Cellular Technologies

Mobile Device Investigations Program

Technical Operations Division - DFB
DHS - FLETC

Basic Network Design

Frequency Reuse and Planning

1. Cellular Technology enables mobile communication because they use of a complex two-way radio system between the mobile unit and the wireless network.

2. It uses radio frequencies (radio channels) over and over again throughout a market with minimal interference, to serve a large number of simultaneous conversations.

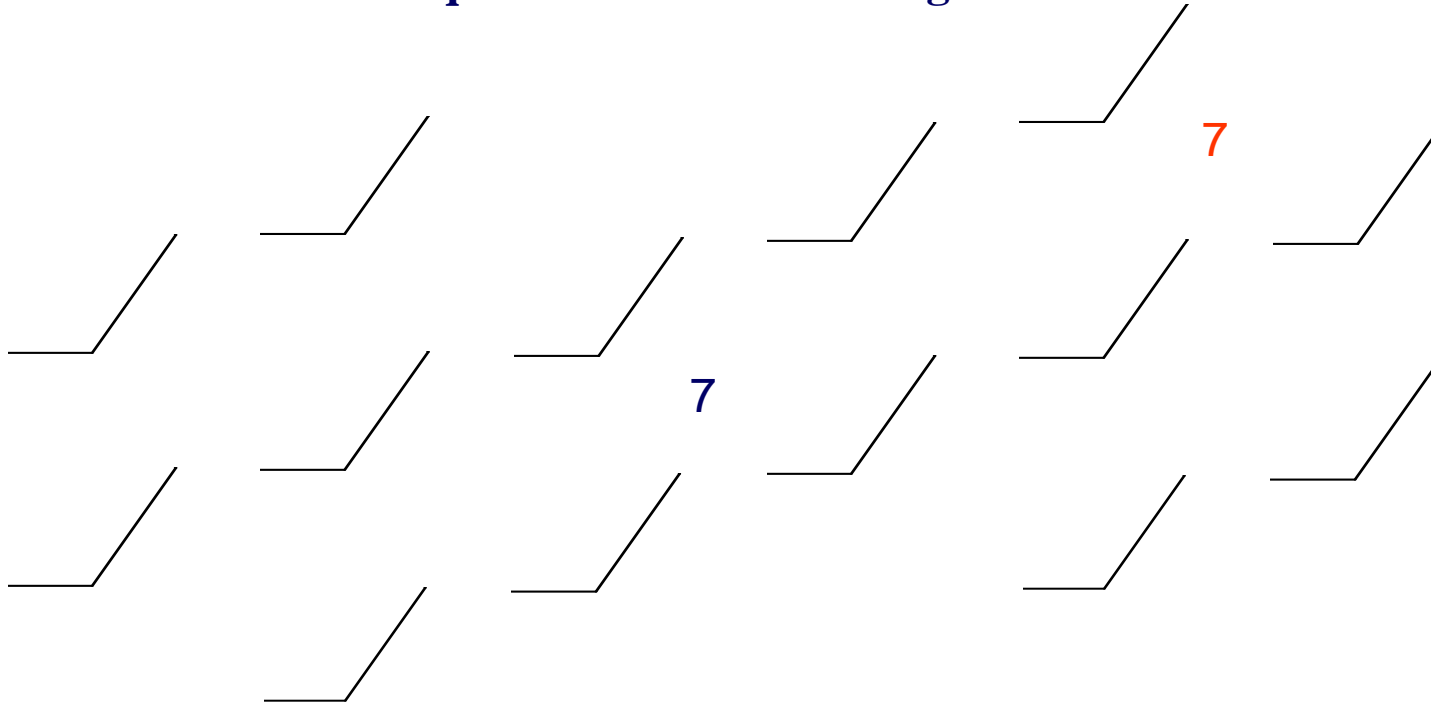3. This concept is the central tenet to cellular design and is called frequency reuse.

Basic Network Design

Frequency Reuse and Planning

1. Repeatedly reusing radio frequencies over a geographical area.

2. Most frequency reuse plans are produced in groups of seven cells.

Basic Network Design

Note: Common frequencies are never contiguous

7

7

The U.S. Border Patrol uses a similar scheme with Mobile Radio Frequencies along the Southern border. By alternating frequencies between sectors, all USBP offices can communicate on just two frequencies

Basic Network Design

Frequency Reuse and Planning

1. There are numerous seven cell frequency reuse groups in each cellular carriers Metropolitan Statistical Area (MSA) or Rural Service Areas (RSA).

2. Higher traffic cells will receive more radio channels according to customer usage or subscriber density.

Basic Network Design

Frequency Reuse and Planning

A frequency reuse plan is defined as how radio frequency (RF) engineers subdivide and assign the FCC allocated radio spectrum throughout the carriers market.

Basic Network Design

How Frequency Reuse Systems Work

In concept frequency reuse maximizes coverage area and simultaneous conversation handling

Cellular communication is made possible by the transmission of RF. This is achieved by the use of a powerful antenna broadcasting the signals.

Basic Network Design

How Frequency Reuse Systems Work

If you have one powerful antenna you would be able to handle conversations based on the number of channels you have available.

The first step necessary for frequency reuse is the cell system of the network.

Basic Network Design

How Frequency Reuse Systems Work

Each antenna in the various cells operate on the same RF that are assigned.

If your original antenna could handle 7 calls and you increased the number of antennas by 10

- 70 simultaneous calls.

The concept goes beyond the number of antennas and deals with how the radio frequency itself is used and reused.

Basic Network Design

How Frequency Reuse Systems Work

1. Each cell has its own antenna and low power Base Station to handle the traffic within it's area.

2. Each Base Station is assigned frequencies with neighboring base Stations being assigned different frequencies.

3. Carriers are then able to reassign these frequencies to other areas that are not too geographically close to the other Base Stations and cells.

Basic Network Design

Consider your local radio station broadcast. As you travel father away from the radio base it weakens until you lose the signal.
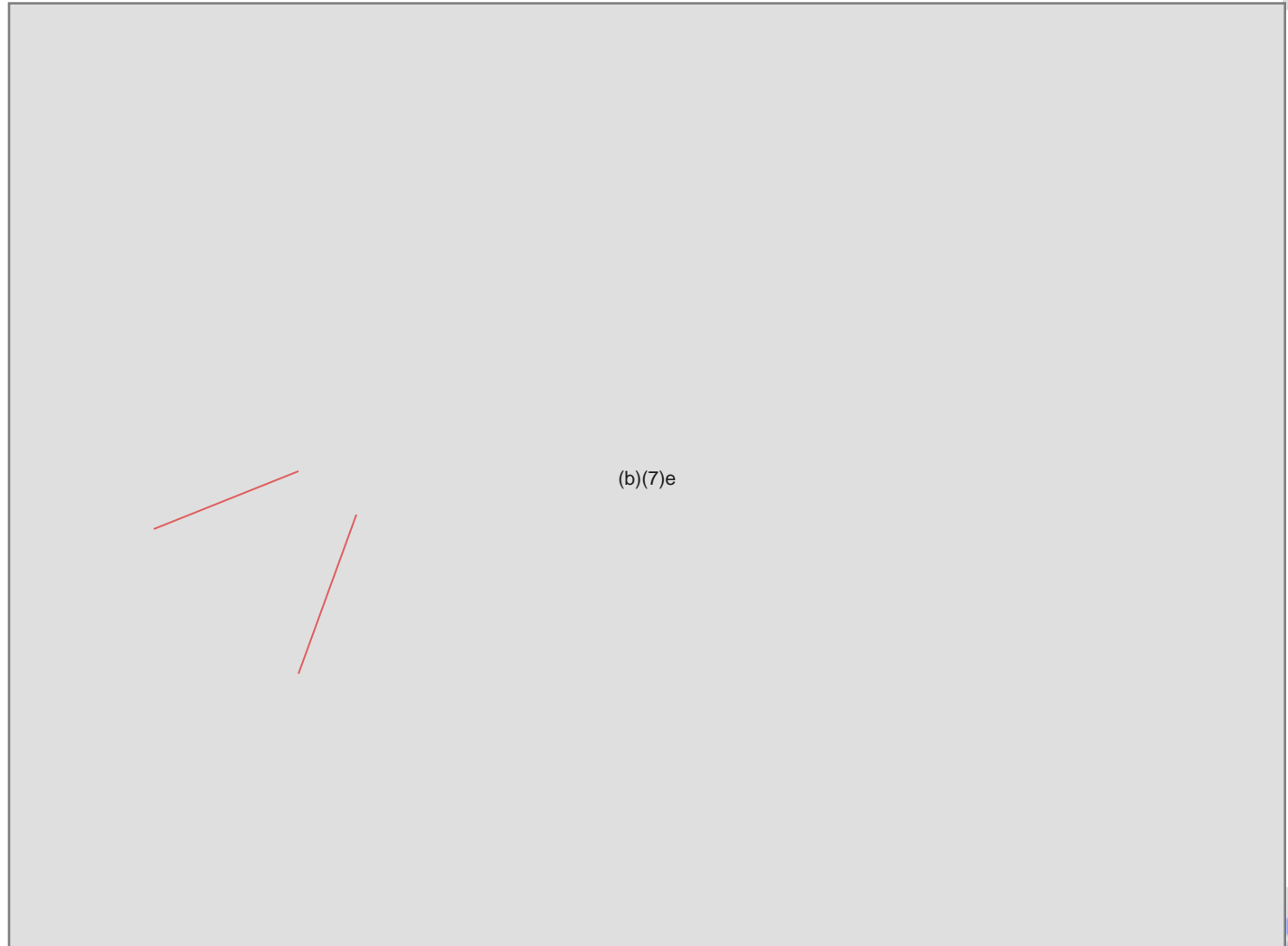
Now consider all the cars driving around you are listening are listening to different stations.

The radio station would be the Base Station and the vehicles would be the cells.

Basic Network Design

Cell Geographical Area

Geographical Limits

(b)(7)e

Basic Network Design

Distance to Reuse Ratio

1. The Distance to Reuse ratio defines how much geographical distance is required between cells in a cell system to avoid and limit interference.

2. The overall geographic size of cell base stations along with the power of the antenna determine the distance to reuse ratio

Basic Network Design

Distance to Reuse Ratio

1. What happens when I move about a cell coverage area or move into another cell area?

2. Another requirement of the wireless system is frequency agility.

3. This is the ability of the mobile unit to operate on any given frequency within their assigned spectrum.

4. This allows the mobile unit to switch from one channel to the another seamlessly and allows for another a important component of cellular technology – Call Hand Off

Basic Network Design

Call Handoff

1. Call handoff can best be described as the process of passing from one Base Transceiver Station (BTS) to another while maintaining connection to your network.

2. When you leave your particular network and move into another network - the roaming process.

This is transparent to the user.
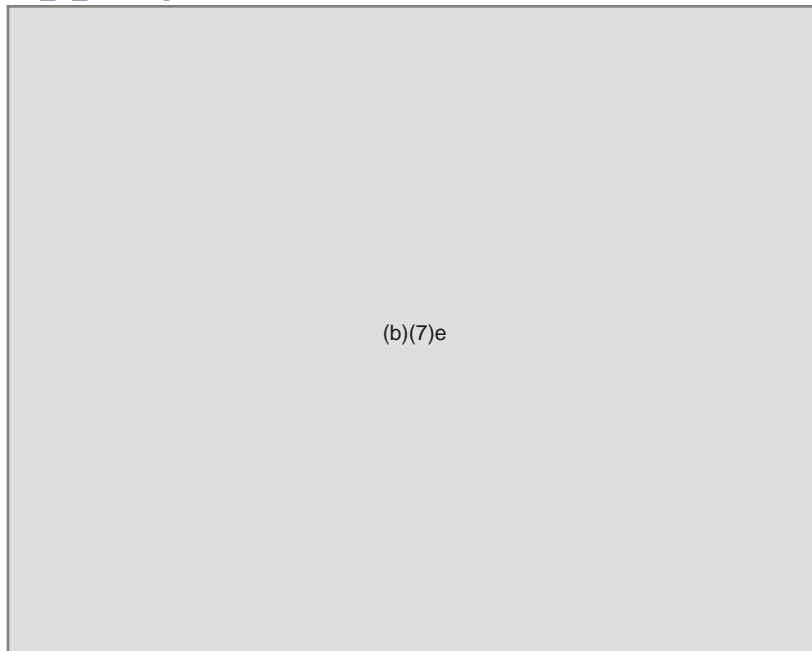
Basic Network Design

Define Call Handoff

1. Without Call Handoff, Frequency Reuse would not be possible and vice versa.

2. The Mobile Switch Center (MSC) monitors the power levels of the mobile units.

3. When the MSC detects the mobile unit power levels degrading it seeks out other BTSs.

Basic Network Design

Define Call Handoff

Base station coverage overlap with other cells in the area and it is this overlapping that allows call handoff to occur.

(b)(7)e

Basic Network Design

1. Base station coverage overlap with other cells in the area and it is this overlapping that allows call handoff to occur.

2. This action is handled by a microprocessor at the MSC and is seamless to the user.

3. This is a complex act that uses frequency synthesizers, the controller, and memory functions within the wireless handset.

4. This is why cellular phones must have frequency agility or the ability to change from one channel to another.

Basic Network Design

Wireless Network Design Maps

The FCC requires the use of United States Geographical Survey maps in the planning and development of the wireless network.

As it relates to planning it is important that all carriers use the same maps to lend conformity to the planning process.

Since the BTS operates at specific power levels it is very important to know where other towers are to avoid and/or minimize interference.
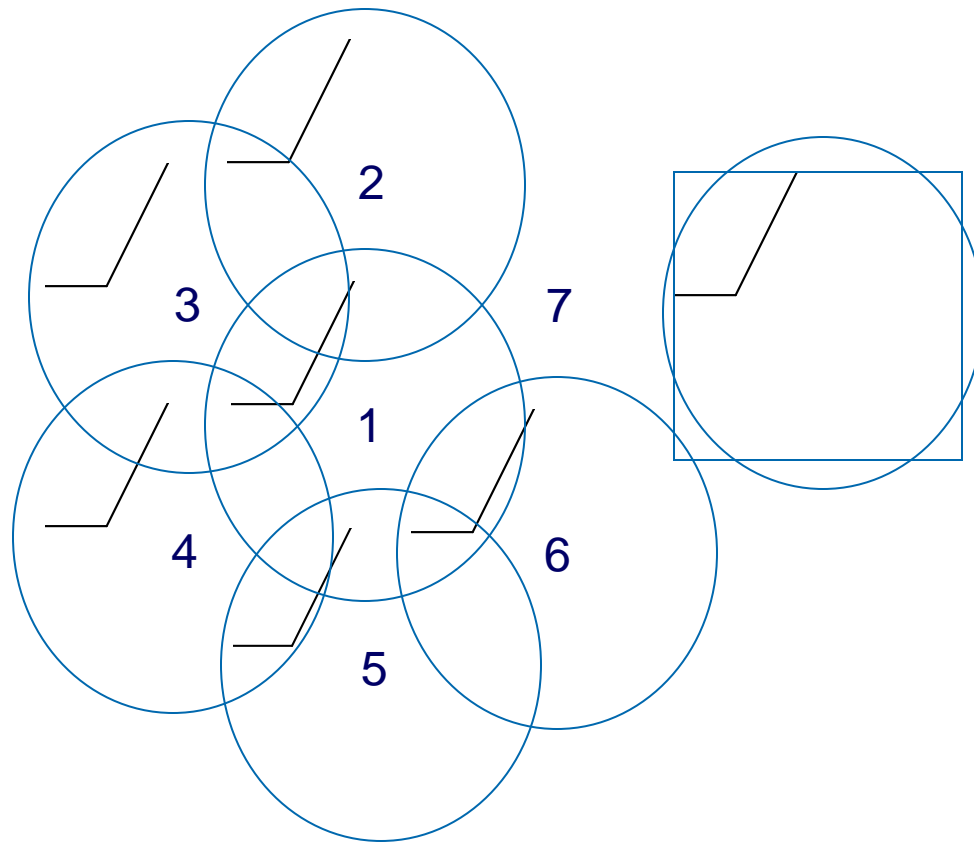
Basic Network Design

Hexagon Grid

The hexagon grid design is the predominant engineering design tool in the wireless industry.

There are other design models configured in squares, circles, octagons, etc. depending on the number of cell towers in the design.

The hexagon is used because it best represents and simulates the seven tower overlapping of circles. Circles being the way radio frequencies are depicted.

Basic Network Design

Hexagon Grid

Basic Network Design

In viewing our hexagon grid we can see where frequencies overlap from one cell to the other.

(b)(7)e

Basic Network Design

Hexagon Grid

1.

2.

(b)(7)e

3.

4.

Basic Network Design

Fundamental Components of a Wireless System

There are five main components to a wireless network. They are:

1. The Mobile Unit
2. The Cell Base Station
3. The Backhaul or Fixed Network
4. The Mobile Switching Center
5. The interconnection to the Public Switched Telephone Network (PSTN)

Page 25 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)e

Basic Network Design

There are two classifications of mobiles units in use today when we speak of cellular telephones and mobile devices.

The Mobile Unit

1. The Portable telephone or device – these are your small handsets, portable devices with network connection capabilities such as PDA's and GPS units.

2. The Mobile telephone or device – devices that are mounted in the locomotion device, such as installed telephones and GPS units.

Basic Network Design

The Cell Base Station

1. The Cell Base Station is the physical location of some of the equipment needed to operate the wireless network, such as antennas, GPS timing systems, cell towers etc.

2. The size of the base station is dependent upon it's location and system needs.

Basic Network Design

The Cell Base Station

1. Raw Land Sites

2. Rooftop Sites

3. Water Tank Sites

4. Co-located Sites

5. Stealth Sites

Basic Network Design

The Cell Base Station

1. Microcells – a outdoors network base station usually on rooftops, water tanks and the like.   The Base Station range of a Microcell is generally 100 meters to 1000 meters.

2. Picocells – the smallest, usually used indoors and intended to provide coverage for a small area.   The Base Station range of a Picocell is generally less than 100 meters. Typically found in airports, e.g.

3. Nanocells – mobile and easily installed. Nanocells can be mounted on walls, in vehicles or outdoor weatherproof enclosure. Coverage is dependant you configuration.

Basic Network Design

The Cell Base Station - Macrocells

Basic Network Design

The Cell Base Station - Microcells

Basic Network Design

The Cell Base Station - Picocells

Basic Network Design

The Backhaul or Fixed Network – Base Station Controller

1. A complex collection of systems that connect the Base Stations to the Base Station Controller.

2. This network connects the mobile users to others on its network and to the outside world.

3. THE BSCs are the brains behind the BTS. They usually control numerous cell sites.

Basic Network Design

The Backhaul or Fixed Network – Base Station Controller

1. The BSC handles the allocation of radio channels, measurements (Power Levels) from mobile devices, and in most cases handoffs from one BTS to another.

2. The BSC concentrates activity to and from the Mobile Switch Center to help with efficiency.

3. It provides data to the Operations Support System to monitor and enhance performance as well as assisting in trouble shooting.

4. The BSC then connects to the Mobile Switching Center.

Basic Network Design

The Mobile Switching Center

1. Often called the brains of a wireless network, the MSC is responsible for switching data packets from one network path to another.

2. This process is called call routing.

3. MSC provides subscriber service information such as user registration, authentication and location updating.

Basic Network Design

1.   The MSC provides connection to

- the Public Switched Telephone Network (PSTN) and

- the Integrated Services Digital Network (ISDN) using SS7 based interconnection.

Basic Network Design

1.   The MSC provides subscriber management functions such as;

- mobile registration
- location updating,
- authentication
- call routing to roaming subscribers.

1.   These functions are carried out by various databases, among which are the Home Location Registry, the Visitor Location Registry, Equipment Identity Register and the Authentication Center AuC in GSM.

Basic Network Design

Home Location Registry – HLR

HLR is a database that contains records of all subscribers.

HLR is used to identify and verify a subscriber on network

The record of what services the subscriber has is kept here

Basic Network Design

1. HLR connects and interacts with a number of other components on the system

    - The Gateway MSC for handling incoming calls

    - The VLR for handling request from mobile phones to attach to the network

    - The SMSC for handling incoming SMS

    - The voice system for delivering notification to the mobile phone that a message is waiting

Basic Network Design

1. In theory the HLR data is stored for as long as the subscriber is with the mobile phone operator

2. The HLR is a systems that directly receives and processes Mobile Application Part (MAP) transactions and messages.

3. If the HLR fails the system fails. The HLR manages the Location updates as mobile phones roam.

4. The HLR is now a powerful server more so than telephone switch hardware

Basic Network Design

1.

(b)(7)e

Basic Network Design

Visitor Location Register (VLR)

1. Stores information about all the mobiles that are currently under the jurisdiction of the MSC

2. The most important is the current Location Area Identity or LAI.

3. LAI identifies under which BSC the Mobile Station is currently

Basic Network Design

Visitor Location Register (VLR)

1. This information is vital in the call setup process.

2. Whenever an MSC detects a new MS in its network, it creates a new record in the VLR,

3. Updates the HLR of the mobile subscriber, apprising it of the new location of that MS.

Basic Network Design

1.

2.

3.

4.

(b)(7)e

Basic Network Design

1.   Relevant data stored there are;

       IMSI – the subscriber's identity number

   - Authentication Data

   - MSISDN – the subscriber's phone number

   - GSM services the subscriber has access to

   - Access Points (GPRS) that are subscribed to, and

   - The HLR address of the subscriber

Basic Network Design

1. The VLR also connects to;

- The Visited MSC (V-MSC), to pass data needed for certain procedures i.e., authentication and call setup

- The HLR to request data for the mobile phones attached to it's service area

- Other VLR to transfer data as the MS roams from one area to the next accessing new VLRs

Basic Network Designs

1. The VLR primary functions are

- To inform the HLR that a MS has arrived in the particular area covered by the VLR

- To track where the subscriber is within a VLR area when it is not active

- (b)(7)e

Basic Network Designs

The VLR other primary functions are;

- To allocate roaming numbers during the process of incoming calls

- (b)(7)e

- The VLR is reset daily

Basic Network Design

Equipment Identity Register (EIR)

1. Identifies what equipment i.e. mobile device or handsets are acceptable in a given network

2.
   (b)(7)e

Basic Network Design

Authentication Center (AUC)

1.   The AUC provides authentication of the MS and encryption of services

  1.

(b)(7)e

Basic Network Design

Gateway Message Switch Center (GMSC)

1. The GMSC provides the interface with the Public Switched Telephone Network or PSTN

2. In order for mobile units to connect to landline users there must be a system in place to achieve these goals.

3. This is completed by having a physical connection to the PSTN (the local land-line phone company).

4. This is done by the use of a data system known as the PDSN or Public Data Switched Node. .

5. There are other forms of connection such as the Asynchronous Transfer Mode or ATM and TCP/IP connections.

Basic Network Design

6.   This is done by the use of a data system known as the PDSN or Public Data Switched Node. .

7.   There are other forms of connection such as the Asynchronous Transfer Mode or ATM and TCP/IP connections.

Radio Frequency Operations and Technology

RF Operation and Technology

1. Radio propagation – the electromagnetic phenomenon discovered by Henrich Hertz in the late 1880's. It's how energy travels through a given medium.

2. The medium can be air, water, aired cable, fiber optics and the like. Radio signals travel at the speed of light through the air – 186,282 miles per second.

3. The only significant difference cellular systems and conventional landlines is the radio link that connects the wireless network to the cell base station.

RF Operation and Technology

Different radio signals have different properties, i.e.

- High frequencies and Low frequencies
- Signal Refraction - signals bend through the atmosphere
- Signal Diffraction - signals bend around obstructions
- Signal Reflection - signals bounce off obstructions or solid objects

RF Operation and Technology

Wireless signals are basically omnidirectional

Omnidirectional; all directions (360°) propagation is often described as waves.

Pebble In Water - size of pebble, water and energy

RF Operation and Technology

Radio Frequency coverage from any base station is determined by three factors;

- **The height of the antenna**
- **The type of antenna used**
- **The Radio Frequency Power Level emitted.**

This is true no matter where the antenna is placed

Signal Fading and Ducting

There are a number of things that may interfer with the propagation of a radio signal.

Some of the ongoing issues wireless carriers have to deal with are:

1. Ducting

2. Signal Fading

Ducting

Ducting is defined as the trapping of RF in the boundary area between two air masses.

Ducting of RF is an atmospheric anomaly known as temperature inversion

Ducting is unavoidable; it is a natural meteorological phenomenon.

Down-tilting or directing the RF toward the ground may compensate for ducting.

Absorption

Absorption describes how a radio signal is absorbed by objects

The greater the amount of absorption the less geographical area can be covered.

Organic material absorbs more wireless signals than inorganic.

Absorption

Absorption can be compensated for in the following ways:

- By using higher-gain antennas
- By using higher RF power levels in order to cover the same geographic area
- By decreasing the distance between Base Stations

Free Space Loss

Free-space Loss or Path Loss describes the attenuation (fading) of a radio signal over a given distance.

The higher the frequency the greater the free space loss. PCS carriers operating at 1.9MHz will have greater loss than wireless carriers operating at 850 MHz.

Power Levels of a Base Station signal and antenna gain will determine when a wireless signal will fade.

Multipath/Rayleigh Fading

Multipath or Rayleigh Fading; the transmitted base signal reacts to physical features or structures creating multiple signal paths.

Using the pebble in the water analogy, think of rocks, sticks or other objects in the water.

Multipath/Rayleigh fading will occur in both directions.

Multipath/Rayleigh Fading

(b)(7)e

Multipath/Rayleigh Fading

Obviously strongest signal will always be the signal directly from the mobile unit to the Base Station.

The indirect signals will arrive at the base either in phase or out of phase with the direct signal.

Wireless Frequency Bands

The radio frequency assigned to the early cellular industry was the mostly unused 850 MHz UHF television spectrum.

The 850 MHz radio propagation is beneficial for the following reasons;

1. It has a very short wavelength, about 12 inches

2. It tends to be line of sight, unlike shortwave radio signals

3. It is easily reflected off objects.

4. It is easily absorbed by foliage, which can be good or bad. It can help with frequency reuse or in certain urban areas or highways degrade the signal.

Wireless Frequency Bands

The 1.9 MHz signal used by PCS carriers is good for wideband services, but has penetration problems as it relates to buildings and the like.

The 1.9 MHz signal does not propagate as well as the 850 MHz signal because it has an even shorter wavelength.

What's a 'Wavelength'?

(b)(7)e

1. The distance between 360-degree points of a wave.

2. Calculated (in air/vacuum) by dividing speed-of-light by frequency (slightly attenuated in air).

- At sub-UHF frequencies (<300Mhz), RF waves are reflected by the troposphere (allowing non-line-of-sight – e.g., AM/FM Radio).

In-Building Coverage

Due to the nature of building construction and structure it is often difficult receive and maintain RF inside.

(b)(7)e

Page 70 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
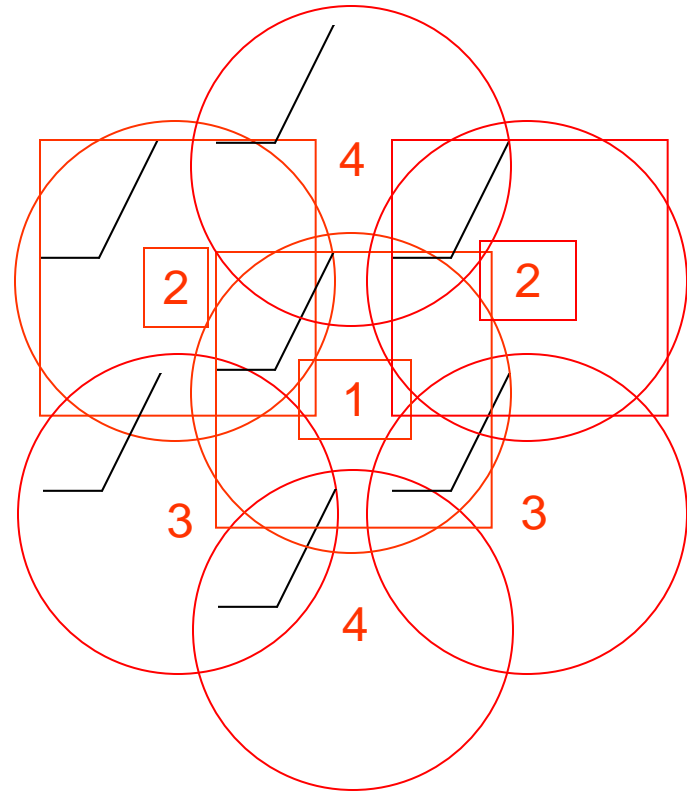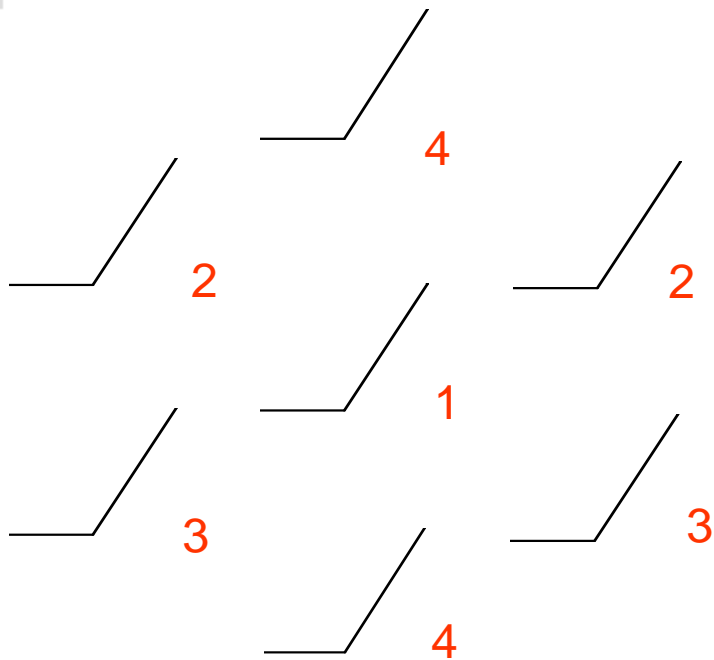(b)(7)e

Frequency Coordination

1. Frequency Coordination is the effort by carrier RF Engineers to place base stations in a orderly fashion to minimize interference.

2. This is done by adhering to the Distance to Reuse ratio within their own system.

3. RF Engineers from the various carriers often coordinate with each other to comply with the FCC mandates.

System Interference

Interference is defined as any adverse interaction between two or more radio signals that cause noises or cancels out each other.

This generally occurs when transmitting RF too close to each other or on the same frequency.

Co-Channel Interference

Co-Channel Interference

The RF Engineer considers the following when planning cell placement;

1. RF power levels at co-channel cell sites

2. Geographic distance between co-channel cells

3. Types of antennas used at co-channel cells

Co-Channel Interference

Options available to the RF Engineer to reduce or eliminate co-channel interference;

1. Downward tilting antennas when and where appropriate
2. Used reduced-gain antennas
3. Decrease RF output at base stations
4. Reduce the height of the tower

Co-Channel Interference

Other types of Channel Interference are:

1. Adjacent Channel Interference – the inability of a mobile unit to filter signals of adjacent channels assigned to nearby cells

2. Intermodulation Interference or IM – IM describes the effect of several signals mixing together to produce unwanted signals or no signals.

Radio Frequency Channelization

All carriers, no matter what air interface, must break up their assigned radio spectrum into usable portions.

Each standard has it's own method of doing so. Regardless of the air interface technology certain functions must be handled.

Paired Channels

All wireless conversations require paired channels to function.

Mobile or portable phones conduct simultaneous two-way transmissions. This is known as Full Duplex.

One channel is used for transmitting and one channel is used to receive.

Depending on the technology, the frequency may be the same or they maybe different.

Paired Channels

When the frequency is the same, this is known as 'Time Division Duplexing'.

When the frequency is not the same it is known as 'Frequency Division Duplexing'.

The only time that duplexing will not take place is when there is one-way transmissions as in SMS or streaming media.

The channel from the base station to the mobile unit is known as the downlink or forward channel. The channel from the mobile unit to the base station is known as the uplink or reverse channel.

Channel Spacing

Channel Spacing refers to the actual bandwidth space that is allocated to every wireless channel allocated out of the total spectrum amount.

The following are the standard Channel Spacing for the listed air interfaces;

AMPS -   30 KHz or 60KHZ for downlink and uplink

GSM -   25 KHz or 50 KHz for downlink and uplink

CDMA -   Since CDMA uses spread spectrum technology it is assigned 1.25 MHz per channel. More Later!!!!

Control Channels

Understanding the function of the Control Channel is one of the most important artifacts a Law Enforcement will need to know.

The Control Channel performs numerous functions that leave evidence of a mobile user's activities.

The Control Channel handles the administrative functions and overhead of wireless systems.

Since the wireless carrier must know at all times if a subscriber is in their service area or not, constant contact with the Control Channel is necessary.

Control Channels

The Control Channel completes this task by having contact with the:

- mobile unit
- cell base stations
- base station controllers
- the mobile switching center

Some of the administrative task assigned the Control Channel are as follows:

Control Channels

Setup wireless calls, mobile originated or terminated (destined), locating mobile phones to make contact with them.

Collecting information for billing operations.

Collecting traffic measurements on base stations.

Control Channels

Autonomous mobile registration, registering the phones on the system (both home and roaming).

Initiating and assisting with call handoff.

Control Channels

Each channel set in a wireless network has a Control Channel.

When a mobile unit is powered on and seeks out the Control Channel:

- The carrier sets one of it's strongest frequencies as the Control Channel when they launch.

- The mobile unit re-tunes to the Control Channel periodically to maintain a strong connection with the Control Channel.

RF Technologies

There are other technologies in use that are being incorporated into the wireless cellular and mobile device arena.

Bluetooth – The most well-known of the technologies. These devices are designed to offer wireless connectivity to devices with a wide range of capabilities.

Bluetooth enables any electrical device to wireless communicate with on the unlicensed 2.5MHz frequency. It is envisioned to replace cable connections using a single radio link.

Bluetooth is a medium to long range enabling technology.

RF Technologies

Bluetooth has a range of 10 – 100 meters and supports point to point data transfer. This data includes voice co-channels as well.

Bluetooth uses frequency hop schemes, which allows it to work in high interference areas.

(b)(7)e

RF Technologies

Ultra-Wideband Wireless or UWB – UWB is a digital pulse technology designed to transmit large amounts of data over a wide spectrum of frequency bands.

UWB carries large amounts of data in distances up to 230 feet at very low power levels.

The digital pulses produced by UWB are timed precisely over the very wide spectrum at the same time.

RF Technologies

UWB can also be defined as wireless communications technology that can transmit data at speeds between 40 megabits and 60 megabits per second.

The two main difference between UWB and other narrowband or wideband systems;

1. The bandwidth of UWB is greater than any other current technology used for communication

2. UWB is typically implemented in a carrier-less fashion, meaning it is not constricted by the RF allotment schemes.

RF Technologies

(b)(7)e

RF Technologies

Two other RF technologies are Software Defined Radio (SDR) and Cognitive Radio (CR).

- Software Defined Radio uses a software package to administer the all the functions used in wireless communication.

- Everything from RF and channel selection, to handoff and logging is handled independently by the software program.

RF Technologies

Cognitive Radio uses software as well but has the ability to store and react to the users dominate needs and typical environment.

This is achieved by either pre-set codes or an algorithm created by the software manufacturer.

The cognitive radio seeks to think and react.

More on both technologies later if time permits.

Code Division Multiple Access Technology

CDMA

Code Division Multiple Access or CDMA has it's roots in WWII era *spread spectrum* technology.

CDMA can be implemented in several ways, two of which are *frequency hopping and direct sequencing.*

In 1985, the FCC allocated three frequency bands to spread spectrum communications.

CDMA

Conventional radio signals operate on a narrowband or a very narrow specific portion of the RF bandwidth.

Conventional radio signals are open to interference because of these narrowband widths.

A single interfering signal operating at or near its frequency can render a radio inoperable.

CDMA

CDMA uses spread-spectrum technology to minimize the problems.

Using spread-spectrum technology allows for the signals to be transmitted over a wide spectrum of the electromagnetic spectrum.

This is achieved by a specific but complex mathematical function.

The receiver must recognize the frequency-versus-time function employed by the transmitter.

CDMA

Spread-spectrum signals are distributed over a wide range of frequencies and then collected on their original frequency at the receiver.

This operation takes place inconspicuously and transparent.

Since spread-spectrum transmitter signals are so much wider they use less power.

This also allows for the use of both narrowband and spread spectrum on a single frequency.

CDMA

Spread-spectrum signals are hard to intercept and spoof.

Spoofing - falsely or maliciously introducing misleading or false traffic and messages.

The is also known as Signal Exploitation.

CDMA

All spread-spectrum systems have a threshold or tolerance level of interference.

This threshold is directly related to the systems Processing Gain.

The processing gain is the ratio between the RF bandwidth and the information bandwidth.

There are two types of spread-spectrum technologies.

Frequency Hopping and Direct Sequencing.

CDMA – Frequency Hopping

Frequency hopping is the easiest spread-spectrum modulation to use.

Frequency hopping conversation requires the addition of pseudo-noise (PN) code generators.

If both receiver and transmitter know in advances what frequencies will be used this is not necessary.

CDMA – Frequency Hopping

De-hopping is achieved by a synchronized PN code generator in the local receivers frequency synthesizer.

The idea behind frequency hopping is to transmit across a broad spectrum, switching frequencies rapidly from one to another

CDMA – Frequency Hopping

The challenge is to keep both the transmitter and receiver synchronized.

An accurate clocking system and a pseudo-random generator makes this simple.

The phone creates the equivalent of a low powered noise pattern system.

CDMA – Direct Sequence

Direct Sequencing is the more practical and all digital form of spread-spectrum.

A Direct Sequence system uses a locally generated PN code to encode the data.

The local PN code runs faster and the encoded data is transmitted at the higher rate of speed.

CDMA – Direct Sequence

Carrier Modulations other than Binary Phases Shift Keying or BPSK is possible.

BSPK is the simplest and most commonly used spread-spectrum modulation.

A spread-spectrum receiver uses a locally generated replica PN code and a receiver correlator.

CDMA – Direct Sequence

The desired information can be voice, data, video and so forth.

A spread-spectrum correlator is a very special matched filter that responds only to a PN code that matches its own.

A spread-spectrum correlator can be tuned to different codes by simply changing its local code.

It will respond only to identical PN codes matching its own.

CDMA – Direct Sequence

Think of a conference room in the United Nations where no two people speak the same language.

All the attendees start to speak at once. This is the noise spread across the spectrum.

A person on the opposite end of the room understand you and blocks out all the other languages.

CDMA – Direct Sequence

Although the others can hear the noise they can not understand what is being said.

Now envision the same conversation being held but you have to move about the room at the right time to hear and understand what is being said.

You are only receiving little bits of information at a time that you must then decode.

CDMA – Direct Sequence

(b)(7)e

CDMA – Spread-Spectrum Operations

These special codes are called Pseudo Random Noise Codes or Walsh codes.

The uses of these special codes make signals appear wideband and noise like.

The information bandwidth can be voice, data, video or image.

CDMA – Spread-Spectrum Operations

Two criteria must be met to qualify as a Spread Spectrum Signal;

1. The signal bandwidth must be wider than the information bandwidth.

2. Some code or pattern, other than the data to be transmitted, determine the actual on air transmit bandwidth

CDMA – Spread Spectrum Advantages

Interference Immunity – Spread Spectrum radios are inherently more noise immune than conventional radios.

Multichannel Capability – Spread Spectrum radios offer the ability to have multiple channels, which can be changed dynamically through software

CDMA Basics

A unique code is assigned to all digital speech bits and the signals spread across the broad spectrum of the RF.

Each CDMA base station can use the same 1.25 MHz carrier at the same time.

There are a maximum of 64 Walsh noise codes per 1.25MHz in a CDMAOne system.

CDMA Basics

CDMA networks have pilot channels which carry no data but are used by the subscriber's mobile unit to acquire the system and assist in the soft handoff process.

A separate pilot channel is transmitted for each sector of a cell site and is uniquely identified by it's own PN code, just like other users

CDMAOne and CDMA 2000

CDMA refers collectively to three CDMA standards that were the first formal specifications assigned to the technology;

1. IS-95A
2. IS-95B
3. J-STD-008

CDMA Architecture – Power Control

What happens if a mobile unit near the base has a higher power level than one far away? – Power Throttle

Power control is necessary to maintain system capacity.

A benefit is reduced cost at the base station and longer battery life for the mobile unit.

CDMA Architecture – Rake Receivers

Rake receivers exist in both the mobile unit and the BTS transceivers.

Rake receivers derive their name from the fact that they look like lawn rakes.

The signal from each is combined to generate a composite signal.

CDMA Architecture – Rake Receivers

There are four rakes in a transceiver and three rakes in a mobile unit.

The strongest signal is combined with the multipath (weaker) signal of the other rakes to form this composite signal.

The multipath signals are added to the direct signal to obtain the cleanest signal. This process is known as diversity combining.

CDMA Architecture – Soft Handoff

Hard Handoff are defines as the milliseconds in which a mobile unit is passed from one cell to the other and there is no connection.

Soft Handoffs in CDMA systems work differently. When a unit is about to leave one cell area and travel to another it seeks out the strongest cell signal it can find.

This information is sent by the mobile unit to the MSC. The MSC verifies the information and connects to the unit to the cell while it is still connected to the previous cell.

CDMA Architecture – Soft Handoff

Once the connection is secure and complete the MSC disconnects the mobile unit from the old cell and the handoff is complete.

Hard Handoffs are known as break-before-make connections.

Soft Handoffs are known as make-before-break connects.

CDMA Architecture – Soft Handoff

The sequence of events on a soft handoff are;

1. After a users completes a call the mobile unit continually scans to determine if it is in range of another cell that has a stronger signal.

2. When the mobile unit determines it has located a stronger signal it now knows that it is in another cell's coverage area.

3. The mobile unit transmits a control message to the MSC, stating it has entered another cell's coverage area. The mobile unit identifies the cell to the MSC.

4. The MSC initiates the handoff by establishing a link between the mobile unit and the new cell site. The MSC maintains a link between the old cell site and the mobile unit.

5. While in the transition region between the two cells the mobile unit is serviced by both cell sites.

6. The original link will only be disconnected when the mobile unit is firmly connected to the new cell site.

CDMA Architecture – Cell Breathing

CDMA is a noise-generated technology. As such the system must monitor its noise floor or ambient noise.

To much noise will cause interference leading to degraded service or dropped calls.

CDMA systems are equipment with a protocol that allows the system to adjust in these situations.

CDMA Architecture – Cell Breathing

When a CDMA base station determines that there is to much noise or interference it begins the process of powering down the cells and the mobile units under control down.

This lowers the noise level and shrinks the cells coverage area.

CDMA Architecture – Cell Breathing

If it is determined that the mobile unit is about to lose the signal it connects the mobile unit to another cell or drops the call if it is unable to do so.

When the MSC determines that the noise level has subsided it powers the entities back up increasing the coverage area.

This activity is what is described as the cell breathing process.

Time Division Multiple Access Technology

TDMA

Time Division Multiple Access or TDMA is a digital transmission technology that allows a number of users to access a single radio frequency (RF) channel without interference by allocating unique times slots to each users within the channel.

TDMA multiplexes three signals (from multiple users) over a single channel.

TDMA

In 1989 the Telecommunications Industry Association and the Cellular Telecommunications & Internet Association chose TDMA over FDMA as the standard to use for 800 Mhz cellular market and the emerging 1.9Ghz markets.

With growing competition between CDMA, GSM and TDMA the CITA decided to let the carriers make their own technology selection

TDMA – How It Works

TDMA takes the digitized audio signal and transmits them on a RF in very short bursts, no longer than milliseconds typically 10 msec.

Audio packets are assigned a time slot on RF with audio burst portions of other communications.

It allocates a channel frequency for a short time and then moves to another channel.

TDMA – How It Works

Consider having four conversations going on at one time on four different channels.

TDMA – How It Works

This is how the same four conversations would look time slotted with TDMA

RF Ch. Freq. 1	Mary had a	Hickory, dickory,	There was an	Jack and Jill
	Slot 1	Slot 2	Slot 3	Slot 4

TDMA – How It Works

The IS-54 and IS-136 in effect tripled the capacity of cellular frequencies by dividing the 30 Khz channel, allowing more users per channel.

Today TDMA and other standards allow for more slotting giving rise to more users on the systems.

Proponents of TDMA such as AT & T Cingular state they will have the ability to carry 40 or more conversations on a single channel in the near future.

Extended TDMA or ETDMA

The weakness in TDMA is the waste of bandwidth, which in effect is a waste of possible on air time.

ETDMA uses a control channel to detect and assign a channel dynamically when voice activity is detected.

When ETDMA determines there is no conversation or there is a pause it reassigns the channel to a party having a conversation

Extended TDMA or ETDMA

Consider the pace in which this presentation is being given.

ETDMA uses these natural pauses to transmit the short millisecond burst of information.

TDMA – Disadvantages

In TDMA systems each user has a predefined time slot.

If the user enters into a cell area in which all the time slots are allocated he/she may not be able to complete a call.

However, most phones and services today are multi-spectrum. If the TDMA is overcrowded, the carrier will flip to another spectrum seamlessly.

Check your own phone. You will probably find it is multi-spectrum.

Global System for Mobile Communication Technology

Mobile Device Investigations Program

GSM Technology

Global System for Mobile Communication or Groupe Special Mobile

To standardize cellular communication thoughout Europe

Prior to it's development there were a number of incompatible systems served Europe

GSM Technology

With GSM European companies agreed to a set of standards

GSM is an open source system

Allows access to code

All operate based on these standards

GSM Technology

GSM operates on the 900 MHz, 1800 MHz and 1900 MHz

GSM uses Digital Communication System or DCS 1800 and is the worlds main 2G standard

When the FCC issued 1900 MHz to PCS in the United States it was based on GSM

DCS 1900 is considered the GSM standard for North America and is called North American GSM.

GSM Technology

GSM is now a worldwide standard

GSM uses Time Division Multiple Access or TDMA technology as their air interface standard

TDMA has limited capabilities

GSM is strictly controlled by a Memorandum of Understanding (MOU)

GSM Architecture and Subsystems

Open architecture according to the Open Systems Interconnect or OSI model for layers 1,2, and 3.

- Layer 1 – Physical Layer
- Layer 2 – Data Link Layer
- Layer 3 – Network Layer

GSM carriers can go to any GSM manufacturer

GSM Architecture and Subsystems

GSM uses voice coders/decoders or vocoders

Vocoders are firmware and chips sets that digitize the human voices

Voice that is sampled and channelized is housed in the vocoder

GSM Architecture and Subsystems

Vocoders packetize the sample of the human speech and transmits it through the handset to the base station

Distant-end vocoders decode the pulses and routes the call to the MSC

A full-rate vocoder allows for eight (8) conversations over a channel

Half-rate vocoders samples at half the rate of speed and allows for more effective use

GSM Architecture and Subsystems

By standard the GSM network is divided into four (4) subsystems

1. The Base-Station Subsystem

2. The Network Subsystem

3. The Operation and Support Subsystem

4. The Mobile Station Subsystem (The Mobile Unit)

GSM Subsystems – Base Station Subsystem

The Base-Station Subsystem is comprised of:

The Base-Station Controller[1] (BSC) -part of the wireless system's infrastructure that controls one or multiple cell sites' radio signals

Performs radio signal management functions for base transceiver stations, managing functions such as frequency assignment and handoff.

The BSC acts as a front-end processor for the MSC.

GSM Subsystems - Base Station Subsystem

Base Transceiver Station[2] (BTS) - The name for the antenna and radio equipment necessary to provide wireless service in an area.

Also called a base station or cell site.

Defines a cell coverage area

Controls the radio link protocols with the mobile station.

GSM Subsystems - Base Station Subsystem

The Air Interface[3] - operating system of a wireless network.

Radio-frequency portion of the circuit between the cellular phone set and the active base station.

As a subscriber moves from one cell to another the active base station controller changes periodically

Each changeover is the same as a handoff.

GSM Subsystems - Network Subsystem

The Network Subsystem is in affect the Mobile Switching Center

The central part of the network.

The MSC provides connection to the Public Switched Telephone Network (PSTN) and the Integrated Services Digital Network (ISDN) using SS7 based interconnection.

GSM Subsystems - Network Subsystem

The MSC provides subscriber management functions such as;

- mobile registration
- location updating,
- authentication
- call routing to roaming subscribers.

The Home Location Register (HLR) and the Visitor Location Register (VLR) are located within the MSC.

The HLRs database contains different types of information;

1. Every Subscriber Identity Module (SIM) card issued by the Mobile Phone Operator.

   The SIM has a unique identifier called the International Mobile Subscriber Identifier or IMSI.

(b)(7)e

The SIM card keeps track of all Mobile Subscriber Integrated Services Digital Network Number or MSISDNs.

These are the telephone numbers that have called the mobile unit.

It is used for making and receiving voice calls and SMS.

The MSISDN can have a second number for receiving data and fax.

Each MSISDN is also a primary key in the rational database.

GSM Subsystems - Network Subsystem

Examples of other data stored in the HLR in a SIM record;

- GSM services the subscriber has requested or been given

- General Packet Radio Service or GPRS settings allow the subscriber access to packet services

- Current location of the subscriber; providing a Serving GPRS Support Node (SGSN- packet roaming)

- Call Divert or Call Forwarding settings

GSM Subsystems - Network Subsystem

(b)(7)e

The HLR is a systems that directly receives and processes Mobile Application Part (MAP) transactions and messages.

If the HLR fails the system fails. The HLR manages the Location updates as mobile phones roam.

The HLR is now a powerful server more so than telephone switch hardware

GSM Subsystems - Network Subsystem

HLR connects and interacts with a number of other components on the system

- The Gateway MSC for handling incoming calls
- The VLR for handling request from mobile phones to attach to the network
- The SMSC for handling incoming SMS
- The voice system for delivering notification to the mobile phone that a message is waiting

GSM Subsystems - Network Subsystem

The main function of the HLR is to manage the movement of SIMs and mobile phones by;

- Managing and updating the position through location areas identified with a LCA. Updates the users location
- Send subscriber information to the VLR when the users roams
- Act as a go between for the GMSC or SMSC with the VLR - receive text or voice messages
- Remove the user of the VLR when he/she has left that roaming area

Visitor Location Register (VLR) Database - stores information about all the mobiles that are currently under the jurisdiction of the MSC. Some of this information include;

- The most important is the current Location Area Identity or LAI.

- LAI identifies under which BSC the Mobile Station is currently

- (b)(7)e

Visitor Location Register (VLR) Database - stores information about all the mobiles that are currently under the jurisdiction of the MSC. Some of this information include

4. Whenever an MSC detects a new MS in its network, it creates a new record in the VLR,

5.
(b)(7)e

GSM Subsystems - Network Subsystem

VLR is a temporary database of the subscribers that have roamed into the area

Each base Station is served by only one VLR

No one subscriber can be on more that one VLR at any given time.

VLR are either linked directly to the V-MSC or are integrated with a special software interface.

GSM Subsystems - Network Subsystem

Relevant data stored there are;

- IMSI – the subscriber's identity number

- Authentication Data

- MSISDN – the subscriber's phone number

- GSM services the subscriber has access to

- Access Points (GPRS) that are subscribed to, and

- The HLR address of the subscriber

The VLR also connects to;

- The Visited MSC (V-MSC), to pass data needed for certain procedures i.e., authentication and call setup

- The HLR to request data for the mobile phones attached to it's service area

- Other VLR to transfer data as the MS roams from one area to the next accessing new VLRs

GSM Subsystems - Network Subsystem

The VLR primary functions are

- To inform the HLR that a MS has arrived in the particular area covered by the VLR

- To track where the subscriber is within a VLR area when it is not active

- To validate (allow/disallow) which services the subscriber may use

GSM Subsystems - Network Subsystem
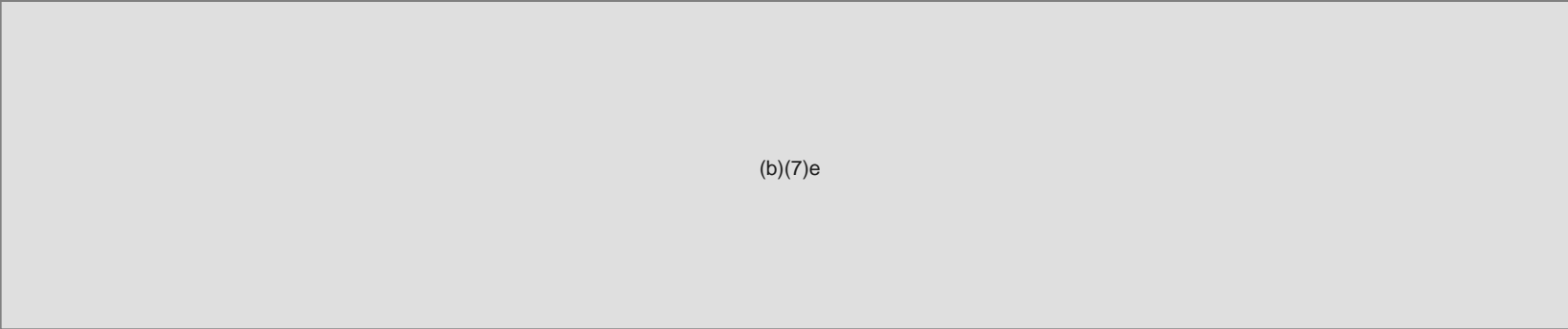
The VLR primary functions are

- To allocate roaming numbers during the process of incoming calls

- To purge the subscribers record if he/she becomes inactive while in its area

- To delete the subscribers record when the subscriber moves into another VLRs area based on the rules of the HLR. The VLR is reset daily

GSM Subsystems - Network Subsystem

Other functions associated with the Network Substation are:

- The Authentication Center - provides authentication of the MS and encryption of services

- The Equipment Identity Register (EIR) – Using the IMSI, the EIR keeps track of valid MS. If one is lost, stolen or service discontinued it is blacklisted on the EIR

- Billing Center (BC) – produces the tolls generated by the VLR and HLR for each subscriber and the roaming data

- Short Message Service Center (SMSC) – the sending and receiving of short messages

- Multimedia Messaging Center – the sending and receiving of images, video, audio or any combination of them

- Voicemail System (VS) – records and stores voice messages

-

(b)(7)e

-

- This systems works with conference calling feature

GSM Subsystems Operations and Support Subsystem

The Operations and Support Subsystem – the command and control center used to monitor the GSM system.

If there is a particular failure in the OSS can identify the problem and determine what course of action is needed

The Mobile Station (Mobile Phone) Subsystem – also known as the User Equipment. GSM phones are segmented for a number of reasons.

The MS has four main components:

1. The Mobile Terminal
2. The Terminal Equipment
3. Terminal Adapter
4. Subscriber Identity Module or SIM

GSM Subsystems - Mobile Station Subsystem

The Mobile Terminal or Handset – identification information is held on the SIM card

The handset's main functions are to transmit, receive, encode and decode voice transmissions.

The SIM card contains the GSM operating program, customer and carrier specific data.

Programmed at the sales office, the SIM card provides authentication, information storage, subscriber account information and data encryption.

SIM cards and handsets are interchangeable.

SIM card will recall all information stored on it, including programmed numbers, SMS saved, ring tones, Contact list and the like.

GSM Subsystems - Mobile Station Subsystem

Some of the Network Specific items used to authenticate and identify subscribers on the Network are;

- Integrated Circuit Card ID or ICCID – International ID, stored in the SIM card and stamp of the card

- International Mobile Subscriber Identity or IMSI- Mobile operators connect mobile phone calls and communicate with their market through SIM cards

- Local Area Identity or LAI – Networks are divided into local areas with a unique number. When you travel from one area to another the unique number is logged in the SIM.

Operator Specific Emergency Number – like "112" or E911 these numbers (5) are programmed into the SIM

Short Message System Center Number or SMSC number – the number used to sent text messages

Service Providers Name or SPN – the telecommunications service providers name and ID

Service Dialing Numbers or SDN – numbers associated with the service provider

(b)(7)e

Depending on storage capacity any type of data may be stored.

In Europe some subscribers store their medical records on their SIM card.

Any data!!!!!!!

Authentication Key or Ki – a 128-bit value used to authenticate the SIM to the mobile network. Assigned by the operator the Ki is contained on the service providers HLR.

GSM was designed from the start with security in mind. The SIM card aids in this security, making fraud on a GSM network unlikely.

Using a series of secret keys and algorithms thwarted cloning of GSM devices.

In GSM Call Handoff, or Call Handover is different in that it is mobile device assisted.

The mobile phone continually monitors base stations in vicinity measuring the strength in the MSC.

The six best prospects are sent back to the MSC who then determines when the handoff will be conducted.

GSM

Often described as a true Intelligence Network, GSM is called the first true wireless network because;

1. It has an open, distributed architecture
2. The separation of switching and service control functions
3. Full use of SS7 as the signaling infrastructure
4. Its clearly defined and specified interfaces
5. The nature of its IN structure

General Packet Radio Service (GPRS) and Enhanced Data Rates for Global Evolution (EDGE - CDMA), are 3G GSM based standards

GSM Adjunct Systems

GSM standards define that certain Adjunct or Secondary Systems work with GSM technology. Some of note are;

1. The Gateway MSC or GMSC – The purpose of which is to query the HLR and determine the location of the subscriber. Calls from another network i.e. PSTN will first go through the GMSC.

2. Short Message Service Center or SMSC – The node that stores and forwards short messages to and from the mobile station.

GSM Adjunct Systems

3. The Equipment Identity Register or EIR – identifies what equipment i.e. handsets are acceptable in a GSM Network

4. The Interworking Function or IWF – used for circuit switched data and fax services and is basically a modem bank

GSM v CDMA

There is a debate as to how long TDMA or IS-136 cell phones will be in existence. GSM and CDMA system now dominate the market.

Both work well on their own as well as with each other.

Some CDMA mobile units use a Removable – User Identity Module or R-UIM which is similar to a SIM. There are Dual R-UIM that allow for use in both GSM and CDMA units.

Both seem positioned to be in place for a period of time.

Integrated Digital Enhanced Network

Mobile Device Investigations Program

*i*DEN

1. Integrated Digital Enhanced Network Technology or *i*DEN

2. In 1987 Nextel was formed and began to change the Specialized Mobile Radio (SMR) market.

3. Originally called Fleet Call, Nextel purchased SMR licenses around the country to form a national network.

iDEN

1. The technology was developed by Motorola who provided trunked radio and cellular telephone.

2. In 1990 Nextel applied for and received permission from the FCC to create Enhanced Specialized Radio Service (ESMR) in six major markets.

3. Nextel chose as its air interface TDMA technology.

*i*DEN

1. Introduced in 1994, *i*DEN combined two-way radio, digital cellular, messages services with acknowledgment and wireless data into a single system.

2. *i*DEN uses Vector Summed Excited Linear Prediction (VSELP) vocoders, which compresses large segments of voice into smaller packets.

3. VSELP uses Forward Error Correction so packets do not become corrupted.

4. The use of VSELP and FEC allows for six audio paths on one RF channel.

*i*DEN

1. One of the unique feature is the Push-to-Talk or Direct Connect feature.

2. As of 2003 Direct Connect has been offered nationwide with no roaming.

3. This dispatch feature is managed by separating talk groups into fleets.

4. Each subscriber has an ID called the Fleet Member Identifier and identifies a user within a fleet.

*i*DEN

1. *i*DEN network work in much the same way and has the same equipment as other cellular networks, but are often identified differently.

2. The basic structure of an *i*DEN network is as follows:

iDEN

1. Enhanced Base Transceiver System – provides the radio frequency link between the network and the landline (PSTN).

2. Mobile Data Gateway – the interface between the Internet (WWW) during Data Packet activity.

3. Dispatch Application Processors – the call managers within the network.

*i*DEN

1. Metro packet Switch – a subsystem that connects the Enhanced Base Transceiver System to the Dispatch Application Processor and packet Duplicators.

2. Mobile Switching Center – GSM based mobile phone system that provides interconnect service.

*i*DEN

1. Digital Access Cross Connect Switch – connect point for T1/E1 lines between *i*DEN equipment and the external transport facilities.

2. Base Site Controller – manages the inter-connect between the Enhanced Base Transceiver System and other network devices

*i*DEN

Operations and Maintenance Center

Establishes, maintains and collects information about the network for presentation to the system operator.

*i*DEN

1. *i*DEN has another distinct feature in its service system. The existence of two sets of Home Location Register and Visitor Location Register.

2. One set operates and maintains information on the digital services provided as in authentication, services allowed, timing and the like.

*i*DEN

1. The second, referred to as the *i*-HLR and the *i*-VLR. This system keeps track of the Dispatch Call function or Push-to-Talk..

2. It should be importantly noted that when requesting information about activity conducted on the Call Dispatch side of the network you must be specific and request the proper data.

Page 189 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)e

*i*DEN

1. In 2004 Sprint and Nextel merged to form Sprint/Nextel.

2. On 2 November 2005, U.S. telecom carrier Sprint Nextel and four cable companies — Advanced/Newhouse Communications, Comcast, Cox Communications and Time Warner Cable — announced plans for a joint venture.

3. The partners will conduct joint marketing and work on integrating with each other's back-office systems to enable a "quadruple play" of voice, video, data and high-speed Internet services over cable and wireless devices.

*i*DEN

1. There is considerable discussions and speculation in the telecom community about the future of *i*DEN.

2. Because of its network nature Sprint/Nextel agreed to work with cities and others using the radio broadcast frequencies to address interference and other issues.

3. As of this date these concerns are being addressed and the outcome unclear.

Personal Communication Service

Mobile Device Investigations Program

Personal Communication Service

1. Personal Communication Service or PCS is referred to as 2G wireless service.

2. The FCC has defined PCS as radio communication that encompasses mobile and fixed communication to individuals and businesses that can be integrated with a variety of competing networks.

Personal Communication Service

PCS refers to integrated networks as the ability to connect to PSTN, WiFi and Worldwide Interoperability for Microwave Access (WiMax) systems.

This can be anything from point to point to full cellular access.

Personal Communication Service

Some other ways to define the mobility of PCS networks;

1. Personal Mobility - the ability of users to access any telecom service at any terminal based on personal identifiers, the networks ability and users profile

2. Terminal Mobility – the wireless subscriber units ability to access services from different locations while in motions

Personal Communication Service

1. Service Mobility – the use of vertical features provided by landlines, users at remote locations or while in motion.

2. PCS refers to services that are user specific as opposed to location specific.

3. PCS is referred to as follow me services.

Personal Communication Service

1. PCS was the first wireless network from its inception. Upon obtaining licenses PCS carriers were allowed to choose their air interface, thus we have TDMA, CDMA and GSM carriers.

2. PCS uses the same type of equipment that cellular services use with the difference being that more PCS base stations are need to cover the same geographic area.

Personal Communication Service

1. There are two types of PCS services; Narrowband and Broadband PCS.

2. Narrowband, using the 3MHz radio spectrum was used primarily for data transmissions.

3. These services were paging an short message systems.

Personal Communication Service

1. Broadband PCS is used for multimedia transmissions such as voice, data. Internet, SMS, image and in the future full motion video.

2. This obviously requires more channel capacity and is set aside on the 140 MHz radio spectrum.

Personal Communication Service

1. The major carriers include AT & T/Cingular, Verizon Wireless, T-Mobile, Sprint PCS (Nextel), Alltel Mobile and U.S. Cellular.

2. There are hundreds of regional PCS Carriers that can be found at http://www.wirelessadvisor.com/resources/wireless-carriers-a-b

Personal Communication Service

1. Only Sprint uses PCS as the primary technology
2. All other major carriers provide PCS as a secondary service.

   - For example, if an Alltel user can not find a CDMA tower (or, all channels are taken), the system will automatically and seamlessly interface with a PCS tower.