CELL-PHONE TECHNOLOGY

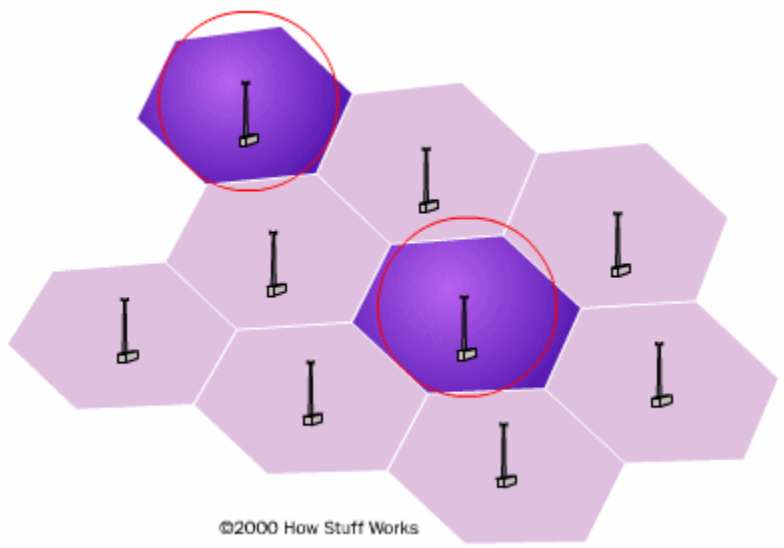
Wireless phones which receive their signals from towers. A cell is typically the area (several miles) around a tower in which a signal can be received.

Cell phones provide an incredible array of functions. Depending on the cell-phone model, you can:

- Store contact information
- Make task or to-do lists
- Keep track of appointments and set reminders
- Use the built-in calculator for simple math
- Send or receive e-mail
- Get information (news, entertainment, stock quotes) from the internet
- Play games
- Watch TV
- Send text messages
- Integrate other devices such as PDAs, MP3 players and GPS receivers

A cell phone is a **full-duplex** device. That means that you use one frequency for talking and a second, separate frequency for listening. Both people on the call can talk at once.

Division of a city into small **cells** allows extensive **frequency reuse** across a city, so that millions of people can use cell phones simultaneously. Cell phones operate within **cells**, and they can switch cells as they move around. Cells give cell phones incredible range. Someone using a cell phone can drive hundreds of miles and maintain a conversation the entire time because of the cellular approach. Each cell has a **base station** that consists of a tower and a small building containing the radio equipment.



A single cell in an analog cell-phone system uses one-seventh of the available duplex voice channels. That is, each cell is using one-seventh of the available channels so it has a unique set of frequencies and there are no collisions:

- A cell-phone carrier typically gets **832 radio frequencies** to use in a city.
- Each cell phone uses two frequencies per call -- a duplex channel -- so there are typically **395 voice channels** per carrier. (The other 42 frequencies are used for control channels)

Therefore, each cell has about **56 voice channels** available. In other words, in any cell, 56 people can be talking on their cell phone at one time. Analog cellular systems are considered first-generation mobile technology, or **1G**. With digital transmission methods (2G), the number of available channels increases. For example, a **TDMA-based** digital system (more on TDMA later) can carry three times as many calls as an analog system, so each cell has about 168 channels available.

Cell phones have **low-power transmitters** in them. Many cell phones have two signal strengths: 0.6 watts and 3 watts. The base station is also transmitting at low power. Low-power transmitters have two advantages:

- The **transmissions** of a base station and the phones within its cell do not make it very far outside that cell. Therefore, 2 different cells can **reuse the same 56 frequencies**. Hence, the same frequencies can be reused extensively across the city.
- The **power consumption** of the cell phone, which is normally battery-operated, is relatively low. Low power means small batteries, and this is what has made handheld cellular phones possible.

The cellular approach requires a large number of base stations in a city of any size. A typical large city can have hundreds of towers. But because so many people are using cell phones, costs remain low per user. Each carrier in each city also runs one central office called the **Mobile Telephone Switching Office** (MTSO). This office handles all of the phone connections to the normal land-based phone system, and controls all of the base stations in the region.

All cell phones have special **codes** associated with them. These codes are used to identify the phone, the phone's owner and the service provider. The various Cell Phone Codes used are as follows:

1. **Electronic Serial Number (ESN) :** It is a unique 32-digit number programmed into the phone when it is manufactured.
2. **Mobile Identification Number (MIN) :** A 10-digit number derived from the phones number
3. **System Identification Code (SID) :** A unique 5-digit number that is assigned to each carrier by the Federal Communications Commission (FCC).

ESN is a permanent part of the phone while both MIN and SID codes are programmed into the phone when a service plan is purchased and the phone is activated.

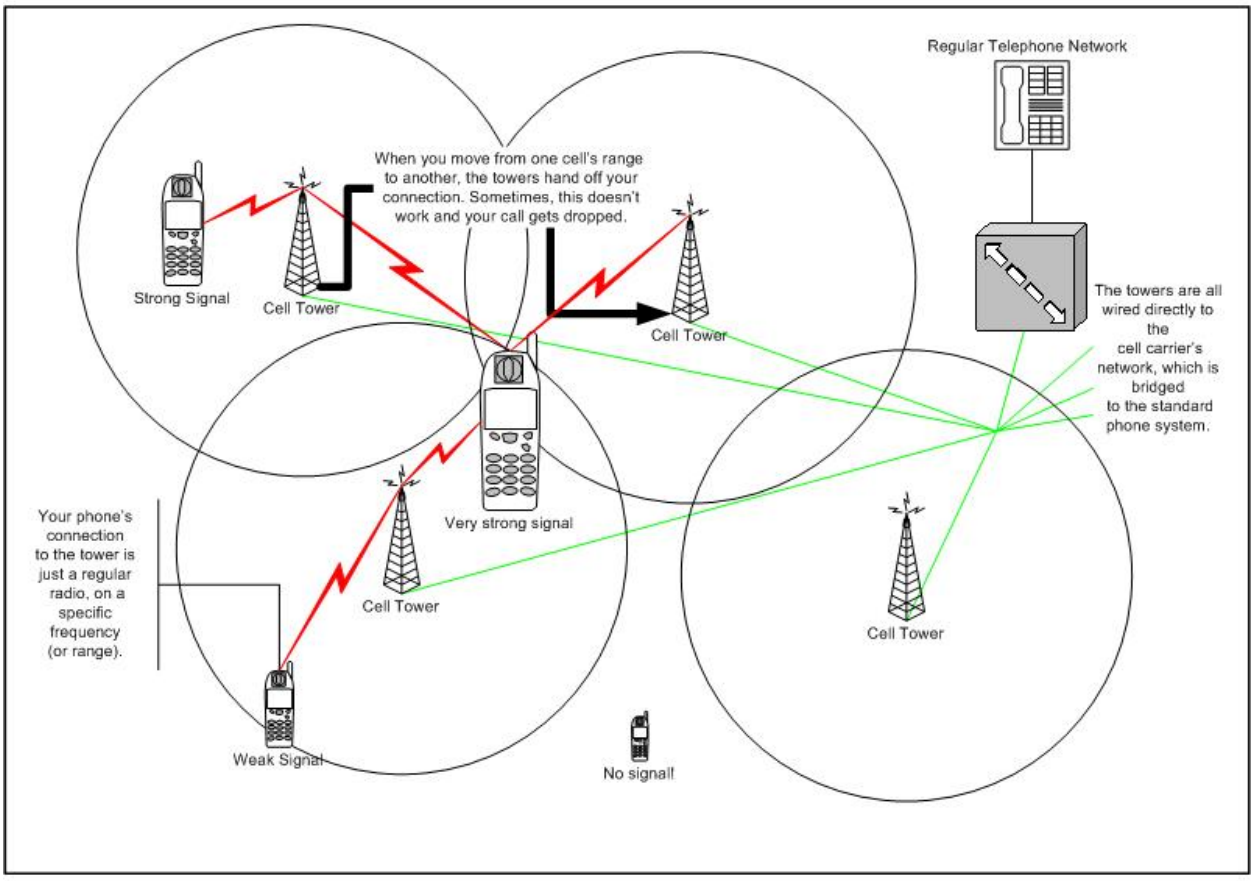
Some of the necessary terminologies for cell-phone connection are described:

1. **Mobile Telephone Switching Office (MTSO) :** The switching office that all base station cell sites connect to. It is a sophisticated computer that monitors all cellular calls, keeps track of the location of all cellular-equipped vehicles traveling in the system, arranges hand-offs, keeps track of billing information, etc. The MTSO in turn interfaces to the PSTN by connection to a Control Office.
2. **Public Switched Telephone Network (PSTN) :** It is the network of the world's public circuit-switched telephone networks, in much the same way that the Internet is the network of the world's public IP-based packet-switched networks. Originally a network of fixed-line analogue telephone systems, the PSTN is now almost entirely digital, and now includes mobile as well as fixed telephones.
3.

If you have a cell phone, you turn it on and someone tries to call you. Here is what happens to the call:

- When you first power up the phone, it listens for an **SID** on the **control channel**. The control channel is a special frequency that the phone and base station use to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, it knows it is **out of range** and displays a "no service" message.
- When it receives the SID, the phone **compares it** to the SID programmed into the phone. If the SIDs match, the phone knows that the cell it is communicating with is part of its **home** system.
- Along with the SID, the phone also transmits a **registration request**, and the MTSO keeps track of your phone's location in a database -- this way, the MTSO knows which cell you are in when it wants to ring your phone.
- The **MTSO** gets the call, and it tries to **find you**. It looks in its database to see which cell you are in.
- The MTSO **picks a frequency pair** that your phone will use in that cell to take the call.
- The MTSO communicates with your phone over the **control channel** to tell it which frequencies to use, and once your phone and the tower switch on those frequencies, the call is **connected**. Now, you are talking by two-way radio to a friend.
- As you move toward the edge of your cell, your cell's **base station** notes that your **signal strength** is diminishing. Meanwhile, the base station in the cell you are moving toward

(which is listening and measuring signal strength on all frequencies, not just its own one-seventh) sees your phone's signal strength increasing. The two base stations coordinate with each other through the MTSO, and at some point, your phone gets a signal on a control channel telling it to change frequencies. This **hand off** switches your phone to the new cell.



If you're on the phone and you move from one cell to another -- but the cell you move into is covered by another service provider, not yours. Instead of dropping the call, it'll actually be handed off to the other service provider.

If the SID on the control channel does not match the SID programmed into your phone, then the phone knows it is **roaming**. The MTSO of the cell that you are roaming in contacts the MTSO of your home system, which then checks its database to **confirm** that the SID of the phone you are using is valid. Your home system **verifies** your phone to the local MTSO, which then tracks your phone as you move through its cells. All of this happens within seconds.

On most phones, the word "roam" will come up on your phone's screen when you leave your provider's coverage area and enter another's. If you want to roam internationally, you'll need a

phone that will work both at home and abroad. Different countries use different cellular access technologies.

ANALOG CELL-PHONES (FIRST GENERATION)

In 1983, the analog cell-phone standard called **AMPS** (Advanced Mobile Phone System) was approved by the FCC and first used in Chicago. AMPS uses a range of frequencies between 824 megahertz (MHz) and 894 MHz for analog cell phones. In order to encourage competition and keep prices low, the U. S. government required the presence of two **carriers** in every market, known as A and B carriers. One of the carriers was normally the **local-exchange carrier** (LEC), a fancy way of saying the local phone company.

Carriers A and B are each assigned **832 frequencies**: 790 for voice and 42 for data. A pair of frequencies (one for transmit and one for receive) is used to create one **channel**. The frequencies used in analog voice channels are typically **30 kHz** wide -- 30 kHz was chosen as the standard size because it gives you voice quality comparable to a wired telephone.

The transmit and receive frequencies of each voice channel are separated by **45 MHz** to keep them from interfering with each other. Each carrier has 395 voice channels, as well as 21 data channels to use for housekeeping activities like registration and paging.

A version of AMPS known as **Narrowband Advanced Mobile Phone Service** (NAMPS) incorporates some digital technology to allow the system to carry about **three times as many calls** as the original version. Even though it uses digital technology, it is still considered analog. AMPS and NAMPS only operate in the 800-MHz band and do not offer many of the features common in digital cellular service, such as e-mail and Web browsing.

DIGITAL CELL-PHONES (SECOND GENERATION)

They use the same radio technology as analog phones, but they use it in a different way. Analog systems do not fully utilize the signal between the phone and the cellular network -- analog signals cannot be compressed and manipulated as easily as a true digital signal. Digital phones convert your voice into binary information (1s and 0s) and then compress it. This **compression** allows between three and 10 digital cell-phone calls to occupy the space of a *single* analog call.

Many digital cellular systems rely on **frequency-shift keying** (FSK) to send data back and forth over AMPS. FSK uses **two frequencies**, one for 1s and the other for 0s, **alternating** rapidly between the two to send digital information between the cell tower and the phone. Clever modulation and encoding schemes are required to convert the analog information to digital, compress it and convert it back again while maintaining an acceptable level of voice quality. Hence, digital cell phones have to contain a lot of processing power.

INSIDE A CELL-PHONE

A basic digital cell phone contains just a few individual parts:

- A circuit board containing the brains of the phone
- An antenna
- An Liquid Crystal Display (LCD) screen
- A keyboard
- A microphone
- A speaker
- A battery

The circuit board is the heart of the system and contains several chips. The analog-to-digital and digital-to-analog conversion chips translate the outgoing audio signal from analog to digital and the incoming signal from digital back to analog. The digital signal processor (DSP) is a highly customized processor designed to perform signal-manipulation calculations at high speed. The microprocessor handles all the functions for the keyboard and display, deals with command and control signaling with the base station and also coordinates the rest of the functions on the board.The Read Only Memory (ROM) and Flash Memory chips provide storage for the phone's operating system and customizable features, such as the phone directory. The Radio Frequency (RF) and power section handles power management and recharging, and also deals with the hundreds of FM channels. Finally, the RF amplifiers handle signals traveling to and from the antenna.

The display has grown considerably in size as the number of features in cell phones have increased. Most current phones offer built-in phone directories, calculators and games. And many of the phones incorporate some type of PDA or **Web browser**. Some phones store certain information, such as the SID and MIN codes, in internal Flash memory, while others use external cards. Cell phones have tiny speakers and microphones.

CELL-PHONE TOWER

A cell-phone tower is typically a steel pole or lattice structure that rises hundreds of feet into the air. The box houses the **radio transmitters and receivers** that let the tower communicate with the phones. The radios transmitters and receivers connect with the antennae on the tower through a set of thick cables. The tower and all of the cables and equipment at the base of the tower are heavily **grounded**.

HOW VIBRATOR WORKS IN CELLPHONE

If you have a cell phone or a pager, then you know that having it ring in the middle of a movie or performance is enough to get you killed in some cities. Vibrating devices that quietly replace the ringer are therefore life-saving devices that are an important part of urban survival!

Figure below shows the inside of a small toy which vibrates heavily similar to a cellphone device.

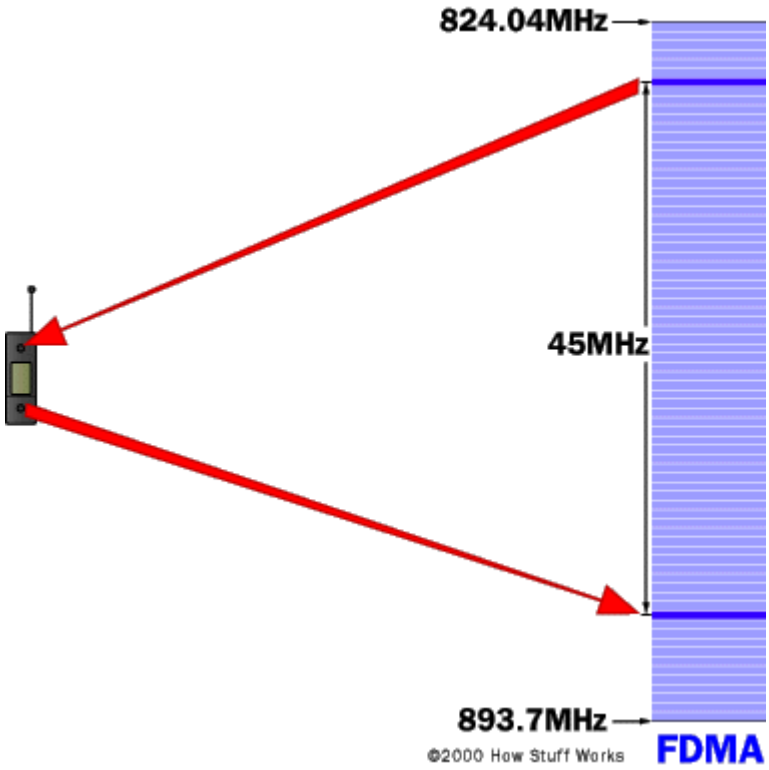
Inside the control unit is a small DC motor which drives the gear. Attached to the gear, there is a small weight. This weight is about the size of a stack of 5 U.S. nickels, and it is mounted off-center on the gear. When the motor spins the gear/weight combination (at 100 to 150 RPM), the off-center mounting causes a strong vibration. Inside a cell phone or pager there is the same sort of mechanism in a much smaller version.

COMMUNICATION TECHNOLOGIES IN SECOND GENERATION CELL-PHONES

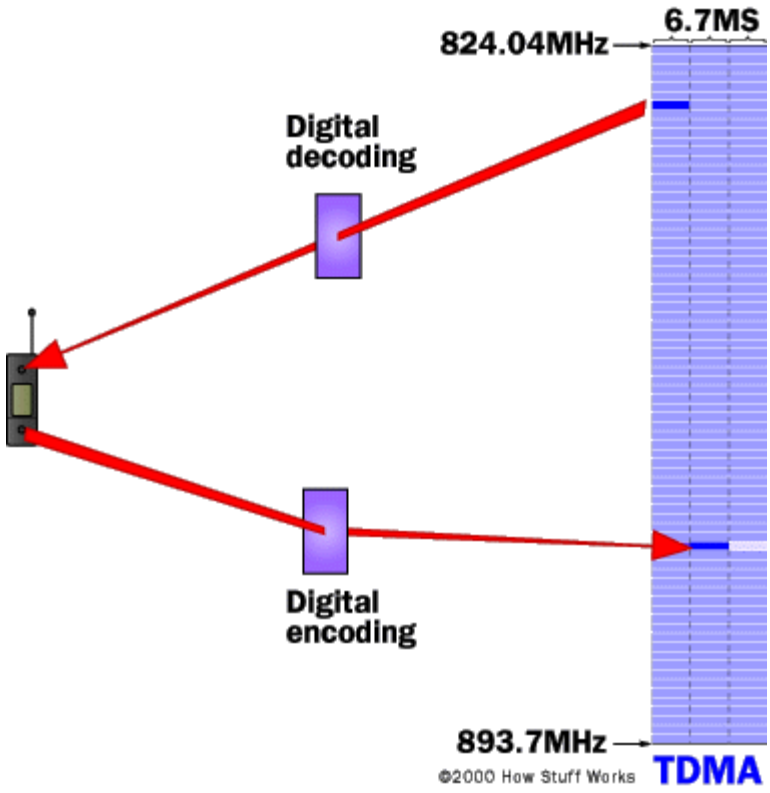
There are four common technologies used by 2G cell-phone networks for transmitting information:

1. **Frequency Division Multiple Access (FDMA) :** FDMA separates the spectrum into distinct voice channels by splitting it into **uniform chunks of bandwidth**. Each call sends its signal at a different frequency within the available band. FDMA is used mainly

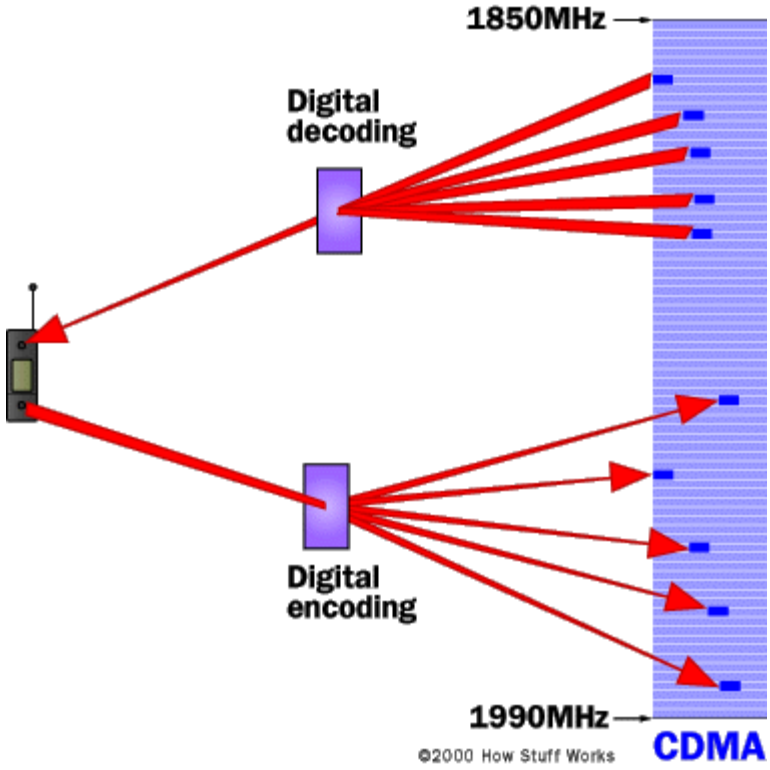
for **analog transmission**.



2. **Time Division Multiple Access (TDMA) :** TDMA is the access method used by the Electronics Industry Alliance and the Telecommunications Industry Association for **Interim Standard 54** (IS-54) and **Interim Standard 136** (IS-136). Using TDMA, a **narrow band** that is 30 kHz wide and 6.7 milliseconds long is split time-wise into **three time slots**. Each conversation gets the signal for one-third of the time. This is possible because voice data that has been converted to digital information is compressed so that it takes up significantly less transmission space. Therefore, TDMA has **three times the capacity** of an analog system using the same number of channels. TDMA systems operate in either the **800-MHz** (IS-54) or **1900-MHz** (IS-136) frequency bands.



3. **Code Division Multiple Access (CDMA) : CDMA** takes an entirely different approach from TDMA. CDMA, after digitizing data, **spreads it out** over the entire available bandwidth. Multiple calls are **overlaid** on each other on the channel, with each assigned a **unique sequence code**. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over a number of the discrete frequencies available for use at any time in the specified range.



4. **Global System for Mobile Communication (GSM) : GSM** implements TDMA in a somewhat different and incompatible way from IS-136. GSM systems use encryption to make phone calls more secure. GSM operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 850-MHz and 1900-MHz band in the United States. It is used in digital cellular and **PCS (Personal Communication Services)-based** systems. GSM is also the basis for **Integrated Digital Enhanced Network** (IDEN), a popular system introduced by Motorola and used by Nextel.

PCS was designed from the ground up for greater user mobility. PCS has **smaller cells** and therefore requires a **larger number of antennas** to cover a geographic area. PCS phones use frequencies between 1.85 and 1.99 GHz (1850 MHz to 1990 MHz).

Technically, cellular systems in the United States operate in the 824-MHz to 894-MHz frequency bands; PCS operates in the **1850-MHz to 1990-MHz** bands. And while it is based on TDMA, PCS has **200-kHz channel spacing** and **eight time slots** instead of the typical 30-kHz channel spacing and three time slots found in digital cellular.

GSM is the international standard in Europe, Australia and much of Asia and Africa. In covered areas, cell-phone users can buy one phone that will work anywhere where the standard is supported. To connect to the specific service providers in these different countries, GSM users simply switch **subscriber identification module** (**SIM**) cards. SIM cards are small removable disks that slip in and out of GSM cell phones. They store all the connection data and identification numbers you need to access a particular wireless service

provider.

The 850MHz/1900-MHz GSM phones used in the United States are **not compatible** with the international system. If you live in the United States and need to have cell-phone access when you're overseas, you can either buy a tri-band or quad-band GSM phone and use it both at home and when traveling or just buy a GSM 900MHz/1800MHz cell phone for traveling.

MULTI-BAND VS. MULTI-MODE CELL-PHONES

1. **Multiple band** - A phone that has multiple-band capability can **switch frequencies**. For example, a dual-band TDMA phone could use TDMA services in either an 800-MHz or a 1900-MHz system. A quad-band GSM phone could use GSM service in the 850-MHz, 900-MHz, 1800-MHz or 1900-MHz band.
2. **Multiple mode** - In cell phones, "mode" refers to the **type of transmission technology** used. So, a phone that supported AMPS and TDMA could switch back and forth as needed. It's important that one of the modes is AMPS -- this gives you analog service if you are in an area that doesn't have digital support.
3. **Multiple band/Multiple mode** - It allows you to switch between frequency bands and transmission modes as needed.

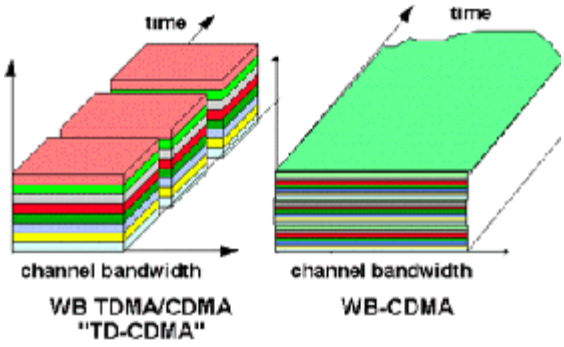
Changing bands or modes is done automatically by phones that support these options. Usually the phone will have a **default option** set, such as 1900-MHz TDMA, and will try to connect at that frequency with that technology first. If it supports dual bands, it will switch to 800 MHz if it cannot connect at 1900 MHz. And if the phone supports more than one mode, it will try the digital mode(s) first, then switch to analog.

You can find both **dual-mode** and **tri-mode** phones. The term "tri-mode" can be deceptive. It may mean that the phone supports two digital technologies, such as CDMA and TDMA, as well as analog. In that case, it is a true tri-mode phone. But it can also mean that it supports one digital technology in two bands and also offers analog support.

COMMUNICATION TECHNOLOGIES IN THIRD GENERATION CELL-PHONES

3G technology is intended for the true multimedia cell phone -- typically called smartphones -- and features increased bandwidth and transfer rates to accommodate Web-based applications and phone-based audio and video files. 3G comprises several cellular access technologies as follows:

1. **CDMA2000 :** based on 2-G Code Division Multiple Access
2. **Wideband Code Division Multiple Access-UMTS (WCDMA-UMTS) :** In W-CDMA interface different users can simultaneously transmit at different data rates and data rates can even vary in time. UMTS networks need to support all current second generation services and numerous new applications and services.



3. **Time Division Synchronous Code Division Multiple Access (TD-SCDMA) :** TD-SCDMA uses the Time Division Duplex (TDD) mode, which transmits uplink traffic (traffic from the mobile terminal to the base station) and downlink traffic (traffic from the base station to the terminal) in the same frame in different time slots. That means that the uplink and downlink spectrum is assigned flexibly, dependent on the type of information being transmitted. When asymmetrical data like e-mail and internet are transmitted from the base station, more time slots are used for downlink than for uplink. A symmetrical split in the uplink and downlink takes place with symmetrical services like telephony.

PROBLEMS WITH CELL-PHONES

1. Generally, non-repairable internal **corrosion** of parts results if you get the phone **wet** or use wet hands to push the buttons. Consider a protective case. If the phone does get wet, be sure it is totally dry before you switch it on so you can try to avoid damaging internal parts.
2. Extreme **heat** in a car can damage the battery or the cell-phone electronics. Extreme cold may cause a momentary loss of the screen display.
3. Analog cell phones suffer from a problem known as "**cloning**." A phone is "cloned" when someone steals its ID numbers and is able to make fraudulent calls on the owner's account. When your phone makes a call, it transmits the ESN and MIN to the network at the beginning of the call. The MIN/ESN pair is a unique tag for your phone -- this is how the phone company knows who to bill for the call. When your phone transmits its MIN/ESN pair, it is possible for nefarious sorts to listen (with a scanner) and capture the pair. With the right equipment, it is fairly easy to modify another phone so that it contains your MIN/ESN pair, which allows the nefarious individual to make calls on your account.

ELECTROMAGNETIC INTERFERENCE

Most of us experience **electromagnetic interference** on a fairly regular basis. For example:

- If you put your cell phone down on your desk near the computer, you can hear loud static in your computer's speakers every time the phone and the tower handshake. In the same way, your car's stereo produces loud static whenever you make a call on your cell phone.
- When you dial a number on your home's wireless phone, you can hear the number being dialed through the baby monitor.
- It is not uncommon for a truck to go by and have its CB radio overwhelm the FM station you am listening to.
- Most of us have come across motors that cause radio or TV static.

None of these things, technically, should be happening. For example, a truck's CB radio is not transmitting on the FM radio bands, so your radio should never hear CB signals. However, all transmitters have some tendency to transmit at lower power on harmonic side bands, and this is how the FM radio picks up the CB. The same thing holds true for the wireless phone crossing over to the baby monitor. In the case of the cell phone affecting the computer's speakers, the wire to each speaker is acting like an antenna, and it picks up side bands in the audible range.

These are not dire problems -- they are just a nuisance. But notice how common they are. In an airplane, the same phenomena can cause big trouble.

An **airplane** contains a number of radios for a variety of tasks. There is a radio that the pilots use to talk to ground control and air traffic control (ATC). There is another radio that the plane uses to disclose its position to ATC computers. There are radar units used for guidance and weather detection, and so on. All of these radios are transmitting and receiving information at specific frequencies. If someone were to turn on a cell phone, the cell phone would transmit with a great deal of power (up to 3 watts). If it happens to create interference that overlaps with radio frequencies the plane is using, then messages between people or computers may be garbled. If one of the wires in the plane has damaged shielding, there is some possibility of the wire picking up the phone's signals just like my computer's speakers do. That could create faulty messages between pieces of equipment within the plane.

Many **hospitals** have installed wireless networks for equipment networking. For example, in case of a heart monitor, the black antenna sticking out of the top of the monitor connects it back to the nursing station via a wireless network. If you use your cell phone and it creates interference, it can disrupt the transmissions between different pieces of equipment. That is true even if you simply have the cell phone turned on -- the cell phone and tower handshake with each other every couple of minutes, and your phone sends a burst of data during each handshake.

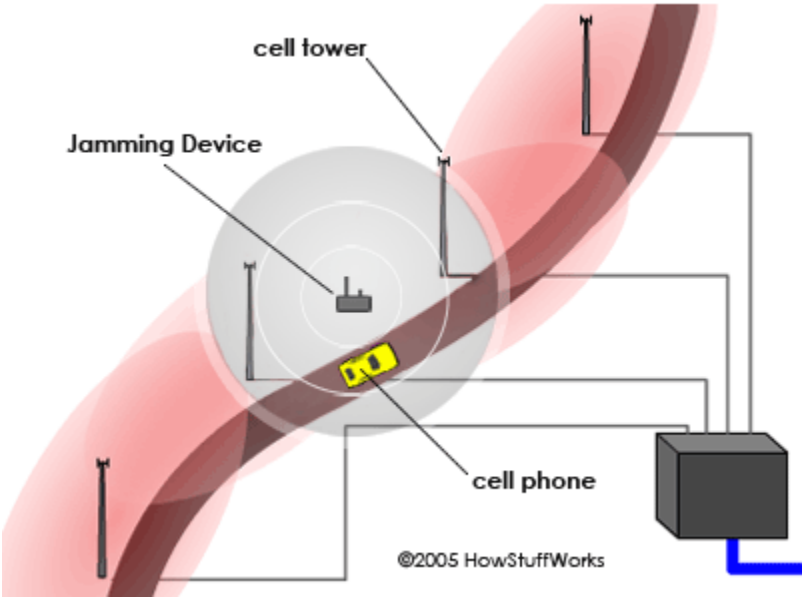
The prohibition on laptops and CD players during takeoff and landing is addressing the same issue, but the concerns here might fall into the category of "better safe than sorry." A poorly shielded laptop could transmit a fair amount of radio energy at its operating frequency, and this could, theoretically, create a problem.

CELL PHONE JAMMERS

It's great to be able to call anyone at anytime. Unfortunately, restaurants, movie theaters, concerts, shopping malls and churches all suffer from the spread of cell phones because not all cell-phone users know when to stop talking. Who hasn't seethed through one side of a conversation about an incredibly personal situation as the talker shares intimate details with his friend as well as everyone else in the area?

Disrupting a cell phone is the same as jamming any other type of radio communciation. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower.

A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the tower. It's a called a **denial-of-service attack**. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device.



Jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone.

Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while

sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once, and others can be tuned to specific frequencies.

Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 1900-MHz (sometimes referred to as 1.9-GHz) band in the United States. Jammers can broadcast on any frequency and are effective against AMPS, CDMA, TDMA, GSM, PCS, DCS,iDEN and Nextel systems. Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming.

The actual range of the jammer depends on its power and the local environment, which may include hills or walls of a building that block the jamming signal. Low-powered jammers block calls in a range of about 30 feet (9 m). Higher-powered units create a cell-free zone as large as a football field. Units used by law enforcement can shut down service up to 1 mile (1.6 km) from the device.

CELL-PHONE JAMMER

Electronically speaking, cell-phone jammers are very basic devices. The simplest just have an on/off switch and a light that indicates it's on. More complex devices have switches to activate jamming at different frequencies. Components of a jammer include:

1. **Antenna :** Every jamming device has an antenna to send the signal. Some are contained within an electrical cabinet. On stronger devices, antennas are external to provide longer range and may be tuned for individual frequencies.
2. **Circuitry :** The main electronic components of a jammer are

   a) **Voltage-controlled oscillator** - Generates the radio signal that will interfere with the cell phone signa

   b) **Tuning circuit** - Controls the frequency at which the jammer broadcasts its signal by sending a particular voltage to the oscillator

   c) **Noise generator** - Produces random electronic output in a specified frequency range to jam the cell-phone network signal (part of the tuning circuit)

   d) **RF amplification** (**gain stage**) - Boosts the power of the radio frequency output to high enough levels to jam a signal

1. **Power Supply :** Smaller jamming devices are battery operated. Some look like cell phone and use cell-phone batteries. Stronger devices can be plugged into a standard outlet or wired into a vehicle's electrical system.

During a hostage situation, police can control when and where a captor can make a phone call. Police can block phone calls during a drug raid so suspects can't communicate outside the area. Cell-phone jammers can be used in areas where radio transmissions are dangerous, (areas with a potentially explosive atmosphere), such as chemical storage facilities or grain elevators. The TRJ-89 jammer from Antenna System & Supplies Inc. carries its own electrical generator and can block cellular communications in a 5-mile (8-km) radius.

Corporations use jammers to stop corporate espionage by blocking voice transmissions and photo transmissions from camera phones. On the more questionable end of the legitimacy spectrum, there are rumors that hotel chains install jammers to block guests' cell-phone usage and force them to use in-room phones at high rates.

CELL-PHONE RADIATIONS

There's a lot of talk in the news these days about whether or not cell phones emit enough radiation to cause adverse health effects. The concern is that cell phones are often placed close to or against the head during use, which puts the radiation in direct contact with the tissue in the head. There's evidence supporting both sides of the argument.

When talking on a cell phone, a **transmitter** takes the sound of your voice and encodes it onto a **continuous sine wave**.A sine wave is just a type of continuously varying wave that radiates out from the antenna and fluctuates evenly through space. Sine waves are measured in terms of **frequency**. Once the encoded sound has been placed on the sine wave, the transmitter sends the signal to the antenna, which then sends the signal out.

Cell phones have low-power transmitters in them. A handheld cell phone operates on about **0.75 to 1 watt** of power. The position of a transmitter inside a phone varies depending on the manufacturer, but it is usually in close proximity to the phone's antenna. The radio waves that send the encoded signal are made up of **electromagnetic radiation** propagated by the antenna. The function of an antenna in any radio transmitter is to launch the radio waves into space; in the case of cell phones, these waves are picked up by a **receiver** in the cell-phone tower.

When talking on a cell phone, most users place the phone against the head. In this position, there is a good chance that some of the radiation will be absorbed by human tissue. All cell phones emit some amount of electromagnetic radiation. Given the close proximity of the phone to the head, it is possible for the radiation to cause some sort of harm to the user. What is being debated in the scientific and political arenas is just how much radiation is considered unsafe, and if there are any potential long-term effects of cell-phone radiation exposure.

There are two types of electromagnetic radiation:

1. **Ionizing radiation** - This type of radiation contains enough electromagnetic energy to strip atoms and molecules from the tissue and alter chemical reactions in the body. Gamma rays and X-rays are two forms of ionizing radiation. We know they cause damage, which is why we wear a lead vest when X-rays are taken of our bodies.
2. **Non-ionizing radiation** - Non-ionizing radiation is typically **safe**. It causes some heating effect, but usually not enough to cause any type of long-term damage to tissue. Radio-frequency energy, visible light and microwave radiation are considered non-ionizing.

On its Web site, the FDA states that "the available scientific evidence does not demonstrate any adverse health effects associated with the use of mobile phones." However, that doesn't mean that the potential for harm doesn't exist. Radiation can damage human tissue if it is exposed to high levels of RF radiation, according to the FCC. RF radiation has the ability to **heat** human tissue, much like the way microwave ovens heat food. Damage to tissue can be caused by exposure to RF radiation because the body is not equipped to dissipate excessive amounts of heat. The **eyes** are particularly vulnerable due to the lack of blood flow in that area.

The added concern with non-ionizing radiation, the type of radiation associated with cell phones, is that it could have **long-term effects**. Although it may not immediately cause damage to tissue, scientists are still unsure about whether prolonged exposure could create problems. This is an especially sensitive issue today, because more people are using cell phones than ever before.

Here are a few illnesses and ailments that have potential links to cell-phone radiation:

1. Cancer
2. Brain Tumers
3. Alzheimers
4. Parkinsons
5. Fatigue
6. Headaches

Studies have only muddled the issue. As with most controversial topics, different studies have different results. Some say that cell phones are linked to higher occurrences of cancer and other ailments, while other studies report that cell-phone users have no higher rate of cancer than the population as a whole. No study to date has provided conclusive evidence that cell phones can cause any of these illnesses. However, there are ongoing studies that are examining the issue more closely.

If you are worried about the potential hazards of cell-phone radiation, here are few ways to reduce your risk:

1. Use a hands-free headset
2. Use a phone that places the antenna as far away from you as possible.

3. Extend the antenna during use.
4. Limit calls inside buildings.
5. Use the phone in open spaces as often as possible.
6. Limit use by children.

CELL-PHONE VIRUSES

The first known cell-phone virus appeared in 2004 and didn't get very far. Cabir.A infected only a small number of Bluetooth-enabled phones and carried out no malicious action -- a group of malware developers created Cabir to prove it could be done. Their next step was to send it to anti-virus researchers, who began the process of developing a solution to a problem that promises to get a lot worse.

A cell-phone virus is basically the same thing as a computer virus -- an unwanted **executable file** that "infects" a device and then copies itself to other devices. But whereas a computer virus or worm spreads through e-mail attachments and Internet downloads, a cell-phone virus or worm spreads via Internet downloads, MMS (multimedia messaging service) attachments and bluetooth transfers. The most common type of cell-phone infection right now occurs when a cell phone downloads an infected file from a PC or the Internet, but **phone-to-phone viruses** are on the rise.

Current phone-to-phone viruses almost exclusively infect phones running the **Symbian** operating system. The large number of proprietary operating systems in the cell-phone world is one of the obstacles to mass infection. Cell-phone-virus writers have no Windows-level marketshare to target, so any virus will only affect a small percentage of phones.

Infected files usually show up **disguised** as applications like games, security patches, add-on functionalities and, of course, pornography and free stuff. Infected text messages sometimes steal the subject line from a message you've received from a friend, which of course increases the likelihood of your opening it -- but opening the message isn't enough to get infected. You have to choose to open the message attachment and agree to install the program, which is another obstacle to mass infection: To date, no reported phone-to-phone virus auto-installs. The installation obstacles and the methods of spreading limit the amount of damage the current generation of cell-phone virus can do.

Phones that can only make and receive calls are not at risk. Only smartphones with a Bluetooth connection and data capabilities can receive a cell-phone virus. These viruses spread primarily in three ways:

1. **Internet downloads** - The virus spreads the same way a traditional computer virus does. The user downloads an infected file to the phone by way of a PC or the phone's own Internet connection. This may include file-sharing downloads, applications available from add-on sites (such as ringtones or games) and false security patches posted on the Symbian Web site.

2. **Bluetooth wireless connection** - The virus spreads between phones by way of their Bluetooth connection. The user receives a virus via Bluetooth when the phone is in discoverable mode, meaning it can be seen by other Bluetooth-enabled phones. In this case, the virus spreads like an airborne illness.
3. **Multimedia Messaging Service** - The virus is an attachment to an MMS text message. As with computer viruses that arrive as e-mail attachments, the user must choose to open the attachment and then install it in order for the virus to infect the phone. Typically, a virus that spreads via MMS gets into the phone's contact list and sends itself to every phone number stored there.

In all of these transfer methods, the user has to agree at least once (and usually twice) to run the infected file. But cell-phone-virus writers get you to open and install their product the same way computer-virus writers do: The virus is typically disguised as a game, security patch or other desirable application.

The **Commwarrior virus** arrived on the scene in January 2005 and is the first cell-phone virus to effectively spread through an entire company via Bluetooth. It replicates by way of both Bluetooth and MMS. Once you receive and install the virus, it immediately starts looking for other Bluetooth phones in the vicinity to infect. At the same time, the virus sends infected MMS messages to every phone number in your address list. Commwarrior is probably one of the more effective viruses to date because it uses two methods to replicate itself.

The first known cell-phone virus, Cabir, is entirely innocuous. All it does is sit in the phone and try to spread itself. Other cell-phone viruses, however, are not as harmless.

A virus might access and/or delete all of the contact information and calendar entries in your phone. It might send an infected MMS message to every number in your phone book -- and MMS messages typically cost money to send, so you're actually paying to send a virus to all of your friends, family members and business associates. On the worst-case-scenario end, it might delete or lock up certain phone applications or crash your phone completely so it's useless. Some reported viruses and their vital statistics are listed below.

The best way to protect yourself from cell-phone viruses is the same way you protect yourself from computer viruses: Never open anything if you don't know what it is, haven't requested it or have any suspicions whatsoever that it's not what it claims to be. That said, even the most cautious person can still end up with an infected phone. Here are some steps you can take to decrease your chances of installing a virus:

1. **Turn off Bluetooth discoverable mode.** Set your phone to "hidden" so other phones can't detect it and send it the virus. You can do this on the Bluetooth options screen.
2. **Check security updates to learn about filenames you should keep an eye out for.** It's not fool-proof -- the Commwarrior program generates random names for the infected files it sends out, so users can't be warned not to open specific filenames -- but many viruses can be easily identified by the filenames they carry.

3. **Install some type of security software on your phone.** Numerous companies are developing security software for cell phones, some for free download, some for user purchase and some intended for cell-phone service providers. The software may simply detect and then remove the virus once it's received and installed, or it may protect your phone from getting certain viruses in the first place. Symbian has developed an anti-virus version of its operating system that only allows the phone's Bluetooth connection to accept secure files.

Future possibilities include viruses that bug phones -- so someone can see every number you call and listen to your conversations -- and viruses that steal financial information, which would be a serious issue if smartphones end up being used as payment devices. Ultimately, more connectivity means more exposure to viruses and faster spreading of infection. As smartphones become more common and more complex, so will the viruses that target them.