U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

OFFICE OF MISSION SUPPORT

TECHNICAL OPERATIONS DIVISION

LESSON PLAN

CELLULAR PHONE TECHOLOGIES

3260 **FEB/11**

~~**WARNING**~~

~~**This document is FOR OFFICIAL USE ONLY (FOUO)/LAW ENFORCEMENT SENSITIVE (LES). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid 'need-to-know' without prior authorization of an authorized Department of Homeland Security Official.**~~

~~**FOR OFFICIAL USE ONLY**~~

LAW ENFORCEMENT SENSITIVE

DEVELOPED BY: (MAR/09)

(b)(6) **nior Instructor, CFI (Team Leader)**
, Senior Instructor, CFI

REVIEWED BY: (JUL/09)

(b)(6) **Senior Instructor, Technical Operations Division (Team**

(b)(6) Program Specialist, Technical Operations Division

LP updated as follows:

Division Title changed from CFI to TOD, and FOUO/LES markings added.

There were no changes to the TPO or EPOs

REVISED BY: (FEB/11)

(b)(6) **Senior Instructor, TOD**
Program Specialist, TOD

Added FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE to lesson plan

TABLE OF CONTENTS

SYLLABUS

COURSE TITLE: **CELLULAR PHONE TECHNOLOGIES**

COURSE NUMBER: **3260**

COURSE DATE: **SEP/10**

LENGTH OF PRESENTATION:

LECTURE	LAB	P.E.	TOTAL	PROGRAM	OPTION
5			5	MDIP	

DESCRIPTION:

There is a large number of Cellular Service Providers (CSP) in the world today with more sure to come in the future. What allows these various CSPs to exist and interact are the various Cellular Phone Technologies. In this course we will examine the various cellular technologies and air interfaces to determine what evidence the Investigator can obtained from them.

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given data as it relates to the various types of cellular technologies and air interfaces the student will define the major cellular technologies and list the evidentiary artifacts to determine what evidence can be derived from them.

ENABLING PERFORMANCE OBJECTIVES (EPO):

EPO #1: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

EPO #2: Define Call Handoff and list the location where evidentiary artifacts are stored.

EPO #3: Define the Hexagon Grid and its importance to the Cellular Network.

EPO #4: List the five main components of a wireless network and their responsibilities.

EPO #5: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

EPO #6: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

EPO #7: List the administrative task of the Control Channel.

EPO #8: Define TDMA and list TDMAs advantages.

EPO #9: Define CDMA and list how its signals are spread.

EPO #10: Define GSM and list the four subsystems required for this standard.

EPO #11: Define SIM Card and the information that is stored there.

EPO #12: Define *i*DEN and list the two types of HLRs and VLRs.

EPO #13: Define PCS and list the two types of services provided by these wireless networks.

STUDENT SPECIAL REQUIREMENTS:

There are no special requirements.

METHOD OF EVALUATION:

Completion of the course.

INSTRUCTOR GUIDE

METHODOLOGIES:

1. Lecture with questions
2. Discussion

TRAINING AIDS/EQUIPMENT:

1. Instructor:
   a. Computer with Power Point and Projector
   b. Writing Surface
2. Student:
   None

INSTRUCTOR SPECIAL REQUIREMENTS:

Comprehensive and practical understanding of Cellular Technology and Air Interfaces.

OUTLINE OF INSTRUCTION

I. INTRODUCTION

A. RAPPORT AND OPENING STATEMENT

1. Cellular technology is relatively new, having inundating contemporary American (and world) culture within the past decade. However, with the flood of cell phones, law enforcement is confronted with new tools of criminal activity and, as well, new investigative tools.
2. Law enforcement largely ignorant of the tremendous investigative assets that accompanies cell phone technology. MDIP addresses that lack by presenting to the journey level law enforcement officer an understanding of this new technology and its investigative benefits.
3. In order to fully understand and apply the investigative tools provided by cellular technology, the officer needs to have a basic understanding of the technology. While this course does not provide an exhaustive discussion of the overwhelming technology involved in cellular communications, it does provide enough material information so that law enforcement officers can understand and apply the technology to their benefit.

B. LESSON PLAN OVERVIEW

1. Terminal performance objective (TPO)

   Given data as it relates to the various types of cellular technologies and air interfaces the student will define the major cellular technologies and list the evidentiary artifacts that can be derived from them.

2. ENABLING PERFORMANCE OBJECTIVES (EPO)

   a. EPO #1: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

   b. EPO #2: Define Call Handoff and list the locations where evidentiary artifacts are stored.

   c. EPO #3: As stated in this block of instruction define the Hexagon Grid and its importance to the Cellular Network.

   d. EPO #4: List the five main components of a wireless network and their responsibilities.

e. EPO #5: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

f. EPO #6: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

g. EPO #7: List the administrative task of the Control Channel.

h. EPO #8: Define TDMA and list TDMAs advantages.

i. EPO #9: Define CDMA and list how its signals are spread.

j. EPO #10: List the two criteria that must be met to qualify as Spread Spectrum technology.

k. EPO #11: Define GSM and list the four subsystems required for this standard.

l. EPO #12: Define SIM Card and the information that is stored there.

m. EPO #13: Define *i*DEN and list the two types of HLRs and VLRs.

n. EPO #14: Define PCS and list the two types of services provided by these wireless networks.

II. PRESENTATION

A. EPO #1: DEFINE FREQUENCY REUSE AND HOW THIS SYSTEM IS GEOGRAPHICALLY POSITIONED TO ENSURE ITS ABILITY TO OPERATE.

1. Cellular Technology enables mobile communication because they use of a complex two-way radio system between the mobile unit and the wireless network. It uses radio frequencies (radio channels) over and over again throughout a market with minimal interference, to serve a large number of simultaneous conversations. This concept is the central tenet to cellular design and is called frequency reuse.

2. Frequency Reuse and Planning is the act of repeatedly reusing radio frequencies over a geographical area. Most frequency reuse plans are produced in groups of seven cells.

   a. There are numerous seven cell frequency reuse groups in each cellular carrier's Metropolitan Statistical Area (MSA) or Rural Service Areas (RSA).

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

3.

4. (b)(7)e

5.

6. Consider your local radio station broadcast. As you travel father away from the radio base it weakens until you lose the signal.

   a. Now consider all the cars driving around you are listening are listening to different stations.

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

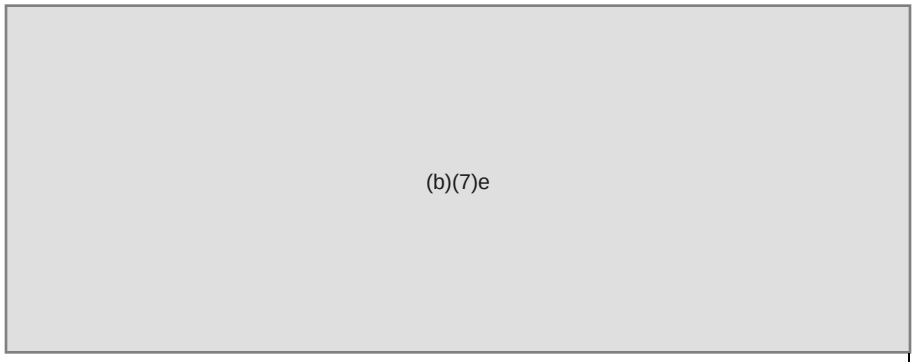
7. A key component in this system is the Distance to Reuse Ratio. The Distance to Reuse ratio defines how much geographical distance is required between cells in a cell system to avoid and limit interference.

   a. (b)(7)e

b.

c.

d.



NOTE: **Place notes to the instructor where appropriate for special guidance. This is an "outside border" with a 10% shading of gray. Shading does not have to be used but it helps if there is a border around the note to make it stand out and easy to read.**

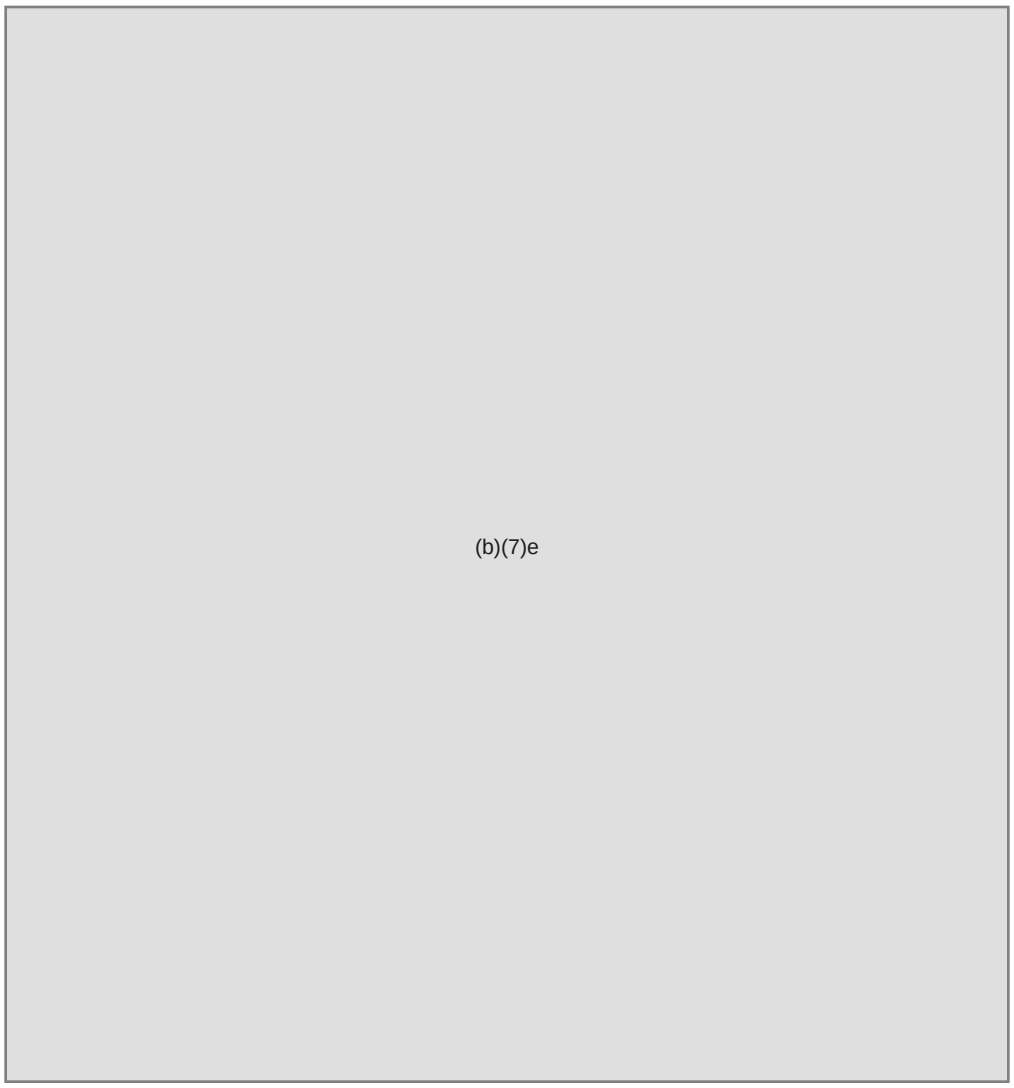
B. EPO #2: DEFINE CALL HANDOFF AND LIST THE LOCATION WHERE EVIDENTIARY ARTIFACTS ARE STORED.

1.

2.

3.

4.



(b)(7)e

C. EPO #3: AS STATED IN THIS BLOCK OF INSTRUCTION DEFINE THE HEXAGON GRID ITS IMPORTANCE TO THE CELLULAR NETWORK.

1.

2.

(b)(7)e

3.

D. EPO #4: LIST THE FIVE MAIN COMPONENTS OF A WIRELESS NETWORK AND THEIR RESPONSIBILITIES.

1. There are five main components to a wireless network. They are;
   a. The Mobile Unit
   b. The Cell Base Station
   c. The Backhaul or Fixed Network
   d. The Mobile Switching Center
   e. The interconnection to the Public Switched Telephone Network (PSTN)
2. The Mobile Unit

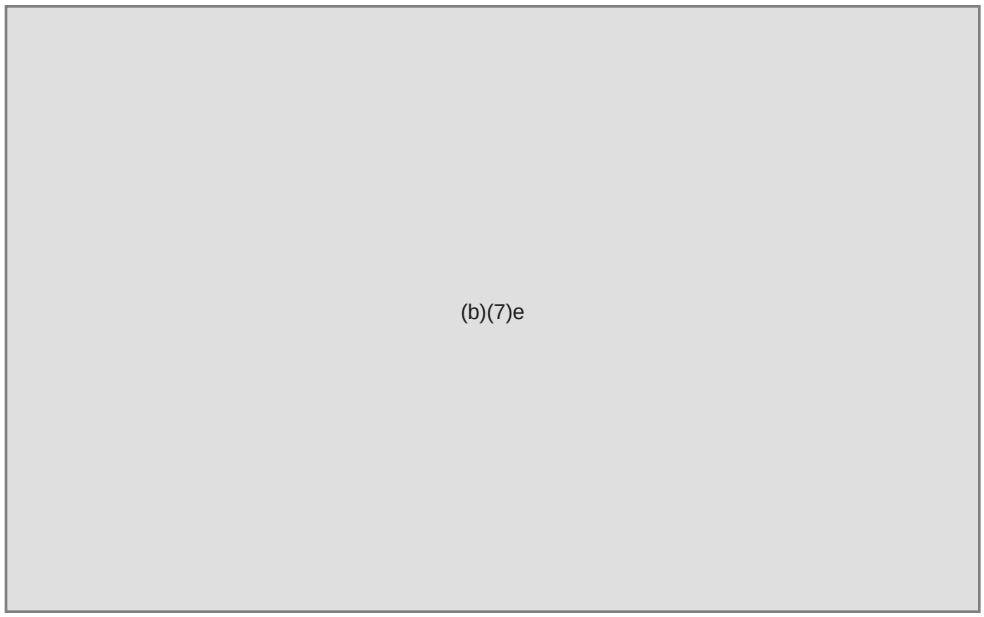
(b)(7)e

3. The Cell Base Station

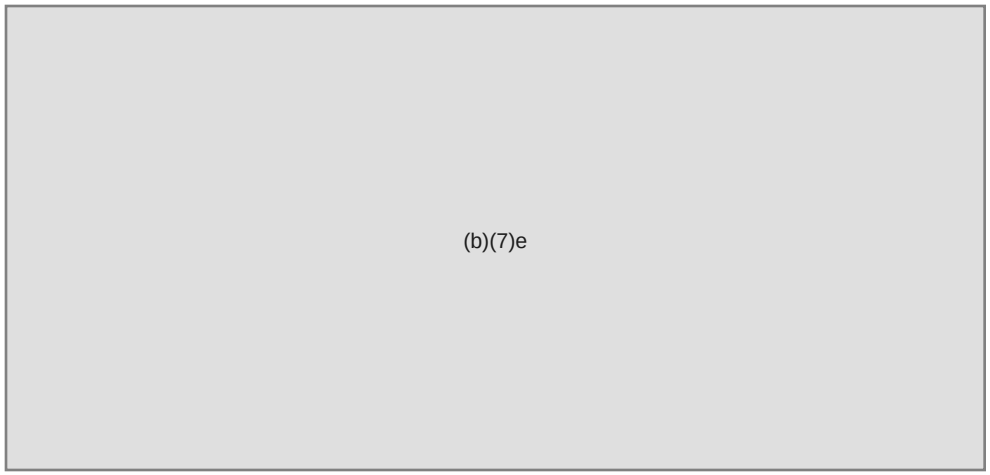
(b)(7)e

(b)(7)e

4. The Backhaul or Fixed Network – Base Station Controller



5. The Mobile Switching Center



6. The MSC provides subscriber management functions such as;

a.
b.
c.
d.

(b)(7)e

(b)(7)e

E. EPO #5: DEFINE THE HOME LOCATION REGISTRY AND THE VISITOR LOCATION REGISTRY AND LIST WHAT INFORMATION IS STORED WITHIN EACH.

1.

2.

3. (b)(7)e

4.

5.

6.

7.

8.

(b)(7)e

9.

10.

11.

12.

(b)(7)e

13.

14.

F. EPO #6: LIST THREE FACTORS OF RADIO FREQUENCY COVERAGE FROM BASE STATIONS AND THE TWO ON-GOING ISSUES FACING WIRELESS CARRIERS.

1. Understanding Radio Frequency technology is an invaluable asset to the Investigator. With a understanding of Radio Frequency technology and propagation the Investigator can also determine the geographical area in which a mobile device had traversed.

2. Radio propagation is the electromagnetic phenomenon discovered by Henrich Hertz in the late 1880's. Its how energy travels through a given medium.

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

4. Different radio signals have different properties such as;

a. High frequencies and Low frequencies

b. Signal Refraction or how signals bend through the atmosphere

c. Signal Diffraction or how signals bend around obstructions

d. Signal Reflection or how signals bounce off obstructions or solid objects

5. Wireless signals are basically omni directional. Omni directional signals are signals that travel in all directions or 360°. Signal propagation is often described as waves or radio waves.

6. When a pebble is thrown into water its wave spread out in all directions. The speed and size of the wave is dependant on the amount of force the object strikes the water and the depth of the water.

7. Radio Frequency coverage from any base station is determined by three factors which are true no matter where the antenna is placed. These factors are;

a. The height of the antenna

b. The type of antenna used

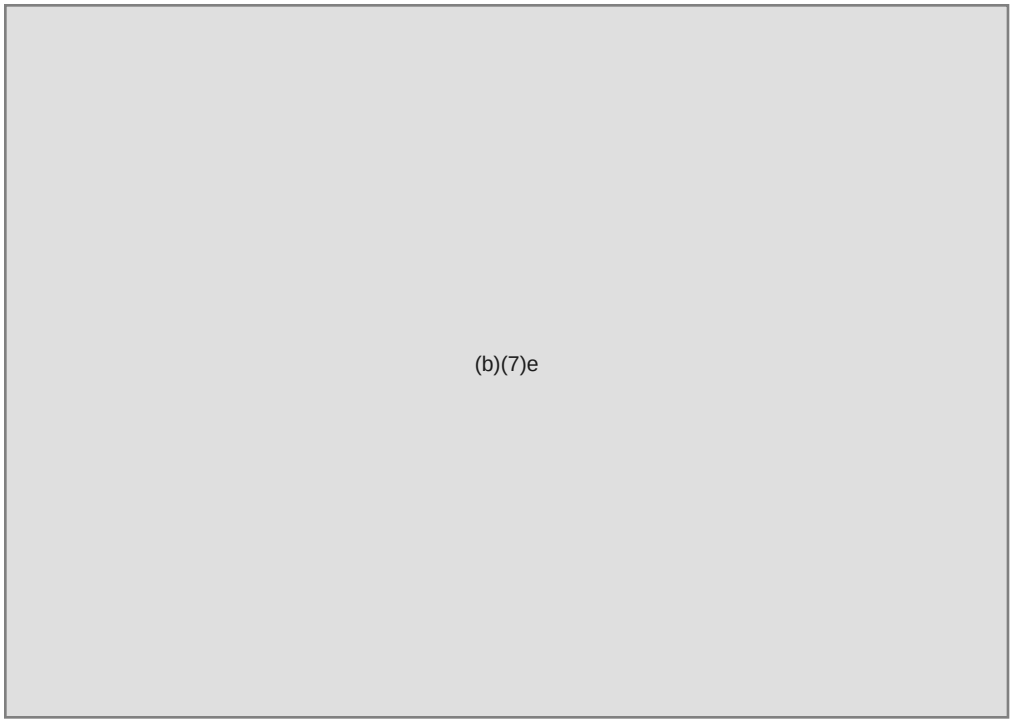
c. The Radio Frequency Power Level emitted.

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

9.

10.

11.



12.

13.

14.

15.

16.

(b)(7)e

17.

18.

19.

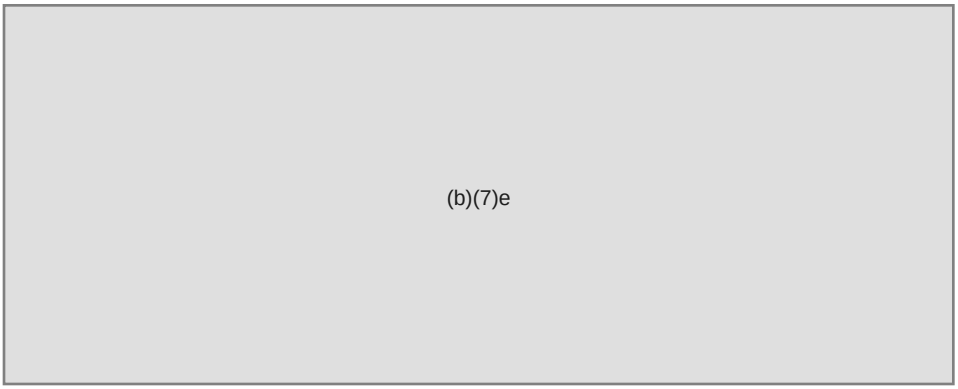
G. EPO #7: LIST THE ADMINISTRATIVE TASK OF THE CONTROL CHANNEL.

1. 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.

2. 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.

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

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



5. When a mobile unit is powered on it seeks out and connects to 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.

H. EPO # 8: DEFINE TDMA AND LIST TDMAS DISADVANTAGES.

1. 

2.

3.

4. (b)(7)e

5.

I. EPO #9: DEFINE CDMA AND LIST HOW ITS SIGNALS ARE SPREAD.

1.

2. (b)(7)e

3.

4.

5.

6.

7.

(b)(7)e

8.

9.

10.

11.

12.

13.

14.

15. (b)(7)e

16.

17.

18.

J. EPO #10: DEFINE GSM AND LIST THE FOUR SUBSYSTEMS REQUIRED FOR THIS STANDARD.

1. Global System for Mobile Communication or Groupe Special Mobile is the standard cellular communication throughout Europe and other parts of the world. Prior to it's development there were a number of incompatible systems serving Europe.

2.

3.

4.

5.

6.

(b)(7)e

7.

8.

9.

10.

11.

(b)(7)e

12.

13.

14.

15.

16.

(b)(7)e

17.

18.

19.

20.

(b)(7)e

21.

22.

23.

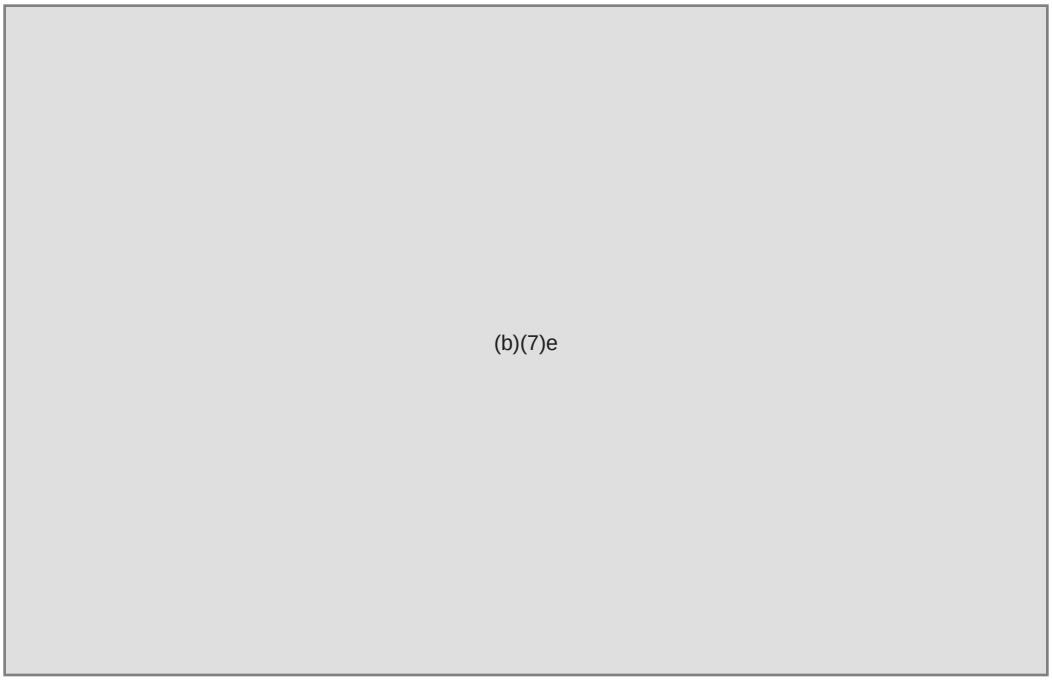
24. (b)(7)e

25.

K. EPO 11: DEFINE SIM CARD AND THE INFORMATION THAT IS STORED THERE.

1.

2. (b)(7)e

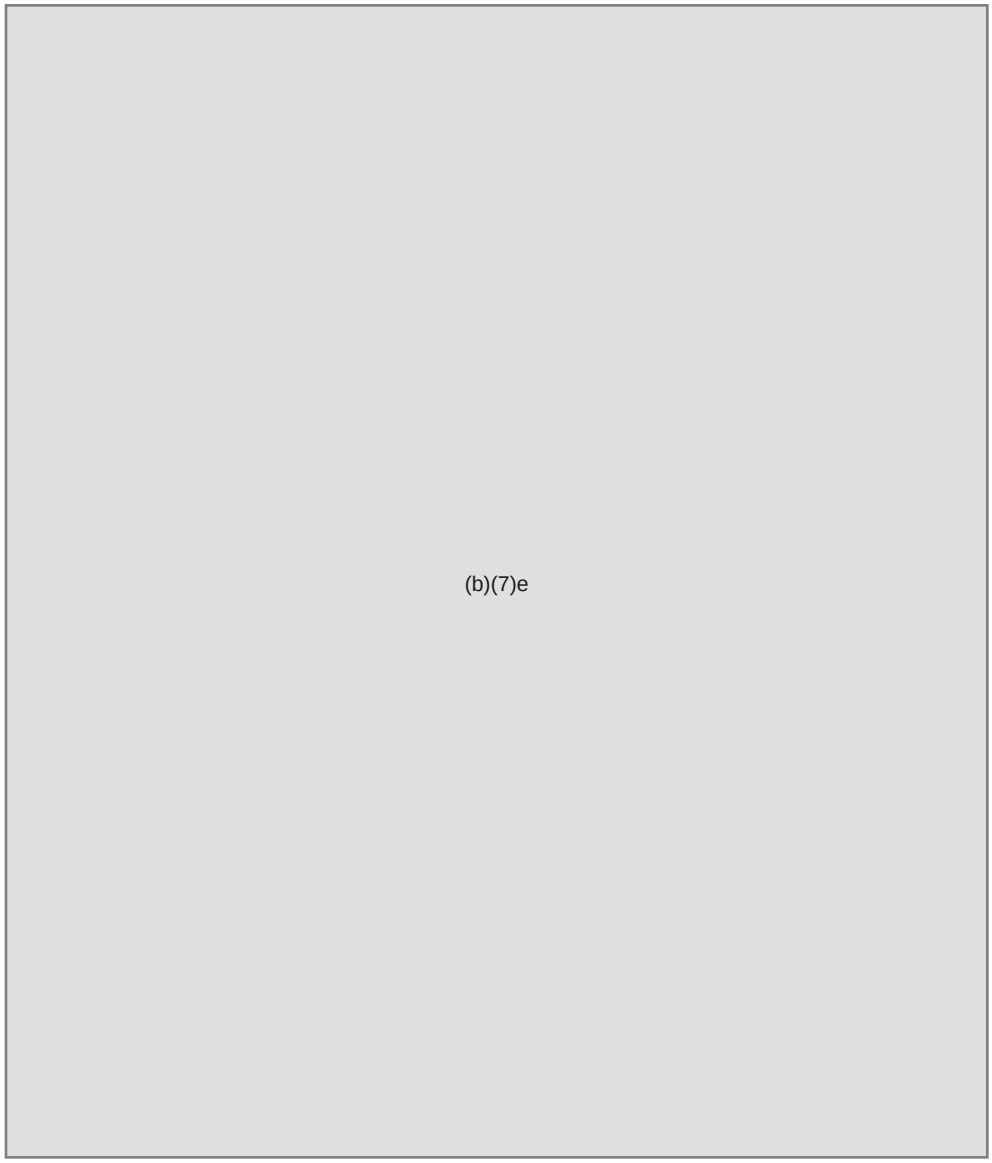


L. EPO #12: DEFINE *i*DEN AND LIST THE TWO TYPES OF HLRS AND VLRS.

1. Integrated Digital Enhanced Network Technology or *i*DEN is a unique network system. In 1987 Nextel was formed and began to change the Specialized Mobile Radio (SMR) market.
2. The technology was developed by Motorola who provided trunked radio and cellular telephone. In 1990 Nextel applied for and received permission from the FCC to create Enhanced Specialized Radio Service (ESMR) in six major markets. Nextel chose as its air interface TDMA technology.
3. Introduced in 1994, *i*DEN combined two-way radio, digital cellular, messages services with acknowledgment and wireless data into a single system.
4. *i*DEN uses Vector Summed Excited Linear Prediction (VSELP) vocoders, which compresses large segments of voice into smaller packets. VSELP also uses Forward Error Correction so packets do not become corrupted. The use of VSELP and FEC allows for six audio paths on one RF channel.
5. One of the unique features is the Push-to-Talk or Direct Connect feature. Originally called Fleet Call, Nextel purchased SMR licenses around the country to form a national network. As of 2003 Direct Connect has been offered nationwide with no roaming.

6. This dispatch feature is managed by separating talk groups into fleets. Each subscriber has an ID called the Fleet Member Identifier which identifies a user within a fleet.

7. The *i*DEN networks work in much the same way and has the same equipment as other cellular networks, but are often identified differently. The basic structure of an *i*DEN network is as follows:



8.

9.

10. 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.

M. EPO # 13: DEFINE PCS AND LIST THE TWO TYPES OF SERVICES PROVIDED BY THESE WIRELESS NETWORKS.

1. The FCC has defined Personal Communication Services or PCS as radio communication that encompasses mobile and fixed communication to individuals and businesses that can be integrated with a variety of competing networks.
2. 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.
3. Some other ways to define the mobility of PCS networks;
    a. Personal Mobility - the ability of users to access any telecom service at any terminal based on personal identifiers, the networks ability and users profile
    b. Terminal Mobility – the wireless subscriber units ability to access services from different locations while in motions
    c. Service Mobility – the use of vertical features provided by landlines, users at remote locations or while in motion.
    d. PCS refers to services that are user specific as opposed to location specific. PCS is referred to as follow me services.
4. 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.
5. 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.
6. There are two types of PCS services; Narrowband and Broadband PCS.
7. One type is Narrowband which uses the 3MHz radio spectrum and is used primarily for data transmissions. These services are paging and short message systems.
8. The other type is Broadband PCS which is used for multimedia transmissions such as voice, data. Internet, SMS, image and in the future full motion video. This obviously requires more channel capacity and is set aside on the 140 MHz radio spectrum.
9. The major PCS carriers include AT & T/Cingular, Verizon Wireless, T-Mobile, Sprint PCS (Nextel), Alltel Mobile and U.S. Cellular.
10. There are hundreds of regional PCS Carriers that can be found at http://www.wirelessadvisor.com/resources/wireless-carriers-a-b

11. 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.

III. SUMMARY

A. REVIEW OF PERFORMANCE OBJECTIVES

EPO #1: Define Frequency Reuse and how this system is geographically positioned to ensure its ability to operate.

EPO #2: Define Call Handoff and list the locations where evidentiary artifacts are stored.

EPO #3: Define the Hexagon Grid and its importance to the Cellular Network.

EPO #4: List the five main components of a wireless network and their responsibilities.

EPO #5: Define the Home Location Registry and the Visitor Location Registry and list what information is stored within each.

EPO #6: List three factors of Radio Frequency coverage from Base Stations and the two on-going issues facing wireless carriers.

EPO #7: List the administrative task of the Control Channel.

EPO #8: Define TDMA and list TDMAs advantages.

EPO #9: Define CDMA and list how its signals are spread.

EPO #10: Define GSM and list the four subsystems required for this standard.

EPO #11: Define SIM Card and the information that is stored there.

EPO #12: Define *i*DEN and list the two types of HLRs and VLRs.

EPO #13: Define PCS and list the two types of services provided by these wireless networks.

IV. APPLICATION

A. LABORATORY

None

B. PRACTICAL EXERCISE

None

REFERENCES

Stetz, Penelope; The Cell Phone Handbook; 2nd Ed.; FindTech, Ltd.; Cleveland, OH; 2002.

Bedell, Paul; Wireless Crash Course; McGraw Hill; New York; 2001.

Layton, Julia, Marshall Brain and Jeff Tyson. "How Cell Phones Work." 14 November 2000. HowStuffWorks.com. <http://electronics.howstuffworks.com/cell-phone.htm> 03 April 2008.

Unaccredited article. “Wireless 101”; 19 May, 2008. Cellular Technology Industry Association. http://www.ctia.org/consumer_info/service/index.cfm/AID/10319.

BIBLIOGRAPHY

None

ATTACHMENTS

None