Right Side Circuit)

IR Transmission:

The transmitter circuit inside the remote controller emits infrared light for every electric pulse given to it. The pulse is generated depending on the button pressed in remote , thus completing the circuit, providing bias to the LED.

One example of remote-control codes which is used for Sony TVs and includes the following 7-bit binary commands:

Button 1 = 000 0000

Button 2 = 000 0001

Button 3 = 000 0010

Button 4 = 000 0011

Channel Up = 001 0001

Channel Down = 001 0011

Power On = 001 0101

Power Off = 010 1111

Volume Up = 001 0010

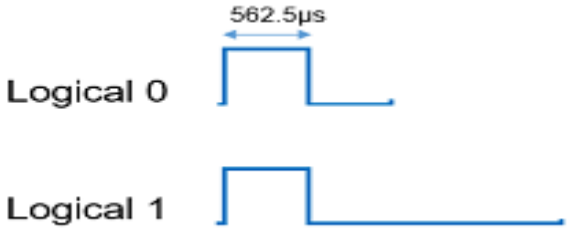
Volume Down = 001 0011

The LED on being biased emits light of the wavelength of 940nm as a series of pulses, corresponding to the button pressed. However since along with the IR LED many other sources of infrared light such as light bulbs, sun, etc, may emit the radiatons at the same time . Due to this,the

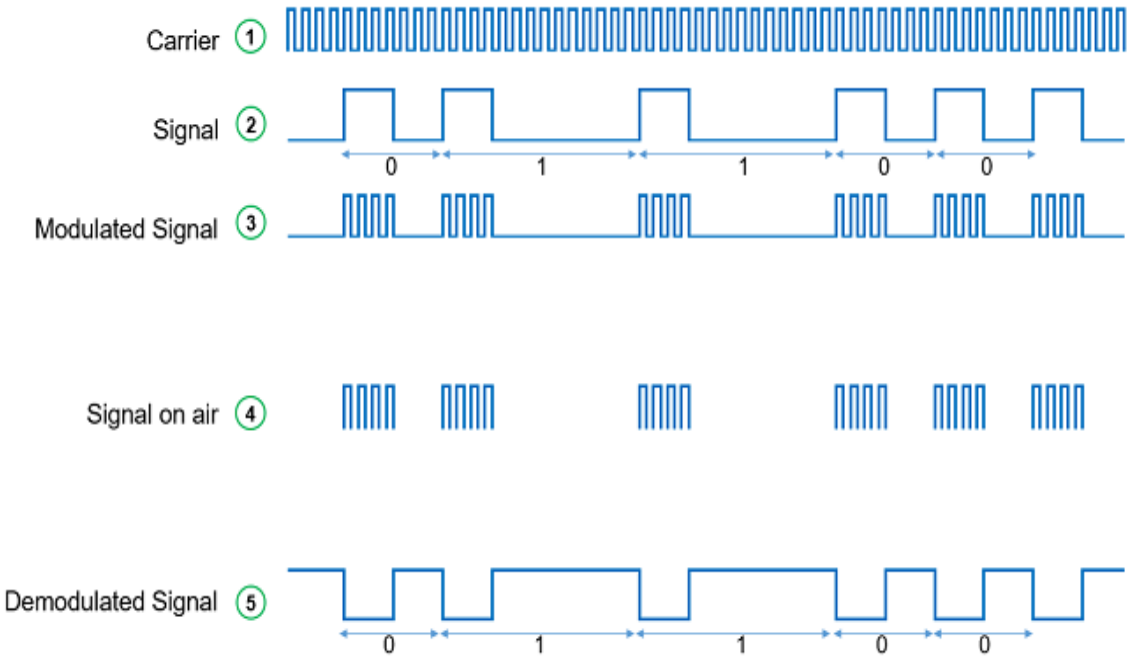
transmitted information can be interfered. A solution to this problem is modulation. The transmitted signal is modulated using a carrier frequency of 38 KHz (or any other frequency between 36 to 46 KHz). The IR LED is made to oscillate at this frequency for the time duration of the pulse. The information or the light signals are pulse modulated and are contained in the 38 KHz frequency.

The NEC Transmission protocol does this modulation which is shown if fig below:

1. Logic 1 is represented as a 562.5µs pulse burst followed by a 1.6875ms space, with a total transmit time of 2.25ms
2. Logic 0 is represented as a 562.5µs pulse burst followed by a 562.5µs space, with a total transmit time of 1.125ms



The below image shows 5 bit "01100" in sequence:



IR Reception:

The receiver consists of a photo detector which develops an output electrical signal as light is incident on it. The output of the detector is filtered using a narrow band filter that discards all the frequencies below

or above the carrier frequency (38 KHz in this case). The filtered output is then given to the suitable device like a Micro controller or a Microprocessor which compares the received bit pattern with the look up table stored in it.If it matches with one of the entries then it sends a signal to TV's main control circuitry which does the corresponding action.

The advantages of Infrared wireless technology are as follows:

1. It has low power consumption.
2. Infrared components are less expensive.
3. It is more secure than radio-frequency signals.
4. Direct line of sight requirement of Infrared enhances its security and minimizes interference, making it suitable for short-range, point-to-point communication.

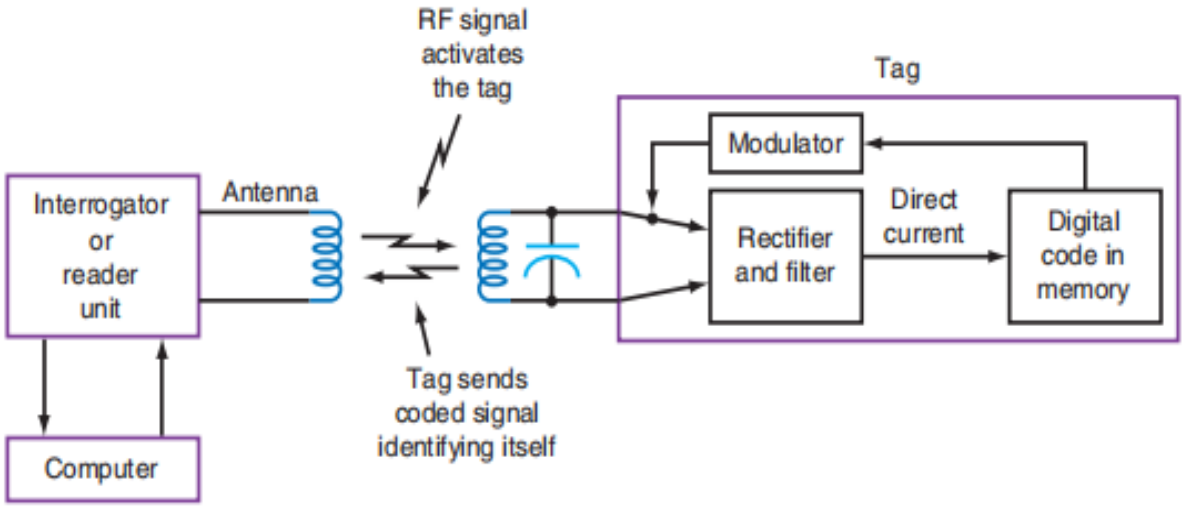
The disadvantages of Infrared wireless technology are as follows:

1. It has limited range of approx 5 meters and it cannot penetrate walls or other obstacles.
2. It works only in direct line of sight between the transmitter and receiver. Even the smallest obstruction will disrupt communication.
3. Infrared communication can take place only between two devices at a time limiting its use to control multiple devices.
4. It has relatively low data transfer speeds compared to technologies like Bluetooth or Wi-Fi.
5. Bright ambient light, including sunlight and strong artificial lighting, can interfere with infrared signals and degrade the quality of communication.

RFID Communication

Another growing wireless technique is radio-frequency identification (RFID).This technology uses thin, inexpensive tags or labels containing passive radio circuits that can be read by a remote wireless interrogation (tag reader) unit.The tags are attached to any item that is to be monitored, tracked, accessed, located, or otherwise identified. RFID tags are widely used in inventory control, container and parcel shipping, baggage handling . They are also widely used for automatic toll collection and parking access for vehicles. Other applications for RFID tags are personnel security checking and access, animal tracking, and theft prevention.

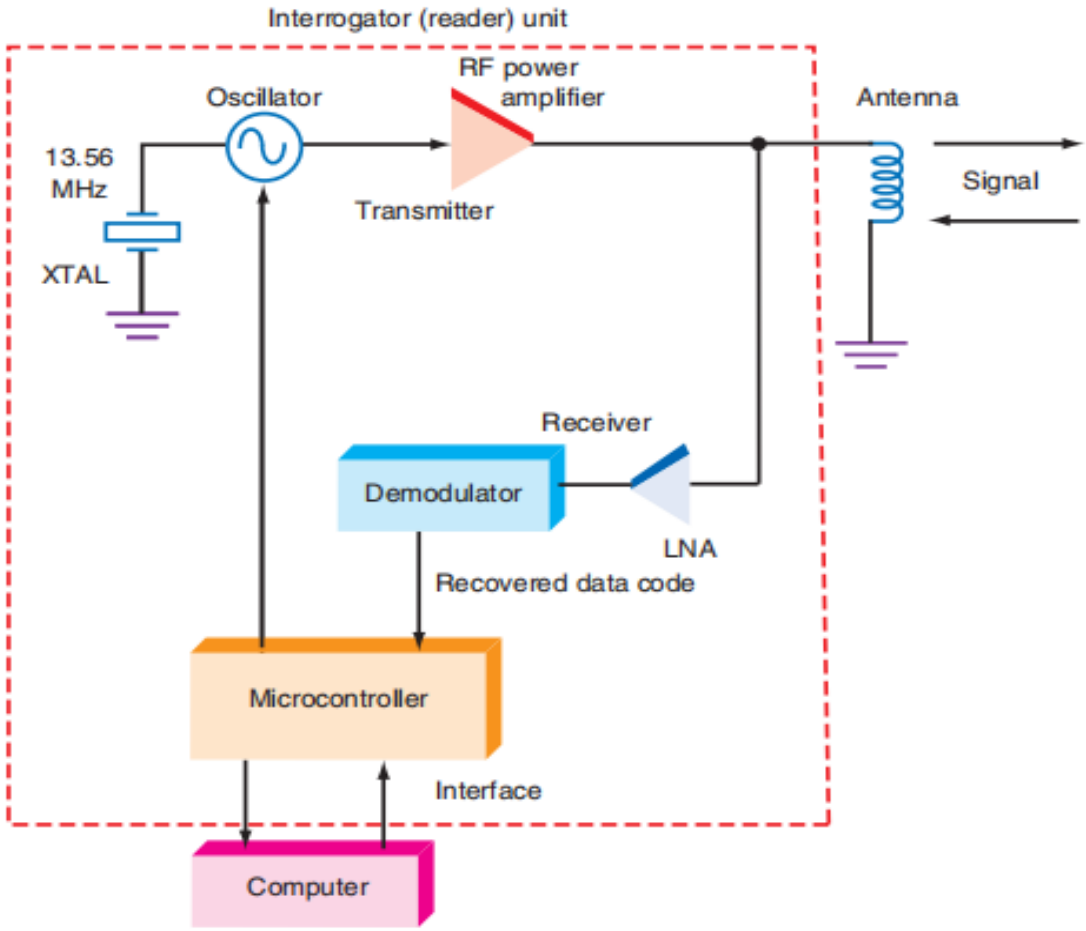
The basic concept of RFID is illustrated in fig below.



The tag is a very thin label like device into which is embedded a simple passive single-chip radio transceiver and antenna.The chip also contains a memory that stores a digital ID code unique to the tagged item. For the item to be identified, it must pass by the interrogation or reader unit, or the reader unit must physically go to a location near the item. Longer-range systems cover a complete building or area. The reader unit sends out a radio signal that may travel from a few inches up to no more than 100 ft or so. The radio signal is strong enough to activate the tag. The tag rectifies and filters the RF signal into direct current that operates the transceiver. This activates a low-power transmitter that sends a signal back to the interrogator unit along with its embedded ID code. The reader then checks its attached computer, where it notes the presence of the item and may perform other processing tasks associated with the application.

RFID systems operate over the full radio spectrum. Commercial systems have been built to operate from 50 kHz to 2.4 GHz. The most popular ranges are 125 kHz, 13.56 MHz, 902 to 928 MHz, and 2.45 GHz. The 125-kHz and 13.56-MHz units operate only over short distances up to several feet, whereas the 902- to 928-MHz and 2.45-GHz units can operate up to about 100 ft. Most of the tags are passive; i.e., they have no power source of their own. They rely upon the interrogator unit to supply a large enough RF signal to rectify for dc power. However, some active tags containing small flat batteries are available, and they can operate over a much larger range.

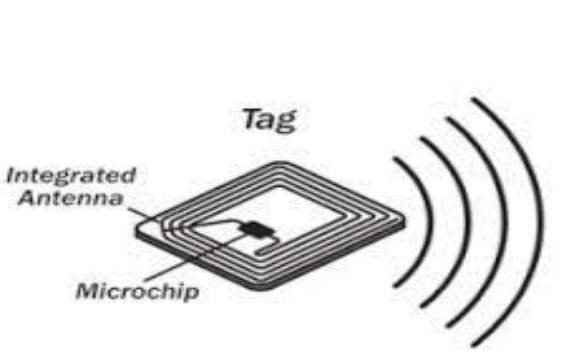
RFID Reader or Interrogator:
The block diagram of a typical 13.56-MHz RFID interrogator unit in shown in fig below:



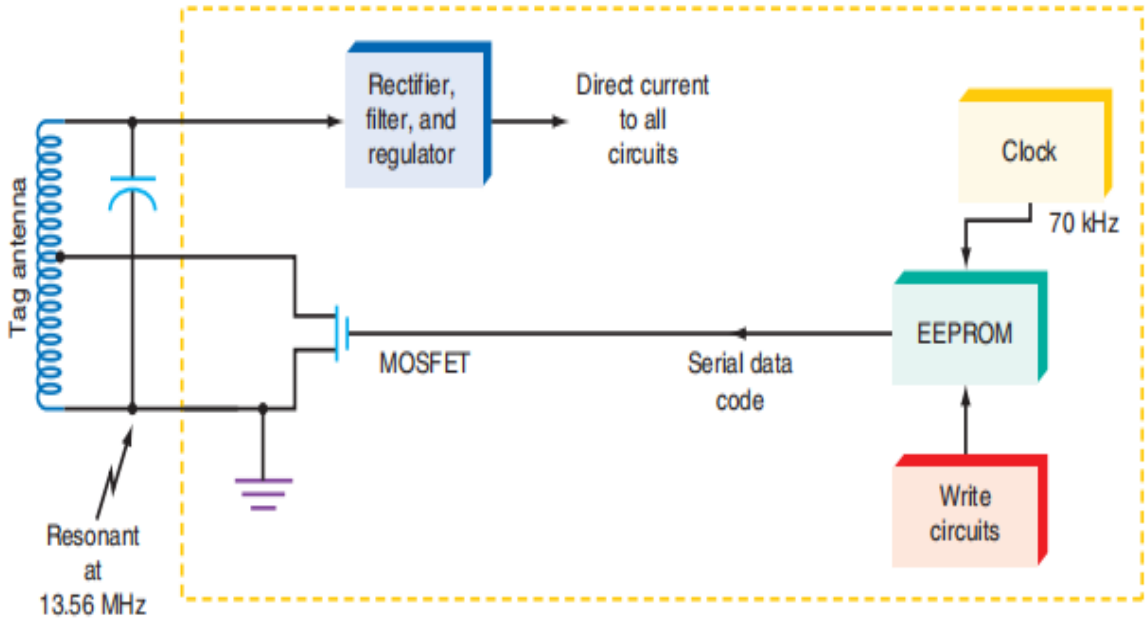
A 13.56-MHz crystal oscillator generates the basic RF signal, which is amplified and sent to the antenna. A microcontroller gates the oscillator on for a short time, and then the receiver waits for a response from the tag. The antenna picks up the weak tag signal. The receiver amplifies and demodulates it and then recovers the serial data code. The microcontroller communicates with the attached computer to do whatever processing is needed in the ID process.

RFID Tag:

The RFID Tag configuration is shown in fig below:



They consist of a flat spiral inductor and a capacitor that make up a 13.56-MHz tuned circuit that serves as the antenna. The transceiver chip is contained in the black dot on the tag.The block diagram of RFID Tag is shown in fig below:



The resonant circuit picks up the interrogator signal as if it were the induced signal in a transformer secondary rather than an actual received electromagnetic radio wave. When the voltage reaches about 4 Vp-p, the power circuits are activated. The RF is rectified in a voltage multiplier circuit, filtered, and regulated into the direct current that operates the remaining circuits.
The unique ID code is stored in an electrically erasable programmable read-only memory (EEPROM) in the tag chip. In this device, the code is 154 bits long.The tag chip contains the EEPROM write circuitry that writes the code into memory.

The ID code in EEPROM is read out serially in NRZ data format, which is then converted to a Manchester or biphase signal that is used to modulate the carrier sent by the reader. The modulation used is a form of amplitude modulation called backscatter modulation..The Manchester code is used so that the clock can be easily recovered from the data in the reader.A MOSFET switching transistor is connected to the tap inside the tag. The data to be transmitted is applied to this transistor. When the transistor is off, the carrier is passed to the tuned circuit and sent to the reader, which reads the signal as a binary 1. When the transistor is turned on, a portion of the coil is shorted, making the external tuned circuit resonant at a frequency of 3 to 6 MHz lower than its 13.56-MHz design

frequency. This signal is out of the frequency range of the reader, so it receives a much lower-level signal that is interpreted as a binary 0. During the time the transistor is on, the signal is said to be cloaking. With the transistor off, the signal is uncloaked. The cloaking and uncloaking process produces amplitude shift keying (ASK) at the reader receiver.

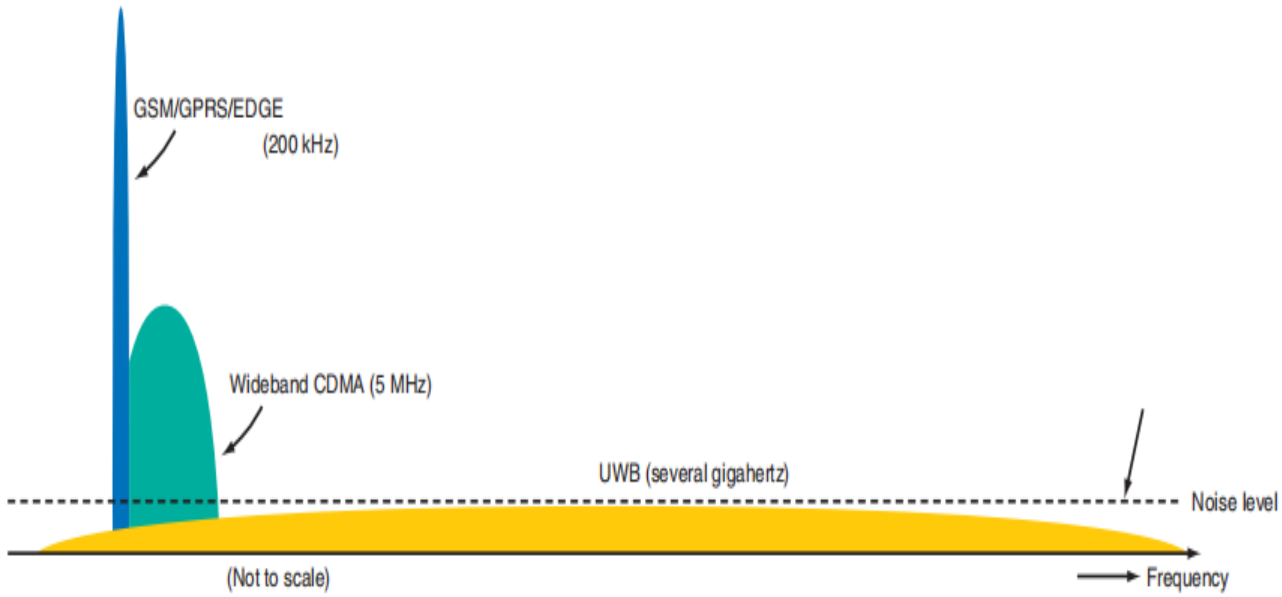
The most recent new RFID standard is called Gen 2 for second generation. It is a standard developed by more than 60 companies worldwide. The standard is under the auspices of EPC Global, the organization that also standardizes the Electronic Product Code (EPC) to be used on all tagged items. The Gen 2 standard operates in the 900-MHz region with different frequencies being used in different countries depending upon the local regulations. The 868-MHz frequency is common in Europe while 915 MHz is common in the United States.

UWB(Ultra Wide Band)

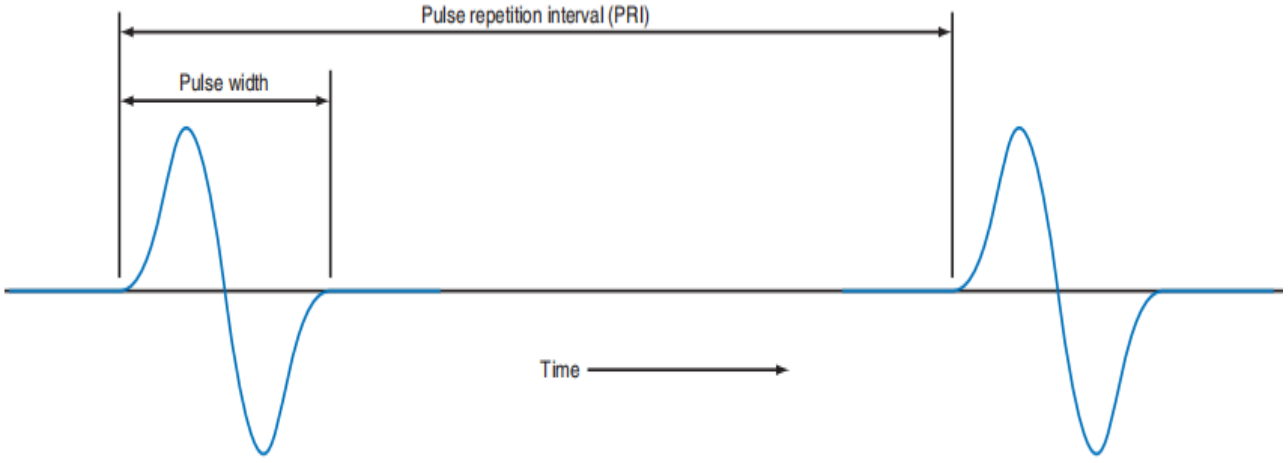
The newest and most unusual form of wireless is known as ultrawideband (UWB) wireless. There are two basic forms of UWB, the original version based on very narrow impulses and the newer kind based on OFDM. Both spread the signal over a very wide range of spectrum but at a very low signal level, so it does not interfere with other signals operating over those frequencies. Both methods are used, but the newer OFDM version appears to have captured the greatest number of manufacturing companies and the applications.

The original UWB discovered in the 1960s is known as impulse, baseband, or carrierless wireless. This form of UWB transmits data in the form of very short pulses, typically less than 1 ns. A UWB signal using very short pulses with a low duty cycle occupies a very wide bandwidth. A UWB signal is defined as having a bandwidth at least 25 percent of the center frequency, or 1.5 GHz minimum. Another definition specifies UWB as occupying more than 500 MHz of spectrum.

The following figure shows a UWB signal spectrum compared to a standard 30-kHz cell phone channel and a 5-MHz wideband CDMA (spread spectrum) cell phone channel.

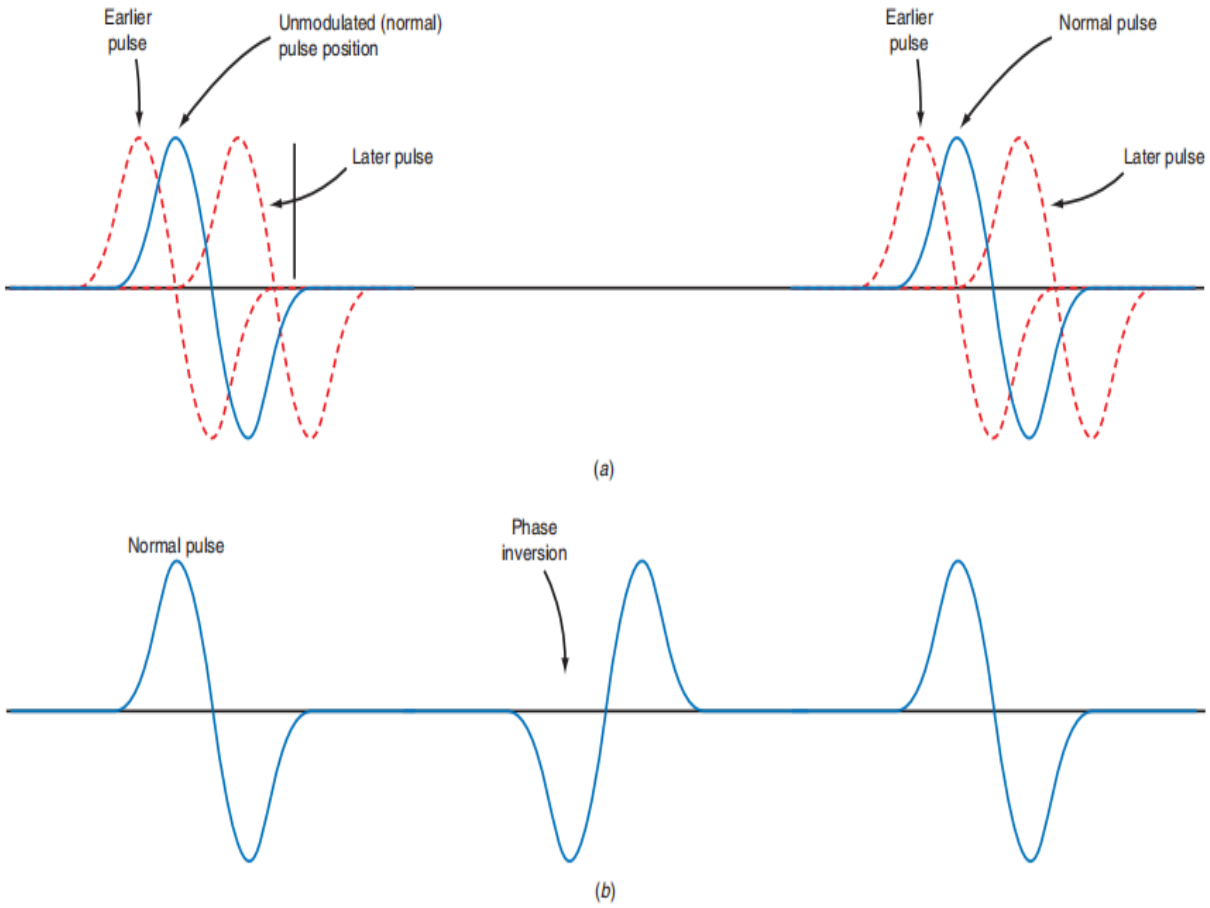


The FCC permits UWB in the 3.1- to 10.6-GHz range. The only other services in this region are satellites, radars, broadband wireless, and wireless networks. UWB equipment spreads its signals over much of that range, but the power level is so low that there is essentially no interference to other services. UWB is like spread spectrum in that many users can share a single wide bandwidth simultaneously.
A UWB signal starts as a very low duty cycle (≤1 percent) rectangular pulse stream at some pulse repetition interval (PRI). The pulses are then Gaussian-filtered and differentiated to produce the final pulses to be transmitted as shown in fig below. The pulses are applied directly to the antenna.The center frequency is approximately the reciprocal of the pulse width.



The serial data to be transmitted is then encoded with a unique pseudorandom code like that used in CDMA. This method effectively "channelizes" the system so that multiple users can share the spectrum but still be individually identified. The coded signal then modulates

the pulse train by either PPM (fig (a))or BPSK (fig (b)). Both methods are illustrated in fig(a) and (b) below:

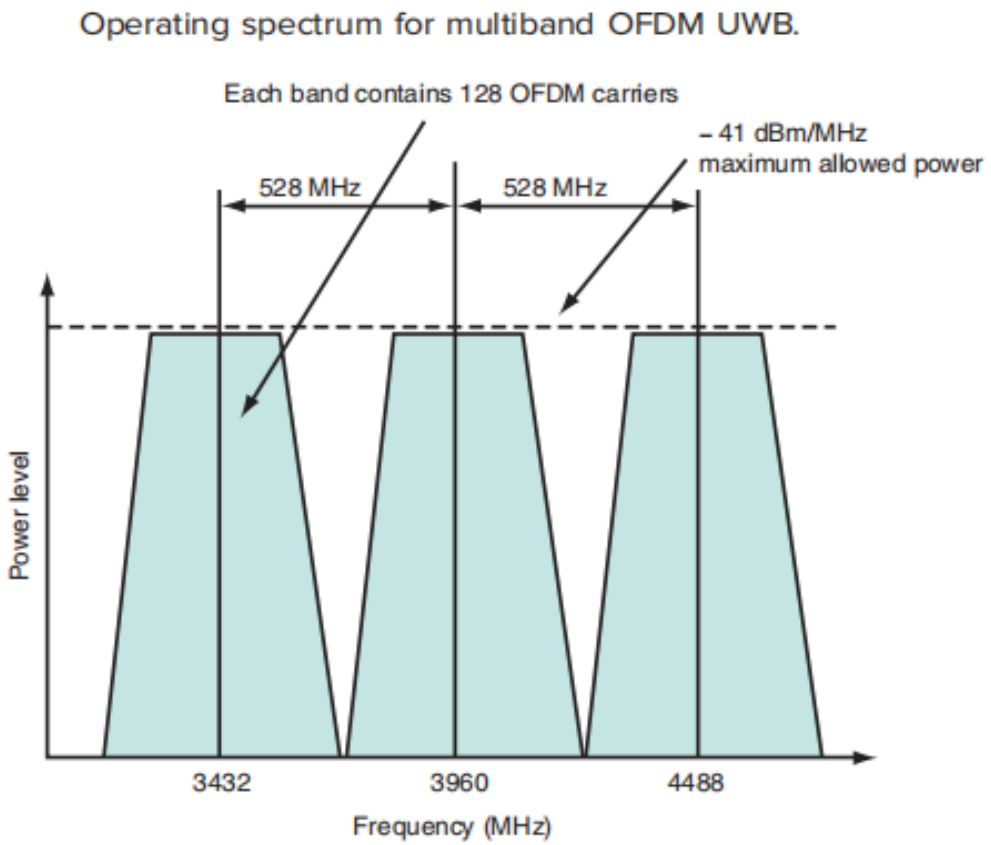


In PPM, the position of the pulse may occur sooner or later in time than a pulse with no modulation. A binary 0 may be represented by an earlier pulse, and a binary 1 as a later pulse, or vice versa. The time shift is small compared to the pulse width. Because of the very small time differences, the timing clock generating the pulses must be very precise and stable to ensure recovery. In BPSK, the PRI is constant, and the data bits produce a normal pulse for a binary 0 and a phase-inverted pulse for a binary 1.

Multiband OFDM UWB:

The newest form of UWB is called multiband OFDM or MB-OFDM UWB. The term multiband is derived from the fact that many OFDM carriers make up the signal. This form of UWB divides the spectrum

3.168 to 4.952 GHz into three 528-MHz-wide channels, as shown in fig below



Each band is designed to hold an OFDM data signal. There are 128 carriers per band, and each carrier has a bandwidth of 4.125 MHz. Of the bands 100 actually carry the data while 12 are used as pilot carriers to aid in establishing communications with nearby nodes. The remaining carriers serve as guard bands on either side to prevent interference between the three portions of spectrum.

The system is designed to permit a wide range of data rates from about 53 to 480 Mbps. The most often mentioned speed is 110 Mbps at a range up to 10 m. A speed of up to 480 Mbps is possible but only at a range of 2 to 3 m. Implementation of an OFDM UWB transceiver is just like that of any OFDM device. DSP chips are used to create the transmit carriers with the inverse fast Fourier transform (IFFT), and a DSP chip in the receiver uses the FFT for recovery of the data. MB-OFDM UWB radios are usually a single-chip IC containing all functions.

There is no UWB standard. Companies worked for years in an IEEE Task Group to create a single standard to be designated 802.15.3a. No consensus could be reached, so companies went their different ways. The

largest group of companies banded together in the WiMedia Alliance to create a standard that most could agree upon. Today the MB OFDM form of UWB is the defacto standard. The WiMedia Alliance maintains this standard.

Advantages of UWB:

UWB offers many benefits to radar, imaging, and communication applications:

1. Superior resolution in radar and imaging.
2. Immunity to multipath propagation effects.
3. License-free operation.
4. No interference to other signals using the same frequency band. UWB signals appear as random noise to conventional radios.
5. Power-efficient, extremely low-power operation. Peak power levels are in the milliwatt region, and average power is in microwatts.
6. Simple circuitry, most of which can be integrated in standard CMOS.
7. Potentially low cost.

Disadvantage of UWB:

1)The primary disadvantage, which is also an advantage, is low power. It severely limits the range of operation. The range can be extended in military radar with higher power levels, but the power level in commercial and consumer applications is severely restricted by the FCC. Typical ranges are from a few inches up to no more than about 100 ft.
2)Low support coverage on mobile devices.

Applications of UWB:

1. The primary application of impulse UWB to date has been in military radar. The very short pulse widths of electromagnetic energy permit very fine resolution of target distance and detail.
2. Short pulses also give UWB the ability to penetrate surfaces to see what is behind them. For this reason, UWB is an excellent electronic imaging technique.
3. UWB radars can even see underground to detect mines, pipes.
4. UWB radar is used by fire, emergency, and police personnel to see through walls and doors.
5. Medical versions permit body imaging for diagnosis.