All-Hazards Communications Technician (COMT)
Pre-Course Study Guide

TABLE OF CONTENTS

INTRODUCTION

This Study Guide was created so that all students of the All-Hazards Communications Technician (COMT) course will have the same foundational knowledge. Some students' skills and experience will be above and beyond what is contained in these pages. Others will be introduced to terms and theories they have not yet experienced. In-class discussion will give students an opportunity to explore further those theories that are new to them. Exercises during the class will then provide an opportunity to test the theories learned. Finally, post-class research and performance as a COMT at incidents and planned events will provide students the opportunity to experiment with and prove the theories in real-world situations.

The Department of Homeland Security Office of Emergency Communications (OEC), through a group of public safety practitioners with many years of incident communications experience, developed this course as an introductory course. Its purpose is to introduce prospective COMTs to the role of the COMT at an incident or planned event, to introduce the technologies that may be deployed in support of an incident, and to provide resources and tools that a prospective COMT can use to better understand what assets are available locally and plan how those resources might be brought to bear in times of crisis.

This Study Guide is a compilation of information extracted from three sources. The complete documents are available for download from the Public Safety Tools website. Go to: http://www.publicsafetytools.info/start_index_v2.php Click on "PS Library" then "Webview" and search on the title of each individual reference document.

1. The Federal Emergency Management Agency (FEMA) *National Urban Search and Rescue Response System Communications Specialist Course Student Workbook.*[1]
2. The U.S. Department of Justice Office of Community Oriented Policing Services (COPS Office) *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*.[2]
3. The National Law Enforcement and Corrections Technology Center–Rocky Mountain Region (NLECTC) *Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning, and Management*.[3]

---

[1] Federal Emergency Management Agency (FEMA), *National Urban Search and Rescue Response System Communications Specialist Course Student Workbook, Volumes 1 and 2*, Washington, D.C.: FEMA, U.S. Department of Homeland Security, June 2007. Hereafter, FEMA Student Workbook.

[2] Dan M. Hawkins, *Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects*, Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006. This publication is available in hard copy at no cost from the COPS Office. See http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=238 for more information. Hereafter, COPS Interoperability Tech Guide.

[3] Kathy J. Imel and James W. Hart, P.E., *Understanding Wireless Communications in Public Safety: A Guidebook to Technology, Issues, Planning and Management*, Denver, Colorado: NLECTC–Rocky Mountain, second edition, January 2003. Hereafter, NLECTC Guidebook.

The information you will need to be successful in the All-Hazards COMT course is contained in specific chapters in these documents and is outlined below; however, if you would like to learn more, please feel free to read these documents in their entirety.

During the COMT course, you will be tested on the information provided in these studies.

GUIDED STUDY

For your convenience, this Study Guide provides a compilation of excerpts from three publications. COMT students are expected to read this Study Guide and be familiar with its content prior to attending the class.

Study 1: Radio Wave Propagation

Reference Material: FEMA Student Workbook, Volume 2-28, June 2007, Chapter 1.

Study 2: Voice versus Data

Reference Material: NLECTC Guidebook, Chapter 5.

Study 3: Voice Communications

Reference Material: COPS Interoperability Tech Guide, Chapter 16, pages 245-258.

Study 4: Characteristics of Radio Systems

Reference Material: NLECTC Guidebook, Chapter 6, pages 41-49.

Study 5: Antennas

Reference Material: FEMA Student Workbook, Volume 2-28, June 2007, Chapter 3.

Reference Material: NLECTC Guidebook, Chapter 6, pages 50-64.

Study 6: Current Public Safety Systems

Reference Material: NLECTC Guidebook, Chapter 7.

Reference Material: COPS Interoperability Tech Guide, Chapter 16, pages 259-282, and Chapter 17.

Study 1: Radio Wave Propagation

Reference Material: FEMA Student Workbook, Volume 2-28, June 2007 - Chapter 1

CHAPTER 1: RADIO WAVE PROPAGATION

Learning Objectives

Upon completing this chapter, you will be able to

- State what radio waves are;
- List the components of a radio wave and define the terms cycle, frequency, harmonics, period, wavelength, and velocity as applied to radio wave propagation;
- Compute the wavelength of radio waves;
- State how radio waves are polarized, vertically and horizontally;
- State what reflection, refraction, and diffraction are as applied to radio waves;
- State what influence the Earth's atmosphere has on radio waves and list the different layers of the Earth's atmosphere;
- Identify a ground wave, a sky wave, and state the effects of the ionosphere on the sky wave;
- Describe propagation paths;
- Describe fading, multipath fading;
- Describe propagation paths;
- State how transmission losses affect radio wave propagation;
- State how electromagnetic interference, man-made/natural interference, and ionospheric disturbances affect radio wave propagation. State how transmission losses affect radio wave propagation;
- State what temperature inversion is, how frequency predictions are made, and how weather affects frequency; and
- State what tropospheric scatter is and how it affects radio wave propagation.

Introduction to Wave Propagation

Of the many technical subjects that Communication Specialists are expected to know, the one least susceptible to change is the theory of wave propagation. The basic principles that enable waves to be propagated (transmitted) through space are the same today as they were 70 years ago. One would think, then, that a thorough understanding of these principles is a relatively simple task. For the electrical engineer or the individual with a natural curiosity for the unknown, it is indeed a simple task. Most technicians, however, tend to view wave propagation as something complex and confusing, and would just as soon see this chapter completely disappear from training manuals. This attitude undoubtedly stems from the fact that wave propagation is an invisible force that cannot be detected by the sense of sight or touch. Understanding wave

propagation requires the use of the imagination to visualize the associated concepts and how they are used in practical application. This manual was developed to help you visualize and understand those concepts. Through ample use of illustrations and a step-by-step transition from the simple to the complex, we will help you develop a better understanding of wave propagation. In this chapter, we will discuss propagation theory on an introductory level, without going into the technical details that concern the engineer. However, you must still use thought and imagination to understand the new ideas and concepts as they are presented.

To understand radio wave propagation, you must first learn what wave propagation is and some of the basic physics or properties that affect propagation. Many of these properties are common everyday occurrences, with which you are already familiar.

What is Propagation?

Early man was quick to recognize the need to communicate beyond the range of the human voice. To satisfy this need, he developed alternate methods of communication, such as hand gestures, beating on a hollow log, and smoke signals. Although these methods were effective, they were still greatly limited in range. Eventually, the range limitations were overcome by the development of courier and postal systems; but there was then a problem of speed. For centuries the time required for the delivery of a message depended on the speed of a horse.

During the latter part of the 19th century, both distance and time limitations were largely overcome. The invention of the telegraph made possible instantaneous communication over long wires. Then a short time later, man discovered how to transmit messages in the form of RADIO WAVES.

As you will learn in this chapter, radio waves are propagated. PROPAGATION means "movement through a medium." This is most easily illustrated by light rays. When a light is turned on in a darkened room, light rays travel from the light bulb throughout the room. When a flashlight is turned on, light rays also radiate from its bulb, but are focused into a narrow beam. You can use these examples to picture how radio waves propagate. Like the light in the room, radio waves may spread out in all directions. They can also be focused (concentrated) like the flashlight, depending upon the need. Radio waves are a form of radiant energy, similar to light and heat. Although they can neither be seen nor felt, their presence can be detected through the use of sensitive measuring devices. The speed at which both forms of waves travel is the same; they both travel at the speed of light.

You may wonder why you can see light but not radio waves, which consist of the same form of energy as light. The reason is that you can only "see" what your eyes can detect. Your eyes can detect radiant energy only within a fixed range of frequencies. Since the frequencies of radio waves are below the frequencies your eyes can detect, you cannot see radio waves.

The theory of wave propagation that we discuss in this section applies to communication equipment.

Electromagnetic Spectrum

Light is one kind of electromagnetic energy. There are many other types, including heat energy and radio energy. The only difference between the various types of electromagnetic energy is the frequency of their waves (rate of vibration). The term SPECTRUM is used to designate the entire range of electromagnetic waves arranged in order of their frequencies. The VISIBLE SPECTRUM contains only those waves which stimulate the sense of sight. You, as a technician, might be expected to maintain equipment that uses electromagnetic waves within, above, and below the visible spectrum.

There are neither sharp dividing lines nor gaps in the ELECTROMAGNETIC SPECTRUM. Figure 1-1 illustrates how portions of the electromagnetic spectrum overlap. Notice that only a small portion of the electromagnetic spectrum contains visible waves, or light, which can be seen by the human eye.

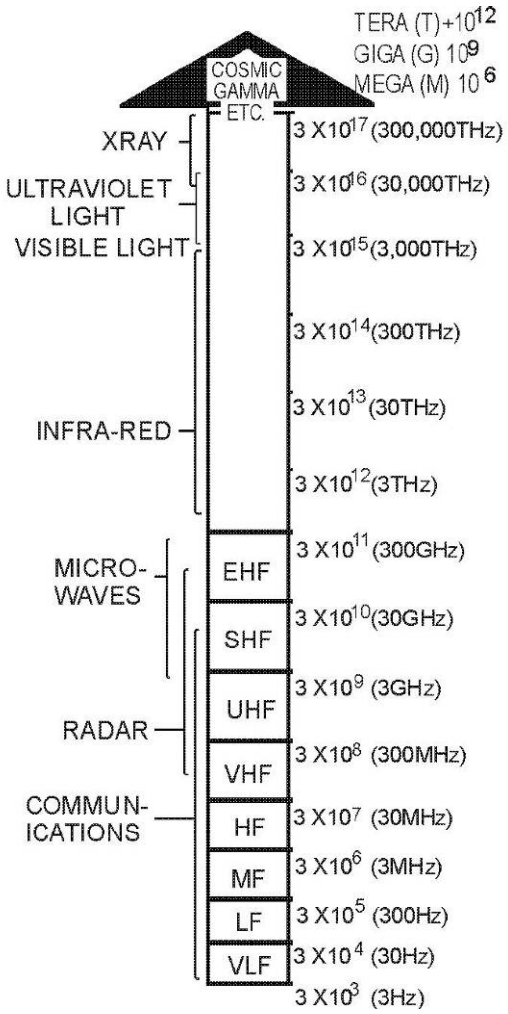


Figure 1-1.—Electromagnetic spectrum.

Electromagnetic Waves

In general, the same principles and properties of light waves apply to the communications electromagnetic waves you are about to study. The electromagnetic field is used to transfer energy (as communications) from point to point. We will introduce the basic ANTENNA as the propagation source of these electromagnetic waves.

The Basic Antenna

The study of antennas and electromagnetic wave propagation is essential to a complete understanding of radio communication, radar, loran, and other electronic systems. Figure 1-2 shows a simple radio communication system. In the illustration, the transmitter is an electronic device that generates radio-frequency energy. The energy travels through a transmission line (we will discuss this in chapter 3) to an antenna. The antenna converts the energy into radio waves that radiate into space from the antenna at the speed of light. The radio waves travel through the atmosphere or space until they are either reflected by an object or absorbed. If another antenna is placed in the path of the radio waves, it absorbs part of the waves and converts them to energy. This energy travels through another transmission line and is fed to a receiver. From this example, you can see that the requirements for a simple communications system are (1) transmitting equipment, (2) transmission line, (3) transmitting antenna, (4) medium, (5) receiving antenna, and (6) receiving equipment.

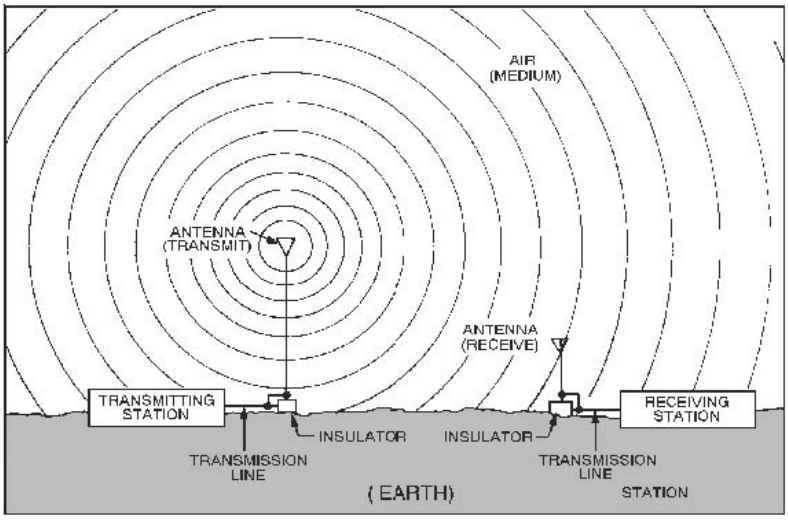


Figure 1-2.—Simple radio communication system.

An antenna is a conductor or a set of conductors used either to radiate electromagnetic energy into space or to collect this energy from space. Figure 1-3 shows an antenna. View A is a drawing of an actual antenna; view B is a cut-away view of the antenna; and view C is a simplified diagram of the antenna.

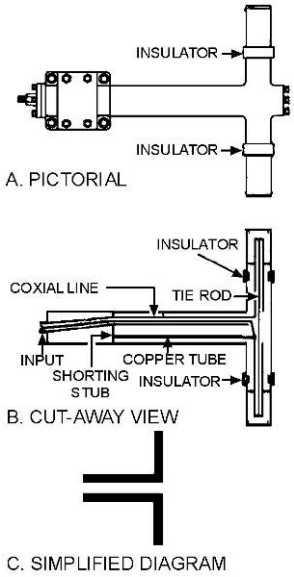


Figure 1-24.—Antenna.

Radio Waves

An energy wave generated by a transmitter is called a RADIO WAVE. The radio wave radiated into space by the transmitting antenna is a very complex form of energy containing both electric and magnetic fields. Because of this combination of fields, radio waves are also referred to as ELECTROMAGNETIC RADIATION. This discussion will explain the Earth's atmosphere and its effect on radio waves.

NOTE: The term radio wave is not limited to communications equipment alone. The term applies to all equipment that generates signals in the form of electromagnetic energy.

Components of Radio Waves

The basic shape of the wave generated by a transmitter is that of a sine wave. The wave radiated out into space, however, may or may not retain the characteristics of the sine wave.

A sine wave can be one cycle or many cycles. Recall from chapter 1 that the number of cycles of a sine wave that are completed in 1 second is known as the frequency of the sine wave. For example, 60 cycles of ordinary house current occur each second, so house current is said to have a frequency of 60 cycles per second or 60 hertz.

The frequencies falling between 3000 hertz (3 kHz) and 300,000,000,000 hertz (300 GHz) are called RADIO FREQUENCIES (abbreviated rf) since they are commonly used in radio communications. This part of the radio frequency spectrum is divided into bands, each band being 10 times higher in frequency than the one immediately below it. This arrangement serves

as a convenient way to remember the range of each band. The rf bands are shown in table 1-1. The usable radio-frequency range is roughly 10 kilohertz to 100 gigahertz.

Table 1-1.—Radio Frequency Bands

DESCRIPTION	ABBREVIATION	FREQUENCY
Very low	VLF	3 to 30 KHz
Low	LF	30 to 300 KHz
Medium	MF	300 to 3000 KHz
High	HF	3 to 30 MHz
Very high	VHF	30 to 300 MHz
Ultrahigh	UHF	300 to 3000 MHz
Super high	SHF	3 to 30 GHz
Extremely high	EHF	30 to 300 GHz

The PERIOD of a radio wave is simply the amount of time required for the completion of one full cycle. If a sine wave has a frequency of 2 hertz, each cycle has a duration, or period, of one-half second. If the frequency is 10 hertz, the period of each cycle is one-tenth of a second. Since the frequency of a radio wave is the number of cycles that are completed in one second, you should be able to see that as the frequency of a radio wave increases, its period decreases.

A wavelength is the space occupied by one full cycle of a radio wave at any given instant. Wavelengths are expressed in meters (1 meter is equal to 3.28 feet). You need to have a good understanding of frequency and wavelength to be able to select the proper antenna(s) for use in successful communications.

The velocity (or speed) of a radio wave radiated into free space by a transmitting antenna is equal to the speed of light–186,000 miles per second or 300,000,000 meters per second. Because of various factors, such as barometric pressure, humidity, molecular content, etc., radio waves travel inside the Earth's atmosphere at a speed slightly less than the speed of light. Normally, in discussions of the velocity of radio waves, the velocity referred to is the speed at which radio waves travel in free space.

The frequency of a radio wave has nothing to do with its velocity. A 5-megahertz wave travels through space at the same velocity as a 10-megahertz wave. However, the velocity of radio waves is an important factor in making wavelength-to-frequency conversions, the subject of our next discussion.

☑Learning Check

1. What is the term used to describe the basic frequency of a radio wave?

Wavelength-to-Frequency Conversions

Radio waves are often referred to by their wavelength in meters rather than by frequency. For example, most people have heard commercial radio stations make announcements similar to the following: "Station WXYZ operating on 240 meters..." To tune receiving equipment that is calibrated by frequency to such a station, you must first convert the designated wavelength to its equivalent frequency.

As discussed earlier, a radio wave travels 300,000,000 meters a second (speed of light); therefore, a radio wave of 1 hertz would have traveled a distance (or wavelength) of 300,000,000 meters. Obviously then, if the frequency of the wave is increased to 2 hertz, the wavelength will be cut in half to 150,000,000 meters. This illustrates the principle that the HIGHER THE FREQUENCY, the SHORTER THE WAVELENGTH.

Wavelength-to-frequency conversions of radio waves are really quite simple because wavelength and frequency are reciprocals: Either one divided into the velocity of a radio wave yields the other. Remember, the formula for wavelength is:

$$\lambda = \frac{v}{f} \quad \text{or} \quad f = \frac{v}{\lambda}$$

Where:

λ = wavelength in meters

v = velocity of radio wave (speed of light)

f = frequency of radio wave (in Hz, kHz or Mhz)

The wavelength in meters divided into 300,000,000 yields the frequency of a radio wave in hertz. Likewise, the wavelength divided into 300,000 yields the frequency of a radio wave in kilohertz, and the wavelength divided into 300 yields the frequency in megahertz.

Now, let us apply the formula to determine the frequency to which the receiving equipment must be tuned to receive station WXYZ operating on 240 meters. Radio wave frequencies are normally expressed in kilohertz or megahertz.

To find the frequency in hertz, use the formula:

$$f = \frac{v}{\lambda}$$

Given:

$v = 300{,}000{,}000$ meters per second

$\lambda = 240$ meters

Solution:

$$f = \frac{300{,}000{,}000 \text{ meters per second}}{240 \text{ meters}}$$

$f = 1{,}250{,}000$ Hz

To find the frequency in kilohertz, use the formula:

$$f_{[kHz]} = \frac{300{,}000}{\lambda}$$

Given:

$\lambda = 240$ meters

Solution:

$$f_{[kHz]} = \frac{300{,}000}{240 \text{ meters}}$$

$f = 1250$kHz

To find the frequency in megahertz, use the formula:

$$f_{[MHz]} = \frac{300}{\lambda}$$

Given:

$\lambda = 240$ meters

Solution:

$$f_{[MHz]} = \frac{300}{240 \text{ meters}}$$

$f = 1.25$MHz

☑Learning Check

2. It is known that WWV operates on a frequency of 10 megahertz. What is the wavelength of WWV?

3. A station is known to operate at 60-meters. What is the frequency of the unknown station?

Polarization

For maximum absorption of energy from the electromagnetic fields, the receiving antenna must be located in the plane of polarization. This places the conductor of the antenna at right angles to the magnetic lines of force moving through the antenna and parallel to the electric lines, causing maximum induction.

Normally, the plane of polarization of a radio wave is the plane in which the E field propagates with respect to the Earth. If the E field component of the radiated wave travels in a plane perpendicular to the Earth's surface (vertical), the radiation is said to be VERTICALLY POLARIZED, as shown in figure 1-4, view A. If the E field propagates in a plane parallel to the Earth's surface (horizontal), the radiation is said to be HORIZONTALLY POLARIZED, as shown in view B.

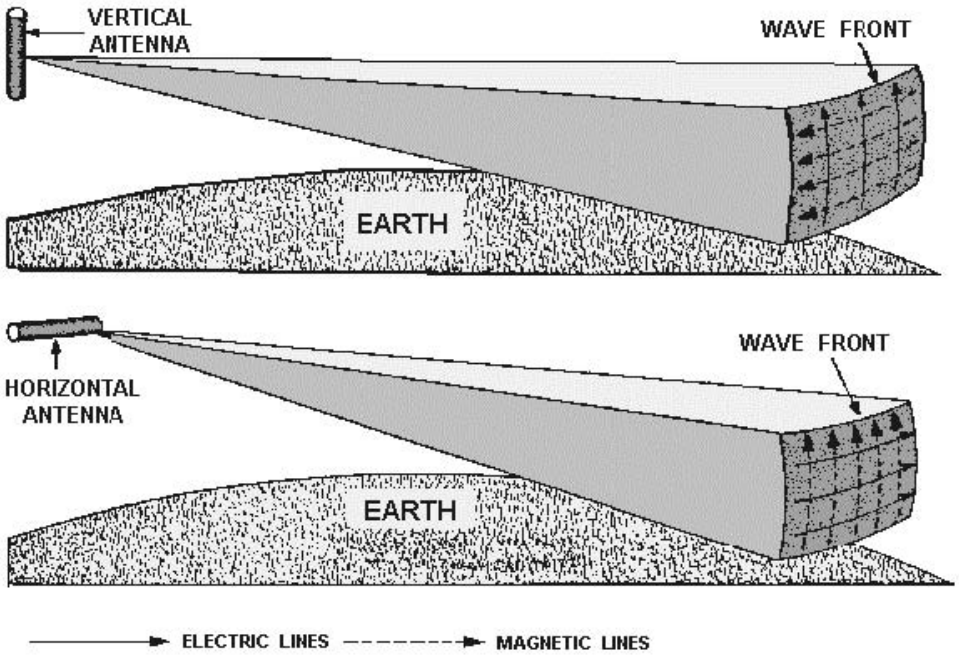


Figure 1-4 Polarization.

Atmospheric Propagation

Within the atmosphere, radio waves can be reflected, refracted, and diffracted like light and heat waves.

Reflection

Radio waves may be reflected from various substances or objects they meet during travel between the transmitting and receiving sites. The amount of reflection depends on the reflecting material. Smooth metal surfaces of good electrical conductivity are efficient reflectors of radio waves. The surface of the Earth itself is a fairly good reflector. The radio wave is not reflected from a single point on the reflector but rather from an area on its surface. The size of the area required for reflection to take place depends on the wavelength of the radio wave and the angle at which the wave strikes the reflecting substance.

When radio waves are reflected from flat surfaces, a phase shift in the alternations of the wave occurs. Figure 1-5 shows two radio waves being reflected from the Earth's surface. Radio waves that keep their phase relationships after reflection normally produce a stronger signal at the receiving site. Those that are received out of phase produce a weak or fading signal. The shifting in the phase relationships of reflected radio waves is one of the major reasons for fading. Fading will be discussed in more detail later in this chapter.

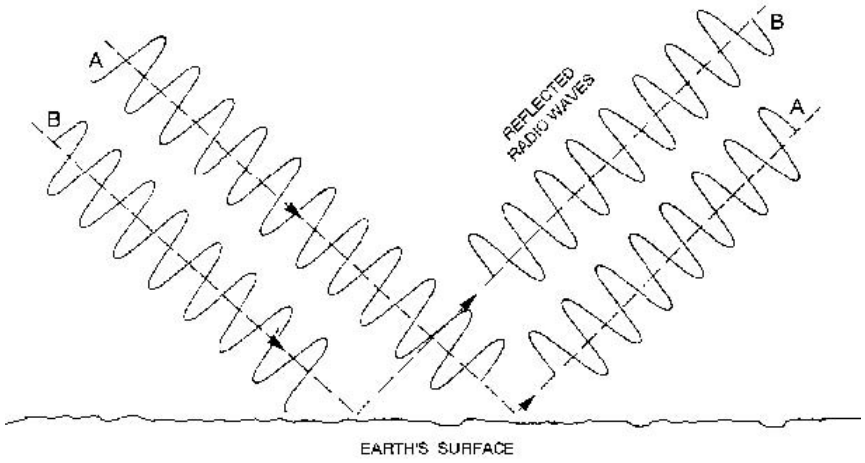


Figure 1-5.—Phase shift of reflected radio waves.

Refraction

Another phenomenon common to most radio waves is the bending of the waves as they move from one medium into another in which the velocity of propagation is different. This bending of the waves is called refraction. For example, suppose you are driving down a smoothly paved road at a constant speed and suddenly one wheel goes off onto the soft shoulder. The car tends to veer off to one side. The change of medium, from hard surface to soft shoulder, causes a change

in speed or velocity. The tendency is for the car to change direction. This same principle applies to radio waves as changes occur in the medium through which they are passing. As an example, the radio wave shown in figure 1-6 is traveling through the Earth's atmosphere at a constant speed. As the wave enters the dense layer of electrically charged ions, the part of the wave that enters the new medium first travels faster than the parts of the wave that have not yet entered the new medium. This abrupt increase in velocity of the upper part of the wave causes the wave to bend back toward the Earth. This bending, or change of direction, is always toward the medium that has the lower velocity of propagation.

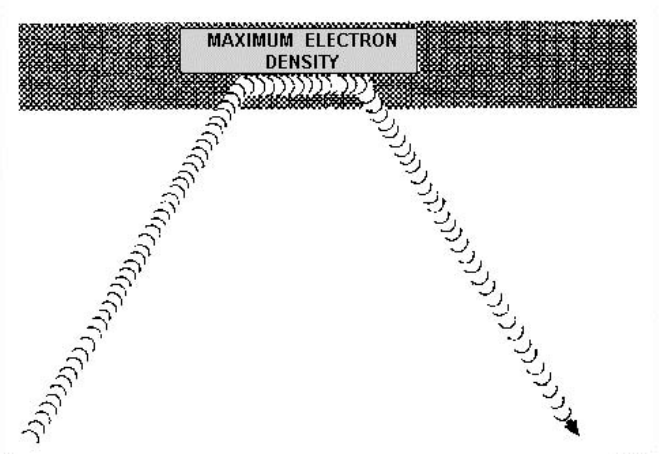


Figure 1-6.—Radio wave refraction.

Radio waves passing through the atmosphere are affected by certain factors, such as temperature, pressure, humidity, and density. These factors can cause the radio waves to be refracted. This effect will be discussed in greater detail later in this chapter.

Diffraction

A radio wave that meets an obstacle has a natural tendency to bend around the obstacle as illustrated in figure 1-7. The bending, called diffraction, results in a change of direction of part of the wave energy from the normal line-of-sight path. This change makes it possible to receive energy around the edges of an obstacle as shown in view A or at some distances below the highest point of an obstruction, as shown in view B. Although diffracted rf energy usually is weak, it can still be detected by a suitable receiver. The principal effect of diffraction extends the radio range beyond the visible horizon. In certain cases, by using high power and very low frequencies, radio waves can be made to encircle the Earth by diffraction.

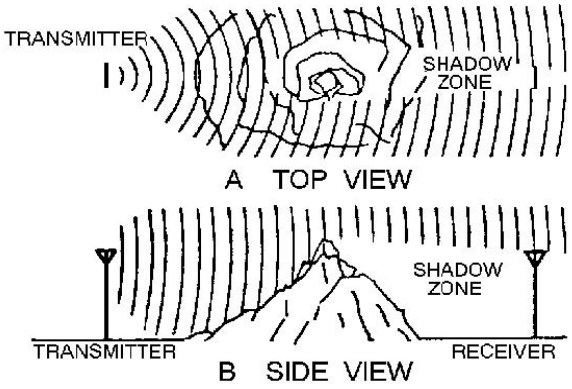


Figure 1-7.—Diffraction around an object.

☑Learning Check

4. What is one of the major reasons for the fading of radio waves which have been reflected from a surface?

The Effect of the Earth's Atmosphere on Radio Waves

This discussion of electromagnetic wave propagation is concerned mainly with the properties and effects of the medium located between the transmitting antenna and the receiving antenna. While radio waves traveling in free space have little outside influence affecting them, radio waves traveling within the Earth's atmosphere are affected by varying conditions. The influence exerted on radio waves by the Earth's atmosphere adds many new factors to complicate what at first seems to be a relatively simple problem. These complications are because of a lack of uniformity within the Earth's atmosphere. Atmospheric conditions vary with changes in height, geographical location, and even with changes in time (day, night, season, year). A knowledge of the composition of the Earth's atmosphere is extremely important for understanding wave propagation.

The Earth's atmosphere is divided into three separate regions, or layers. They are the TROPOSPHERE, the STRATOSPHERE, and the IONOSPHERE. The layers of the atmosphere are illustrated in figure1-8.

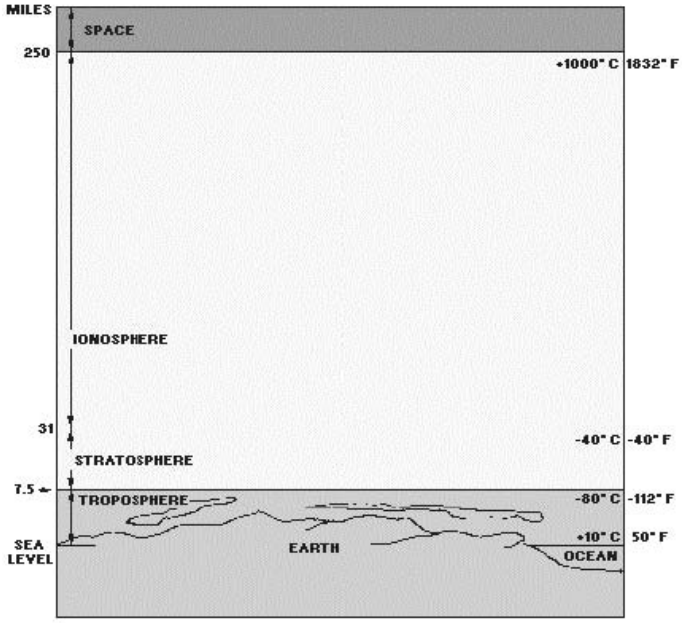


Figure 1-8—Layers of the earth's atmosphere.

Troposphere

The troposphere is the portion of the Earth's atmosphere that extends from the surface of the Earth to a height of about 3.7 miles (6 km) at the North Pole or the South Pole and 11.2 miles (18 km) at the equator. Virtually all weather phenomena take place in the troposphere. The temperature in this region decreases rapidly with altitude, clouds form, and there may be much turbulence because of variations in temperature, density, and pressure. These conditions have a great effect on the propagation of radio waves, which will be explained later in this chapter.

Stratosphere

The stratosphere is located between the troposphere and the ionosphere. The temperature throughout this region is considered to be almost constant and there is little water vapor present. The stratosphere has relatively little effect on radio waves because it is a relatively calm region with little or no temperature changes.

Ionosphere

The ionosphere extends upward from about 31.1 miles (50 km) to a height of about 250 miles (402 km). It contains four cloud-like layers of electrically charged ions, which enable radio waves to be propagated to great distances around the Earth. This is the most important region of the atmosphere for long distance point-to-point communications.

☑Learning Check

5. What are the three layers of the atmosphere?

6. Which layer of the atmosphere has relatively little effect on radio waves?

Radio Wave Transmission

There are two principal ways in which electromagnetic (radio) energy travels from a transmitting antenna to a receiving antenna. One way is by GROUND WAVES and the other is by SKY WAVES. Ground waves are radio waves that travel near the surface of the Earth (surface and space waves). Sky waves are radio waves that are reflected back to Earth from the ionosphere. (See figure 1-9.)

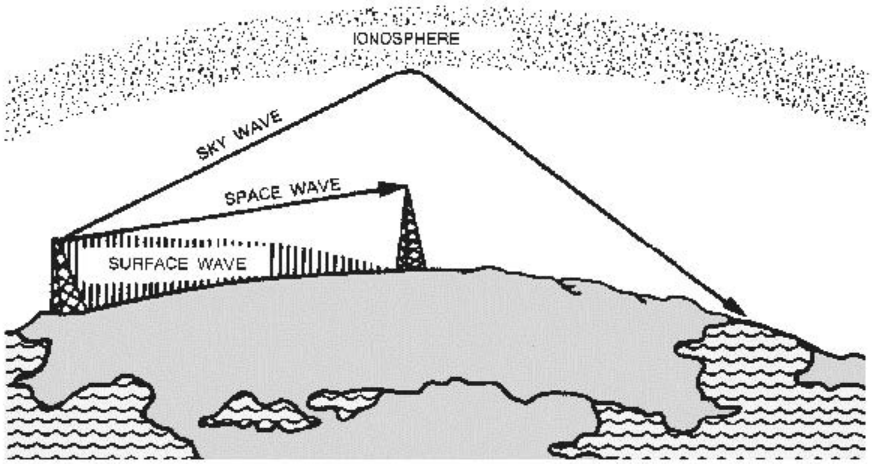


Figure 1-9.—Ground waves and sky waves.

Ground Waves

The ground wave is actually composed of two separate component waves. These are known as the SURFACE WAVE and the SPACE WAVE (fig. 1-9). The determining factor in whether a

ground wave component is classified as a space wave or a surface wave is simple. A surface wave travels along the surface of the Earth. A space wave travels over the surface.

SURFACE WAVE.—The surface wave reaches the receiving site by traveling along the surface of the ground as shown in figure 1-10. A surface wave can follow the contours of the Earth because of the process of diffraction. When a surface wave meets an object and the dimensions of the object do not exceed its wavelength, the wave tends to curve or bend around the object. The smaller the object, the more pronounced the diffractive action will be.

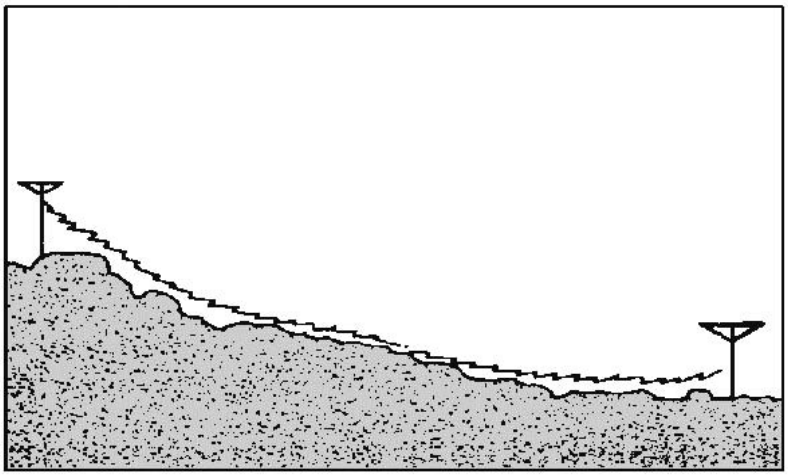


Figure 1-10.—Surface wave propagation.

As a surface wave passes over the ground, the wave induces a voltage in the Earth. The induced voltage takes energy away from the surface wave, thereby weakening, or attenuating, the wave as it moves away from the transmitting antenna. To reduce the attenuation, the amount of induced voltage must be reduced. This is done by using vertically polarized waves that minimize the extent to which the electric field of the wave is in contact with the Earth. When a surface wave is horizontally polarized, the electric field of the wave is parallel with the surface of the Earth and, therefore, is constantly in contact with it. The wave is then completely attenuated within a short distance from the transmitting site. On the other hand, when the surface wave is vertically polarized, the electric field is vertical to the Earth and merely dips into and out of the Earth's surface. For this reason, vertical polarization is vastly superior to horizontal polarization for surface wave propagation.

The attenuation that a surface wave undergoes because of induced voltage also depends on the electrical properties of the terrain over which the wave travels. The best type of surface is one that has good electrical conductivity. The better the conductivity, the less the attenuation. Table 1-2 gives the relative conductivity of various surfaces of the Earth.

Table 1-2.—Surface Conductivity

Surface	Relative Conductivity
Sea water	Good
Flat, loamy soil	Fair
Large bodies of fresh water	Fair
Rocky terrain	Poor
Desert	Poor
Jungle	Unusable

Another major factor in the attenuation of surface waves is frequency. Recall from earlier discussions on wavelength that the higher the frequency of a radio wave, the shorter its wavelength will be. These high frequencies, with their shorter wavelengths, are not normally diffracted but are absorbed by the Earth at points relatively close to the transmitting site. You can assume, therefore, that as the frequency of a surface wave is increased, the more rapidly the surface wave will be absorbed, or attenuated, by the Earth. Because of this loss by attenuation, the surface wave is impractical for long-distance transmissions at frequencies above 2 megahertz. On the other hand, when the frequency of a surface wave is low enough to have a very long wavelength, the Earth appears to be very small, and diffraction is sufficient for propagation well beyond the horizon. In fact, by lowering the transmitting frequency into the very low frequency (vlf) range and using very high-powered transmitters, the surface wave can be propagated great distances.

SPACE WAVE.—The space wave follows two distinct paths from the transmitting antenna to the receiving antenna—one through the air directly to the receiving antenna, the other reflected from the ground to the receiving antenna. This is illustrated in figure 1-11. The primary path of the space wave is directly from the transmitting antenna to the receiving antenna. So, the receiving antenna must be located within the radio horizon of the transmitting antenna. Because space waves are refracted slightly, even when propagated through the troposphere, the radio horizon is actually about one-third farther than the line-of-sight or natural horizon.

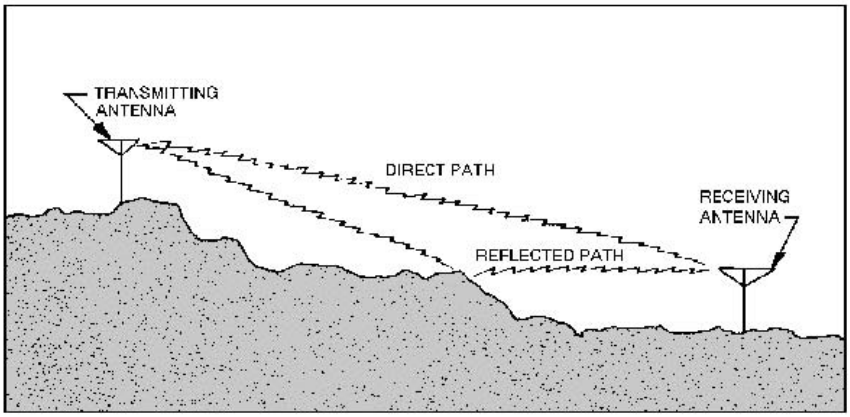


Figure 1-11.—Space wave propagation.

Although space waves suffer little ground attenuation, they nevertheless are susceptible to fading. This is because space waves actually follow two paths of different lengths (direct path and ground reflected path) to the receiving site and, therefore, may arrive in or out of phase. If these two component waves are received in phase, the result is a reinforced or stronger signal. Likewise, if they are received out of phase, they tend to cancel one another, which results in a weak or fading signal.

☑Learning Check

7. What is the determining factor in classifying whether a radio wave is a ground wave or a space wave?

8. What is the best type of surface or terrain to use for radio wave transmission?

9. What is the primary difference between the radio horizon and the natural horizon?

10. What three factors must be considered in the transmission of a surface wave to reduce attenuation?

Sky Wave

The sky wave, often called the ionospheric wave, is radiated in an upward direction and returned to Earth at some distant location because of refraction from the ionosphere. This form of propagation is relatively unaffected by the Earth's surface and can propagate signals over great distances. Usually the high frequency (hf) band is used for sky wave propagation.

Refraction in the Ionosphere

When a radio wave is transmitted into an ionized layer, refraction, or bending of the wave, occurs. As we discussed earlier, refraction is caused by an abrupt change in the velocity of the upper part of a radio wave as it strikes or enters a new medium. The amount of refraction that occurs depends on three main factors: (1) the density of ionization of the layer, (2) the frequency of the radio wave, and (3) the angle at which the wave enters the layer.

Skip Distance/Skip Zone

In figure 1-12, note the relationship between the sky wave skip distance, the skip zone, and the ground wave coverage. The SKIP DISTANCE is the distance from the transmitter to the point where the sky wave is first returned to Earth. The size of the skip distance depends on the frequency of the wave, the angle of incidence, and the degree of ionization present.

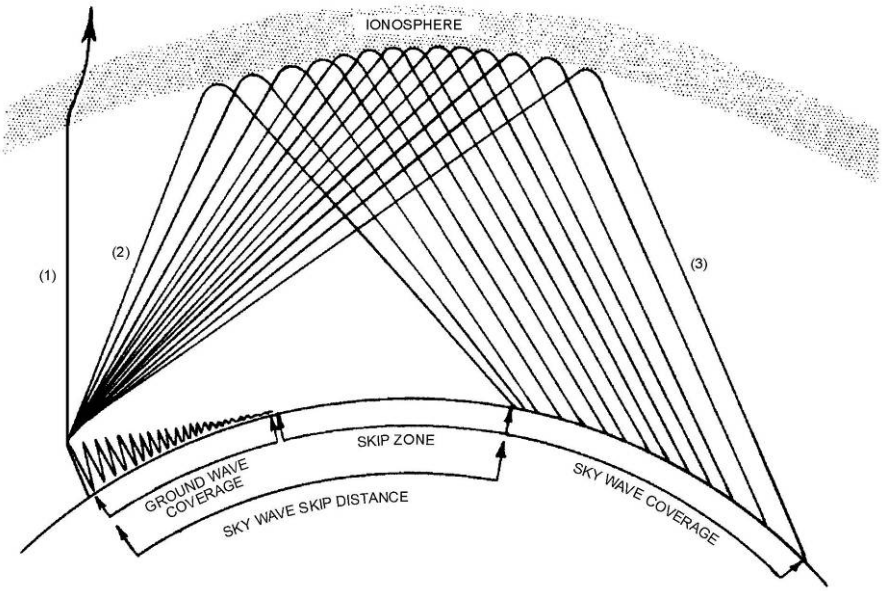


Figure 1-12.—Relationship between skip zone, skip distance, and ground wave.

The SKIP ZONE is a zone of silence between the point where the ground wave becomes too weak for reception and the point where the sky wave is first returned to Earth. The size of the skip zone depends on the extent of the ground wave coverage and the skip distance. When the

ground wave coverage is great enough or the skip distance is short enough that no zone of silence occurs, there is no skip zone.

Occasionally, the first sky wave will return to Earth within the range of the ground wave. If the sky wave and ground wave are nearly of equal intensity, the sky wave alternately reinforces and cancels the ground wave, causing severe fading. This is caused by the phase difference between the two waves, a result of the longer path traveled by the sky wave.

Fading

The most troublesome and frustrating problem in receiving radio signals is variations in signal strength, most commonly known as FADING. There are several conditions that can produce fading. When a radio wave is refracted by the ionosphere or reflected from the Earth's surface, random changes in the polarization of the wave may occur. Vertically and horizontally mounted receiving antennas are designed to receive vertically and horizontally polarized waves, respectively. Therefore, changes in polarization cause changes in the received signal level because of the inability of the antenna to receive polarization changes.

Fading also results from absorption of the rf energy in the ionosphere. Absorption fading occurs for a longer period than other types of fading, since absorption takes place slowly.

Usually, however, fading on ionospheric circuits is mainly a result of multipath propagation.

Multipath Fading

MULTIPATH is simply a term used to describe the multiple paths a radio wave may follow between transmitter and receiver. Such propagation paths include the ground wave, ionospheric refraction, reradiation by the ionospheric layers, reflection from the Earth's surface or from more than one ionospheric layer, etc. Figure 1-13 shows a few of the paths that a signal can travel between two sites in a typical circuit. One path, XYZ, is the basic ground wave. Another path, XEA, refracts the wave at the E layer and passes it on to the receiver at A. Still another path, XFZFA, results from a greater angle of incidence and two refractions from the F layer. At point Z, the received signal is a combination of the ground wave and the sky wave. These two signals having traveled different paths arrive at point Z at different times. Thus, the arriving waves may or may not be in phase with each other. Radio waves that are received in phase reinforce each other and produce a stronger signal at the receiving site. Conversely, those that are received out of phase produce a weak or fading signal. Small alternations in the transmission path may change the phase relationship of the two signals, causing periodic fading. This condition occurs at point A. At this point, the double-hop F layer signal may be in or out of phase with the signal arriving from the E layer.

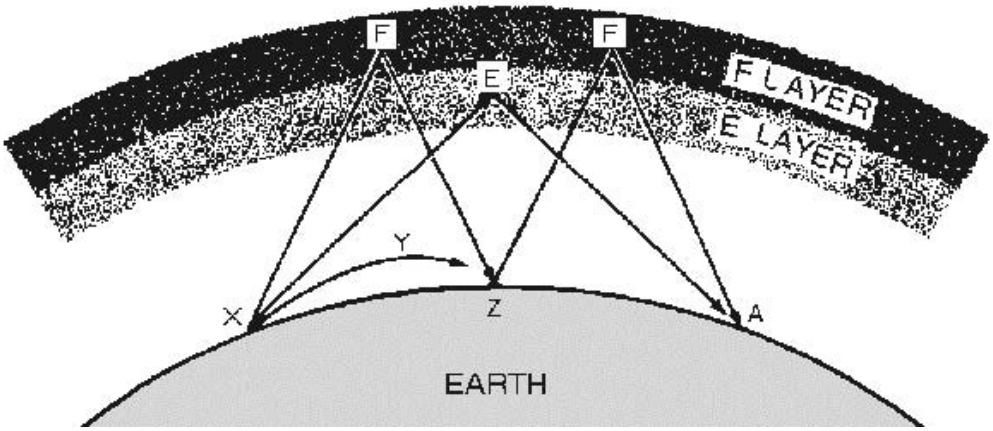


Figure 1-13.—Multipath transmission.

Multipath fading may be minimized by practices called SPACE DIVERSITY and FREQUENCY DIVERSITY. In space diversity, two or more receiving antennas are spaced some distance apart. Fading does not occur simultaneously at both antennas; therefore, enough output is almost always available from one of the antennas to provide a useful signal. In frequency diversity, two transmitters and two receivers are used, each pair tuned to a different frequency, with the same information being transmitted simultaneously over both frequencies. One of the two receivers will almost always provide a useful signal.

☑Learning Check

11. What is the skip zone of a radio wave?

12. Where does the greatest amount of ionospheric absorption occur in the ionosphere?

13. What is meant by the term "multipath"?

Transmission Losses

All radio waves propagated over ionospheric paths undergo energy losses before arriving at the receiving site. As we discussed earlier, absorption in the ionosphere and lower atmospheric levels account for a large part of these energy losses. There are two other types of losses that also significantly affect the ionospheric propagation of radio waves. These losses are known as ground reflection loss and free space loss. The combined effects of absorption, ground reflection loss, and free space loss account for most of the energy losses of radio transmissions propagated by the ionosphere.

Ground Reflection Loss

When propagation is accomplished via multihop refraction, rf energy is lost each time the radio wave is reflected from the Earth's surface. The amount of energy lost depends on the frequency of the wave, the angle of incidence, ground irregularities, and the electrical conductivity of the point of reflection.

Free Space Loss

Normally, the major loss of energy is because of the spreading out of the wavefront as it travels away from the transmitter. As the distance increases, the area of the wavefront spreads out, much like the beam of a flashlight. This means the amount of energy contained within any unit of area on the wavefront will decrease as distance increases. By the time the energy arrives at the receiving antenna, the wavefront is so spread out that the receiving antenna extends into only a very small fraction of the wavefront. This is illustrated in figure 1-14.

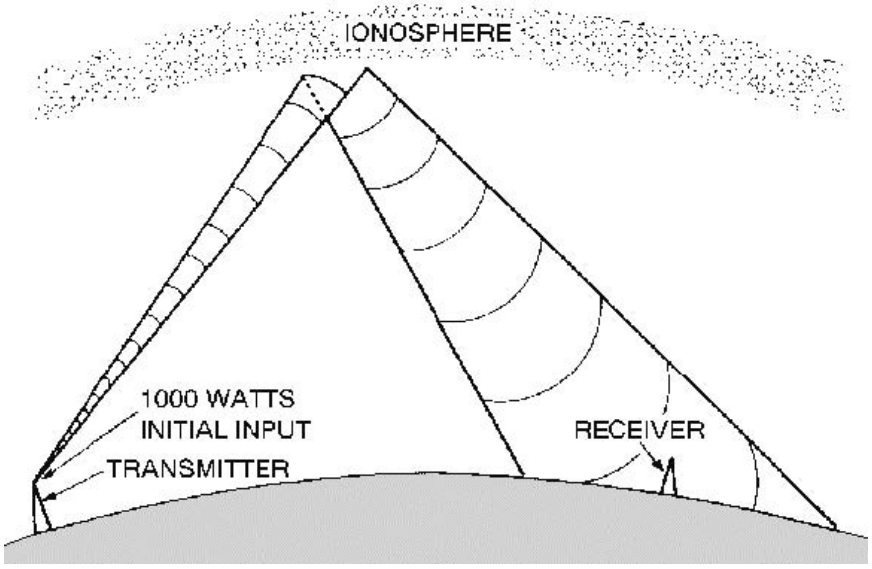


Figure 1-14.—Free space loss principle.

Electromagnetic Interference (EMI)

The transmission losses just discussed are not the only factors that interfere with communications. An additional factor that can interfere with radio communications is the presence of ELECTROMAGNETIC INTERFERENCE (EMI). This interference can result in annoying or impossible operating conditions. Sources of emi are both man-made and natural.

Man-Made Interference

Man-made interference may come from several sources. Some of these sources, such as oscillators, communications transmitters, and radio transmitters, may be specifically designed to generate radio frequency energy. Some electrical devices also generate radio frequency energy, although they are not specifically designed for this purpose. Examples are ignition systems, generators, motors, switches, relays, and voltage regulators. The intensity of man-made interference may vary throughout the day and drop off to a low level at night when many of these sources are not being used. Man-made interference may be a critical limiting factor at radio receiving sites located near industrial areas.

Natural Interference

Natural interference refers to the static that you often hear when listening to a radio. This interference is generated by natural phenomena, such as thunderstorms, snowstorms, cosmic sources, and the sun. The energy released by these sources is transmitted to the receiving site in roughly the same manner as radio waves. As a result, when ionospheric conditions are favorable for the long distance propagation of radio waves, they are likewise favorable for the propagation of natural interference. Natural interference is very erratic, particularly in the hf band, but generally will decrease as the operating frequency is increased and wider bandwidths are used. There is little natural interference above 30 megahertz.

Control of EMI

Electromagnetic interference can be reduced or eliminated by using various suppression techniques. The amount of emi that is produced by a radio transmitter can be controlled by cutting transmitting antennas to the correct frequency, limiting bandwidth, and using electronic filtering networks and metallic shielding.

Radiated emi during transmission can be controlled by the physical separation of the transmitting and receiving antennas, the use of directional antennas, and limiting antenna bandwidth.

☑Learning Check

14. What are the two main sources of emi with which radio waves must compete?

15. Thunderstorms, snowstorms, cosmic sources, the sun, etc., are a few examples of emi sources. What type of emi comes from these sources?

16. Motors, switches, voltage regulators, generators, etc., are a few examples of emi sources. What type of emi comes from these sources?

17. What are three ways of controlling the amount of transmitter-generated emi?

18. What are three ways of controlling radiated emi during transmission?

Weather versus Propagation

Weather is an additional factor that affects the propagation of radio waves. In this section, we will explain how and to what extent the various weather phenomena affect wave propagation.

Wind, air temperature, and water content of the atmosphere can combine in many ways. Certain combinations can cause radio signals to be heard hundreds of miles beyond the ordinary range of radio communications. Conversely, a different combination of factors can cause such attenuation of the signal that it may not be heard even over a normally satisfactory path. Unfortunately, there are no hard and fast rules on the effects of weather on radio transmissions since the weather is extremely complex and subject to frequent change. We will, therefore, limit our discussion on the effects of weather on radio waves to general terms.

Precipitation Attenuation

Calculating the effect of weather on radio wave propagation would be comparatively simple if there were no water or water vapor in the atmosphere. However, some form of water (vapor, liquid, or solid) is always present and must be considered in all calculations. Before we begin

discussing the specific effects that individual forms of precipitation (rain, snow, fog) have on radio waves, you should understand that attenuation because of precipitation is generally proportionate to the frequency and wavelength of the radio wave. For example, rain has a pronounced effect on waves at microwave frequencies. However, rain hardly affects waves with long wavelengths (hf range and below). You can assume, then, that as the wavelength becomes shorter with increases in frequency, precipitation has an increasingly important attenuation effect on radio waves. Conversely, you can assume that as the wavelength becomes longer with decreases in frequency, precipitation has little attenuation effect.

Rain

Attenuation because of raindrops is greater than attenuation because of other forms of precipitation. Attenuation may be caused by absorption, in which the raindrop, acting as a poor dielectric, absorbs power from the radio wave and dissipates the power by heat loss or by scattering (fig. 1-15). Raindrops cause greater attenuation by scattering than by absorption at frequencies above 100 megahertz. At frequencies above 6 gigahertz, attenuation by raindrop scatter is even greater.

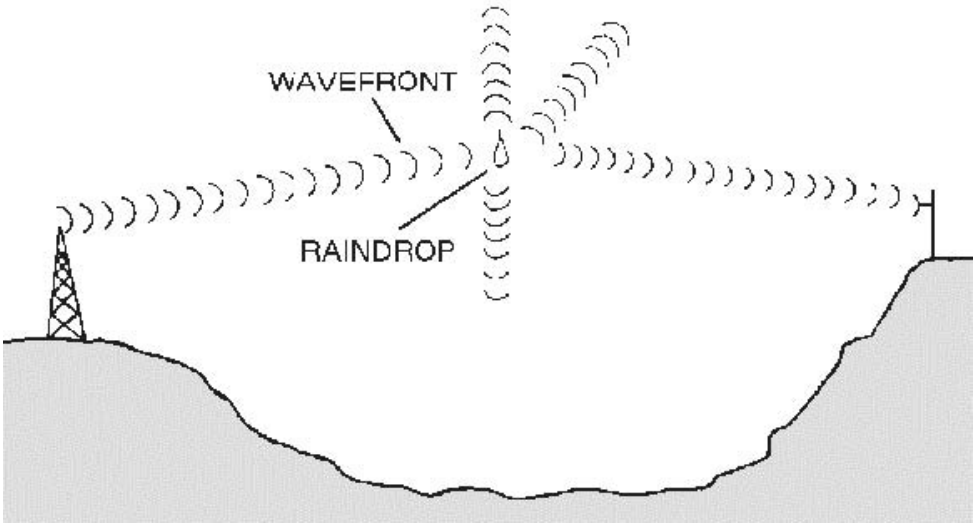


Figure1-15.—Rf energy losses from scattering.

Fog

In the discussion of attenuation, fog may be considered as another form of rain. Since fog remains suspended in the atmosphere, the attenuation is determined by the quantity of water per unit volume and by the size of the droplets. Attenuation because of fog is of minor importance at frequencies lower than 2 gigahertz. However, fog can cause serious attenuation by absorption, at frequencies above 2 gigahertz.

Snow

The scattering effect because of snow is difficult to compute because of irregular sizes and shapes of the flakes. While information on the attenuating effect of snow is limited, scientists assume that attenuation from snow is less than from rain falling at an equal rate. This assumption is borne out by the fact that the density of rain is eight times the density of snow. As a result, rain falling at 1 inch per hour would have more water per cubic inch than snow falling at the same rate.

Hail

Attenuation by hail is determined by the size of the stones and their density. Attenuation of radio waves by scattering because of hailstones is considerably less than by rain.

Temperature Inversion

Under normal atmospheric conditions, the warmest air is found near the surface of the Earth. The air gradually becomes cooler as altitude increases. At times, however, an unusual situation develops in which layers of warm air are formed above layers of cool air. This condition is known as TEMPERATURE INVERSION. These temperature inversions cause channels, or ducts, of cool air to be sandwiched between the surface of the Earth and a layer of warm air, or between two layers of warm air.

If a transmitting antenna extends into such a duct of cool air, or if the radio wave enters the duct at a very low angle of incidence, vhf and uhf transmissions may be propagated far beyond normal line-of-sight distances. When ducts are present as a result of temperature inversions, good reception of vhf and uhf television signals from a station located hundreds of miles away is not unusual. These long distances are possible because of the different densities and refractive qualities of warm and cool air. The sudden change in density when a radio wave enters the warm air above a duct causes the wave to be refracted back toward Earth. When the wave strikes the Earth or a warm layer below the duct, it is again reflected or refracted upward and proceeds on through the duct with a multiple-hop type of action. An example of the propagation of radio waves by ducting is shown in figure 1-16.

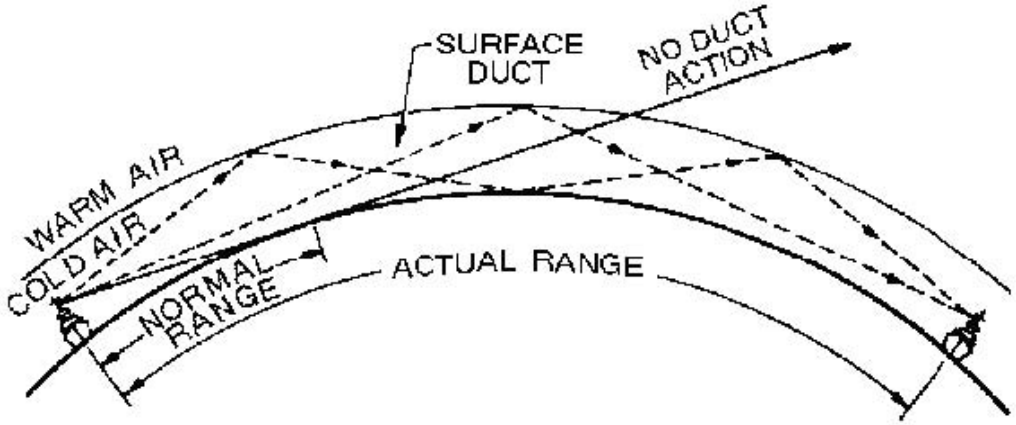


Figure 1-16.—Duct effect caused by temperature inversion.

☑Learning Check

19. How do raindrops affect radio waves?

20. How does fog affect radio waves at frequencies above 2 gigahertz?

21. How is the term "temperature inversion" used when referring to radio waves?

22. How does temperature inversion affect radio transmission?

Tropospheric Propagation

As the lowest region of the Earth's atmosphere, the troposphere extends from the Earth's surface to a height of slightly over 7 miles. Virtually all weather phenomena occur in this region. Generally, the troposphere is characterized by a steady decrease in both temperature and pressure as height is increased. However, the many changes in weather phenomena cause variations in humidity and an uneven heating of the Earth's surface. As a result, the air in the troposphere is in constant motion. This motion causes small turbulences, or eddies, to be formed, as shown by the bouncing of aircraft entering turbulent areas of the atmosphere. These turbulences are most intense near the Earth's surface and gradually diminish with height. They have a refractive quality that permits the refracting or scattering of radio waves with short wavelengths. This scattering provides enhanced communications at higher frequencies.

Recall that in the relationship between frequency and wavelength, wavelength decreases as frequency increases and vice versa. Radio waves of frequencies below 30 megahertz normally have wavelengths longer than the size of weather turbulences. These radio waves are, therefore, affected very little by the turbulences. On the other hand, as the frequency increases into the vhf range and above, the wavelengths decrease in size, to the point that they become subject to tropospheric scattering. The usable frequency range for tropospheric scattering is from about 100 megahertz to 10 gigahertz.

☑Learning Check

23. In what layer of the atmosphere does virtually all weather phenomena occur?

Study 2: Voice versus Data

Reference Material: NLECTC Guidebook - Chapter 5

Chapter 5

Voice Versus Data

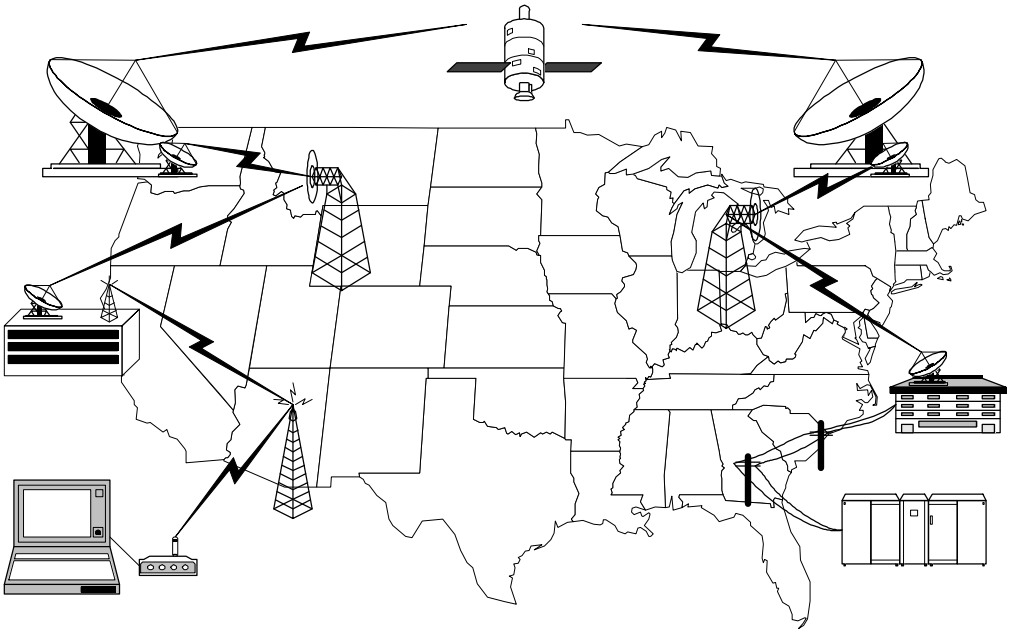
Voice Versus Data

Two types of communications, voice and data, have been traditionally sent over public safety radio systems. Voice communications includes all audio transmissions, which start as voice and end as voice.

Data communications involves the transmission of data from one computer to another, through one or more communications channels (standard telephone lines, radios, etc.). When data are sent over long distances, it is likely that a number of different types of communications channels will be used.

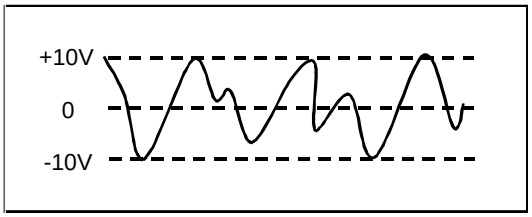
For example, figure 5-1 shows the various communications methods involved in sending data from an agency in California to an agency in Florida.

Figure 5-1. Cross-country Communications



Voice normally occurs as an analog signal. In other words, the signal may vary continuously over a specific range of values. In figure 5-2, the voltage of the analog signal may take on any value between -10 volts and +10 volts.

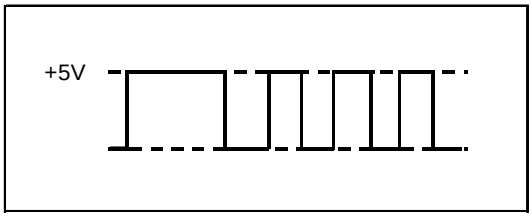
Figure 5-2. Analog Signal



Computers store data electronically. Circuits in the computer can detect the presence or absence of electronic impulses. A bit (binary digit) is the smallest piece of information contained in a data transmission and can only represent one of two values: a zero (0) or a one (1). Combinations of bits are strung together to represent numbers, letters, and other special characters.

Data can also be represented as a digital signal, which can only assume discrete values. For example, in figure 5-3 below, the voltage of the digital signal may only take on the values of either 0 volts (“off” or zero) or +5 volts (“on” or one).

Figure 5-3. Digital Signal



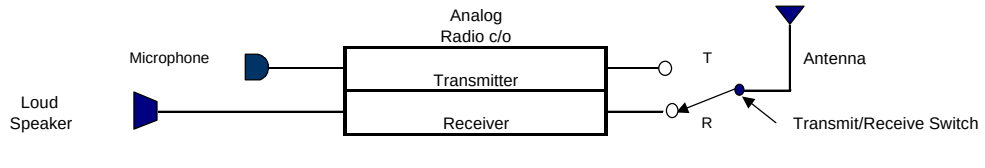
Analog Versus Digital

Voice and data can both be packaged and transmitted using either analog or digital signals. This section discusses the differences between using an analog transmission method and a digital transmission method.

Analog Radio Systems

Analog radio systems continuously transmit radio waves that are usually modulated by a voice. A typical analog voice radio consists of a transmitter and receiver (figure 5-4).

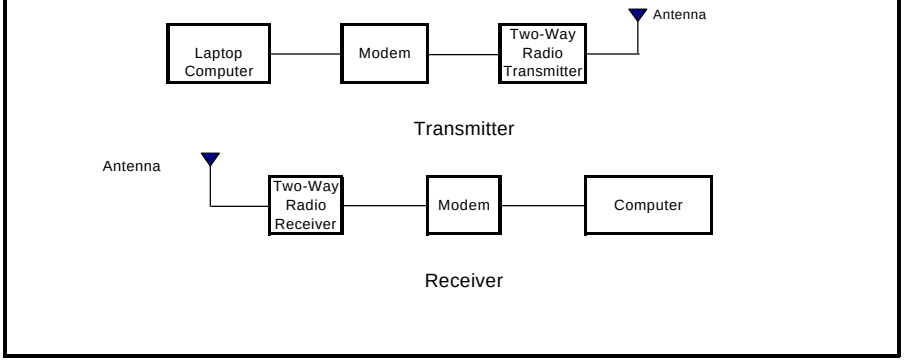
Figure 5-4.Block Diagram of a Typical Radio System



An analog system may also carry data. However, the data, which are in digital form of binary digits, or bits (i.e., ones and zeros), must first be converted to an analog signal. A modem (modulate/demodulate unit) is used to convert the ones and zeros into two analog tones representing either a one or a zero. When the analog data arrive at the receiver, they are converted back to digital form again using another modem.

Figure 5-5 shows a laptop computer connection through a modem to a typical two-way FM radio. The laptop generates data as ones and zeros that are converted via the modem to analog tones that go into the radio transmitter. Once received, the detected tones pass through a second modem that converts the signal back to digital data and sends them on to another computer for additional processing (e.g, display, printing, query to NCIC).

Figure 5-5. Block Diagram of an Analog Cellular Phone with a Laptop Computer



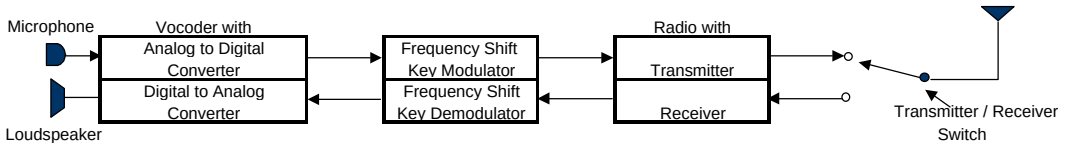
Digital Radio Systems

People cannot usually understand digital signals. Our senses are analog oriented and can only respond to continuous signals or impressions. Therefore, we must hear voice transmissions on a loudspeaker or a set of headphones and see visual signals, on either a video monitor or a printer, as words and pictures.

Voice transmissions may be sent over digital radio systems by sampling voice characteristics and then changing the sampled information to ones and zeros to modulate the carrier. This is done using a circuit called a voice coder, or "vocoder." At the receiver, the process is reversed to convert the digital voice samples back into analog voice.

A diagram of a typical digital voice radio system is shown in figure 5-6.

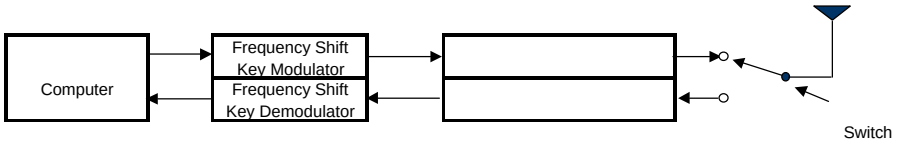
Figure 5-6. Block Diagram of a Voice Modulated Digital Radio System



A digital radio system transmits data directly, by digitally modulating a carrier. One simple method of modulation is to change the carrier frequency by shifting it different amounts for each type of bit. (This is called *frequency shift keying*, or FSK.) The receiver then receives the signal as a zero or as a one and re-creates the original signal.

A simplified digital radio is shown in figure 5-7. The ones and zeros are detected and regenerated at a receiver for use in a computer.

Figure 5-7. Block Diagram of a Typical Digital Radio System



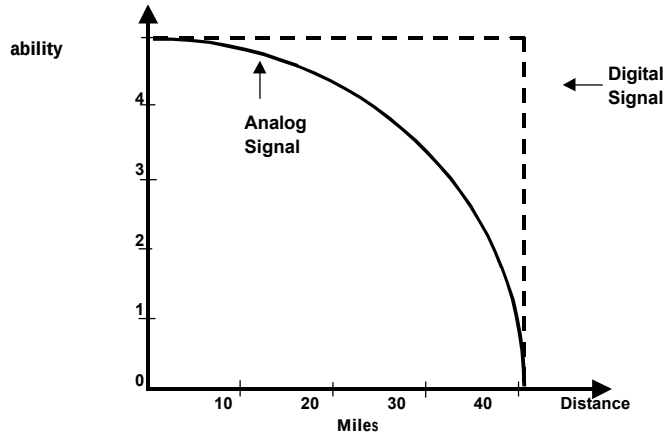
Transmission Differences

Analog and digital radio systems have vastly different transmission characteristics. As you move away from an analog radio transmitting site, the signal quality decreases gradually while noise levels increase. The signal becomes increasingly more difficult to understand until it can no longer be heard as anything other than static.

A digital signal has fairly consistent quality as it moves away from the transmitter until it reaches a threshold distance. At this point, the signal quality takes a nose dive and can no longer be understood.

A comparison of the transmission differences between analog and digital signals is shown in figure 5-8.

Figure 5-8. An Analog Versus Digital Signal



Encryption

Encryption is a methodology that scrambles a voice or data message to protect its content from unauthorized use, or from those who would use it to the disadvantage of the agency or the public (such as the media during a hostage situation).

Encryption technology is regulated by the federal government and is generally broken into 4 types: Type I is restricted to federal agencies for uses involving national security; Type II is currently not defined; Type III is available for use by local/state government agencies; and Type IV is available for use by the general public.

Older analog radio systems employed encryption systems that chopped voice spectrum into pieces and rearranged or inverted these pieces to make them difficult to understand. The resulting encrypted audio was often high-pitched, sounding like a cartoon character talking. There was no change in system coverage with this technology.

Later digital implementations of encryption converted the analog voice spectrum to a digital waveform and transmitted it with a different modulation. While much more secure than analog inversion systems, the range of these systems was often severely degraded when operating in encrypted mode.

Study 3: Voice Communications

Reference Material: COPS Interoperability Tech Guide - Chapter 16, Pages 245-258

Understanding the Technologies

SAFECOM Library The SAFECOM online library is a prime source for technical information about voice communications systems. It includes documents from multiple sources, including the past Public Safety Wireless Network (PSWN) Program. See **http://www.safecomprogram.gov/SAFECOM/library/technology/**.

Public safety communications technology parallels consumer and other commercial technologies. As more digital communications are used, voice becomes more indistinguishable as the "payload" over much of the networks connecting senders and receivers of information. It has unique features that shape how it's moved from the analog world of sound, handled over digital transmission systems, and then converted back to sound. However, in most ways it can be transported and stored in digital form just like more traditional data.

While voice and data communications for public safety services have long been conducted over both wired and wireless links, we focus here mostly on the latter. It's there that the greatest communications interoperability challenges have occurred for first responders. Recognize that advanced radio systems increasingly include many wired components at their cores, just as voice and data are increasingly intertwined in emergency response communications.

FCC Classification of Radio Systems

Before we look at the primary voice radio technologies, let's pause to clarify some terminology and look at FCC classifications of radio systems.

The FCC uses specific terms to distinguish radio technologies and their uses. The term *type* is used to distinguish different fundamental technologies, while *services* distinguish between different applications of the technology.

The FCC distinguishes radio *types* and *services*.

The term *type acceptance* is commonly used in the radio world. It refers to the FCC's formal process of evaluating and approving technologies. Individual manufacturer radio models must receive FCC-type acceptance before they can be made commercially available. It's not uncommon to hear manufacturer representatives speak of new models and note they are awaiting type acceptance before they will be mass-manufactured and sold.

Several *radio services* are used by public safety agencies, including:

- Broadcast
- Aeronautic
- Unlicensed
- Commercial
- Maritime
- Land mobile
- Specialized mobile
- Amateur.

Traditional dispatch, car-to-car, and field communications used by public safety is *land mobile radio* (LMR). This term is commonly used by industry and in regulations in reference to terrestrial radio services to support mobile users. Portable and car radios are both classified as "mobile" at this level of discussion.

The FCC classifies most public safety radio systems as *private radio*.

While several of the radio services listed above are probably recognizable to readers, others may be confusing. Most public safety radio networks are regulated by the FCC as *private radio* systems. Where common carrier systems are made commercially available for general public use, those built and operated for private use are considered private systems. In this case, "private" refers to how they're used, rather than owned.

More than 300 agencies in South Carolina use the Palmetto 800 System, an 800 MHz system shared with power utility companies. For further information, see: **http://www.cio.sc.gov/cioContent.asp?pageID=756&menuID=411**.

Many commercial industries have their own private radio systems. A few are actually shared with public safety agencies, but the vast majority of police, fire, and EMS voice radio communications takes place over systems owned and operated by the agencies themselves. Most of these systems require FCC licensing. Unlicensed radio technologies, such as those that might be used for wireless local area networks (WLAN), are regulated separately.

Whether licensed or unlicensed, private or common carrier, radio technologies are broadly subject to FCC regulations. Rely on your radio technicians, vendor representatives, frequency coordinators, and professional associations to help you sort out details if you intend to be heavily involved in radio technology.

Analog and Digital Radio Technologies

For the first century of radio, analog radio technologies predominated. Those technologies include *amplitude modulated* (AM) and *frequency modulated* (FM) radios that we're all familiar with from broadcast radio services. Others exist, but all analog technologies are based on use of audio tones (frequencies) being superimposed on radio frequencies (RF) in a standardized manner.

Audio frequencies, such as those delivered electronically by radio microphones, are mixed with RF within analog radio circuitry, further amplified, and then transmitted. At distant receivers, the audio is extracted electronically in more or less the reverse manner. Data can be transmitted much like voice over analog systems by encoding bits using different audio tones and other techniques of shaping the transmitted RF signal.

■ Channel Bandwidth

FM is by far the most common analog radio mode today. It is also the compatibility or legacy mode for digital radios. However, transmitters and receivers not only have to use common means of putting information on the RF signal (i.e., modulating it), they also have to use compatible channel widths and operate in the same frequency band, such as VHF, UHF, or 800 MHz.

Public safety frequency bands for voice communications are typically described in megahertz, while channel bandwidths are described in kilohertz.

Frequency bands for common public safety voice purposes are typically described in millions of radio wave cycles per second, or megahertz (MHz) (Figure 16-2). They are occupied by channels of a certain *bandwidth*. That is, they take up a specific amount of the frequency band.

Channel bandwidths are described in thousands of cycles per second (kilohertz is abbreviated as kHz). A channel is a slice of some part of the radio frequency spectrum. That is, we talk about a traditional 25 kHz voice channel in the 450 MHz public safety frequency band. A traditional voice channel in that band has been allotted 25 kHz of RF spectrum.

■ Narrowband Channels

Narrowbanding, as discussed in Chapter 14 (Page 223), is an FCC regulatory effort that will affect all analog radio users. Its goal is to reduce the amount of RF spectrum occupied by a single channel to increase the number of channels that can fit in a given band. This is not the first time the FCC has split channels for this purpose and we can expect it to happen again.

The FM radio channel has existed for decades as nominally 25 kHz in width. We say "nominally" because channel width is more an absolute under regulations than under the laws of physics. It actually varies in width according to transmitter adjustments and characteristics of the audio being carried. In addition, the transmitted power isn't all contained within the defined channel; a progressively smaller fraction exists farther and farther away from the channel center.

The FCC requires that public safety operations move to 12.5 kHz channels or the equivalent by January 1, 2013.

FCC rules will have all public safety voice operations between 150 and 512 MHz moved to narrowband (12.5 kHz) channels by January 1, 2013. Technically, the requirement is that a channel can occupy no more than 12.5 kHz or the effective

equivalent. This last clause can be a bit confusing. There are proprietary techniques to interweave two separate conversations, both using the whole 25 kHz, but splitting use of the channel second by second. Most commonly, the narrowband channel will be used wholly for a single communications path.

One net effect of this transition is that narrowband analog transmitters will have less spectral space to put RF energy, thus reducing the power and range of an analog channel relative to the wider band channel. Just how much is the subject of debate, but recognize that the range of a narrowband transmitter will be less than that of its wider band cousin.

While digital uses of these radio bands are similarly affected, existing digital technologies already use 12.5 kHz channels or allow multiple voice conversations to occur within a traditional 25 kHz channel. Narrowbanding is thus leading to wider adoption of digital techniques.

■ Digital Radio

Digital radios use many of the same components as their analog relatives. For voice radio purposes, microphone audio frequencies are first converted into bits by the *voice encoder* or *vocoder*. This is a particularly important part of the digital radio system; not all vocoders are created equally. For public safety purposes, great work has gone into testing and choosing vocoders that efficiently produce a digital stream to make most use of the radio channel, while still faithfully representing it.

A vocoder converts analog sound to digital bits.

The process of creating digitized audio, transmitting it over the largely inhospitable airwaves, and decoding it on receivers is fraught with danger for the lowly voice bit. Project 25,[57] which produced the national standard for public safety digital voice radio systems, took on the challenge. It undertook a significant effort to find a vocoder sufficiently efficient, yet producing resiliently encoded audio for the most critical missions, in some of the most difficult radio environments. The Project 25 vocoder standard was selected as a careful balance of efficiency, robustness, and fidelity.

The P25 vocoder standard carefully balances efficiency, robustness, and fidelity.

Digital radio standards for public safety don't stop at speech encoding, however. As a matter of fact, the vocoder is just a small part of the technology that takes audio,

[57] Initiated by the Association of Public-Safety Communications Officials – International (APCO), in cooperation with the National Association of State Telecommunications Directors (NASTD) and with support of other public safety organizations like the International Association of Chiefs of Police (IACP). Project 25 received its name following APCO's tradition of numbering its broad initiatives to affect the public safety communications world. P25, as it is also commonly known, is the association's best-known project. The specifications have been codified by standards development organizations. For further information, see **http://www.project25.org**.

Radio transmissions are weakened over distance and by the environment.

encodes it, packages it up, inserts it aboard the radio channel train, and assures it can be unpackaged successfully on the other end.

Another key piece of the Project 25 standard is its *Common Air Interface* (CAI). Without going into depth, the CAI provides the standardized means for receiving radios to recognize what is coming over the airwaves and extract an intelligible signal. Any digital receiver has to know how to decode the audio bit stream once received and passed to internal microprocessors, and then convert it back to audio frequencies that can be heard through speakers. That's not all, though. Receiving radios also have to know when and where a package of bits begins and ends, how to deal with inevitably missing or erroneous bits, how to recognize other embedded codes, and more. Project 25's CAI is the standard for how that's done with public safety digital voice radios.

The P25 Common Air Interface is the public safety standard for digital, RF transmissions.

Standards are absolutely essential for interoperability of radio systems.

■ The Radio Environment – Analog

Once transmitted, radio waves are subjected to the same environmental effects regardless of their payload. The laws of physics aren't particularly concerned with whether they're bearing analog or digitally encoded information.

It's a hostile environment. Received radio signals may be millions and millions of times weaker than they were at their source. Not only do signals diminish geometrically as a function of distance, they also are weakened or *attenuated* by the environment over and through which they pass. Manmade and natural obstructions both tend to absorb radio waves. Similarly, each time a radio wave is reflected or diffracted (which is often!), it scatters and loses a bit more energy. Add to this the additional challenges imposed by relatively rapidly moving transmitters and receivers and it's nothing short of fundamental magic that any intelligence can be extracted from distant transmissions!

Anyone who has listened to an FM broadcast recognizes the sound of a station fading in and out. If you've listened carefully in areas where FM broadcast stations overlap on the same frequency, you've also heard the effects of two roughly equal signals competing in your receiver. "Roughly" in the radio world is measured in factors of tens and hundreds. A signal that is 100 times or stronger than competing signals will generally be the only one heard on a channel. In the radio environment, signals can vary by a factor of a hundred within the distance of a few feet.

FM has something called the *capture effect* whereby once a receiver is locked on to a given signal, it rejects a competing one up to a point. As the new signal becomes increasingly stronger, the receiver finally gives up on the first and locks onto the

second. In between, distorted and mixed audio is heard. Portable and mobile radio users of two-way FM channels quickly learn to recognize the signs of one user "walking on" another through overlapping transmissions.

■ The Radio Environment – Digital

Digital radio technologies designed for public safety use error correction techniques to recover intelligible audio from signals that are battered about by the environment and other radio users. *Forward error correction* (FEC) techniques are used to allow a receiver to recreate a damaged signal from, in effect, redundant parts of the digital stream. Additional signal information takes up part of the digital channel for FEC purposes.

The term *bit error rate* (BER) is used to describe the percentage of received bits in a digital stream that are "broken." While public safety radio technologies can recover nearly original audio with bit error rates in the vicinity of 2 percent, recovered audio starts to degrade as error rates increase.[58] See Figure 16-3, Anyone who has used a cellular telephone in recent years has noticed the effect of weak digital signals on caller voice intelligibility. At some point the BER becomes too high for digital signal processors to recover accurate audio from the digital stream, leading the receiver to shut off digital-to-audio conversion rather than pushing noise to its speaker.

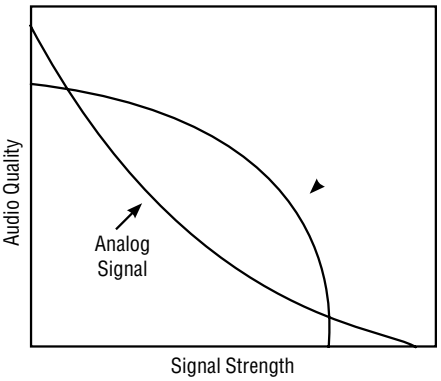


Figure 16-3: Recovered Audio Quality by Signal Type

While the human ear and brain has a remarkable ability to recover intelligent audio in the presence of relatively high noise levels, digital radio receivers are more limited. At some point they have to stop trying lest they start making up sounds that weren't originally there. By comparison, intelligible audio can be discerned by the human ear

[58] Vanderau, John M., Delivered Audio Quality Measurements on Project 25 Land Mobile Radios, NTIA Report 99-358 (Washington, D.C.: U.S. Department of Commerce, Institute for Telecommunications Science, 1998). A BER of 2 percent corresponds to a Delivered Audio Quality (DAQ) measure of 3.4. See **http://www.its.bldrdoc.gov/pub/ntia-rpt/99-358/**.

through an FM or other analog receiver at a lower signal level than a digital receiver can use. On the other hand, a digital receiver can recreate the identical audio signal that was sent, while the received analog signal gains increasing background noise as it gets weaker.

Let's move on to the different types of systems that put analog and digital radio technologies to work.

Conventional and Trunked Radio Systems

There are two broad categories of radio systems used for voice communications today: Conventional and trunked. In order to understand the difference, it's useful to first understand a few basic system principles and common building blocks.

■ Building Blocks – Simplex Communications

Land mobile radio systems are commonly designed to allow one party in a conversation to talk while others listen. By contrast, telephone systems throughout the years have been designed so both parties may speak simultaneously. Voice radio protocols in public safety have evolved around the fact that only one speaker has access to a channel at a time.

The common term for this form of communications is *simplex.* In radio usage, the term carries further meaning. Simplex radio channels carry conversations conducted on a single frequency where participant radios transmit (Tx) and receive (Rx) on the same frequency. In Figure 16-4, "Frequency 1" (F_1) is used for all transmissions.

The radio depicted at the tower is referred to as a *fixed-base station*, whether it is closely or remotely attached to agency facilities. The base station could be placed on a mountaintop far from dispatch facilities, for example, and controlled remotely.

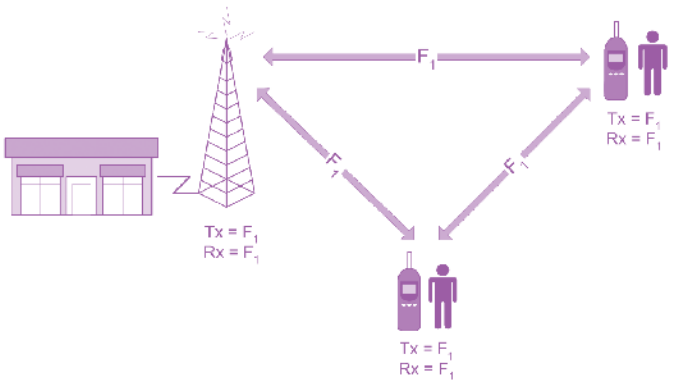


Figure 16-4: Simplex Radio Example

This approach to radio communications works well and is the simplest, most resilient form of coverage when all radio users are within range of one another. It becomes problematic, though, when radio end users move out of range of each other.

In all two-way voice systems, from the simplest to most complex, radio coverage is, well, a two-way street. It's relatively easy to increase the transmission range of a base station by increasing its power, but that doesn't help users of mobile and portable radios, which are comparatively weaker, talk back to the base. Radio engineers work to balance the "talk-in" and "talk-out" of systems.

■ Building Blocks – Duplex and Half-duplex Communications

When transmissions need to be relayed to include all users on a channel, a different class of radio station is used that can simultaneously receive a transmission from one user and retransmit it to all others. This capability is referred to as *duplex* communications. User radios typically can transmit or receive, but not do both simultaneously. As a whole, such systems of users and fixed stations are considered to be *half-duplex* because end users are transmitting or receiving, while stations relaying communications in the middle are doing both, simultaneously.

True duplex communications, as commonly experienced with telephones, allow the most natural forms of conversation. Since land mobile radio has evolved for one-to-many conversations in which at any moment there is one speaker and many more listeners, full duplex systems are unusual. As anyone who has ever been part of a telephone conference call can attest, having simultaneous "transmission" capabilities across all participants can actually impede communications at times.

■ Building Blocks – Repeaters

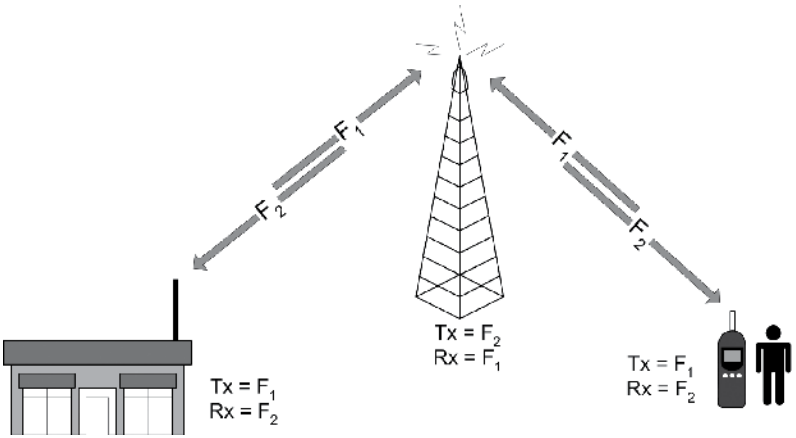
Half-duplex relays are fundamental building blocks of public safety radio systems. "Mobile relay" is the official term for this class of station, but they're widely known as "repeaters." Repeaters as described have been used by public safety agencies for decades to automatically relay transmissions for system users who would otherwise be restricted in range by direct, simplex systems.

A repeater retransmits on one frequency what it receives on another, well separated from one another to reduce interference.

Repeaters are typically placed permanently with a well-situated antenna high up on a tower, building, or hilltop. From this vantage point, a repeater receives transmissions on one frequency and retransmits them on another. This serves to extend the effective range of a lesser powered radio, such as a portable, allowing other users of the channel to hear and talk with others at greater distances. Other fixed radio stations—at dispatch, for example—can also transmit through the repeater. These are known as *control stations*.

The repeater's frequencies have to be separated sufficiently from a spectrum point of view to keep the transmitter from overpowering the receiver. If not, the repeater's transmitter effectively prevents its receiver from "hearing" the relatively much weaker, distant signals. Some of the magic of radio engineering is dedicated to avoidance of these and more complex interference effects. Sophisticated antenna systems are used to isolate a repeater's transmissions from its receiver so it doesn't become the radio equivalent of an alligator: All mouth and no ears.

Figure 16-5 shows how frequencies are split between the repeater and its users. Note that the repeater's frequency pairing is the reverse of the other radios. Field users, including those at the station, transmit on Frequency 1 (F_1) but receive on Frequency 2 (F_2)—the repeater's transmission frequency. The repeater does the reverse.



something of an electromagnetic disadvantage compared to those on vehicle roofs. The human body, itself, tends to block radio waves that would otherwise be received or transmitted by the portable. To this, add the fact that portables can be and are often carried into locations far less friendly to radio emissions than the streets where vehicular radios operate.

Radio system design is hugely affected by whether primary coverage is sought for portable or mobile radio use. Two-way radio networks, voice and data alike, are built to take into account differences between fixed and mobile devices on the network.

■ System Building Blocks – Simulcast and Receiver Voting Systems

Coverage needs lead to use of simulcast systems where multiple sites transmit the same signal simultaneously to cover an area.

The technologies discussed so far have been in use for decades. In these *conventional* radio systems, there is a one-to-one correspondence between each frequency (or pair of frequencies in duplex or half-duplex operations) and a channel. In effect, channels are simply defined by who has and uses the designated frequencies within a given area of operation.

Large-scale, wide area systems have been built for years with conventional technologies. Public safety agencies have put up multiple repeaters to provide needed channel capacity for simultaneous operations and to cover wider areas. Capacity and coverage demands call for multiple repeaters at a single site in some cases and multiple sites in others. It's not uncommon to use multiple sites to provide coverage that can't be had from a single site. With such systems, users are relied upon to use the appropriate channel (i.e., frequency) depending on their job and location.

It's possible with conventional systems to simultaneously transmit the same signal from multiple locations. This is referred to as *simulcasting*. It requires careful synchronization of the individual transmitters and a healthy backbone of microwave or some other form of dedicated telecommunications circuit to deliver the outbound signal to all sites simultaneously.

In the example shown in Figure 16-6, audio to be transmitted from all sites simultaneously originates from the central facility—a dispatch center, for example.

While simulcasting reduces the need for users to manually "steer" their radios by the channel selector knob as they move around a geographic area, it adds system complexity and a reliance on the circuits connecting to remotely operated base stations. It also brings a need for the system to deal with the common situation of two or more sites receiving a transmission from a field user. Just as a field user's radio will likely receive a transmission simultaneously from multiple sites, it will also likely be heard by multiple ones when it's transmitting.

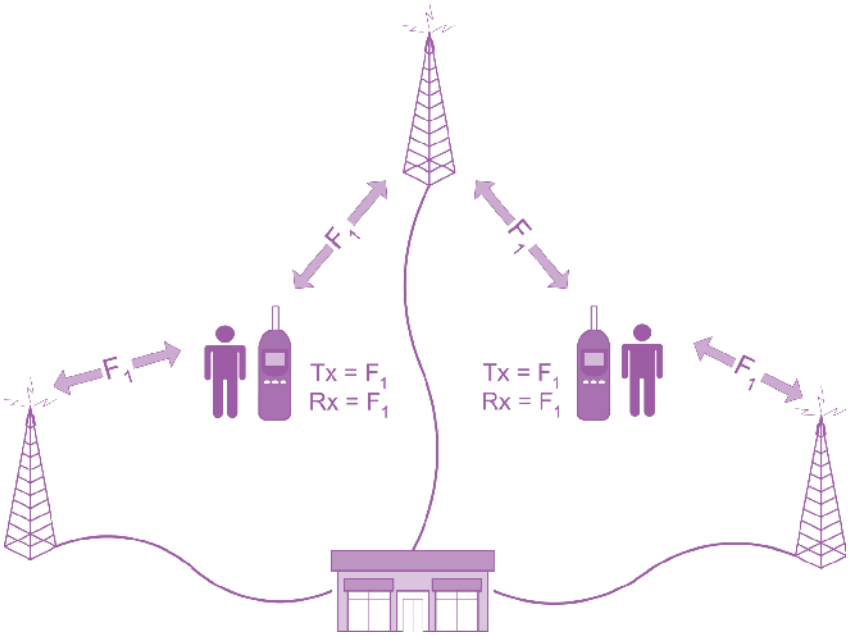


Figure 16-6: Simulcast Simplex Radio Example

Additional electronics are added to the heart of the system to select the best signal received by the sites. In the example shown in Figure 16-6, two sites might receive decent signals from a user, while the third site receives a weak signal. Central electronics pick out the best signal and pass it to users at the fixed facility.

This is known as a *simulcast* system with receiver voting. For practical purposes, the system can be thought of as a single base station with the wide, composite coverage provided by all the separate sites. The effect is a single channel that covers a wide expanse. While useful in low-traffic, routine operations, such wide-area, blanket coverage can be a problem during periods of high demand when the load across all sites can overwhelm a single channel.

The final conventional radio example to be presented here combines multiple technologies and adds a new one: Remote receivers. Actually, remote receivers have been depicted in the previous examples, too, but have been paired with their associated transmitters.

Figure 16-7 depicts a repeater system with additional remote receivers. Sites labeled "Rx Only" are simply receivers that send back received signals to the central site where a *voter* can pick out the best received signal. Remote receivers are often used to

accommodate portable radios that can "hear" the more powerful and well-situated fixed transmitter sites, but are unable to "talk" back to them due to the distance or terrain.

Remote receivers allow weaker signals to get into the system.

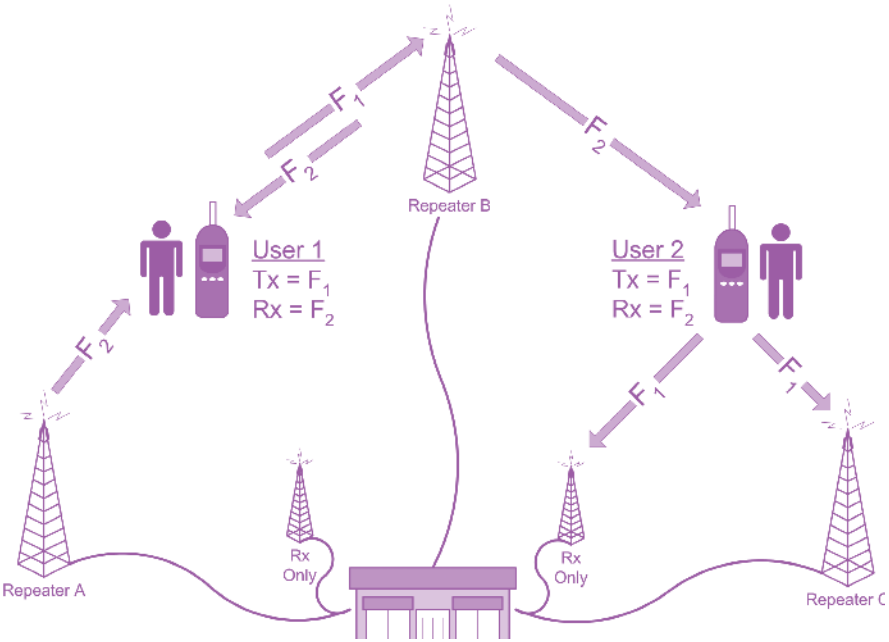


Figure 16-7: Simulcast Repeaters with Remote Receivers

In this example, some possible receive and transmit paths have been omitted for the sake of clarity. It depicts a circumstance where Repeater A can be heard by User 1, but that user can only be heard by Repeater B. Repeater B can be heard by both users, but User 2 can only be heard by Repeater C and one of the remote receivers.

The combinations and permutations of which transmitter can be heard by which receiver—both fixed and mobile—are nearly endless in a large system. Imagine how complex this can become with dozens of fixed sites with multiple channels. It should be no wonder that radio engineers are needed to design and carefully tune all the components that make such an electromagnetic marvel operate!

■ System Building Blocks – Trunking

The next major technology used for public safety operations is *trunking*. Simply put, trunking is the means to share a limited number of frequencies between users, with each set of users having its own virtually private channels.

Trunking is widely used in telecommunications systems. Users of the public switched telephone network serving businesses, residences, and emergency response agencies worldwide are well experienced at using a trunked system—even if they are unaware of it. Complex technology assigns circuits (channels) dynamically upon requests for access, such as occurs when a telephone number is dialed. The newly assigned circuit may have just been used for an entirely different telephone call between different locations, but now is being reassigned.

Radio systems can be constructed to operate the same way. The primary value of trunking is channel efficiency. That is, rather than having sets of users occupy a channel fixed by frequency, leaving the channel empty at times and overloaded at others, the trunked system takes multiple channels and assigns them to sets of users as needed. This also enables groups of users that could never have a separate conventional channel to have a trunked one for private use.

Trunking provides multiple virtual channels for separate conversations.

With a conventional system, three repeaters at a single site might have served police, fire, and EMS, individually, with all users from one of the disciplines operating on a single channel. With these three repeaters trunked, a nearly limitless number of virtual channels can be assigned and used without interference between users. However, the number of *simultaneous* conversations is still limited to the total number of talk repeaters at the site.

This brings up an important point: Most public safety trunking systems reserve one repeater at each site for the *system or control channel*. This is the channel of communications over which the radios talk among themselves behind the scenes to coordinate who goes to which frequency, at which site and what time, to become part of a conversation. This system traffic goes on nearly continuously as portable and mobile users move around between sites and change their channel selectors to become part of a different conversation.

A trunked channel is called a talkgroup.

While there is a direct correlation in conventional radio systems between channels and frequencies, trunked systems abstract the notion of a channel. Rather than being a fixed pair of frequencies, a trunked channel is a temporarily assigned repeater for use among a predefined group of users. In trunking parlance, the channel and its defined users are both known as a *talkgroup*.

Any individual user radio can be part of many talkgroups. The user may, depending on agency policy and radio programming, choose to scan multiple talkgroups during normal operations, just as they may have scanned multiple conventional channels with an earlier system. In a trunked system, the user radio literally notifies the system that it wants to be part of any conversations occurring among the selected talkgroups. Still limited by the fact that the radio can only receive one transmission at a time,

the user also has to select a single talkgroup on which to transmit using the radio's channel selector knob.

Because trunked talk channels are set up and torn down as needed, end-user radios rely on the system to tell them when a talkgroup is coming active and to get directions on where to tune. This takes place over the control channel, normally in a fraction of a second. As soon as an open repeater is available, which may actually be multiple repeaters if the network spans more than one site, the transmitting radio is allowed to talk and all other radios in the talkgroup automatically tune to the transmission frequency(s).

All talkgroup conversations go through the system. A central controller connected to all sites and each repeater steers system resources to maximize capacity according to preset parameters. The system can be programmed, for example, to give certain user groups preference over others as they queue up waiting for assignment of a channel. It can automatically spread conversations over multiple overlapping sites to reduce bottlenecks.

Trunked systems can also be managed on the fly by dispatchers and system administrators to collapse multiple talkgroups into a single one. This has a strong implication for interoperability. Where several talkgroups may be operating independently from one another during an incident, and thus unable to communicate between their various users, a dispatcher appropriately authorized can combine the talkgroups into one. All users of the affected talkgroups can effectively be moved to a common one. While increasing interoperability, this also has the effect of increasing traffic on the newly combined channel.

■ Trunked System Pros

Trunked systems are commonly built with all the simulcast and remote receiver capabilities described for conventional systems. In addition, the systemwide ability to create virtual channels and assign radio resources as needed brings great flexibility to user agencies. The system, itself, can contribute by balancing demand across physical radio resources. Again, the greater channel efficiency of trunked systems may mean they are the only choice in jurisdictions where spectrum resources have otherwise been exhausted.

■ Trunked System Cons

With all of this power, there are downsides to trunked radio systems. First, they are costly. Agencies can expect to pay upwards of 50 percent more for the cost of a trunked system over a conventional one with the same number of sites and radios.

Study 4: Characteristics of Radio Systems

Reference Material: NLECTC Guidebook - Chapter 6, Pages 41-49

Chapter 6

Characteristics of Radio Systems

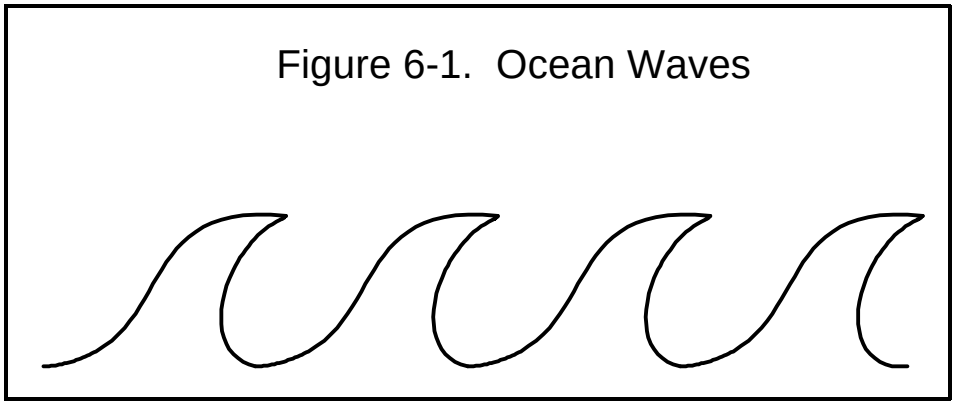
Understanding Radio Terms

Radio technology is full of confusing terms that come straight from a physics book. Sometimes when you ask a radio engineer a question, you even get an answer that is a formula. The authors have tried to simplify the terms as much as possible to allow you to get a good handle on the concepts. The goal in this section is not to turn you into radio experts, but it is hoped that you'll be able to understand the experts a little better when they talk to you.

Wave

The basic building block of radio communications is the radio wave. Like waves on the ocean, a radio wave is merely a stream of repeating peaks and valleys (figure 6-1).

Figure 6-1. Ocean Waves

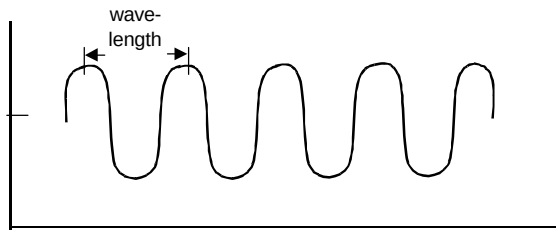


One big difference between ocean waves and radio waves is that ocean waves are visible, while radio waves are not. People can see how far apart or how high the peaks are on the ocean. Radio waves have those same characteristics; people just cannot see them.

Wavelength

The length of a wave is measured from one point to its next corresponding point. In other words, the wavelength could be the distance from one peak to the next peak or from one valley to the next valley and so on, as shown in figure 6-2.

Figure 6-2. Wavelength

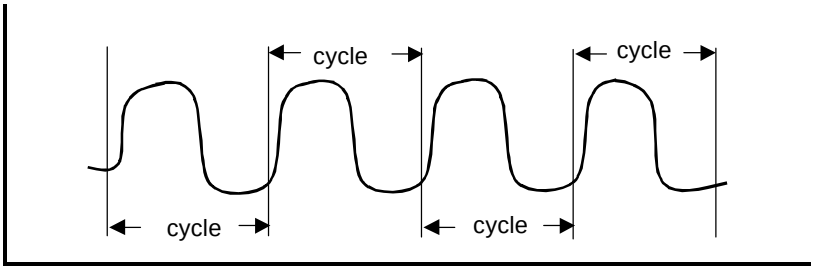


In radio terms, a *short* wavelength would mean that the peaks are relatively close together. A *long* wavelength would mean that the peaks are relatively far apart.

Cycle

The entire pattern of the wave, before it begins to repeat itself, is called a cycle. A repeating pattern of cycles that make up a wave is shown in figure 6-3.

Figure 6-3. Cycles



Frequency

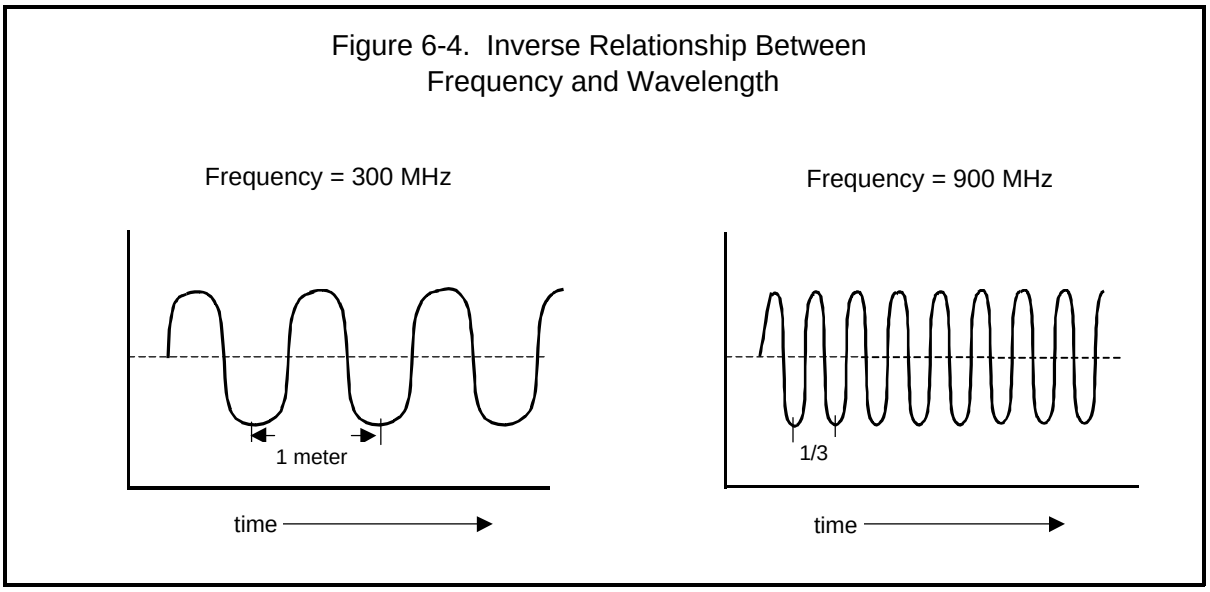
Cycles repeat over time. The fact that they do is the basis for one of the most important terms in radio communications: *frequency*. Frequency is defined as the number of cycles that occur each second.

When they talk about frequency, radio engineers use a shorthand term for "cycles per second," which they call "Hertz." (The word Hertz is usually shortened to "Hz" when written.) Both terms mean the same thing. So, if you were told the frequency of the wave was 10 Hertz, you would know that meant 10 cycles per second.

Thousands of radio wave cycles usually repeat themselves each second, so engineers have adopted the practice of writing kilohertz (shortened to KHz), which means 1,000 cycles per second, megahertz (MHz), which means 1 million cycles per second, or gigahertz (GHz), which means 1 billion cycles per second, when they refer to radio frequency. Thus, 10 million cycles per second can also be written as 10 MHz.

Frequency and wavelength are inversely related. In other words, the higher the frequency, the shorter the wavelength, and conversely, the lower the frequency, the longer the wavelength. These relationships are illustrated in figure 6-4. At 300 MHz (300 million cycles per second), the distance between the peaks of the wave is 1 meter. When the frequency is tripled to 900 MHz (900 million cycles per second), the wavelength is reduced to 1/3 meter (1/3 of the previous distance between the peaks).

Figure 6-4. Inverse Relationship Between Frequency and Wavelength



At extremely high frequencies (above 30 GHz), the distance between the peaks of the wave becomes so small (1 centimeter or less) that a raindrop would not fit between them. In fact, at these extremely high frequencies, it is possible for rainy weather to disrupt the wave and distort or completely block the resulting signal.

Spectrum and Bands

The complete range of possible frequencies that are now or could be used for radio communications is called the *spectrum*. The audible frequency range is usually considered to range from 20 to 18,000 cycles per second or Hertz. For practical purposes, the useful radio spectrum ranges from approximately 30 KHz up to more than 300 GHz.

Radio professionals often discuss frequencies by grouping them into ranges, which are called *bands*. The bands are often referred to by names like HF (high frequency), VHF (very high frequency), UHF (ultra-high frequency), SHF (superhigh frequency), EHF (extremely high frequency), and infrared.

Public safety bands. Two of the radio frequency bands are of particular interest to law enforcement agencies installing their own mobile radio systems. These are the VHF and UHF bands, whose ranges are designated as VHF 30 - 300 MHz and UHF 300 - 3,000 MHz.

Specific bands and frequencies used for public safety wireless communications are shown in table 6-1.

Table 6-1. Bands and Frequencies Used by Public Safety

Public Safety Band Name	Frequencies (MHz)	Channel Separation (KHz)[1]	Services
VHF (low band)	25 - 50 72 - 76	20	Mixed base and mobile Mixed base and mobile
VHF (high band)	150 - 174	15	Mixed base and mobile
UHF	450 - 512	12.5	Mixed base and mobile
UHF (700/800/900)	750/800/900	6.25/12.5/25	Mixed base, mobile, and cellular
2 GHz	2,000	10/20/30 MHz	Personal Communications Services

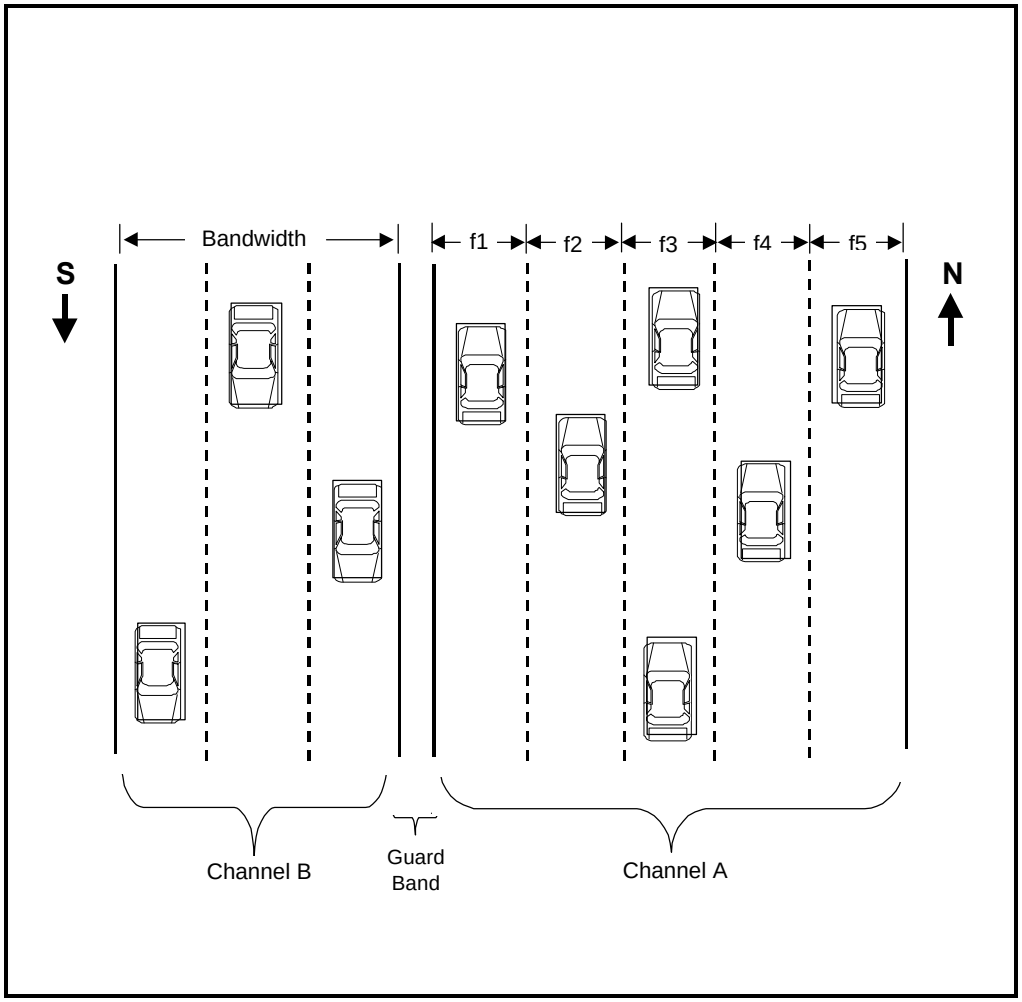
[1] This is the separation most of the time. New equipment below 512 MHz has separations of 12.5 or 15 KHz until 2006, when the separations will be halved again (i.e., in the 150 MHz band, the bandwidth will be 7.5 KHz in 2006).

Channels

The Federal Communications Commission (FCC) arbitrarily groups frequencies into categories they call *channels*. When the FCC licenses a channel to you, it specifically identifies the center frequency (sometimes called carrier frequency) for that channel. This central frequency is the main frequency for carrying the information to be transmitted. Thus, the radio information is transmitted over the several frequencies contained within a single channel. The more frequencies in a channel, the greater its width (called *bandwidth*), and the greater the amount of information it can carry.

For example, if a channel were similar to a multilane highway, then the frequencies would be like all the lanes of the highway that travel in the same direction, say northbound (see figure 6-5). The information traveling over the channel is like the cars that travel on the highway. The width of the highway (i.e., the bandwidth) will equal the total width of all the lanes combined. Therefore, the more lanes on the highway,

the more cars that highway can handle. The center lane on the highway would be similar to the center or carrier frequency.



In a similar way, a second channel could be compared to the other side of the highway where all of the lanes travel in a different direction (southbound). A concrete barrier or median strip exists to separate the northbound lanes from the southbound lanes. A similar non-overlap space exists between channels and is called the *guard band*.

One more note: In our example, the northbound highway has five lanes, while the southbound highway has only three. Like highways, not all channels need be the same width, even if they occur in the same band.

As mentioned before, generally, the wider the bandwidth, the more information may be transmitted. However, with microprocessors and sophisticated software techniques, more information can now be sent

through less bandwidth than was possible just a decade ago (sort of like car pooling). As a result, *spectrum efficiency* has improved.

Mobile Radio System Frequencies

The FCC has assigned frequencies so that there are typically 25 KHz between channels in the UHF band. In other words, a 460 MHz frequency assignment (the center frequency) means that the information transmission falls between 459,987.5 KHz and 460,012.5 KHz (i.e., 12.5 KHz on either side of the center frequency).

In its goal to promote the efficient use of the spectrum, the FCC is changing most of the bandwidths of radio channels below 512 MHz in a process it calls "refarming." It is presently reducing channel bandwidths in half and will reduce the bandwidths in half again in the year 2006. In other words, the first step is to reduce the channel bandwidth from 30 KHz to 15 KHz, then to 7.5 KHz (or, for a 25 KHz VHF channel bandwidth, to 12.5 KHz, and then to 6.25 KHz).

Frequencies covering TV channels 60–69 have been reallocated from television to private use and public safety use. The nonpublic safety frequencies being reallocated will be auctioned off by the FCC. The 24 MHz of public safety spectrum includes the 764-776 and 794-806 MHz portions of this band. The FCC has required that all systems in this band employ digital modulation. The band has been split into two sections. The voice portion of this spectrum is based on 6.25 KHz channel width building blocks that can be combined up to 25 KHz maximum. The use of conventional equipment using the Project 25 common air interface standard is required on the 64 interoperability voice channels designated in this band. The wideband data portion of this band is built on 50 KHz building blocks that can be combined up to 150 KHz maximum, with an interoperability standard now under development for interoperability data channels.

Spectrum planning in this band is under the auspices of Regional Planning Committees in the same manner as with the earlier 800 MHz NPSPAC band. The FCC formed a Federal Advisory Committee called the National Coordination Committee (NCC) to assist it in developing operational and technical guidelines for this band. Reports and Recommendations from the NCC are available on the FCC website.

Frequency Selection Considerations

Coverage. In general, the lower the frequency, the better the coverage for a given power level. VHF low band has the best coverage for a given *effective radiated power* (ERP). This is because the attenuation increases or the signal level decreases as a function of ($1/\text{frequency}^2$). This is why UHF TV stations are permitted to transmit with ERPs of 5 megawatts, compared with VHF TV stations that transmit with 100 to 300 kilowatts. This equalizes the received signals at a far distance.

Building penetration. UHF frequencies with shorter wavelengths (typically within the range of 200 MHz to 2000 MHz) have better building penetration through building openings, such as windows and doors, than do VHF frequencies below 200 MHz.

Skip. At VHF low band, stations can experience "skip" (the radio wave reflects from the ionosphere during the height of the sunspot cycle), often causing so much interference that local communications cannot be carried out.

Noise. Natural and manmade noise is worse the lower the frequency. Higher bands experience much less noise interference.

Antenna size. The lower the frequency, the larger the antennas for a given amount of gain. (Reasons for this are discussed in the upcoming section on antennas.)

In summary, selection of the frequency band of operation is dependent upon the desired system characteristics. Table 6-2 summarizes the above-mentioned characteristics.

Table 6-2. Technical Frequency Selection Criteria

Parameter/Band	Low Band VHF	High Band VHF	UHF
Propagation[1]	Very good	Good	Poor
Building penetration[2]	Poor	Better	Good
Skip interference	Very susceptible	Little skip	No skip
Manmade noise	High noise	Less noise	Lowest noise
Antenna size[3]	Large	Smaller	Smallest

[1] For a given ERP (signal attenuation is proportional to $1/f^2$).

[2] For a dense (concrete) building with windows.

[3] For a given amount of antenna gain.

Transmitters and Receivers

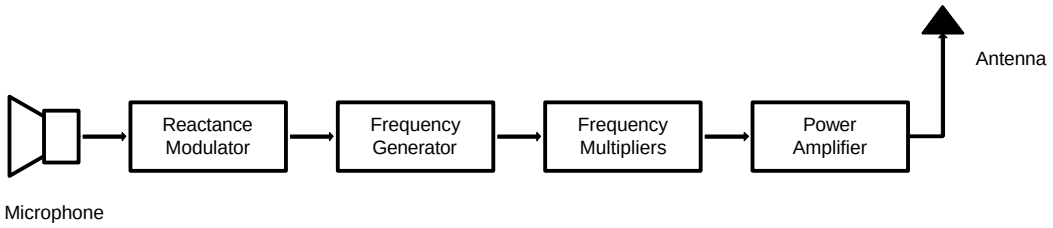
Base, mobiles, and handheld radios consist of components called *transmitters* and *receivers*. In most cases, some circuitry is used for both transmitting and receiving, so a radio is said to be a *transceiver*.

Transmitters

A transmitter generates a radio wave or signal. A diagram of a simple transmitter is shown in figure 6-6.

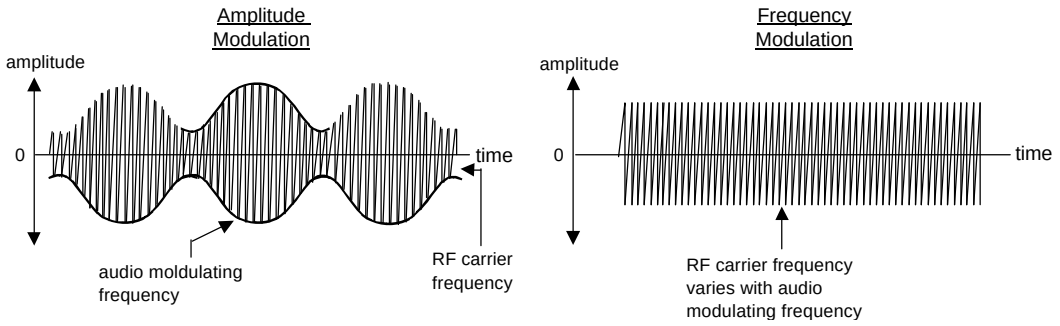
The frequency generating component is called an *oscillator*. *Frequency multipliers* multiply the frequency up to the final output frequency. A power *amplifier* increases the power of the signal to obtain the necessary power output to the antenna.

Figure 6-6. A Simplified FM Radio Transmitter



The output frequency is a continuous wave (CW) called a carrier. Intelligence is added to the transmitter by varying the *amplitude* of the carrier (amplitude modulation or AM) or by varying the frequency of the carrier (frequency or phase modulation or FM). Figure 6-7 shows the difference between amplitude and frequency modulation. The most noticeable user difference between AM and FM modulation is that FM is less susceptible to interference from RF noise.

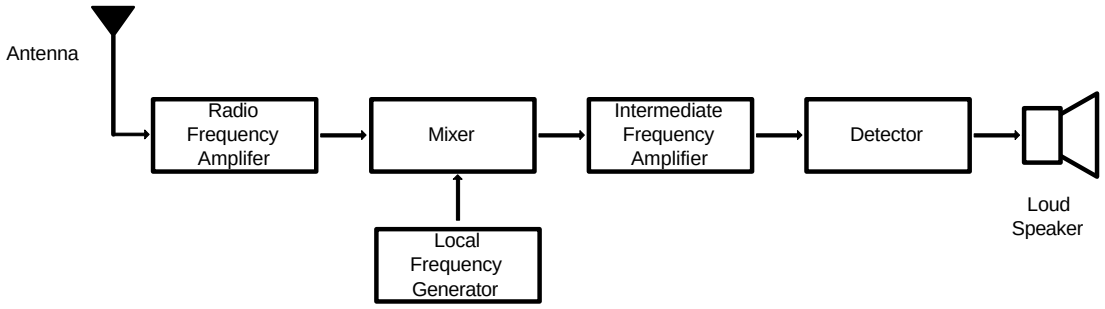
Figure 6-7. Comparison of Amplitude versus Frequency Modulation



Receivers

The receiver is the opposite of the transmitter. It receives the modulated carrier, processes it, and sends it to a detector section, which strips off the modulation signal from the carrier to restore the original intelligence. A diagram for a simple receiver is shown in figure 6-8.

Figure 6-8. A Simplified Radio Receiver



Radio systems are generally designed for AM or FM. Voice transmission is produced using a microphone at the input of the transmitter and a loud speaker at the output of the receiver. The signals are usually analog, or continuous, signals.

Data are transmitted using binary signals. One simple method of transmitting a binary signal uses frequency shift keying (FSK). A zero is represented by transmitting a particular carrier frequency, and a one is represented by shifting the carrier frequency to a different frequency (usually with less than 1,000 Hz difference). The receiver interprets the ones and zeroes and reconstructs the binary data stream.

This is just one simple scheme for transmitting data. Most of today's systems use much more complex methods to maximize spectrum efficiency.

As stated elsewhere in this book, human beings cannot directly interpret most digital signals. People live in an analog world, one with continuous audio frequency loud speakers, printers, television, or computer screens. The exception to this is the use of Morse Code, which consists of ones and zeros. Skillful Morse Code operators can interpret the dots and dashes in their heads into letters and numbers. For digital radio, however, a digital-to-analog converter is necessary to communicate with human beings.

Note that figure 6-8 is greatly simplified. All communications receivers used in dispatch-type communications have squelch circuits before the audio circuits, which keeps the output off when there is no signal (so that you do not have to listen to noise) and passes the detected signal through when the correctly coded signal is received. Several different types of squelch are used. Commonly used squelch schemes are continuous tone-coded squelch system (CTCSS) and the continuous digital-coded squelch system (CDCSS).

Study 5: Antennas

Reference Material: FEMA Workbook, Volume 2-28, June 2007, Chapter 3

CHAPTER 3: ANTENNAS

Learning Objectives

Upon completion of this chapter, you will be able to:

- State the basic principles of antenna radiation and list the parts of an antenna;
- Describe how electromagnetic energy is radiated from an antenna;
- Explain polarization, gain, and radiation resistance characteristics of an antenna;
- Describe the theory of operation of half- wave and quarter-wave antennas;
- List the various array antennas;
- Describe the directional array antennas presented and explain the basic operation of each; and
- Identify various special antennas presented, such as ground-plane, and corner-reflector; describe the operation of each.

Introduction

If you had been around in the early days of electronics, you would have considered an ANTENNA (AERIAL) to be little more than a piece of wire strung between two trees or upright poles. In those days, technicians assumed that longer antennas automatically provided better reception than shorter antennas. They also believed that a mysterious MEDIUM filled all space, and that an antenna used this medium to send and receive its energy. These two assumptions have since been discarded. Modern antennas have evolved to the point that highly directional, specially designed antennas are used to relay worldwide communications in space through the use of satellites and Earth station antennas (fig. 1-24). Present transmission theories are based on the assumption that space itself is the only medium necessary to propagate (transmit) radio energy.

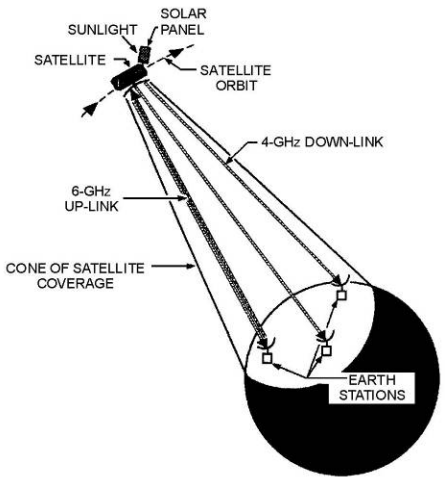


Figure 1-24.—Satellite/earth station communications system.

A tremendous amount of knowledge and information has been gained about the design of antennas and radio-wave propagation. Still, many old-time technicians will tell you that when it comes to designing the length of an antenna, the best procedure is to perform all calculations and try out the antenna. If it doesn't work right, use a cut-and-try method until it does. Fortunately, enough information has been collected over the last few decades that it is now possible to predict the behavior of antennas. This chapter will discuss and explain the basic design and operation of antennas.

Principles of Antenna Radiation

After an rf signal has been generated in a transmitter, some means must be used to radiate this signal through space to a receiver. The device that does this job is the antenna. The transmitter signal energy is sent into space by a TRANSMITTING ANTENNA; the rf signal is then picked up from space by a RECEIVING ANTENNA.

The rf energy is transmitted into space in the form of an electromagnetic field. As the traveling electromagnetic field arrives at the receiving antenna, a voltage is induced into the antenna (a conductor). The rf voltages induced into the receiving antenna are then passed into the receiver and converted back into the transmitted rf information.

The design of the antenna system is very important in a transmitting station. The antenna must be able to radiate efficiently so the power supplied by the transmitter is not wasted. An efficient transmitting antenna must have exact dimensions. The dimensions are determined by the transmitting frequencies. The dimensions of the receiving antenna are not critical for relatively low radio frequencies. However, as the frequency of the signal being received increases, the design and installation of the receiving antenna become more critical. An example of this is a television receiving antenna. If you raise it a few more inches from the ground or give a slight turn in direction, you can change a snowy blur into a clear picture.

The conventional antenna is a conductor, or system of conductors, that radiates or intercepts electromagnetic wave energy. An ideal antenna has a definite length and a uniform diameter, and is completely isolated in space. However, this ideal antenna is not realistic. Many factors make the design of an antenna for a communications system a more complex problem than you would expect. These factors include the height of the radiator above the earth, the conductivity of the earth below it, and the shape and dimensions of the antenna. All of these factors affect the radiated-field pattern of the antenna in space. Another problem in antenna design is that the radiation pattern of the antenna must be directed between certain angles in a horizontal or vertical plane, or both.

Most practical transmitting antennas are divided into two basic classifications, HERTZ (half-wave) ANTENNAS and MARCONI (quarter-wave) ANTENNAS. Hertz antennas are generally installed some distance above the ground and are positioned to radiate either vertically or horizontally. Marconi antennas operate with one end grounded and are mounted perpendicular to the Earth or to a surface acting as a ground. Hertz antennas are generally used for frequencies above 2 megahertz. Marconi antennas are used for frequencies below 2 megahertz and may be used at higher frequencies in certain applications.

A complete antenna system consists of three parts: (1) The COUPLING DEVICE, (2) the FEEDER, and (3) the ANTENNA, as shown in figure 1-25. The coupling device (coupling coil) connects the transmitter to the feeder. The feeder is a transmission line that carries energy to the antenna. The antenna radiates this energy into space.

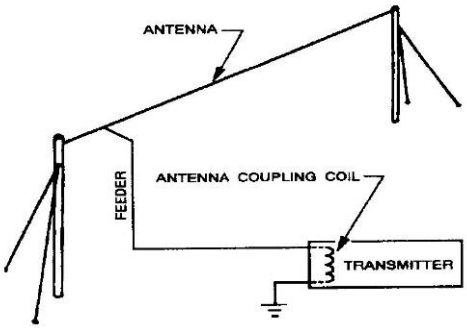


Figure 1-25.—Typical antenna system.

The factors that determine the type, size, and shape of the antenna are (1) the frequency of operation of the transmitter, (2) the amount of power to be radiated, and (3) the general direction of the receiving set. Typical antennas are shown in figure 1-26.

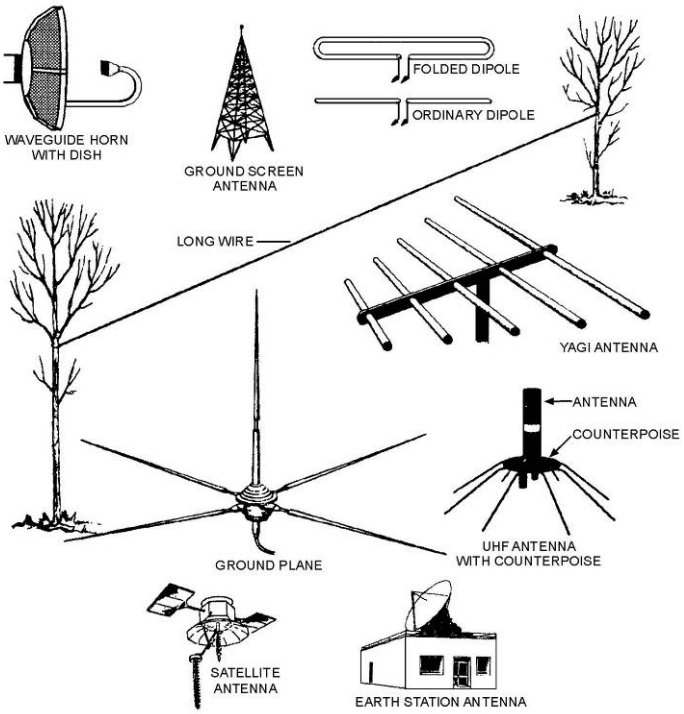


Figure 1-26.—Typical antennas.

Antenna Characteristics

You can define an antenna as a conductor or group of conductors used either for radiating electromagnetic energy into space or for collecting it from space. Electrical energy from the transmitter is converted into electromagnetic energy by the antenna and radiated into space. On the receiving end, electromagnetic energy is converted into electrical energy by the antenna and is fed into the receiver.

Fortunately, separate antennas seldom are required for both transmitting and receiving rf energy. Any antenna can transfer energy from space to its input receiver with the same efficiency that it transfers energy from the transmitter into space. Of course, this is assuming that the same frequency is used in both cases. This property of interchangeability of the same antenna for transmitting and receiving is known as antenna RECIPROCITY. Antenna reciprocity is possible because antenna characteristics are essentially the same for sending and receiving electromagnetic energy.

Reciprocity of Antennas

In general, the various properties of an antenna apply equally, regardless of whether you use the antenna for transmitting or receiving. The more efficient a certain antenna is for transmitting, the more efficient it will be for receiving on the same frequency. Likewise, the directive properties of a given antenna also will be the same whether it is used for transmitting or receiving.

Assume, for example, that a certain antenna used with a transmitter radiates a maximum amount of energy at right angles to the axis of the antenna, as shown in figure 1-27, view A. Note the minimum amount of radiation along the axis of the antenna. Now, if this same antenna were used as a receiving antenna, as shown in view B, it would receive best in the same directions in which it produced maximum radiation; that is, at right angles to the axis of the antenna.

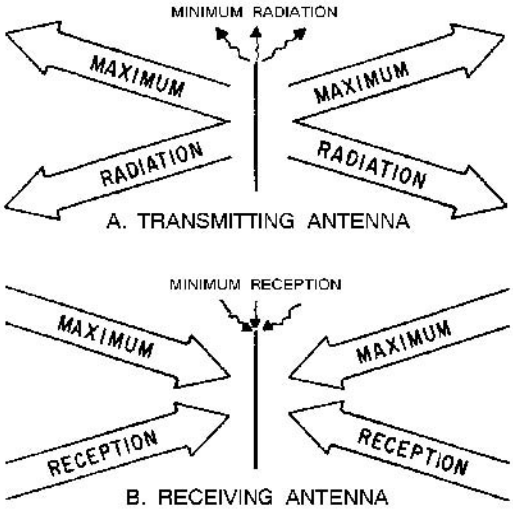


Figure 1-27.—Reciprocity of antennas.

Antenna Gain

Another characteristic of a given antenna that remains the same whether the antenna is used for transmitting or receiving is GAIN. Some antennas are highly directional that is, more energy is propagated in certain directions than in others. The ratio between the amount of energy propagated in these directions compared to the energy that would be propagated if the antenna were not directional is known as its gain. When a transmitting antenna with a certain gain is used as a receiving antenna, it will also have the same gain for receiving.

Polarization

The radiation field is composed of electric and magnetic lines of force. These lines of force are always at right angles to each other. Their intensities rise and fall together, reaching their maximums 90 degrees apart. The electric field determines the direction of polarization of the wave. In a vertically polarized wave, the electric lines of force lie in a vertical direction. In a horizontally polarized wave, the electric lines of force lie in a horizontal direction. Circular polarization has the electric lines of force rotating through 360 degrees with every cycle of rf energy.

Advantages of Vertical Polarization

Simple vertical antennas can be used to provide OMNIDIRECTIONAL (all directions) communication. This is an advantage when communications must take place from a moving vehicle.

In some overland communications, such as in vehicular installations, antenna heights are limited to 3 meters (10 feet) or less. In such instances vertical polarization results in a stronger receiver signal than does horizontal polarization at frequencies up to about 50 megahertz. From approximately 50 to 100 megahertz, vertical polarization results in a slightly stronger signal than does horizontal polarization with antennas at the same height. Above 100 megahertz, the difference in signal strength is negligible.

For transmission over bodies of water, vertical polarization is much better than horizontal polarization for antennas at the lower heights. As the frequency increases, the minimum antenna height decreases. At 30 megahertz, vertical polarization is better for antenna heights below about 91 meters (300 feet); at 85 megahertz, antenna heights below 15 meters (50 feet); and still lower heights at the high frequencies. Therefore, at ordinary antenna mast heights of 12 meters (40 feet), vertical polarization is advantageous for frequencies less than about 100 megahertz.

Radiation is somewhat less affected by reflections from aircraft flying over the transmission path when vertical polarization is used instead of horizontal polarization. With horizontal polarization, such reflections cause variations in received signal strength. This factor is important in locations where aircraft traffic is heavy.

When vertical polarization is used, less interference is produced or picked up because of strong vhf and uhf broadcast transmissions (television and fm). This is because vhf and uhf transmissions use horizontal polarization. This factor is important when an antenna must be located in an urban area having several television and fm broadcast stations.

Advantages of Horizontal Polarization

A simple horizontal antenna is bi-directional. This characteristic is useful when you desire to minimize interference from certain directions. Horizontal antennas are less likely to pick up man-made interference, which ordinarily is vertically polarized.
When antennas are located near dense forests or among buildings, horizontally polarized waves suffer lower losses than vertically polarized waves, especially above 100 megahertz. Small changes in antenna locations do not cause large variations in the field intensity of horizontally polarized waves. When vertical polarization is used, a change of only a few meters in the antenna location may have a considerable effect on the received signal strength. This is the result of interference patterns that produce standing waves in space when spurious reflections from trees or buildings occur.

When simple antennas are used, the transmission line, which is usually vertical, is less affected by a horizontally mounted antenna. When the antenna is mounted at right angles to the transmission line and horizontal polarization is used, the line is kept out of the direct field of the antenna. As a result, the radiation pattern and electrical characteristics of the antenna are practically unaffected by the presence of the vertical transmission line.

Basic Antennas

Before you look at the various types of antennas, consider the relationship between the wavelength at which the antenna is being operated and the actual length of the antenna. An antenna does not necessarily radiate or receive more energy when it is made longer. Specific dimensions must be used for efficient antenna operation.

Nearly all antennas have been developed from two basic types, the Hertz and the Marconi. The basic Hertz antenna is 1/2 wavelength long at the operating frequency and is insulated from ground. It is often called a DIPOLE or a DOUBLET. The basic Marconi antenna is 1/4 wavelength long and is either grounded at one end or connected to a network of wires called a COUNTERPOISE. The ground or counterpoise provides the equivalent of an additional 1/4 wavelength, which is required for the antenna to resonate.

Half-Wave Antennas

A half-wave antenna (referred to as a dipole, Hertz, or doublet) consists of two lengths of wire rod, or tubing, each 1/4 wavelength long at a certain frequency. It is the basic unit from which many complex antennas are constructed. The half-wave antenna operates independently of ground; therefore, it may be installed far above the surface of the Earth or other absorbing bodies.

Radiation Patterns

In the following discussion, the term DIPOLE is used to mean the basic half-wave antenna. The term DOUBLET is used to indicate an antenna that is very short compared with the wavelength of the operating frequency. Physically, it has the same shape as the dipole.

RADIATION PATTERN OF A DOUBLET.—The doublet is the simplest form of a practical antenna. Figure 1-28 shows the development of vertical and horizontal patterns for a doublet. This in NOT a picture of the radiation, but three-dimensional views of the pattern itself. In three

views the pattern resembles a doughnut. From the dimensions in these views, two types of polar-coordinate patterns can be drawn, horizontal and vertical. The HORIZONTAL PATTERN view A is derived from the solid pattern view C by slicing it horizontally. This produces view B, which is converted to the polar coordinates seen in view

A. The horizontal pattern illustrates that the radiation is constant in any direction along the horizontal plane.

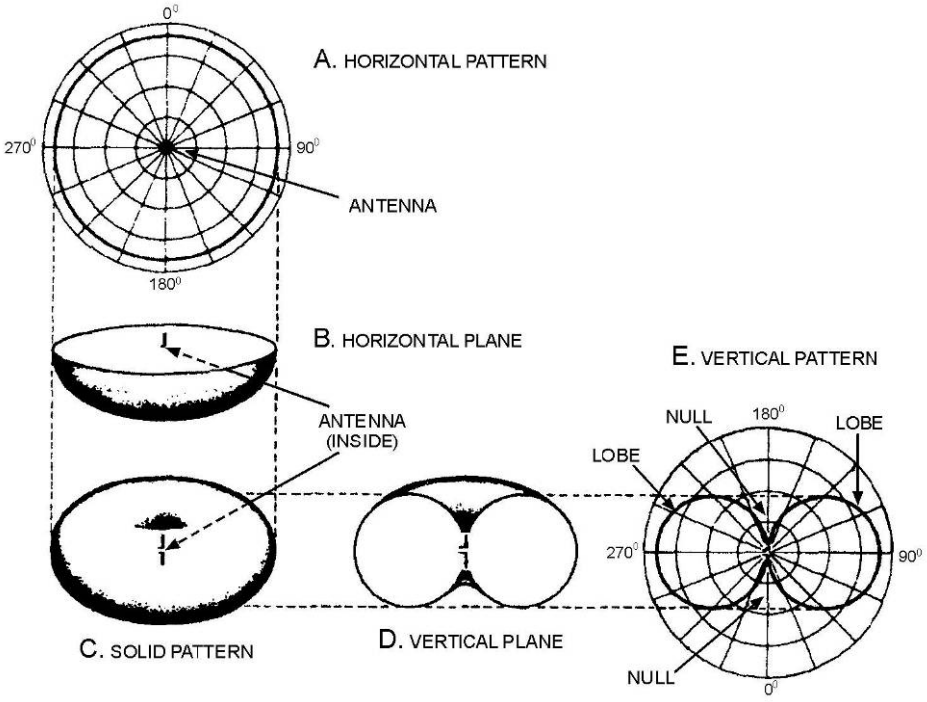


Figure 1-28.—Development of vertical and horizontal patterns.

A VERTICAL PATTERN view E is obtained from the drawing of the vertical plane view D of the radiation pattern view C. The radiation pattern view C is sliced in half along a vertical plane through the antenna. This produces the vertical plane pattern in view D. Note how the vertical plane in view D of the radiation pattern differs from the horizontal plane in view B. The vertical pattern view E exhibits two lobes and two nulls. The difference between the two patterns is caused by two facts: (1) no radiation is emitted from the ends of the doublet; and (2) maximum radiation comes from the doublet in a direction perpendicular to the antenna axis. This type of radiation pattern is both NONDIRECTIONAL (in a horizontal plane) and DIRECTIONAL (in a vertical plane).

From a practical viewpoint, the doublet antenna can be mounted either vertically or horizontally. The doublet shown in figure 1-28 is mounted vertically, and the radiated energy spreads out

about the antenna in every direction in the horizontal plane. Since ordinarily the horizontal plane is the useful plane, this arrangement is termed NONDIRECTIONAL. The directional characteristics of the antenna in other planes is ignored. If the doublet were mounted horizontally, it would have the effect of turning the pattern on edge, reversing the patterns given in figure 4-14. The antenna would then be directional in the horizontal plane. The terms "directional" and "nondirectional" are used for convenience in describing specific radiation patterns. A complete description always involves a figure in three dimensions, as in the radiation pattern of figure 1-28.

☑Learning Check

32. What terms are often used to describe basic half-wave antennas?

33. If a basic half-wave antenna is mounted vertically, what type of radiation pattern will be produced?

34. In which plane will the half-wave antenna be operating if it is mounted horizontally?

RADIATION PATTERN OF A DIPOLE.—The radiation pattern of a dipole (fig. 1-29) is similar to that of the doublet (fig. 1-28). Increasing the length of the doublet to 1/2 wavelength has the effect of flattening out the radiation pattern. The radiation pattern in the horizontal plane of a dipole is a larger circle than that of the doublet. The vertical-radiation pattern lobes are no longer circular. They are flattened out and the radiation intensity is greater.

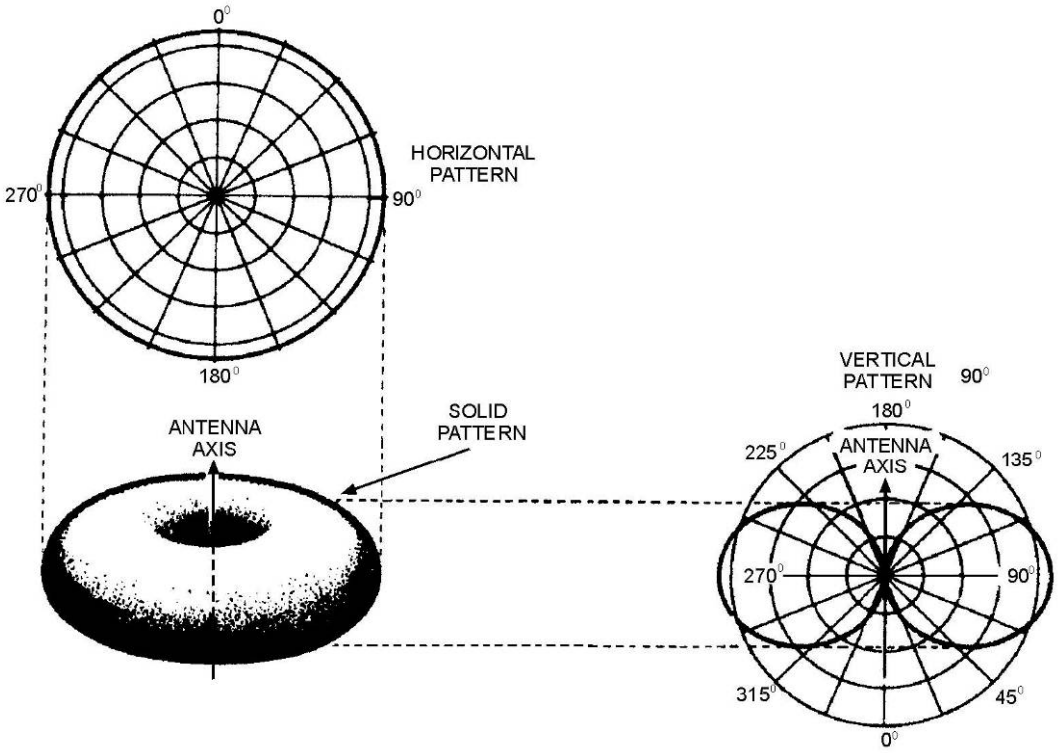


Figure 1-29.—Radiation pattern of a dipole.

Quarter-Wave Antennas

As you have studied in the previous sections, a 1/2 wavelength antenna is the shortest antenna that can be used in free space. If we cut a half-wave antenna in half and then ground one end, we will have a grounded quarter-wave antenna. This antenna will resonate at the same frequency as the ungrounded half-wave antenna. Such an antenna is referred to as a QUARTER-WAVE or Marconi antenna. Quarter-wave antennas are widely used in the military. Most mobile transmitting and receiving antennas (fig. 1-30) are quarter-wave antennas.

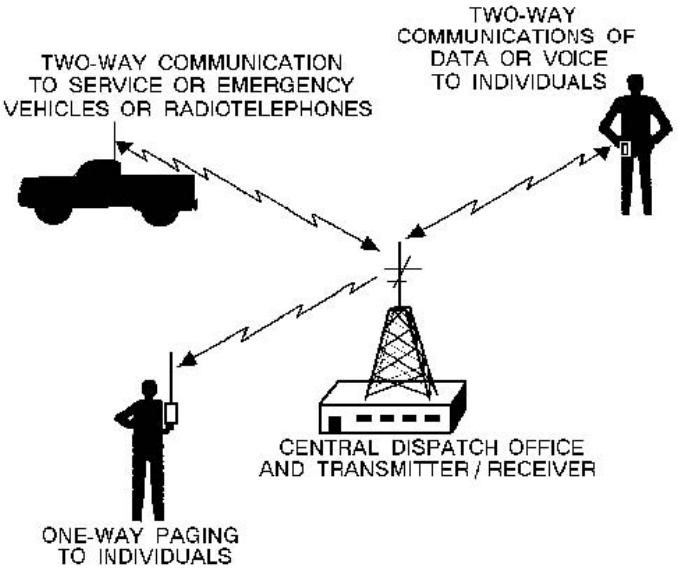


Figure 1-30.—Mobile antennas.

As stated above, a grounded quarter-wave antenna will resonate at the same frequency as an ungrounded half-wave antenna. This is because ground has high conductivity and acts as an electrical mirror image. This characteristic provides the missing half of the antenna, as shown in the bottom part of figure 1-31. In other words, the grounded quarter-wave antenna acts as if another quarter-wave were actually down in the earth.

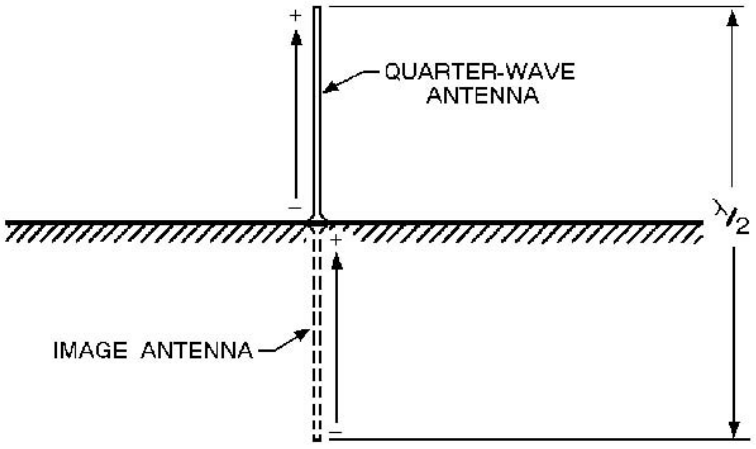


Figure 1-31.—Grounded quarter-wave antenna image.

Characteristics of Quarter-Wave Antennas

The grounded end of the quarter-wave antenna has a low input impedance and has low voltage and high current at the input end, as shown in figure 1-31. The ungrounded end has a high impedance, which causes high voltage and low current. The directional characteristics of a grounded quarter-wave antenna are the same as those of a half-wave antenna in free space.

As explained earlier, ground losses affect radiation patterns and cause high signal losses for some frequencies. Such losses may be greatly reduced if a perfectly conducting ground is provided in the vicinity of the antenna. This is the purpose of a GROUND SCREEN (figure 1-32, view A) and COUNTERPOISE view B.

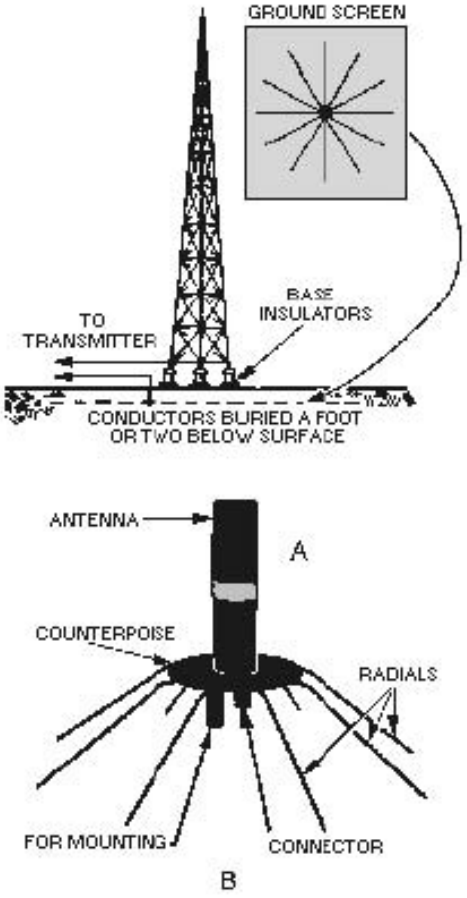


Figure 1-32.—Groundscreen and counterpoise.

The ground screen in view A is composed of a series of conductors buried 1 or 2 feet (0.3 to 0.6 meter) below the surface of the earth and arranged in a radial pattern. These conductors reduce

losses in the ground in the immediate vicinity of the antenna. Such a radial system of conductors is usually 1/2 wavelength in diameter.

A counterpoise view B is used when easy access to the base of the antenna is necessary. It is also used when the earth is not a good conducting surface, such as ground that is sandy or solid rock. The counterpoise serves the same purpose as the ground screen but it is usually elevated above the earth. No specific dimensions are necessary in the construction of a counterpoise nor is the number of wires particularly critical. A practical counterpoise may be assembled from a large screen of chicken wire or some similar material. This screen may be placed on the ground, but better results are obtained if it is placed a few feet above the ground.

☑Learning Check

35. What is the radiation pattern of a quarter-wave antenna?

36. Describe the physical arrangement of a ground screen.

Folded Dipole

The use of parasitic elements and various stacking arrangements causes a reduction in the radiation resistance of a center-fed, half-wave antenna. Under these conditions obtaining a proper impedance match between the radiator and the transmission line is often difficult. A convenient method of overcoming these difficulties is to use a FOLDED DIPOLE in place of the center-fed radiator. (See views A and B of figure 1-33).

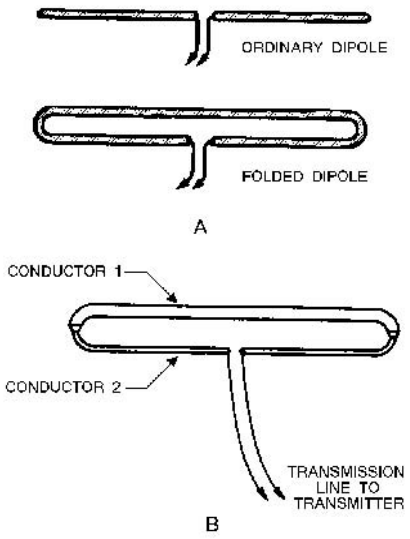


Figure 1-33.—Folded-dipole antennas.

A FOLDED DIPOLE is an ordinary half-wave antenna that has one or more additional conductors connected across its ends. Additional conductors are mounted parallel to the dipole elements at a distance equal to a very small fraction of a wavelength. Spacing of several inches is common.

The directional characteristics of a folded dipole are the same as those of a simple dipole. However, the reactance of a folded dipole varies much more slowly as the frequency is varied from resonance. Because of this the folded dipole can be used over a much wider frequency range than is possible with a simple dipole.

☑Learning Check

37. Which has a wider frequency range, a simple dipole or a folded dipole?

Array Antennas

An array antenna is a special arrangement of basic antenna components involving new factors and concepts. Before you begin studying about arrays, you need to study some new terminology.

Arrays can be described with respect to their radiation patterns and the types of elements of which they are made. However, you will find it useful to identify them by the physical placement of the elements and the direction of radiation with respect to these elements. Generally speaking, the term BROADSIDE ARRAY designates an array in which the direction of maximum radiation is perpendicular to the plane containing these elements. In actual practice, this term is confined to those arrays in which the elements themselves are also broadside, or parallel, with respect to each other.

A COLLINEAR ARRAY is one in which all the elements lie in a straight line with no radiation at the ends of the array. The direction of maximum radiation is perpendicular to the axis of the elements.

The FRONT-TO-BACK RATIO is the ratio of the energy radiated in the principal direction compared to the energy radiated in the opposite direction for a given antenna.

Directivity

The DIRECTIVITY of an antenna or an array can be determined by looking at its radiation pattern. In an array propagating a given amount of energy, more radiation takes place in certain directions than in others. The elements in the array can be altered in such a way that they change the pattern and distribute it more uniformly in all directions. The elements can be considered as a group of antennas fed from a common source and facing different directions. On the other hand, the elements could be arranged so that the radiation would be focused in a single direction. With no increase in power from the transmitter, the amount of radiation in a given direction would be greater. Since the input power has no increase, this increased directivity is achieved at the expense of gain in other directions.

Directivity and Interference

In many applications, sharp directivity is desirable although no need exists for added gain. Examine the physical disposition of the units shown in figure 1-34. Transmitters 1 and 2 are sending information to receivers 1 and 2, respectively, along the paths shown by the solid arrows. The distance between transmitter 1 and receiver 1 or between transmitter 2 and receiver 2 is short and does not require high-power transmission. The antennas of the transmitters propagate well in all directions. However, receiver 1 picks up some of the signals from transmitter 2, and receiver 2 picks up some of the signals from transmitter 1, as shown by the broken arrows. This effect is emphasized if the receiving antennas intercept energy equally well in all directions.

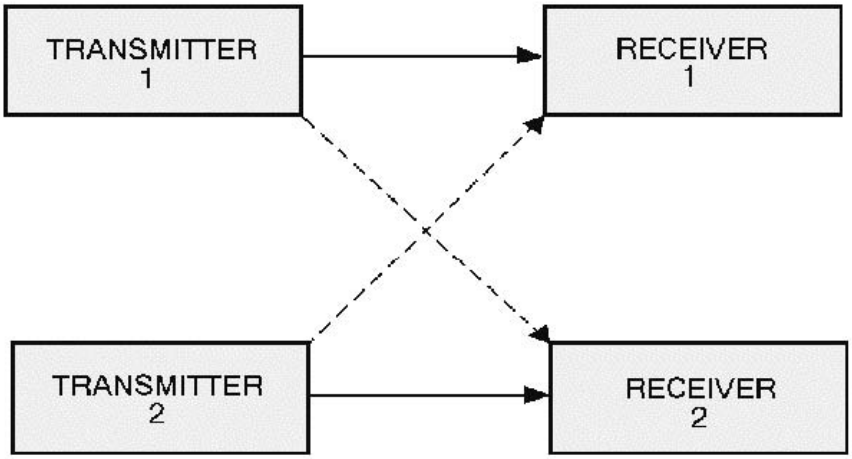


Figure 1-34.—Directivity and interference.

The use of highly directional arrays as radiators from the transmitters tends to solve the problem. The signals are beamed along the paths of the solid arrows and provide very low radiation along the paths of the broken arrows. Further improvement along these lines is obtained by the use of narrowly directed arrays as receiving antennas. The effect of this arrangement is to select the desired signal while discriminating against all other signals. This same approach can be used to overcome other types of radiated interference. In such cases, preventing radiation in certain directions is more important than producing greater gain in other directions.

Look at the differences between the field patterns of the single-element antenna and the array, as illustrated in figure 1-35. View A shows the relative field-strength pattern for a horizontally polarized single antenna. View B shows the horizontal-radiation pattern for an array. The antenna in view A radiates fairly efficiently in the desired direction toward receiving point X. It radiates equally as efficiently toward Y, although no radiation is desired in this direction. The antenna in view B radiates strongly to point X, but very little in the direction of point Y, which results in more satisfactory operation.

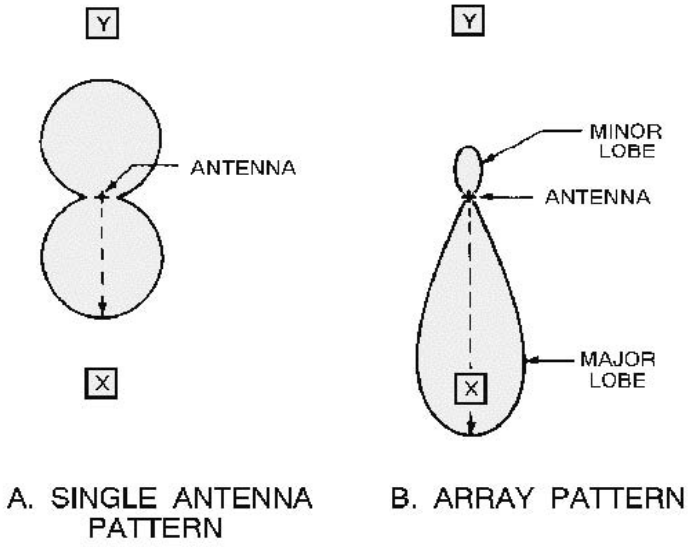


Figure 1-35.—Single antenna versus array.

Major and Minor Lobes

The pattern shown in figure 1-35, view B, has radiation concentrated in two lobes. The radiation intensity in one lobe is considerably stronger than in the other. The lobe toward point X is called a MAJOR LOBE; the other is a MINOR LOBE. Since the complex radiation patterns associated with arrays frequently contain several lobes of varying intensity, you should learn to use appropriate terminology. In general, major lobes are those in which the greatest amount of radiation occurs. Minor lobes are those in which the radiation intensity is least.

☑Learning Check

38. What is the primary difference between the major and minor lobes of a radiation pattern?

Directional Arrays

You have already learned about radiation patterns and directivity of radiation. These topics are important to you because using an antenna with an improper radiation pattern or with the wrong directivity will decrease the overall performance of the system. In the following paragraphs, we discuss in more detail the various types of directional antenna arrays mentioned briefly in the "definition of terms" paragraph above.

Collinear Array

The pattern radiated by the collinear array is similar to that produced by a single dipole. The addition of the second radiator, however, tends to intensify the pattern. Compare the radiation pattern of the dipole (view A of figure 1-36) and the two-element antenna in view B. You will see that each pattern consists of two major lobes in opposite directions along the same axis, QQ1. There is little or no radiation along the PP1 axis. QQ1 represents the line of maximum propagation. You can see that radiation is stronger with an added element. The pattern in view B is sharper, or more directive, than that in view A. This means that the gain along the line of maximum energy propagation is increased and the beam width is decreased. As more elements are added, the effect is heightened, as shown in view C. Unimportant minor lobes are generated as more elements are added.

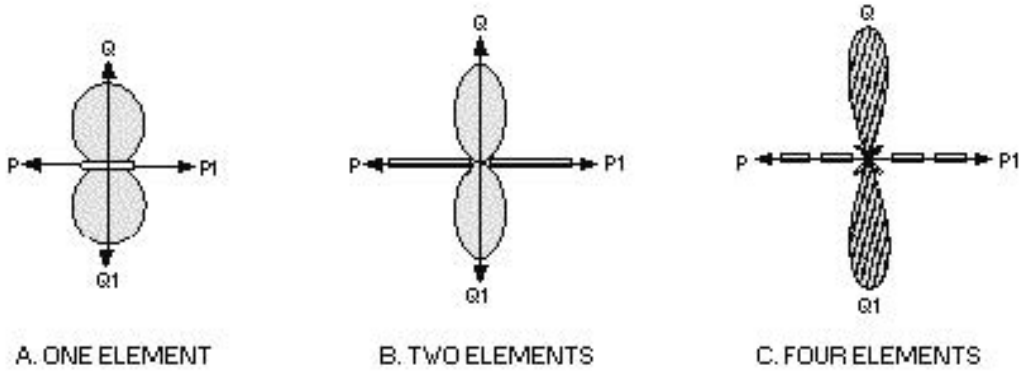


Figure 1-36.—Single half-wave antenna versus two half-wave antennas in phase.

More than four elements are seldom used because accumulated losses cause the elements farther from the point of feeding to have less current than the nearer ones. This introduces an unbalanced condition in the system and impairs its efficiency. Space limitations often are another reason for restricting the number of elements. Since this type of array is in a single line, rather than in a vertically stacked arrangement, the use of too many elements results in an antenna several wavelengths long.

RADIATION PATTERN.—The characteristic radiation pattern of a given array is obtained at the frequency or band of frequencies at which the system is resonant. The gain and directivity characteristics are lost when the antenna is not used at or near this frequency and the array tunes

too sharply. A collinear antenna is more effective than an end-fire array when used off its tuned frequency. This feature is considered when transmission or reception is to be over a wide frequency band. When more than two elements are used, this advantage largely disappears.

Multielement Parasitic Array

A MULTIELEMENT PARASITIC array is one that contains two or more parasitic elements with the driven element. If the array contains two parasitic elements (a reflector and a director) in addition to the driven element, it is usually known as a THREE-ELEMENT ARRAY. If three parasitic elements are used, the array is known as a FOUR-ELEMENT ARRAY, and so on. Generally speaking, if more parasitic elements are added to a three-element array, each added element is a director. The field behind a reflector is so small that additional reflectors would have little effect on the overall radiation pattern. In radar, from one to five directors are used.

CONSTRUCTION.—The parasitic elements of a multi-element parasitic array usually are positioned as shown in figure 1-37, views A and B. Proper spacings and lengths are determined experimentally. A folded dipole (view B) is often used as the driven element to obtain greater values of radiation resistance.

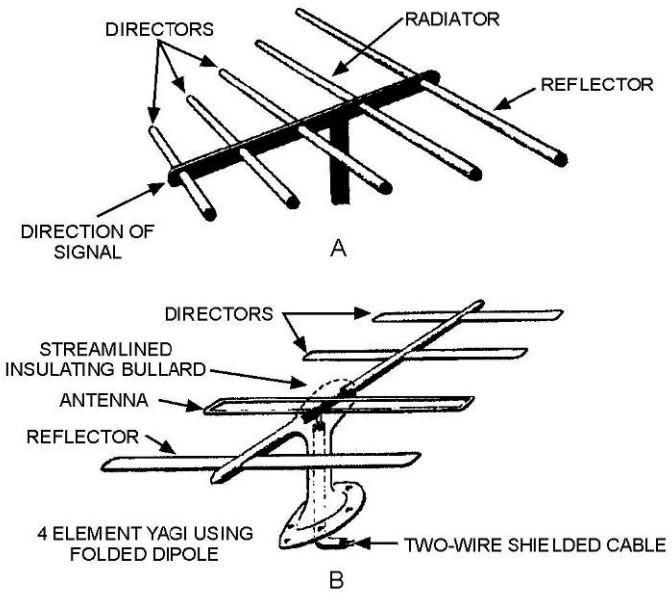


Figure 1-37.—Yagi antenna.

YAGI ANTENNAS.—An example of a multielement parasitic array is the YAGI ANTENNA (figure 1-37, views A and B). The spacings between the elements are not uniform. The radiation from the different elements arrives in phase in the forward direction, but out of phase by various amounts in the other directions.

The director and the reflector in the Yagi antenna are usually welded to a conducting rod or tube at their centers. This support does not interfere with the operation of the antenna. Since the driven element is center-fed, it is not welded to the supporting rod. The center impedance can be increased by using a folded dipole as the driven element.

The Yagi antenna shown in figure 1-37, view A, has three directors. In general, the greater number of parasitic elements used, the greater the gain. However, a greater number of such elements causes the array to have a narrower frequency response as well as a narrower beamwidth. Therefore, proper adjustment of the antenna is critical. The gain does not increase directly with the number of elements used. For example, a three-element Yagi array has a relative power gain of 5 dB. Adding another director results in a 2 dB increase. Additional directors have less and less effect.

☑Learning Check

39. What is the advantage of adding parasitic elements to a Yagi array?

40. The Yagi antenna is an example of what type of array?

Ground-Plane Antenna

A vertical quarter-wave antenna several wavelengths above ground produces a high angle of radiation that is very undesirable at vhf and uhf frequencies. The most common means of producing a low angle of radiation from such an antenna is to work the radiator against a simulated ground called a GROUND PLANE. A simulated ground may be made from a large metal sheet or several wires or rods radiating from the base of the radiator. An antenna so constructed is known as a GROUND-PLANE ANTENNA. Two ground-plane antennas are shown in figure 1-38, views A and B.

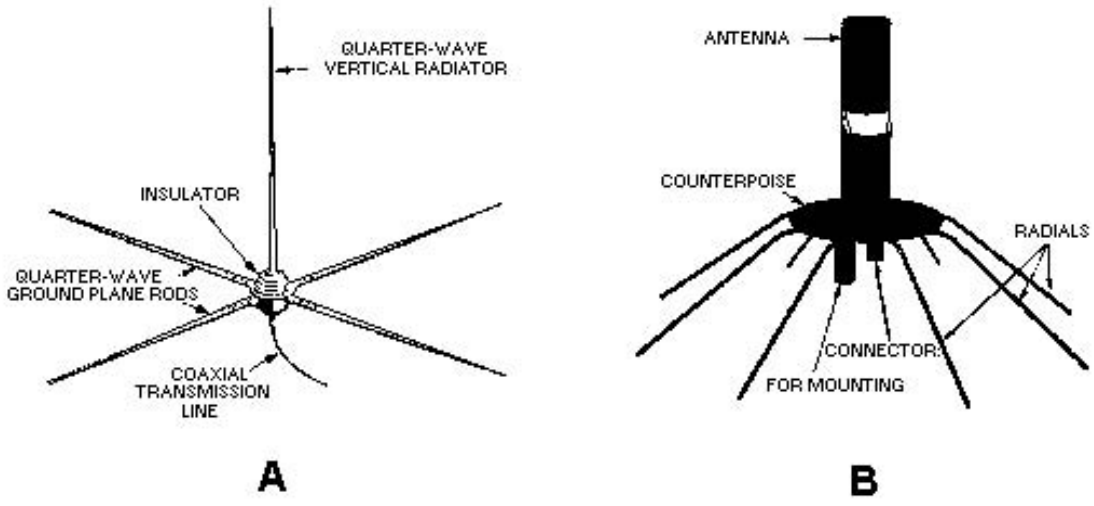


Figure 1-38.—Ground-plane antennas.

Corner Reflector

When a unidirectional radiation pattern is desired, it can be obtained by the use of a corner reflector with a half-wave dipole. A CORNER-REFLECTOR ANTENNA is a half-wave radiator with a reflector. The reflector consists of two flat metal surfaces meeting at an angle immediately behind the radiator. In other words, the radiator is set in the plane of a line bisecting the corner angle formed by the reflector sheets. The construction of a corner reflector is shown in figure 1-39. Corner-reflector antennas are mounted with the radiator and the reflector in the horizontal position when horizontal polarization is desired. In such cases the radiation pattern is very narrow in the vertical plane, with maximum signal being radiated in line with the bisector of the corner angle. The directivity in the horizontal plane is approximately the same as for any half-wave radiator having a single-rod type reflector behind it. If the antenna is mounted with the radiator and the corner reflector in the vertical position, as shown in view A, maximum radiation is produced in a very narrow horizontal beam. Radiation in a vertical plane will be the same as for a similar radiator with a single-rod type reflector behind it.

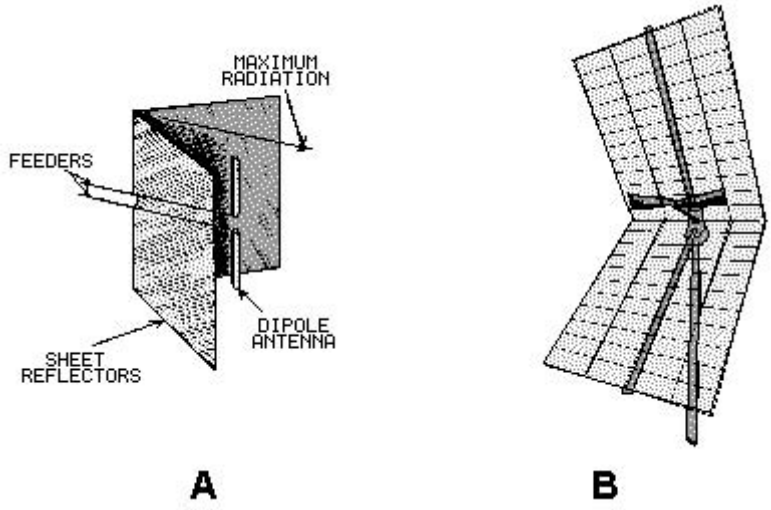


Figure 1-39.—Corner-reflector an

Study 5: Antennas (Continued)

Reference Material: NLECTC Guidebook, Chapter 6, Pages 50-64

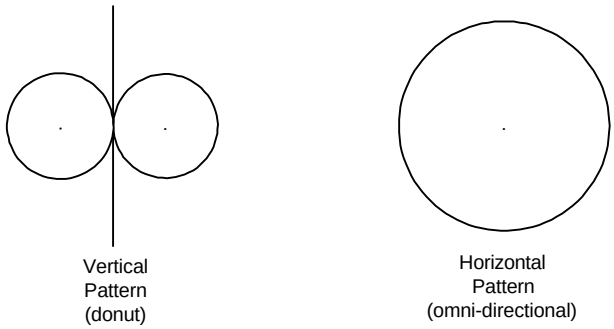
Antennas

An *antenna* allows a radio transmitter to send energy into space and allows a receiver to pick up energy from space. Generally, the higher an antenna is above the ground, the larger the coverage of the radio signal.

The fundamental antenna is the *dipole*, which consists of a wire or rigid metal rod. A dipole's length is set to be approximately one-half the wavelength of the carrier frequency. Thus, a 300 MHz carrier, with a wavelength of 1 meter, would need to use a dipole that is ½ meter long. Similarly, the dipole for a 900-MHz carrier, whose wavelength is 1/3 meter, would be 1/6 meter long (approximately 6 **e** inches).

Assuming the wire is vertical, the three-dimensional radiation pattern is *omnidirectional* around the wire in the horizontal plane and is donut shaped in the vertical plane, as shown in figure 6-9. (Omnidirectional means that the same amount of radiation can be measured the entire way around, at any given cross-section of the donut.)

Figure 6-9. Dipole Antenna Patterns



If the antenna is vertical to the earth's surface, its electric field will be vertical, and the antenna is said to have vertical *polarization*. If the antenna is horizontal and the electric field is parallel to the earth's surface, the polarization is horizontal. Almost all mobile operations use vertical polarization.

Antenna Gain

Antennas are the transmitting and receiving elements of a radio system. *Gain* is the focusing of the antenna's radio frequency (RF) electromagnetic energy toward certain directions. By focusing the energy from or to a dipole antenna in a particular direction, you can increase the effective transmitted power outward towards that direction plus increase the received signal strength from that direction. This is important for two reasons: 1) you may be able to use less power to transmit a signal for the same signal

level at a receiving site; and 2) interfering signals from other directions will decrease in level causing less radio frequency interference for you.

Suppose an antenna that radiates equally in all directions (an *isotropic radiator*) were represented by a perfectly round air-filled balloon with air as energy, then the energy per unit area (in watts/cm^2) on the surface of the sphere would be equal anywhere on the sphere.

We can, however, manufacture a "donut radiator" by feeding energy into a half-wave dipole antenna with a resulting radiation pattern like the one shown in figure 6-9. (Note that only the elevation (vertical) pattern is increased; the azimuth (horizontal plane) pattern is a circle.)

If you were to grab the center of the spherical "isotropic balloon" and squeeze it in the middle so that you had a barbell with equal spherical balloons on each end, a cut through the middle would look like a donut without the hole, similar to the vertical pattern of the dipole shown in figure 6-9. The same watts of energy as in the original sphere (air in our analogy) are now concentrated in the two barbell ends. In addition, the length from the center of the donut to the furthest point on the spheres is now increased, i.e., the original energy is now focused in the two spheres. This increase in length compared to the radius of the original balloon is the "gain" over the isotropic radiator. (The increase in this amplitude over the original balloon radius is 1.64 times, or 2.15 dBi.)

Next, if our hypothetical balloon is squeezed down further, the barbells go out further and the maximum gain in the elevation direction increases (total gain increases). This might occur when two dipoles are fed in phase so the gain is now 3 dBd (or 3 dB greater than that of a dipole), as seen in figure 6-10. Note that in the horizontal direction the pattern is still a circle, although its diameter (3 dBd gain) is twice that of the dipole.

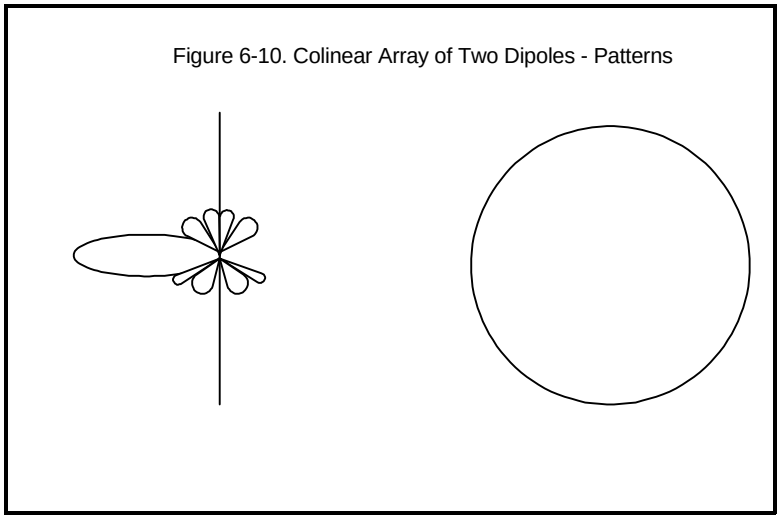


Figure 6-10. Colinear Array of Two Dipoles - Patterns

One way to achieve this type of gain is to stack dipoles end to end with some vertical separation between them. This type of antenna is called a colinear gain antenna. As the gain is increased in the elevation pattern, the vertical angle of the beam is reduced. Since the phase of the RF energy into each dipole is not perfect, "side lobes" are developed, as seen in the left side of figure 6-10. The side lobe amplitudes are much less than that of the main lobe. The beam width of the main lobe is defined as the angle between the half power points.

Both isotropic and dipole antennas are used as references for the gain of other antennas. That is, the maximum radiation of an actual focused antenna is compared with that of either an isotropic radiator or a dipole antenna. (Isotropic radiators are generally used for frequencies of 1 GHz or above.) If the reference

is an isotropic radiator antenna, the decibel measurements are designated as dBi. If the reference is a dipole antenna, the decibel measurements are given in dBd. The gain of the dipole is related to the gain of the isotropic radiator as 2.15 dB.[1] In general, the larger the aperture or the length of an antenna for one frequency, the higher the gain and the smaller the beam width.

Because the vertical beam width is narrowed as a base station's antenna gain is increased, it is necessary to make sure that the main beam will hit the receiving station antenna. If there are large differences in elevation between transmitting and receiving antennas, there is a possibility of missing them. Base or repeater stations that are placed on very tall buildings or on mountaintops often are designed with a "downtilt" on their patterns to make sure that the maximum radiation hits close-in mobile units.

Gain is important because of its relationship to RF power requirements. For example, if the gain at a base station is doubled in the direction of a mobile, the mobile receiver will receive twice the signal strength power. Similarly, a mobile transmitting towards the base station will have twice the signal strength at the base station. Plus, potential co-channel interfering signals coming from other directions will be lessened with respect to the desired signal.

To summarize, by increasing the gain (or directivity) of an antenna in a two-way radio circuit, you may save money by buying a less powerful transmitter, achieve higher received signal levels from stations in the gain direction, and discriminate against signals on the frequency from other directions.

Types of Antennas

Base station antennas. Most base station antennas are omnidirectional in the horizontal plane (azimuth) so that mobile and portable radios may communicate with a base station from any direction. To increase the transmitter and receiver directivity, many base stations use colinear arrays of dipoles for up to 6-decibel gain at VHF stations and up to 12-decibel gain for UHF stations.

Directional antennas. If you need to direct the RF energy in one direction and do not need an omnidirectional pattern in the horizontal plane, an antenna may be constructed to shape the pattern toward the single direction. Some of these kinds of antennas are corner reflectors (see figure 6-11), Yagi antennas (see figure 6-12) and parabolic dishes. The patterns in both the horizontal and vertical planes are focused

[1] Gain = $10[\log_{10}(P/P_{REF})]$, where P = the maximum power density of a given antenna and P_{REF} is the maximum power density of either the isotropic radiator or the dipole.

Figure 6-11. Corner Reflector

Figure 6-12. Yagi Antenna

and increase the gain considerably over an omnidirectional dipole. (Photographs courtesy of Decibel Products, Dallas, TX.)

Mobile antennas. The simplest mobile antenna is a quarter-wave whip antenna. It consists of a single vertical element, approximately 1/4 wavelength long, mounted onto the metal roof of an automobile, and is called a monopole.

The roof acts as a "ground plane" reflector so that the antenna radiation pattern emulates a dipole antenna.

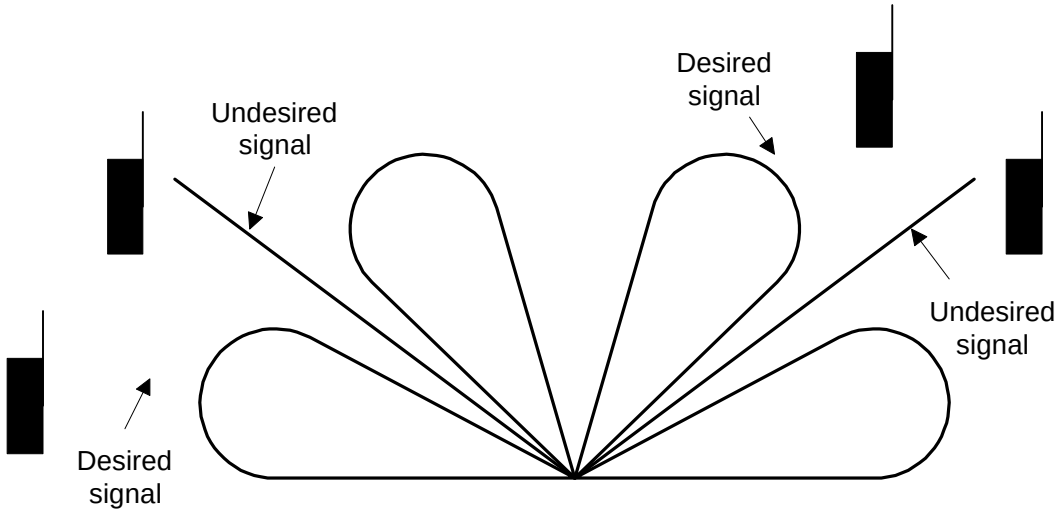
At VHF low band (50 MHz), a quarter wave monopole antenna is about 5 feet long. As the frequency is increased, the length of a monopole antenna is reduced. At 850 MHz, a monopole is only 3.5 inches long.

Portable antennas. Portable radios usually use helically wound or rod antennas attached to the radio. These are usually less efficient than base or mobile antennas. There are also times when your body is between the portable and the base with which it is communicating, causing a decrease in signal. In addition, the height of the portable antenna (belt mounted versus a lapel-mounted speaker-microphone antenna) can make a significant difference in radio coverage. All of these characteristics must be accounted for in designing a system.

Smart antennas. A major development has occurred in the design of "smart antenna arrays" which are able to adjust to their environment so that they enhance desired received signals while discriminating against interference from undesired signals. The antennas are made of a large number of antenna elements each of which are controlled using computer technology in near real time.

An example of a smart antenna is shown in figure 6-13. The main lobes of the antenna are placed directly on the desired signals while nulls are placed at the angle of interfering signals. Each element of the antenna is "tuned" so the composite beam is adjusted to maximize desired signals and minimize undesired interfering signals.

Figure 6-13. Pattern of Smart Antenna Adaptive Array



Our human ears work in a similar way at a noisy party. Even though there are several conversations occurring simultaneously, we are able to distinguish between them and focus on only one. Usually we do this by turning towards the desired conversation and concentrating our listening efforts toward the mouth of the desired speaker while “tuning out” the other undesired conversations.

Smart antennas adapt themselves automatically toward the direction of incoming desired signals via digital signal processing (DSP). With DSP, a series of microprocessors changes the phase and amplitude of the elements to focus the antenna pattern in the desired directions while discriminating against interfering signals. The most sophisticated antenna arrays are able to adjust to many different desired signals via space division multiple access (SDMA) so as to process the antenna lobes to accommodate the signals simultaneously.

Although smart antennas are quite costly, the economical trade-off is increasing the capacity of antenna systems to support an increased number of users.

Effective Radiated Power (ERP)

Effective Radiated Power, or ERP, is a term used in land mobile radio to indicate the "effective" power radiating from the antenna. ERP in decibels equals the transmitter power output into the transmission line, less the losses in the transmission system (including that of the transmission line, filters, couplers, etc.) plus the gain of the antenna in dBd. It is expressed as:

$$ERP = P_{IN} - L + G_{ANT}$$

ERP	= Effective radiated power in decibels above one watt
P_{IN}	= Power output from the transmitter in decibels above one watt
L	= All transmission losses in decibels
G_{ANT}	= Antenna gain in decibels above a dipole reference

An example of this is a transmitter with an output power of 100 watts, a coaxial cable with a loss of 2 dB, a combiner loss of 1 dB (total loss of 3 dB), and an antenna with a gain of 6 dBd. The resulting ERP would be calculated as follows:

P_{IN} = 20 dBW
L = -3 dB
G_{ANT} = 6 dBd
ERP = 23 dBW

When this is converted from dBW to watts, the effective radiated power is 200 watts[2]. One might ask: "How can we have an ERP of 200 watts when the transmitter only puts out 100 watts into the coaxial cable?" There is conservation of power. No physics law has been broken.

ERP is a fictitious number indicating the effectiveness of a transmission as compared to that of a transmitter connected to a dipole with no transmission losses. There is a real point to it. To the receiver listening to this transmission, the transmission will be 3 dB stronger than it would if it came from the same transmitter using a cable with no loss and a dipole antenna.

Interference

With the advent of cellular, PCS, specialized mobile radio (SMR) and enhanced specialized mobile radio (ESMR) systems, many new antenna installations must be made throughout the country. To minimize the number of new antenna sites (and associated towers), installations with a multitude of radios combined on a few antennas are becoming more prevalent.

[2] Watts in dBW = 10 logP, where P is in watts. To get the power in watts, we divide dBW by 10 and raise the answer to that power: Power in Watts = $10^{(\text{power in dBW}/10)}$.

As the number of radios and antennas is increased at a site, the *interference* potential of generating and/or receiving spurious signals is increased. Therefore, filters and isolators (discussed in the next section) must be added to the antenna circuits. Usually, the last station to build at the site causes the interference and is responsible for the additional filtering equipment. Some sites have full-time managers who screen an applicant's plans to anticipate any interference potential.

Interference may be predicted using a software program by inputting the transmitted signal frequencies and bandwidths and the receiver frequencies and bandwidths. This allows you to determine the intermodulation product frequencies and harmonics that might be generated externally or internally in the equipment. Knowing what may be expected allows you to take preventive action. Some types of filters used are discussed in the duplexers, combiners, and multicouplers sections of this book.

Radiation

A potential problem of exposure to harmful radiation exists around transmitting antennas. Service personnel in the vicinity of a tower or climbing a tower could be exposed to harmful radiation. It may be necessary to reduce power or shut down transmitters before climbing a tower. Wearable exposure alarms are available to warn of excessive radiation from Narda Microwave, a division of Lockheed Martin.

The radiation danger is highest when there are high-power broadcast stations at common sites. Radiation exposure requirements for the public are less than for personnel associated with the site (see table 9-1 in chapter 9). To help prevent public exposure, security fences usually are constructed around towers, and the fences are posted with "Hazardous RF" signs.

Local Regulations Controlling Antennas

Most cities have zoning ordinances that control the use of land for radio sites. These usually include maximum tower heights and setbacks, as well as the antenna types and radiation characteristics. Usually an application for a radio site is prepared by an applicant and submitted to the zoning board for processing and a recommendation. County commissioners or city council members have the final approval. Members of the public often have the opportunity to voice their opinions regarding the aesthetics and requested use of the site before approval. It is not unusual for a government entity to add stipulations for disguising a tower and antenna. Recent examples include requiring a tower to look like a tree and using a church steeple to house an antenna.

Radio Coverage

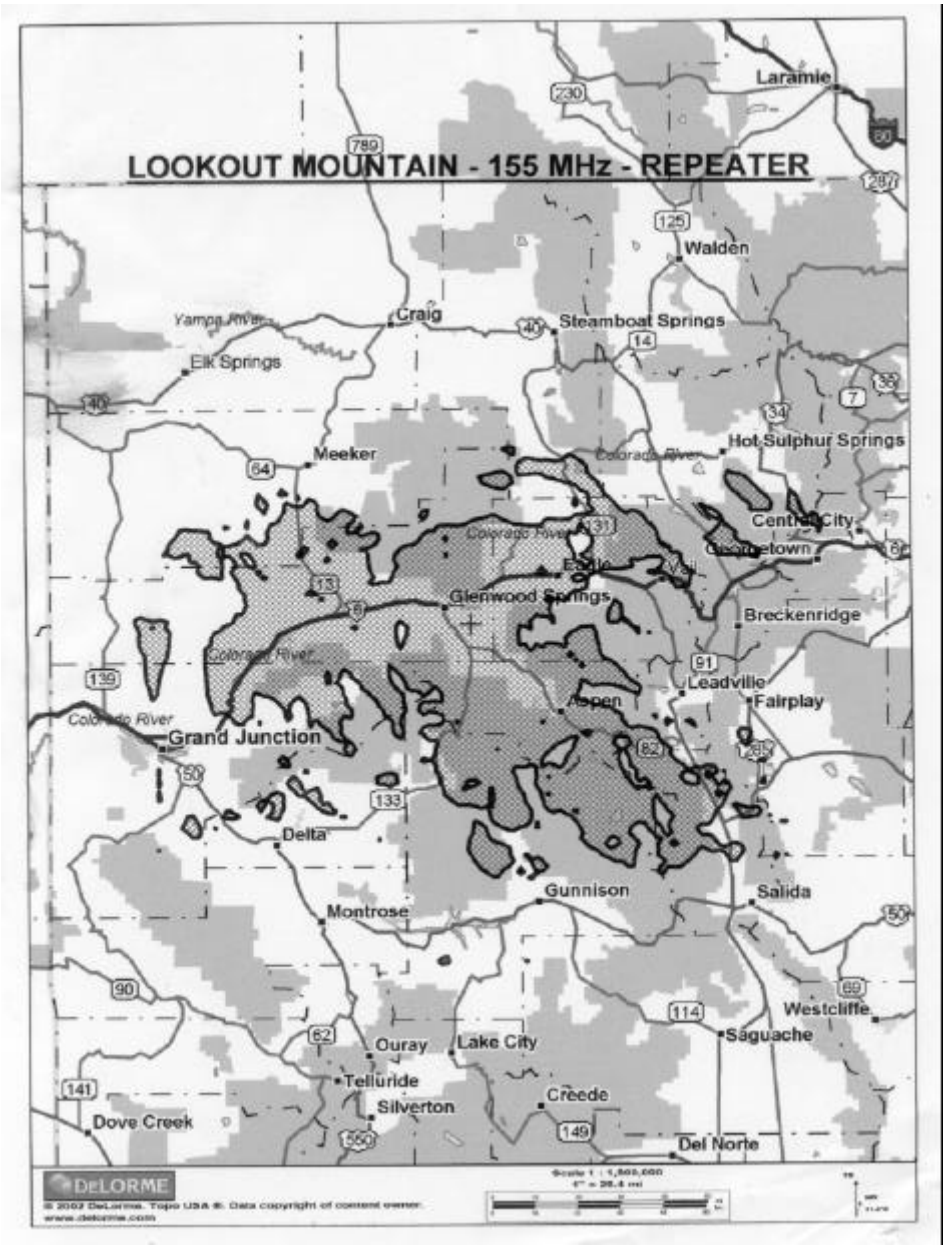
One of the most important characteristics of a radio system is its *coverage*. That is, it is important to know exactly where the base or repeater station signals may be received by mobile or handheld radios and exactly where mobile or handheld radio stations may be heard by a base or repeater station.

All parameters must be placed into one of several computer models (called propagation models) to get a reasonably accurate output. These include transmitter power out, transmission line losses, antenna gain and

directivity, foliage losses, building losses (if required), receiver sensitivity, and antenna and transmission line characteristics.

Figure 6-14 shows a typical coverage pattern for a base station (the cross hatched area outlined in black). Notice that there are some holes in the main contour (white areas within the cross hatched area) where signals are not heard, and there are some places (hills) outside of the main contour where there is reception.

Figure 6-14. Sample Coverage Map (courtesy Hartech, Inc.)



Mobile and handheld radios have different characteristics than base stations due to their lower power and to poorer antenna efficiency. Coverage patterns should be made for each kind of radio used in a system so that you know exactly where to expect coverage. If you don't know that an officer's portable radio transmission will not be heard at a repeater, it could put the officer's life in jeopardy.

Coverage should *always* be verified by running actual tests after a system is constructed. There are testing procedures available from some of the larger system suppliers. These include the use of vehicular calibrated receiver systems, which measure the station signal strengths versus location at points along a predetermined route. Standards are being developed by a Telecommunications Industry Association (TIA) committee consisting of industry and user representatives.

Duplexers, Combiners, Multicouplers

Duplexers, combiners, and multicouplers are components that make it possible to connect multiple transmitters and receivers to antennas. These important filtering and isolating components are used in a radio system to optimize its operation and minimize interference with itself as well as other systems.

A single *repeater*, consisting of a transmitter and a receiver operating on different frequencies, is most often connected to a common antenna. If the transmitter energy gets into the receiver, it can burn out the front-end components or cause severe interference in the receiver and, as a result, in your overall system.

You can use two antennas, one above the other, but this configuration may still not provide enough isolation. Therefore, a duplexer may be used to increase the isolation and to keep the transmission from interfering with received signals.

Duplexers

To shield the receiver from the transmitter, *cavity filters* are often added in the transmitter and receiver transmission lines to form a circuit called a *duplexer*. There are several configurations.

One method of duplexing is by placing a "pass" filter in the transmitting line and a "reject" filter in the receiving line with both filters tuned to the transmitter frequency, as shown in figure 6-15. When the appropriate isolating components are selected, the receiver does not experience interference from the transmitter. A typical duplexer is pictured in figure 6-16.

Figure 6-15. Duplexer

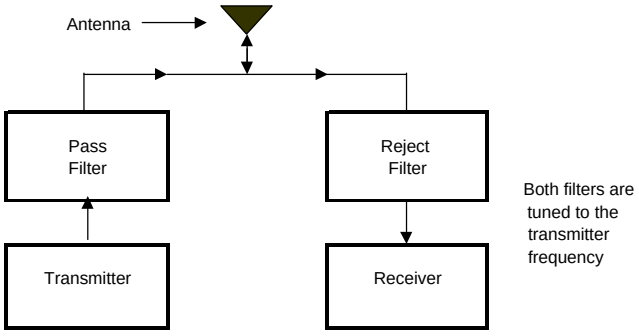


Figure 6-16. Typical Transmitter - Receiver Duplexer

Combiners

When trunked radio systems are used with a multitude of transmitters connected to an antenna, a circuit element called a *combiner* is used to combine the output signals. The combiner (shown in figure 6-17) allows the transmitter outputs to be coupled together, sending the output power of each transmitter to the antenna with minimal loss. A typical transmitter combiner is pictured in figure 6-18 (photos in figure 6-16 and 6-18, courtesy of TX RX Systems, Inc.).

Figure 6-17. Transmitter Combiner

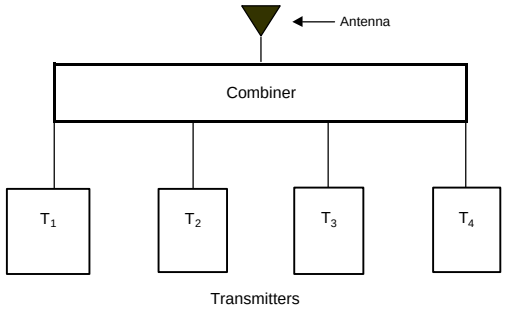
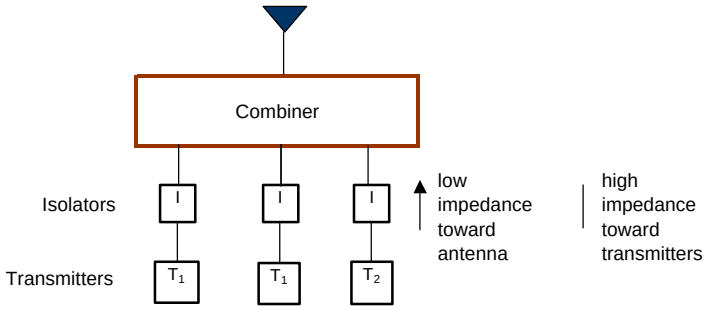


Figure 6-18. Typical Transmitter Combiner

An additional element may be used in the circuit between each transmitter and the combiner to increase isolation to the other transmitter outputs. Such an element is called an *isolator*, as shown in figure 6-19.

Figure 6-19. Isolators

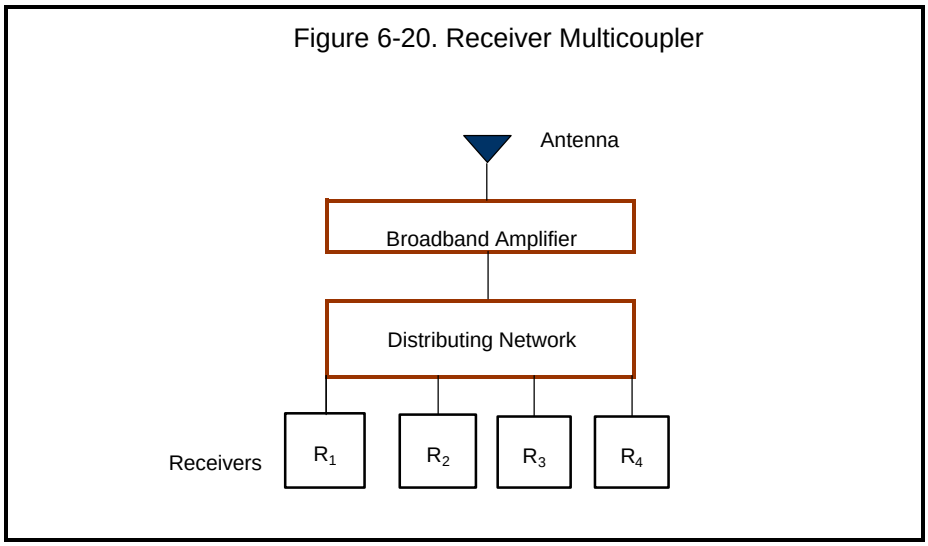


If there is inadequate isolation, the mixing of the transmitted signals can cause the generation of additional frequencies called intermodulation products, or IM products, which may cause interference to nearby receivers.

Multicouplers

A device similar to a combiner, called a *multicoupler*, is used to connect a multitude of receivers to a single antenna. Usually, a multicoupler contains an amplifier that covers all the receiving frequencies and then splits and sends each signal to its particular receiver, as shown in figure 6-20.

Figure 6-20. Receiver Multicoupler



Multiple Access Systems

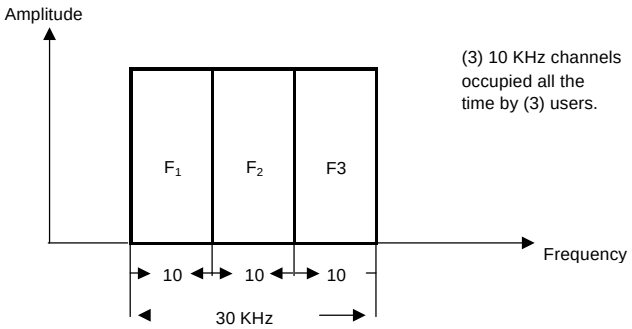
Several cellular radio systems are used to improve spectrum efficiency, allowing more users to employ a channel or frequency band. The primary technologies used today are frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). Public safety radio systems primarily use FDMA and TDMA technologies. To better illustrate these technologies, the examples below describe their implementation by the cellular telephone industry.

Frequency Division Multiple Access (FDMA)

The original cellular radio channels were 30 KHz wide and accommodated one voice signal subscriber. As the number of subscribers increased, some cellular radio companies opted to divide the 30 KHz channels into three 10 KHz channels, which would allow a 3:1 increase in subscribers, as shown in figure 6-21. The process is called frequency division.

Multiple access is accomplished by the cellular radio system control computer having the ability to assign each of the channels to different subscribers. When one subscriber has completed a call or moves into a new cell, the channel may be reassigned to another subscriber.

Figure 6-21. Frequency Division Muliple Access (FDMA)

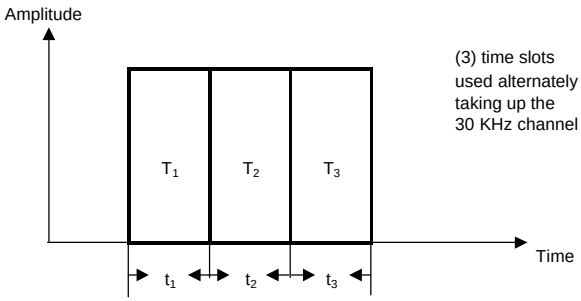


Time Division Multiple Access (TDMA)

Another scheme used by cellular companies is to take the same 30 KHz channel, but instead of dividing it into three narrower channels, it is set up for transmission in three time periods so that three subscribers still use the total 30 KHz; now each subscriber would talk for one-third of the time, thus increasing the number of users by 3:1. By allowing each subscriber to talk for a few milliseconds in rotation, three conversations now take place within the same 30 KHz channel. See figure 6-22.

For time division transmission to work, the voice signal must be digitized by a vocoder (voice coder) and each digitized signal is sent in sequence over the 30 KHz spectrum. The subscriber's phone must be perfectly synchronized with the transmission so that it only decodes the desired subscriber's signal in its vocoder. Cell phone and PCS companies have found that by using TDMA, up to eight subscribers may use the same 30 KHz spectrum. Multiple access is accomplished in the same manner as in FDMA above.

Figure 6-22. Time Division Multiple Access (TDMA)



Group of special mobile (GSM), which was developed in Europe and is being used by a number of U.S. companies, provides TDMA transmission with 200 KHz wide channels in the 2 GHz band.

Code Division Multiple Access (CDMA)

CDMA is a digital modulation that uses spectrum spreading techniques and is more complex than either FDMA or TDMA. The transmission spectrum is always much wider than that required for a single transmission, allowing many simultaneous transmissions to be interspersed within the same bandwidth.

Two types of systems are used: *frequency hopping* and *direct sequence.* Both systems use vocoders to digitize the signal.

Frequency hopping. The frequency hopping concept is easy to visualize. The transmitter changes frequency every few milliseconds in a prescribed manner as it transmits information. A perfectly synchronized receiver follows the frequency change sequences of the transmitter from one frequency to another to receive the information.

By having as many different frequency changing sequences as there are radios in a given area, many conversations may occur at the same time over the same spectrum. When two transmitter signals collide on the same frequency, the receiving phone transmits a message that it was not received and the original information is resent.

☞ Did you know?

The original patent for CDMA was assigned to Hedy Lamarr, the movie star, who developed the concept during World War II.

Direct sequence. In the direct sequence CDMA, the transmitted digital signals are coded by a "spreading algorithm" in each transmitter. Each receiver has a decoder that deciphers the spread signal and recovers the voice. By using several different spreading codes within each algorithm, this system accommodates many different users at the same time.

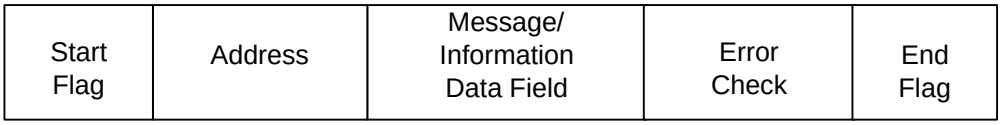
Packaging Data

Packet radio is a heavily used technology for transmitting and receiving data, such as National Crime Information Center (NCIC) data, from a patrol car to NCIC. Packet radio is a computer-to-computer communications mode in which information is broken into short bursts containing a message. The bursts (packets) also contain addressing and error detection information.[3]

One method for packaging data is called Cellular Digital Packet Data (CDPD). Additional discussion of this particular method is given in chapter 7.

A typical packet frame protocol as composed on a computer is shown in figure 6-23. The packet begins

Figure 6-23. Typical Packet Frame



[3] *1995 ARRL Handbook,* 72nd Edition, P. 1.10, Newington, CT: American Radio Relay League.

with a flag that signals the beginning of a frame. Next is the address of the packet, then the message or information data field, next an error-checking portion, and finally an end-of-frame flag. Usually about 1,000 bytes are transmitted in a packet. When the packet arrives at the address receiving computer, the packet information is stripped off and checked for errors.

If a message is so large that several packets must be sent, the field contains information for the computer to reassemble the original message in the proper order. If a packet is lost, the receiving computer acknowledges the loss to the originating computer, and the packet is resent.

There are several world standards for packet communications. One well-used standard for data packet transmission is CCITT X.25. Specialized software is required to run packet radio systems.

Study 6: Current Public Safety Systems

Reference Material: NLECTC Guidebook, Chapter 7

Chapter 7

Current Public Safety Radio Systems

Paging Systems

Paging systems are single-frequency, one-way radio systems used for making people aware that they are being sought. The original local government pagers were voice pagers used for calling out volunteer fire departments (many of which are still in use). Modern pagers have alphanumeric readouts and are capable of storing a number of messages. Pagers are used by volunteer fire departments, police officers, emergency medical personnel, service personnel and technicians, and even children whose parents wish to keep track of them.

Very reliable commercial paging services are available in most regions of the United States at reasonable subscription rates. Many are used by local police, fire, and emergency medical services (EMS) units.

Alerts are given by a tone or a set of tones or by a built-in vibrator for use where tones are not permissible. There are many local and national suppliers of paging services and pagers.

Paging is accomplished at many different frequency bands including VHF, UHF, and FM broadcast. Two standards are especially popular at this time, but many others exist. These include the British Post Office standard, called POCSAG (Post Office Code Standardization Advisory Group), and Motorola's FLEX™ system.

Statewide and nationwide paging is accomplished by transmitting the paging information over telephone lines or via satellites to paging transmitters for retransmission. When it is necessary to page over a wide area, a multitude of paging transmitters are activated at the same time in a simulcasting fashion.

The FCC has auctioned off a number of pairs of frequencies for two-way paging in the 900 MHz band (PCS narrowband). Each uses a 50 KHz bandwidth in one direction to accommodate high-speed data transmission, which is paired with either 50 KHz or 12.5 KHz in the reverse direction for returning data. The FCC also authorized some paging response frequencies for paging users who are already licensed under parts 22 and 90 of the FCC Rules, under certain circumstances.

Short Messaging Systems (SMS)

Short Messaging Systems (SMS) are capable of transmitting and receiving messages with up to 160 characters (like Western Union telegrams) with either a special modem using cellular technology or over a land line. The development has been confined to companies utilizing GSM networks in Europe and is just making its debut in the United States, where only a small number of systems are equipped to handle the GSM protocol. These include AT&T Wireless, Cingular Wireless and T-Mobile Wireless Corporation who offer some SMS capable phones. Other companies will follow as the technology becomes economical to use. As we write this, the number of U.S. users for SMS is few; however, it is estimated that as many as 20 billion SMS messages are sent monthly in the rest of the world.

The cell phone and/or PDA requires a keyboard and a wireless modem for the transmission of point to point data to an internet service provider (ISP). Specialized software allows a user to send and receive messages without being constantly connected to the internet service. Messages can be stored at the ISP station for forwarding once a cell phone is turned on and a connection is made. In other words, this is an e-mail service for a few characters which may be used for instant transmissions or for store and forward operation. Because of the limited number of characters, short cut methods similar to the 10-10 code (or amateur radio Q code) messaging system are used for repetitive messages.

In the civilian world, SMS is proposed for turning up the heat at home when leaving the office; turning on ovens to accommodate meals when arriving home; keeping inventories of food in freezers so a simple inquiry will deliver a grocery list to allow for a stop and purchase on the way home; and so forth.

The potential of running short messaging from a wireless radio or a land line may be an especially valuable tool for police surveillance to remotely turn on tape recorders, cameras or other apparatus. It may also be a methodology for the automatic transmission of smoke alarm information directly to a responsible fire department. Security still remains a problem to be solved in the near future until reliable, encrypted, and dependable SMS is possible. There will be many opportunities for SMS use in the overall justice system as usage increases.

Two-Way Simplex Radio Systems

Two-way radio systems using one frequency are called simplex radio systems. Base stations, mobiles, and handheld radios communicate on a single frequency. All new equipment being placed into service today for both VHF (excepting the 220 MHz band) and UHF bands is required to be 12.5 and 15 KHz wide, respectively, as required by part 90 of the FCC Rules. However, users with 25 and 30 KHz bandwidth equipment may continue to use their existing systems.

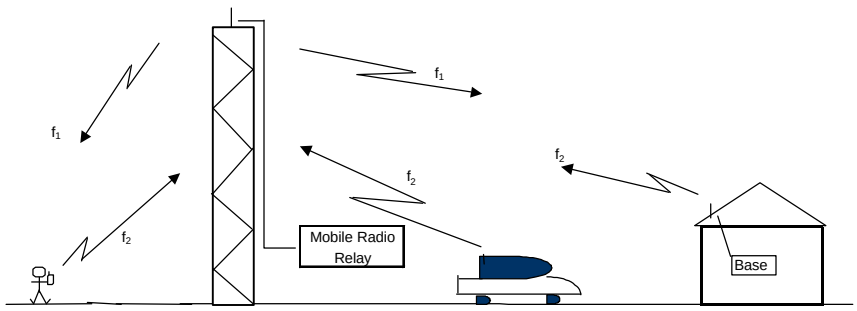
Base stations usually have high antenna installations to make sure that they can attain the desired radio coverage area. One problem with a simplex system is that handheld and mobile radios cannot communicate very far with each other because of their low antenna heights and are usually limited to just a few miles in flat terrain. Therefore, the person at the base station must repeat transmissions from one mobile to another. To alleviate this situation, the mobile relay or repeater was developed.

Two-Way Mobile Relay Systems

Two-way mobile relay systems are also called mobile repeaters, or just plain repeaters. In this discussion, these terms are used interchangeably.

The repeater makes use of two frequencies. The repeater radio functions as an amplified relay station receiving high- or low-power base stations, low-level mobile, and handheld radio signals, changing their frequency, amplifying the signals, and re-transmitting them on the repeater output frequency. Figure 7-1 shows the use of frequencies in a repeater configuration. In the figure, f_1 is the output frequency of the repeater and the input frequency to all base, mobile, and handheld radios and f_2 is the output frequency of the base, mobile, and handheld radios and the input frequency of the repeater. Repeaters are generally installed on the highest points within the coverage areas, including high buildings and mountaintops where the topography allows for maximum coverage and penetration. Thus, regardless of the output or the antenna heights on handheld, mobile, and base radios, the repeater signal is always the same strength at any receiving site.

Figure 7-1. Repeater System



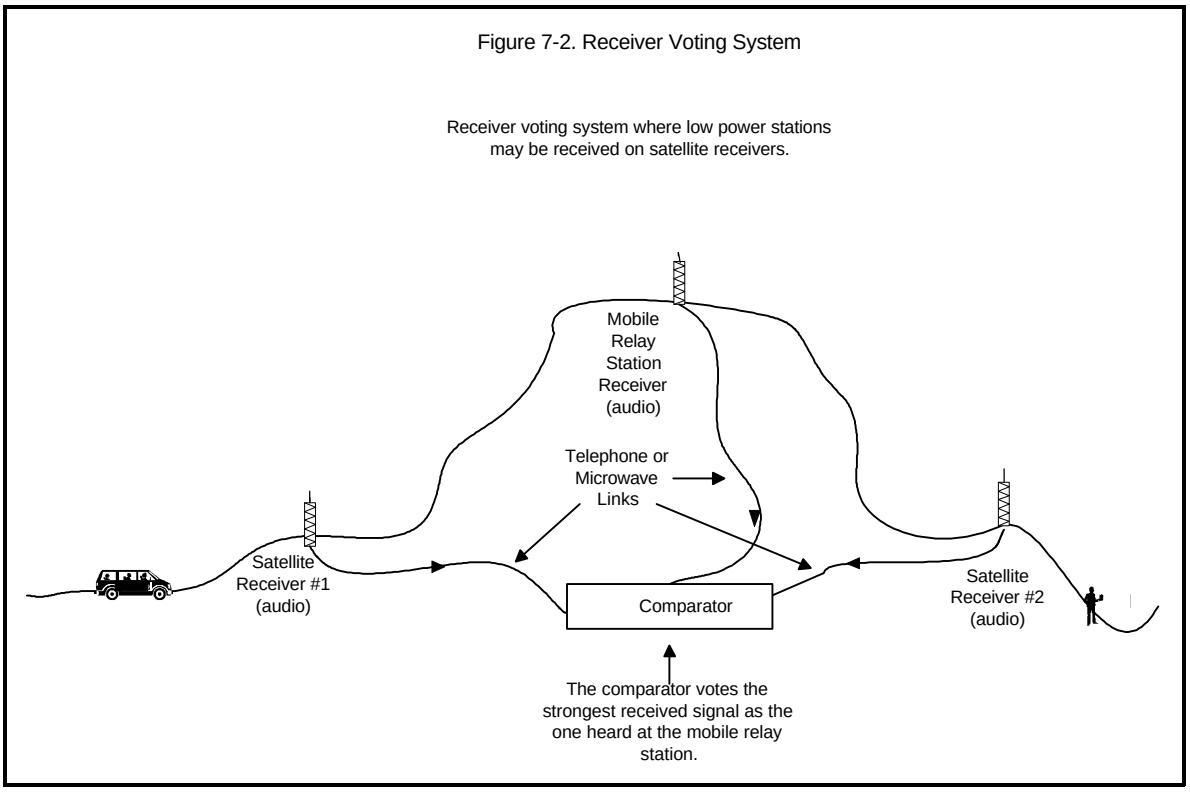
Mobiles, low power base and handheld radios transmit on frequency f_2. The signals are detected by the repeater and remodulate a transmitter on f_1 at the mobile relay site.

Twice the bandwidth of a simplex system is now required, further aggravating the spectrum efficiency problem. Voice FM simplex and repeater radio systems suffer from other disadvantages too. For example, when a base or repeater station is placed on a high point, it can cover distances of 60 miles or more in radius and thus, although not usually needed by the licensee, negates the option of relicensing the frequency to another user up to 120 miles from the licensee.

Repeater Innovations

Repeater stations are usually high-power stations, 600 to 3,500 watts ERP, and cover a large area. Handheld radios, with their low output power of 0.5 to 3 watts ERP, are often unable to be heard at the repeater site, particularly in hilly or mountainous terrain or in urban areas having numerous tall buildings. To correct this power imbalance, one or more satellite receiving sites may be set up in these coverage areas close to the low-power radios to receive the low-power signals. Each satellite receiver's output is sent via telephone line or microwave radio transmission to a signal comparator at a central site, where the strongest signal is selected through "voting" and utilized to drive the repeater. The scheme is shown in figure 7-2.

Figure 7-2. Receiver Voting System

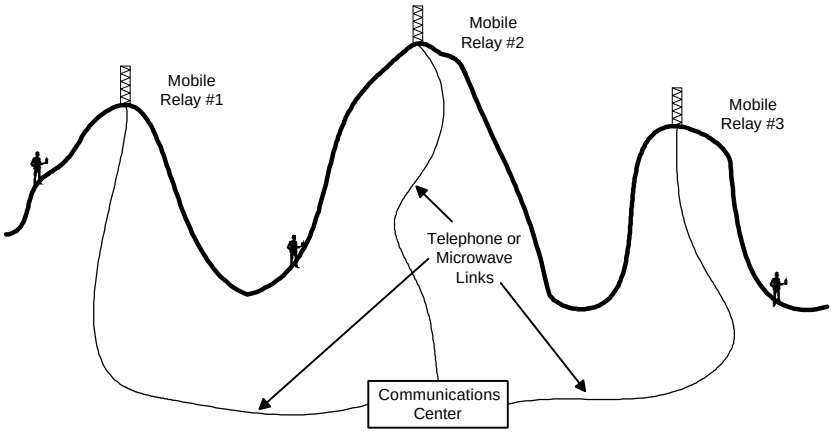


Another scheme used where there are problems transmitting to and receiving from mobiles and handheld radios due to large changes in topography requires several repeaters at different locations that may be switched at a central position, usually at the police communications dispatch center, to the repeater receiving the highest signal level. In this way the signal is "steered" toward the station, as shown in figure 7-3.

Where very large areas are to be covered, for example several counties, simulcast systems using multiple repeaters operating on the same frequency may be employed. In this case, all transmitters operate simultaneously and send a composite signal to receivers in the field. Special emphasis must be placed on frequency stability of the carriers, for they must be within a few Hertz at all stations; the modulation must be transmitted at exactly the same time, or there will be interference in the overlap zones of the repeaters.

Frequency and time stability can be accomplished by the use of microwave communications systems or by using the clock signals received from a global satellite system (such as GPS).

Figure 7-3. Repeater Steering



At the Communications Center, the repeater that receives the strongest signal is the one used to transmit to that user.

Mobile Repeaters

Small vehicular repeaters have been used to relay transmissions from handheld radios through the main vehicle radio to headquarters when an officer is in an area where he or she cannot reach the base repeater. An example of this is when an investigator, located in the concrete basement of a shopping center, can use a small 450 MHz repeater in the investigator's vehicle to bridge communications between the basement and headquarters.

These repeaters have been used traditionally in the 150 and 450 MHz bands, and the concept is being explored for 800 MHz use by agencies and frequency coordinators.

Trunked Radio Systems

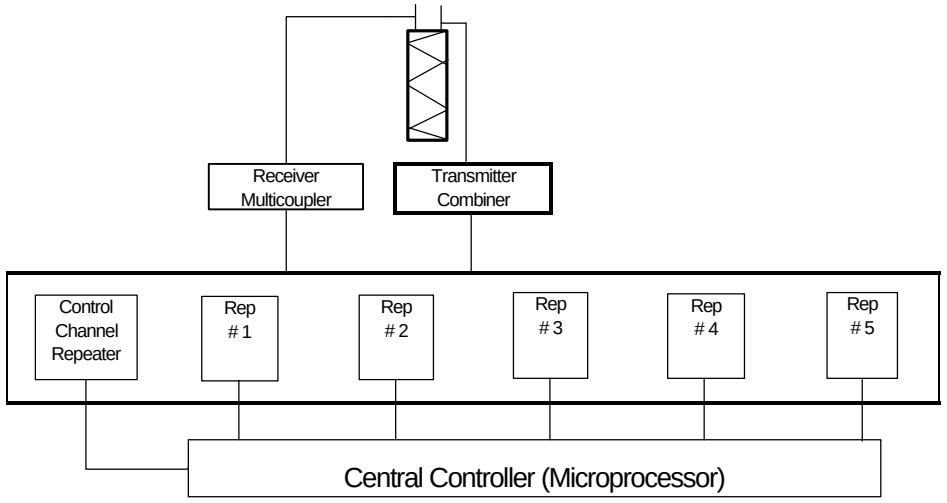
Public safety organizations have traditionally used dedicated repeaters. For example, in many communities, separate repeaters are used by the police department, the fire department, administrative departments, and road maintenance department, although the transmission loading is unequal for the departments most of the time.

If a police department needs to use two repeaters for operation and the road maintenance department's repeater is available, the police department may be unable to use it. To use it requires that the police department's mobiles tune their receivers to road maintenance's frequency and that the police dispatch has an extra base station to contact the road maintenance repeater. This scenario is not very practical.

A repeater cannot be borrowed by another user, so it often sits vacant on a usable frequency while a user needing to transmit more information on his or her radio system must wait until their own repeater is free. To solve this problem and to improve the spectrum efficiency, the industry developed a "trunked" system concept borrowed from the telephone company industry.

With reference to figure 7-4, one can think of this as a box containing a number of repeaters, each of which may be switched into a radio circuit as needed. For example, if there are five trunked repeaters and repeaters #1 and #2 are in use, a central controller will designate #3 as the next repeater to be used when the need arises. If #1, #3, #4, and #5 are in use, it will designate #2 for the next user. In this way, repeaters do not stand vacant and the spectrum is more fully used.

Figure 7-4. Simplified Five Channel Trunked Radio System



Control channel is a dedicated data channel. Mobile units monitor the control channel. If a mobile wishes to contact a base or other mobile station, it initiates a call with its ID and the ID of the unit to be called over the control channel. The called station constantly monitors the control channel. The central controller selects an unused repeater and sends data to both units to set up the repeater's transmitting and receiving frequencies on their units. A conversation can then take place. When done the units again monitor the control repeater.

When it issued rules for the 800 MHz band, the FCC required that most licensees requiring five or more channels *must* use a trunked radio scheme.[4] Systems in place before the regulation was issued are "grandfathered in" and may continue to add single repeater stations as necessary.

[4] FCC Docket 18262.

Two technological breakthroughs have made trunked radio systems possible: 1) the development of microprocessors and personal computers, with their associated software and 2) synthesized frequency generators. Microprocessors allow the logical selection of frequencies for the repeaters. Frequency synthesizers at the repeater and mobile and portable stations allow the radios to set up individual transmitting and receiving frequencies as designated by the base station microprocessor called the "central controller."

One scheme used to inform the central controller that there is a need for a repeater is a dedicated data control channel (repeater), which monitors mobiles and handheld stations at the base station. If a user desires to speak with another user or a group of users, he or she initiates a transmission on the data control channel indicating his or her ID number and requesting that he or she talk with another user or a group of users by indicating the group's or individual's ID number. The control channel repeater acknowledges the transmission, and the central controller determines the available repeater and commands the initiator and the target station(s) to change their operating frequencies to that of the assigned repeater. Typically within 1/4 second, a voice conversation may then take place. After the conversation, the radios return to monitoring the control channel and the central controller determines that the repeater is now available for other use. Note that these systems are totally software driven.

Besides dedicating a single repeater for control, there are other schemes that can be used. For example, the control channel may be rotated from one channel to another. Each time it is moved, the subscriber's units must change frequency and track it.

Trunked radio systems are generally used in the 700/800/900 MHz bands. The latest FCC Rules now allow for trunking on public safety spectrum below 512 MHz, provided that these systems do not interfere with existing radio systems in surrounding areas.

Major U.S. suppliers of trunked radio systems are Motorola, the EFJohnson Division of EFJ, Inc., and the M/A-COM Division of Tyco International.

Specialized Mobile Radio (SMR)

Besides local government and law enforcement, trunked radio systems are used by large electric, gas, oil, and other industries to improve their efficiencies. A specific class of service, called "specialized mobile radio" was designated by the FCC to allow the set up of trunked systems that could be used to sell radio services to commercial and government users. The authors discuss these offerings later in this book as a reliable option, where available, for law enforcement.

The channel bandwidth set up for trunked activities is 30 KHz wide in the 800/900 MHz band. Original applicants used analog radios; however, enhanced specialized mobile radio has been the name given for digital SMR systems. Nextel is one supplier providing ESMR services nationally. Commercial services of trunked SMRs and ESMRs also are examined later in this guidebook.

APCO Project 16 Trunked Radio System

The Law Enforcement Assistance Administration (LEAA) in 1977 provided a grant to the Association of Public-Safety Communications Officials International (APCO) to make possible the opportunity for the public safety community to develop test beds and study various parameters associated with UHF band trunking systems.

APCO Project 16 members were charged with evaluating the technical, economic, and regulatory questions raised by the 800/900 MHz spectrum made available by the FCC. Studies were made on three experimental systems in Chicago, Miami, and Orange County, California.

When the study was completed, APCO published a document defining the mandatory and desirable functional capabilities for a public safety analog trunked radio system. It was issued in March 1979 and was called *900 MHz Trunked Communications System Functional Requirements Development.* The requirements were tailored for law enforcement and addressed channel access times, automated priority recognition, data systems interface, individuality of system users, command/control flexibility, systems growth capability, frequency utilization, and reliability.[5]

APCO 16 trunking systems are presently being used by many large and medium-sized government agencies. To make the technology available to smaller government groups in adjoining cities, some communities are sharing systems. This has cut down on both capital investment and operating costs for any single entity.

The APCO 16 specification had no interoperability or encryption requirements; thus systems supplied by different manufacturers do not talk to one another. This limits competitive bidding for expansion and replacement parts.

A new digital system specification, under the Project 25 Steering Committee, has been in process for years to correct some of the interoperability difficulties, improve spectrum efficiency, and take into account the changing world to more efficiently and economically manufacture digital radio systems.

Project 25 Digital Trunked Radio System

In 1989, APCO, the National Association of State Telecommunications Directors, and a group of federal agencies jointly formed a working group called Project 25 (or P-25) to undertake development of a series of standards to define a digital radio system (conventional and trunked). Current federal sponsors include the Federal Law Enforcement Wireless Users Group (FLEWUG), National Communications System (NCS), and the National Telecommunications and Information Administration (NTIA). Other agencies and organizations (including the Department of Defense, APCO Canada, and the British Home Office) have all contributed to this effort in ensuing years, resulting in a worldwide standard for digital public safety land mobile radio. The Telecommunications Industry Association has provided ongoing technical and standards

[5] APCO, *900 MHz Trunked Communications System Functional Requirements Development,* Executive Summary, March 1979.

development support. The resulting suite of standards has been approved by the American National Standards Industry (ANSI) as a national standard (the ANSI/TIA/EIA-102 series). Completed standards include conventional and trunked radio for phase I (12.5 kHz bandwidth) and Phase II (6.25 kHz bandwidth) FDMA architectures. Work is in progress on TDMA standards for 12.5 kHz (2-slot) and 25 kHz (4-slot) TDMA architectures.

The objectives of Project 25 are: to maximize spectrum efficiency; to ensure competition in life cycle procurements; to allow effective and efficient inter- and intra-agency communications; and to provide "user-friendly" equipment and operation. Services defined include digital voice address including individual, group, and broadcast calls; circuit data including protected and unprotected data; packet data; and a set of nine supplementary services including encryption. Both conventional and trunked air interface specifications are included. The specification will be used for unit-to-unit direct communications, base station to limited field units, multisite simulcast, voting receiver systems, and wide and local area trunking at frequencies from 100 to 1000 MHz.

As stated above, the APCO Project 16 standard resulted in a number of competing analog systems that were unable to communicate with one another, and high on Project 25's list of requirements is a common air interface between systems of different manufacturers enabling interoperability. In addition, there are common interfaces spelled out for the data port for laptop and other terminals, the host computer and other networks, the public telephone system interconnect, the network manager, and for connecting multiple systems (inter-system). Thus, competing companies may design their own offerings provided the common interface requirements are met.

☞ Did you know?

Project 25 got its name from the APCO Project Series that included the development of the 10-codes. Projects are APCO's way of identifying and funding specific efforts. As the primary sponsor of this digital standards activity, APCO simply assigned the next sequential number (25) in its series.

After a number of different systems were investigated, the committee chose an FDMA access scheme proposed by Motorola, Inc. The scheme initially involved 12.5 KHz channel bandwidth, later to migrate to 6.25 KHz bandwidth.

A migration strategy has been defined in Project 25 that allows forward migration to 6.25 KHz bandwidth and backward migration to 25 KHz trunked radio systems, including the APCO Project 16 systems. The system is heavily software driven, and Motorola has licensed its scheme and software to other vendors without royalties so that other vendors may produce Project 25 compliant systems in competition with them.

The 12.5 KHz air interface has been published, although the data port, data host, and network management interfaces are still being worked on.

Several large-scale Project 25 systems are now in use, including State government systems for Florida, Michigan, and New Hampshire.

The Federal government (including Department of Defense for base operations) has mandated Project 25 for its digital systems throughout the U.S. Likewise, the American Association of Railroads has standardized on Project 25 for all railroads in North America.

TErrestrial Trunked RAdio (TETRA)

While the Project 25 committee elected to standardize on a FDMA scheme for the 12.5 KHz first phase of Project 25, a European standards committee selected a TDMA trunking technology it called TErrestrial Trunked RAdio (TETRA). TETRA uses 25 KHz of bandwidth that allow packet-switched data at rates up to 28 kbps. The standard can provide up to four voice or data channels within a 25 KHz bandwidth, thus providing the equivalent efficiency of a single channel of 6.25 KHz (which is required in Phase 2 of Project 25). The Project 25 steering committee is considering the integration of TETRA technology within Phase 2. Over-the-air interoperability and other standard interface requirements of Phase 2 still need to be met. The first TETRA law enforcement communications system was employed in Finland using Nokia equipment. Motorola has supplied a system to public safety organizations for the Island of Jersey (United Kingdom), New Zealand, Poland, and Hong Kong. These systems use trunked radio configurations driven by software, so that many different schemes may be dynamically employed to adjust to different situations.

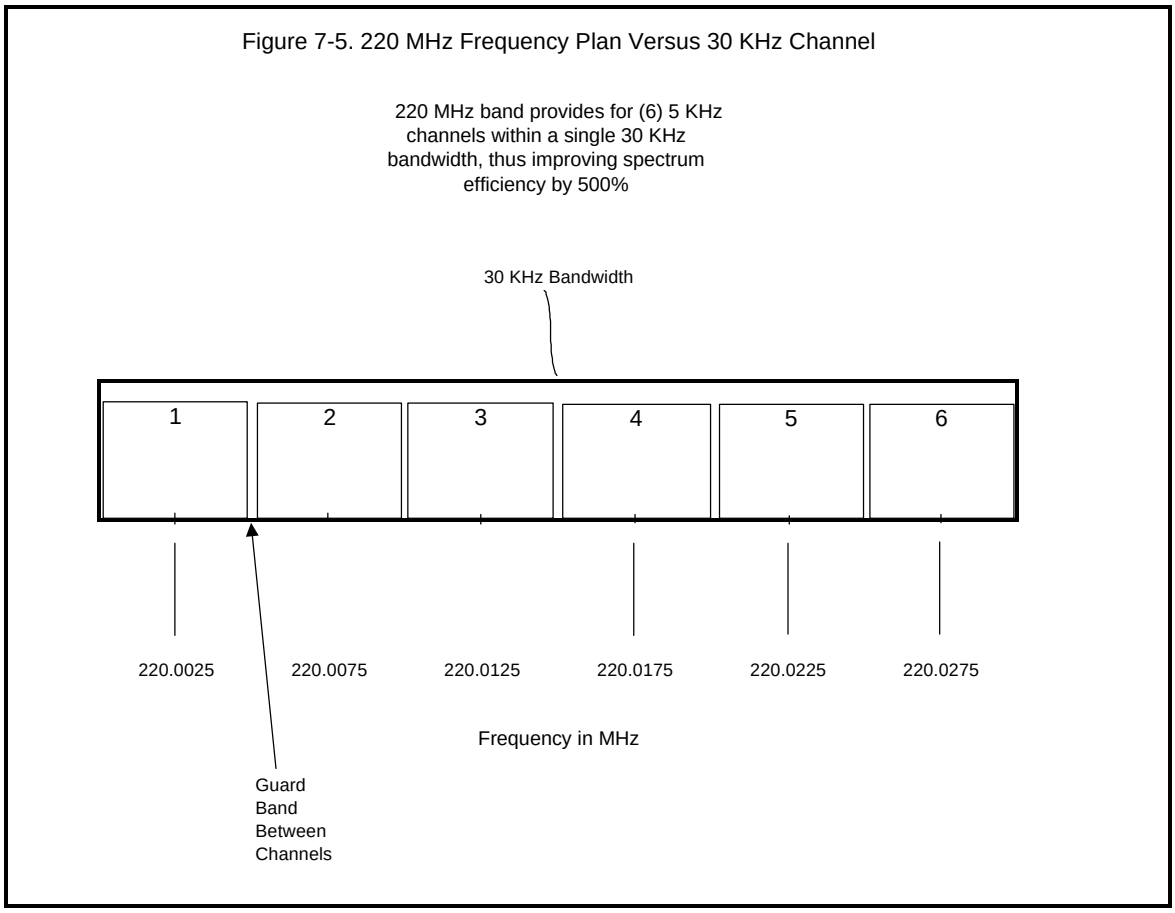
220 MHz Narrow Bandwidth Band

The FCC reallocated the frequencies from 220 to 222 MHz for narrow bandwidth communications use. The channel bandwidth in this frequency band is only 5 KHz so as many as six channels may be substituted for a single 30 KHz FM channel (i.e., six signals where there was one, with a subsequent increase in spectrum efficiency of 5:1). See figure 7-5. The FCC has auctioned off frequencies in this band for regional and nationwide licensing.

One method to accomplish getting a voice channel within 5 KHz is to use a type of modulation called “amplitude compandered single sideband” (ACSB). Other narrowband techniques were developed along with ACSB, some resulting in the ability to transmit voice and data at rates up to 16.8 Kbps.[6]

[6] *Linear Modulation Brochure,* Midland USA, Inc., 1998.

Figure 7-5. 220 MHz Frequency Plan Versus 30 KHz Channel



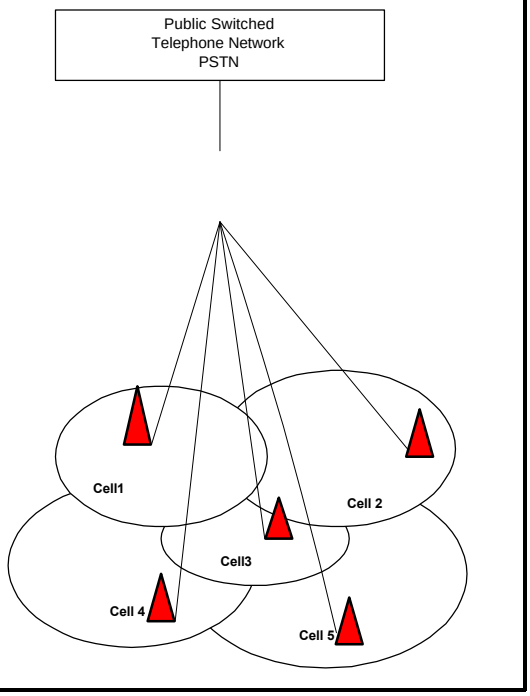
Cellular Radio/Telephone Systems

Cellular mobile radio was developed by AT&T. Originally, two licenses were awarded in each coverage area: one to a wire company and the other to a wireless company in almost all metropolitan and rural areas. The cellular scheme allows for a large number of users over a given coverage area to connect to the Public Switched Telephone Network (PSTN). A great deal of the United States is now covered by cellular radio, and many law enforcement departments use cellular to supplement their radio communications systems.

The cellular system employs a number of coverage cells within a geographical area, as shown in figure 7-6. Each cell uses a trunked radio system to supply repeaters to users within the cell. Cells are connected to a Mobile Telephone Switching Office (MTSO) by trunked phone lines, fiberoptic cables, or microwave links. Cells can range from 30 miles down to 0.5 miles in diameter. When a cell reaches the maximum capacity of subscribers, it may be divided in two by adding new antennas and trunked radios and reducing power output to double the original capacity.

When a cellular telephone is turned on, it automatically registers with the local cellular carrier, and an indicator shows whether there is sufficient signal to connect to a cell. When a number is called, a dedicated radio control channel receives the information and sends it through the MTSO to the PSTN system to ring the called person's number. When the call is answered, the MTSO sets up a dedicated cell repeater for the subscriber to use for the conversation.

Figure 7-6. Cellular Radio System



During the time of the conversation, the cell phone signal strength is monitored at the cell where the conversation is taking place, as well as at adjacent cells. If the signal strength gets stronger in another cell, the MTSO requests that a new repeater in that cell take over the conversation. The "hand-off" is accomplished seamlessly within 1/5 of a second. When the conversation is completed and the subscriber hangs up, the MTSO returns the repeater channel for use in another phone call.

If a call is made from the PSTN to a cellular subscriber, a set of dedicated paging channels at all the cell sites calls the subscriber's number. When the subscriber's cell phone hears the page, the called subscriber answers the cell phone and the phone signals back through the control channel that the call has been answered. This triggers the MTSO to set up a repeater for the conversation. When the subscriber hangs up, the MTSO releases the channel for another call, as described above.

The original cellular system, called Advanced Mobile Phone System (AMPS), uses frequency modulated repeaters with 30 KHz of bandwidth in each direction for one conversation. To improve the spectrum efficiency, a frequency division multiplexing system allowing three 10 KHz channels in the 30 KHz bandwidth was developed called Narrowband Advanced Mobile Phone System (NAMPS). As the service developed over the years, several even more efficient technologies were developed using time division multiple access (TDMA) and code division multiple access (CDMA), which are discussed in the previous chapter.

Characteristics of cellular systems include:

1. A very large number of subscribers can be accommodated.

2. As the subscriber numbers in a cell reach the cell capacity, the cell may be divided to double its capacity.

3. By keeping the transmitter power low in each cell, transmitting frequencies may be repeated in nearby cells, thus increasing spectrum efficiency.

4. Cellular radio systems tend to be very reliable even under the worst environmental conditions.

5. With the various modulation schemes now being used, every cell phone does not work in every system. However, multimode phones have been developed to solve this problem.

Personal Communications Systems (PCS)

Because of the need for more frequencies for personal communications and the popularity and demand for cellular radio, the FCC reallocated several megahertz of frequencies in the 900 MHz range and a large portion of the 2 GHz band for PCS. These frequencies were auctioned off to the highest bidder by the FCC.

The 900 MHz spectrum is allocated into 50 KHz channels, some paired with other 50 KHz channels and some with 12.5 KHz channels.[7] These are being used for two-way paging, data transmission systems for carrying stock market and other information, and other uses conceived by the auction winners.

The 2 GHz band was auctioned off in much larger bandwidth segments, up to 30 MHz. (A small portion of the band was allocated for unlicensed operation to operate wireless PBX's and other in-building voice and data communications networks.) The broadband spectrum contains very few technical limitations for service offerings so that companies with unique communications schemes might make creative use of the spectrum. However, so far, most offerings made public appear to be for additional cellular radio systems.

Buildouts are proceeding initially in high-density population areas where licensees can get a quick payback, so many rural areas may have to wait for service. Because of the number of winners in various areas, there may be as many as six competitors in the densely populated areas.

Some seven different de facto technical approaches to these new cellular radio systems exist, so a telephone used in one system will not necessarily work with another. Some confusion also exists between the 800 MHz cellular services and the 2 GHz PCS cellular services because of advertising claims. Today, technologies used for cellular and PCS are basically the same and the offerings are very similar. However, PCS has the potential to provide other services in addition to cellular. People must wait and see as the technologies mature.

Cellular Digital Packet Data (CDPD)

Cellular Digital Packet Data, or as it's more commonly called, CDPD, consists of using cellular radio repeaters for the transmission of small bursts of data known as packets. The CDPD process allows the insertion of packets of data in between lightly modulated cellular radio voice channels without reducing cell phone voice capabilities. CDPD is an open transmission methodology for sending data on existing Advanced Mobile Phone Service (AMPS) cellular networks at a transmission rate of 19.2 kilobits per second. The need for sending digital packet data has increased over the years, so dedicated CDPD channels

[7] FCC *Rules and Regulations*, Section 24.129, Frequencies.

have been set up by some of the cellular providers. With the recent FCC decision to allow cellular carriers to drop AMPS analog service in 2005, CDPD may no longer be available after that time.

Law enforcement agencies have found that using laptop computers to obtain critical information in patrol cars without having to go through radio dispatchers improves their officers' efficiency, decreases the information delivery time, and reduces errors. Using CDPD to bypass a dispatcher, field officers may obtain information directly from local, state, or NCIC databases to check driver's license validity, existing warrants, and other information that may be of use to an officer in processing a suspect.

The option of using CDPD minimizes the capital outlay by a public safety agency, since it is only necessary to purchase the in-vehicle equipment (e.g., laptop computers with modems and software) rather than purchasing the entire radio communications network for data transmission support.

CDPD pricing is sometimes based on the number of bits transmitted, which is difficult to estimate for budgeting. Recognizing the fixed budget nature of public safety departments, many vendors now offer fixed monthly fee contracts.

The network architecture uses the protocol used in the Internet (i.e., Transmission Control Protocol/ Internet Protocol, or TCP/IP). Therefore, any standard personal computer modem that works with the Internet will operate with a CDPD system; however, special software must be used.

Public safety agencies wanting to use CDPD should check with cellular service providers in their region to see if they offer CDPD. Then they need to carefully check coverage to make sure that their operating area is adequately covered. Most cellular radio suppliers provide coverage diagrams for subscribers, and many are available instantly over the Internet. A major drawback to some CDPD systems is that the data system competes with the voice component of the system, and can often face severe delays during peak usage (such as commute times) when public safety may have its highest demand for service.

Point-To-Point Microwave Communications Systems

Often you need to connect telephone circuits from one terminal to another, voice and control circuits to repeaters and trunked systems, voting receiver inputs from satellite sites to a comparator, T1 (1.5 Mbps) or T3 (45 Mbps) data circuits, and other communications circuits from one point to another point. Generally, these needs may be fulfilled economically and reliably by leasing wire or fiber-optic circuits from the local telephone or cable company.

When a telephone company expands capacity, it usually overbuilds to allow for future customers. If the circuits exist, leasing payments involve only operational and maintenance costs. However, if the circuits do not exist, you must pay the up-front capital costs involved in constructing the new facilities.

The economies of building a private microwave system usually are in your favor when it is necessary to provide service to an area that would require new facility construction by the telephone company.

The microwave bands include frequencies generally above 960 MHz, or approximately 1 GHz. (Frequency bands used for commercial purposes are in the 960 MHz and 2, 4, 6, 11, 18, and 23 GHz areas.) The 960 MHz band can be used to transmit up to 15 narrowband voice or data channels; the other frequency bands have considerably wider bandwidths to accommodate many more voice and data channels. Microwave systems may be either analog or digital radio systems.

Microwave propagation is considered “line of sight” (LOS), so transmissions must be repeated at approximately 25-mile increments in bands up to12 GHz. In mountain areas, the spacing may be as great as 60 miles. Above 10 GHz, rain attenuation usually causes a distance limitation, so repeaters must be more closely spaced depending upon the amount of rain in different parts of the country.

Microwave System Engineering and Licensing

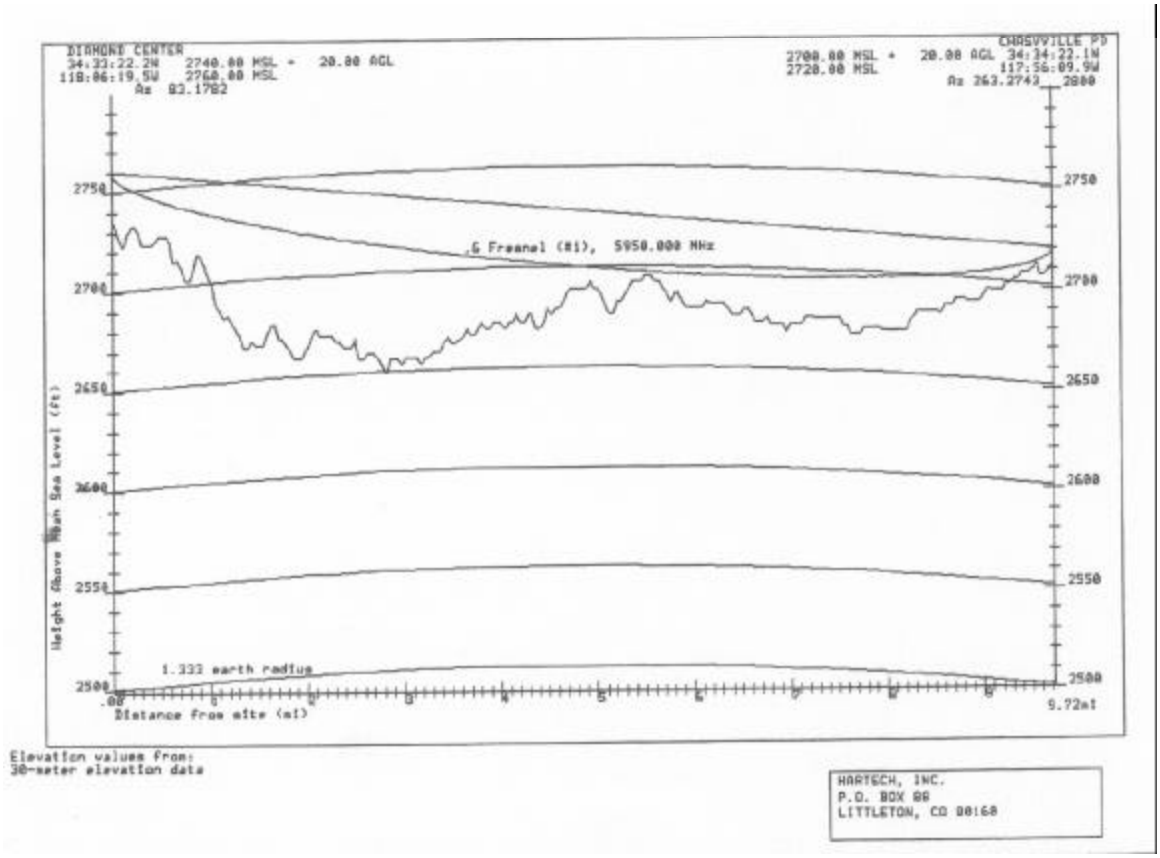
A typical microwave system requires several engineering criteria to be met. The first is that the path between two microwave terminals must be free of obstacles which might impair the wave front as it travels between terminals. The second requirement is the signal strength must be high enough to meet either the signal to noise ratio requirements (for an analog radio system) or the bit error rate requirements (for a digital radio system) for a maximum allowable path outage time. The last condition is the path must be free from either causing interference to another microwave communications user or receiving interference from another user. A typical path profile to meet the first condition is shown as figure 7-7.

Most microwave communications systems require FCC licensing under Part 101 of the FCC Rules and Regulations. Frequency coordination is required and the applicant must utilize the FCC's Universal Licensing System (ULS) at the FCC website (see resources in appendix B) for all applications. There is a class of microwave systems not requiring licensing by the Commission under Part 15 of the rules.

Most unlicensed systems use spread spectrum modulation which spreads the power over a large bandwidth. The unlicensed systems must still meet the above engineering requirements excepting there is no interference protection available.

Additional information regarding licensing is given in chapter 8.

Figure 7-7. Sample Microwave Path Profile



Wireless Local Area Networks (WLAN)

Wireless LAN technologies are rapidly becoming integrated into public safety wireless infrastructures in North America and Europe. Carrying data at speeds up to 54 megabits/second, these inexpensive off-the-shelf technologies offer interesting capabilities when properly incorporated into the wireless environment. Because these technologies operate at frequencies above 2 GHz, they typically provide very short range communications (100 to 500 feet). Thus, coverage is characterized by operational "hot spots" with a radius of several hundred feet rather than seamless coverage across a wide area. The central "base station" serving a hot spot is called a wireless access point or WAP, an off-the-shelf device costing $100-200. WAPs typically connect to a wired network via a standard connection such as 10- or 100-baseT. Field terminals are typically linked to the WAP with a simple wireless card that plugs into a PCMCIA slot.

The technology, often called 802.11 after the designation assigned to this class of standards by the Institute of Electrical & Electronic Engineers (IEEE) who developed the standards, is an alphabet soup of protocols (a, b, e, f, g, h, i and 1x), as indicated in table 7-1.

Table 7-1. IEEE 802.11 Protocols and Standards				
Protocol	**Band**	**Data Rate or Description**	**Physical Network**	**Standard Completed?**
a	5 Ghz	6 to 54 Mbps	Yes	Yes
b	2.4 Ghz	1 to 11 Mbps	Yes	Yes
e[1]	All	Quality of service standard	No	No
f[2]	All	Inter-access point interoperability	No	Yes
g	2.4 Ghz	Up to 24 Mbps	Yes	No
h[3]	All	Dynamic frequency and power control	No	No
i[4]	All	Enhanced hotspot security standard	No	No
lx	All	Network authentication protocol standard	No	Yes

[1] Without strong quality of service (QoS) assurance, the existing version of the 802.11 standard doesn't optimize the transmission of voice and video. 802.11e will improve QoS for better support of audio and video applications. It will apply to all 802.11 wireless LANs and should be implemented as a simple software upgrade to existing products.

[2] The existing 802.11 standard doesn't specify the communications between access points in order to support users roaming from one access point to another. The problem, however, is that access points from different vendors may not interoperate when supporting roaming. 802.11f is currently working on specifying an inter-access point protocol that provides the necessary information that access points need to exchange to support the 802.11 distribution system functions (e.g., roaming). In the absence of 802.11f, you should utilize the same vendor for access points to ensure interoperability for roaming users. In some cases a mix of access point vendors will still work, especially if the access points are Wi-Fi-certified. The inclusion of 802.11f in access point design will eventually open up your options and add some interoperability assurance when selecting access point vendors.

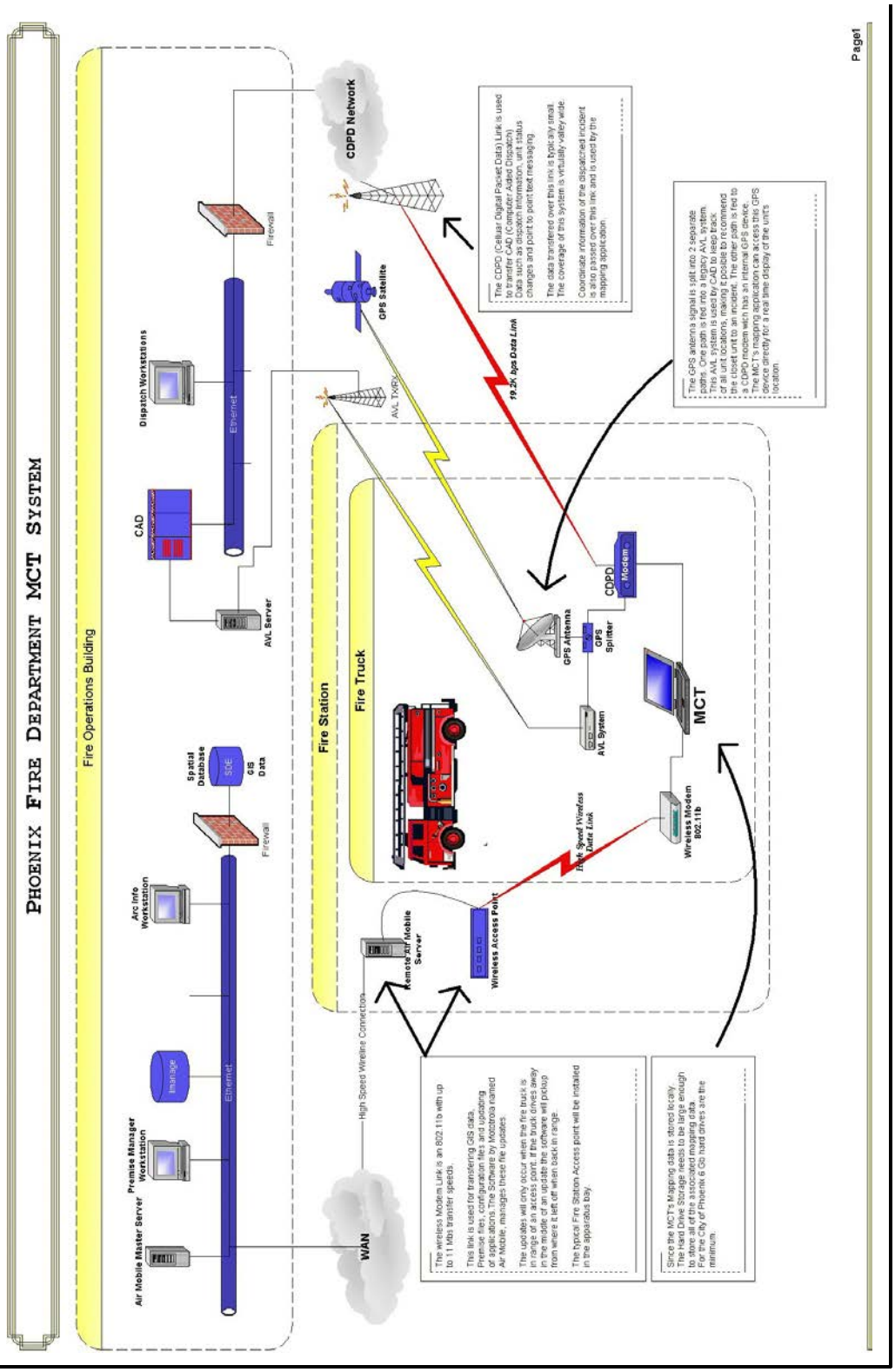
[3] 802.11h is being developed for the European market.

[4] 802.11i is actively defining enhancements to counter the issues related to wired equivalent privacy (WEP), making your wireless network as secure as your wired network. The existing 802.11 standard specifies the use of relatively weak encryption keys without any form of key distribution management. This makes it possible for hackers to access and decipher WEP-encrypted data on your WLAN. 802.11i will incorporate 802.1x and stronger encryption techniques, such as the Advanced Encryption Standard (AES). It should be possible to upgrade existing access points with software upgrades. The implementation of AES, however, may require new hardware.

802.11b Networks

The most common network now being implemented is 802.11b. These networks are being installed by both the public and private sectors, including many private businesses and residences. Using a series of WAPs around an agency's service area tied back to its wired backbone, it is possible to rapidly transmit large amounts of non-time critical information (such as reports) back to a central point, or to distribute information (such as bulletins and photos) out to field units. By placing WAPs at locations where mobile terminals often congregate, such as headquarters, precinct houses, fire stations, hospitals, public buildings or near major travel routes, specialized software applications that detect connectivity to the WLAN will automatically transfer waiting data when in range of the system.

Figure 7-8. Phoenix, Arizona, Fire Department Mobile Computer Terminal System Using WLAN



The left side of figure 7-8 depicts the system used by the Phoenix, Arizona, Fire Department to link its mobile fire apparatus to its wired data network using 802.11b. WAPs are located at fire stations, the training academy and the service shop. Information that is automatically and routinely updated includes maps, hazard and inspection information, aerial photographs, and general information files. The system is also capable of automatically updating software applications on the mobile terminals.

In standalone applications, a mobile-mounted WAP can be used to link video cameras, terminals and other data-intensive applications from a command post vehicle at the scene of a major incident to each other and (via other wired or wireless links) back to a central system. Command post vehicles such as the InfraLynx provided by the US Department of Justice with its Prepositioned Equipment Pods for response to weapons of mass destruction incidents provide the capability to link real-time data and video applications to local and/or remote applications (see figure 7-9).

Figure 7-9. InfraLynx Mobile Command Post

Wireless Local Links - Bluetooth

Electronic devices interconnect to each other in a variety of ways. Computers have a CPU, keyboard, monitor and mouse that all connect with different cables. Your TV set, VCR, and cable box all interconnect with cables, while each generally has its own wireless remote control unit. Your personal MP3 player connects to a pair of headphones with a wire lanyard. Each of the various pieces and parts of these systems makes up a community of electronic devices that communicate with each other using an assortment of cables, infrared beams and radio waves, and a more complex set of connectors and protocols.

Suppose there was a way for all of these devices to intercommunicate with each other without wires and without the necessity for human intervention. This is the concept known as Bluetooth. More than 1000 electronic equipment manufacturers worldwide have jointly developed a specification for a very small radio

module that fits into many kinds of electronic components. These include cell phones, computers, headphones, keyboards, PDAs and a multitude of similar devices.

Bluetooth operates at two levels. At the basic physical level, it is a radio frequency standard operating at 2.45 GHz. It is also a link-level standard that defines how and when data bits are sent, what each means, and how all involved devices assure that what is being sent by one device is the desired message received by the other device(s). It is a technology that is designed to operate without human intervention once a device is turned on in the presence of other devices with which it is designed to communicate. By its very nature, it is designed to be very short range. The transmitter power limit of 1 milliwatt limits the range of Bluetooth technologies to about 30 feet between devices.
When Bluetooth-enabled devices come within range of each other, a wireless communication automatically takes place during which it is determined if the devices have data to share, and/or if one needs to control the other. Each device has an address assigned from a group of addresses reserved for each class of devices. When one Bluetooth device detects another, this address range is searched to see if the new device is a companion device.

☞ Did you know?

Bluetooth is named after Harald Baatand II, King of Denmark. Harald - nicknamed Bluetooth - is famous for uniting Denmark and parts of Norway into a single kingdom at the end of the last millennium and for bringing Christianity to Denmark. His name was chosen for the standard to show the importance of the Scandinavian countries (Denmark, Finland, Norway and Sweden) in the International telecommunications industry, and to signify the intent of the Bluetooth Consortium to unify wireless connectivity.

If there is a need to communicate, the devices form a personal area network (PAN, or piconet) that could fill a room (for a computer or stereo system), or simply link an MP3 player on the belt to a set of headphones being worn by the user. Different piconets establish their own random frequency hopping algorithm, limiting interference between devices within range of each other. Communications speeds vary from 57 kbps in one direction and 721 kbps in the other, to a bi-directional speed of 432.6 kbps.

With such a wide range of Bluetooth devices, interference is an important consideration. Bluetooth uses spread-spectrum frequency hopping across 79 random frequencies within a specified range at a rate of 1600 frequency changes per second. Thus, it is rare that two incompatible devices within range of each other would occupy the same frequency at the same time. Since the 2.45 GHz band is shared with non-Bluetooth devices, frequency hopping tends to limit the interference from these other devices. However, Bluetooth shares this radio band with a number of other industrial, scientific and manufacturing devices (including 802.11b and microwave ovens), a number of which may cause interference to Bluetooth devices. It is thus critical that public safety users carefully evaluate the environment where Bluetooth might be used. Bluetooth is especially not recommended for mission critical applications in a mobile environment because of the difficulty in isolating this technology from potential sources of interference.

Bluetooth technology offers the ability to move many public safety devices using several distinct components from the wired to the wireless environment. From headphones and keyboards to cameras and PDAs, Bluetooth technology is slowly entering the public safety marketplace, providing added freedom of movement to agency personnel.

Study 6: Current Public Safety Systems (Continued)

Reference Material: COPS Interoperability Tech Guide, Chapter 16, Pages 259-282 and Chapter 17

Trunked System Policies
The complexity and configurability of trunked systems **require** great care in implementation and ongoing management. Design such complex systems through careful needs analysis (Chapter 6), implement them using functional acceptance tests mapped to user requirements (Chapter 10), and manage their flexibility through strict adherence to both technical and operational policies and procedures (Chapter 12).

Second, all this power comes at the cost of greater complexity and potential for failure. While modern system design calls for "fail-soft" systems that still operate in a degraded mode as components fail or become unavailable, trunking still ultimately depends on fixed infrastructure to work. The final fail-soft mode for trunked radio systems is to operate conventionally—that is, with radios talking directly on predesignated frequencies chosen for specific purposes.

Communications in Buildings and Tunnels

Emergency responders face great coverage challenges in both urban and rural areas. Where the challenge in mountainous terrain is overcoming natural obstacles, radio systems in more populous areas are equally challenged to overcome manmade mountains, canyons, and caves. Since the earliest days of radio, engineers have looked for ways to provide communications in buildings and tunnels.

Radio system coverage in buildings and tunnels requires additional infrastructure.

Fixed, point-to-point communications in such environments are relatively straightforward. On the other hand, communications with field units—whether vehicular-mounted mobile radios or personally-carried portables—is the biggest challenge. Portable radio communications are most difficult to accommodate, of course, because of their relatively low output power and limited antennas. Portable communications are further handicapped by how they are generally used, being worn in close proximity to the body, which serves a lot better as a signal absorber than reflector. Recognize that portable and mobile uses are similarly affected by coverage challenges, only to different degrees.

SAFECOM LIBRARY: TRUNKED SYSTEM RESOURCES

Several useful reports on trunked radio can be found on the SAFECOM web site, including these:

Comparisons of Conventional and Trunked Systems (1999):

http://www.safecomprogram.gov/SAFECOM/library/technology/1179_conventionaland.htm

Operational Best Practices for Managing Trunked Land Mobile Radio Systems (2003):

http://www.safecomprogram.gov/SAFECOM/library/systems/1049_OperationalBest.htm

How 2 Guide for Establishing and Managing Talkgroups:

http://www.safecomprogram.gov/SAFECOM/library/systems/1047_HowTo.htm

■ Area Solutions

The most basic technique used to improve communications in buildings and tunnels is to put additional system sites in denser urban areas. This increases the fixed station (base or repeater) signal into nearby buildings and provides it a somewhat stronger signal from the field unit. Because the greatest weakness is usually the fixed station's ability to "hear" the portable transmission, a more advanced technique is not to add entire fixed stations (transmitters *and* receivers), but more receivers strategically placed. This allows the relatively weak portable signal to "get into the system" from more places.

While basic, this approach can be satisfactory in some locales and reduce requirements for specialized technology and the additional expense of in-building systems. System managers face an ongoing challenge in assuring that new construction in and around the areas of interest doesn't reduce coverage or otherwise interfere with the balance achieved.

■ Point Solutions

More and more often, peripheral technology is being used. This requires placement of special repeating equipment within buildings, tunnels, and other signal-challenged areas.

Bi-directional Amplifiers (BDA) are placed within the building to, as the name implies, improve signals both inbound and outbound. Internal and external antennas are linked by the BDA to capture weaker signals from within and retransmit them beyond, and vice versa. Large structures may require a more elaborate, distributed system of internal coverage antennas connected together, then linked to the outside world through a single "donor" antenna.

Some areas, such as tunnels, are well suited to use of a special type of distributed antenna system built from radiating coaxial cable. Traditionally, coaxial cable (coax) of various forms is used to connect radios to their antennas. Properly speaking, the cable is part of the antenna system, but is intended to quietly move signals from each end to the other.

Radiating cable, on the other hand, is constructed to "leak" signals in and out along its length. This can be a very effective sort of distributed antenna, although, as might be expected, some careful engineering is needed for systems of this sort. Figure 16-8 shows an example of a BDA.

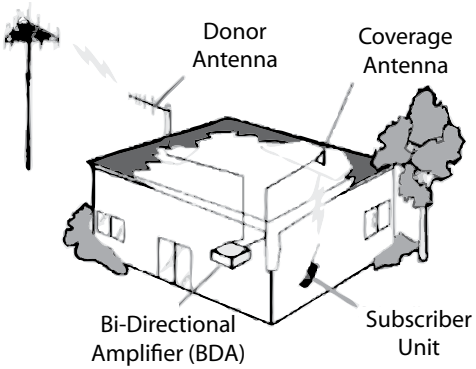


Figure 16-8: Bi-Directional Amplifier Example

Source: PSWN, November 2002

■ Governmental Regulation of In-building Coverage

There has been increasing interest post-9/11 in local ordinances requiring building and structure owners to assure public safety radio coverage inside. While the need for coverage improvements is indisputable, systems are sufficiently specialized that they don't promise to improve communications interoperability outside of the improved coverage of a single, targeted system. In other words, they don't broadly improve interoperability.

A 2002 report by PSWN on the topic concluded that such ordinances "have no noticeable impact on interoperability between public safety organizations."[59]

Satellite Communications

Recent natural disasters have brought increased interest in satellite communications to overcome the damaged and destroyed land-based radio systems. Hurricane Katrina, which ravaged the United States Gulf Coast late in August 2005, widely disrupted radio systems. Not only was cellular telephone infrastructure damaged and nonexistent in many places, but public safety radio systems were disabled in many locations (Figure 16-9). Whenever basic agency radio systems are damaged, interagency communications suffer.

[59] *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report*, Public Safety Wireless Network Program, November 2002, p. 14. See **http://www.safecomprogram.gov/SAFECOM/library/technology/1032_PublicSafety.htm**.

Figure 16-9: Plaquemines Parish (Louisiana) Radio Tower – August 29, 2005

Source: Plaquemines Parish web site, **http://www.plaqueminesparish.com**

Satellites provide a backup means of communicating, particularly when terrestrial infrastructure is nonexistent. They are regularly used in wildland fire and other disasters, both to provide telephone services and data communications. In a traditional or newly created wilderness, satellite communications may be the only way to talk out from an incident scene.

Satellite services are available from a variety of vendors. Some are provided by way of *geosynchronous* satellites that appear to the user to be fixed at a spot in the sky. At an altitude of 22,241 miles, such satellites orbit at the same rate the earth rotates. Similar to direct broadcast satellite (DBS) television, these services require a fixed antenna that is pointed at the satellite or one that is electronically steered to keep itself so.

Other services are provided through low earth orbit (LEO) or medium earth orbit (MEO) satellites that are relatively much closer, though still far distant compared to cellular and terrestrial public safety radio infrastructure. LEO satellites orbit in a band from a few to several hundred miles above the earth. This distance still challenges the portable communications needs of first responders.

Despite their value for disaster telephone and data services, satellites are not a complete replacement for terrestrial voice radio systems used by public safety for several reasons:

- **One-to-many communications are inadequate**. Voice communications as most commonly used via space is limited to telephone-like services where a user can dial up another telephone user—whether on the public switched telephone network or elsewhere on a satellite system. Satellites do not offer the immediate, one-to-many sort of radio conversations needed by public safety responders.
- **Coverage is inadequate**. First responders moving about with portable radios need coverage in all areas. Less penetrating than even cellular telephone signals, satellite signals don't reach far inside buildings or into dense vegetation. Public safety radio systems are engineered to provide coverage far beyond what satellite systems provide.
- **Portable capabilities are inadequate**. Even LEO satellites are many times farther away in distance than traditional land mobile radio infrastructure. Since both use radio frequencies to communicate, satellite signals are reduced in strength even more across the distance, requiring bulkier antennas and higher power. Even with adaptive power modes that reduce battery demand, satellite handsets require more battery power than a responder's standard portable radio transmitting a much shorter distance. The demanding emergency response environment leads to greater power consumption as users move in and out of clear view of the sky.
- **Capacity is inadequate**. Communications between emergency responders on scene during events is frequent. Many channels are needed for larger events, such as those that would take out terrestrial infrastructure, and near-instantaneous communications is needed in most cases. A single responder often needs to communicate instantly with dozens of others. Satellites don't provide this ad hoc broadcast capability.

Satellite communications are vital in response to disaster. Their primary value is as a replacement for cellular and other terrestrial telephone systems. In times of disaster, there may be no alternative. Running a close second in value, data communications via satellite are indispensable from any location out of range of terrestrial wireless systems due to distance or events.

VoIP in Voice Systems

A bright star on the communications horizon is Voice over Internet Protocol or VoIP. Most simply, it is the semistandardized means of taking voice or other audio that has been digitized, then pushing it over networks similar to any other form of data. Internet Protocol (IP) is part of the suite of standards that powers—imagine this—the Internet and most other data networks today.

We refer to VoIP as "semistandardized" because there are limitless ways to move digitized voice over IP-based data networks. It's not as simple as just throwing voice data packets on the wire and reassembling them at the end. The process is much more complex and requires more communications between sending and receiving systems than just the voice data. Different means are used by different vendors and for different purposes to control the "envelope" of what we would consider a conversation that is stuffed with voice bits and bytes.

■ Basics of Digital Audio

Digitized audio has been passed over backbone telecommunications circuits for years. VoIP differs in that the audio (voice or otherwise) is passed over modern data networks that can route and reroute packets across a variety of intermediate networks. They can, and do, pass over networks used for other data purposes. There are tradeoffs, though.

Voice communications is much more time-sensitive than data communications. Network delays that would be unnoticed by the typical data user become noticeable and even intolerable when the user is trying to carry on a two-way conversation. Most cellular and many other telephone systems today exhibit such delays and we all are becoming increasingly familiar with how it affects normal conversation.

This isn't an effect of VoIP, per se, but rather of digital networks being slowed due to demand or disruptions. IP-based networks traditionally used for data will dynamically adapt to such factors and are designed to trade speed for certainty of delivery. That is, the network will try and try again to get a packet that has been lost or damaged so it can package them reliably and deliver the complete lot at once.

Voice communications, on the other hand, can survive an occasional dropped packet better than it can handle delays. Each packet contains a small piece of audio information. The human brain is remarkably able to extract an intelligible message from disrupted audio.

■ VoIP in Public Safety Communications

Public use of VoIP telephone systems has brought all sorts of challenges to the public safety world, particularly in delivery of 9-1-1 services. However, it has proven to be a boon in other ways.

Transmission of voice and other audio over IP-based data networks has rapidly become a critical, underlying means of connecting agencies for interoperability. VoIP is used to interconnect private telephone systems, dispatcher consoles, and parts of the radio infrastructure. For practical purposes, it is an underlying protocol rather than an end-user application, though.

For example, dispatch consoles have been connected for decades to remote base stations through dedicated telephone circuits—typically analog ones much like plain old telephone service (POTS—seriously). As telecommunications infrastructure has moved to digital from analog, lines that tie one fixed point with another have also migrated. VoIP is increasingly used in this case to move the dispatcher's voice to the radio transmitter and the user's voice back from the receiver.

■ A Fundamental Tool

VoIP is a fundamental tool, but not a silver bullet.

VoIP is growing as a fundamental tool connecting pieces of public safety communications systems. Unfortunately, it has been subject to a lot of interoperability hype. While it may today and in the future be an underlying protocol for connecting systems at an audio level, it doesn't solve the problems posed by any gateway between disparate radio systems, as described further in the next section, **Approaches to Interoperability**.

VoIP is the current, logical choice for connecting pieces of a system where dedicated telephone circuits may have been used in the past. As any higher level communications protocol, it relies on underlying network infrastructure to carry data. VoIP offers the possibility of passing voice over networks used for other data communications, but in the process naturally puts those packets in contention with other traffic on the network.

Critical systems need dedicated network services.

The state of the art in VoIP telephone systems is to use dedicated data networks—physical or virtual—to reduce that contention and assure acceptable service. Critical public safety systems need high-quality service, as well.[60]

■ "Radio over IP"

The term "radio over IP" has been used to describe VoIP used in radio applications. It's a confusing term and one we advise against using. It's the logical equivalent of "Air over Esperanto."

Without getting deep into theory,[61] data being transmitted using Internet Protocol can pass over many different physical mediums, both wired and wireless. Voice, as

---

[60] Several years ago, the Public Safety Wireless Network Program released an assessment of VoIP for public safety radio systems. See *Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology*, December 2001, **http://www.safecomprogram.gov/SAFECOM/library/technology/1171_softwareenabledwireless.htm**.

[61] The Open Systems Interconnection (OSI) model is fundamental in telecommunications theory, having originated in 1977. It describes systems in terms of a layered stack and defines interoperability between layers. Radio is a low, physical layer, while Internet Protocol is in the middle. Voice as an application of a system would be at the top of the model. For further information, see **http://en.wikipedia.org/wiki/Open_Systems_Interconnect. htm**.

an application, runs over IP and other protocols, then over one or more mediums en route to one or more final destinations. "Radio over IP" is backwards.

In addition, modern radio systems use VoIP to move voice and other audio, such as signaling tones, across their infrastructure. They don't, however, use it over the airwaves. Land mobile radio systems reassemble the voice packets and transmit them over the air using the system's fundamental operating mode—whether analog or digital, as in P25. This is analogous to what a receiver does with digital music before it sends it to its speakers in a classic stereo system.

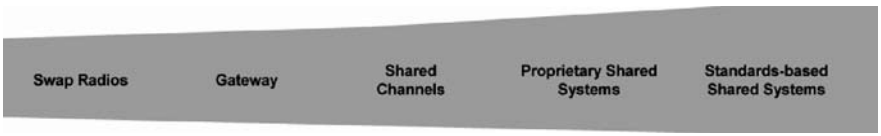
VoIP is a fundamental tool in today's telecommunications systems, but it's not a silver bullet.

Let's move on to how these technologies are used in pursuit of interoperability.

Approaches to Interoperability

Communications interoperability has been hindered in the past due to the simple lack of a common vocabulary for discussing the topic. SAFECOM's *Interoperability Continuum* has improved the situation greatly through practitioners' definition of five critical dimensions of interoperability. It also provides simple measures for assessing relative stages of development. Of the five dimensions, technology in particular is the subject of only one. Proportionally, this continuum effectively represents the fact that the great majority of work in achieving interoperability is in the *human* aspects of governance, procedures, training, and familiarity through frequent use.[62]

The *Interoperability Continuum* provides a simple, effective description of the technology choices available to provide interagency voice communications. These means of communications provide a convenient way of examining the range of choices, sophistication, and completeness of voice radio technology. As in the *Interoperability Continuum*, technology choices are listed below in order of increasing capabilities.



Let's take a look at these approaches individually.

[62] SAFECOM's *Interoperability Continuum* is included in this Guide as Appendix G.

Swapping radios or maintaining a cache of standby radios is an age-old solution that provides results but is often time-consuming, management-intensive, expensive, and may only provide limited results due to channel availability.

—SAFECOM *Interoperability Continuum*

Technology Approach: Swap Radios

As noted in the SAFECOM description, agencies have swapped radios to enable communications among themselves since the earliest days of public safety radio usage. To this day, agencies exchange spare radios with key cooperators on incident scenes for the sake of interoperability. In some cases, they do so even though their respective systems are otherwise technologically compatible. For example, this may occur because the users either don't have common channels programmed into their radios or they use different channel naming and naming conventions. Whether due to technological incompatibilities or a lack of prior planning, the end result is the same: A conclusion that this, the most basic means of interoperability, is necessary.

During incidents when agencies respond with incompatible equipment—using different frequency bands, for example—swapping radios provides responders with the ability to talk to the other agency via that other agency's system. Obviously, while this can and does work for very simple operations, it becomes unworkable as more and more agencies arrive.

A common use of this technique is in deployment of radio caches. A *radio cache* is simply a supply of radios, typically portables, held aside for larger incidents. The cache may include spare batteries, antennas, and carrying cases to simplify deployment. Typically, the cache is left stored away until a request is made for its deployment.

The use of radio caches is, unfortunately, fraught with pitfalls. Common troubles include the following:

- Unknown or nonexistent procedures for request and deployment
- Inadequate maintenance of the equipment, particularly batteries that can be damaged from both too little and too much charging
- Poorly documented channel programming, leading to inadequate usage
- Lack of training on the equipment, its available channels, and their appropriate use.

By far the majority of multiagency emergencies handled day-to-day in this country arise and are handled much too rapidly for caches of radios to be deployed. On the other hand, large-scale emergencies often call for the use of cached radios to allow multiple responding agencies use of a single system.

Two examples of cached radio equipment are notable in this approach to communications interoperability.

■ National Interagency Incident Communications Division

During the seemingly annual natural disasters that plague the American West, the National Interagency Fire Center (NIFC) in Boise, Idaho provides logistical support to federal, state, and local agencies. A prime resource is radio equipment from its communications cache.

The NIICD radio cache is jointly maintained by the U.S. Departments of Agriculture and the Interior.

NIFC's National Interagency Incident Communications Division (NIICD),[63] operated jointly by agencies of the U.S. Departments of Agriculture and the Interior, provides equipment in response to natural and manmade disasters of all sorts. Its cache was heavily tapped for equipment and trained ICS Communications Unit personnel in response to the Gulf Coast following Hurricanes Katrina and Rita.

NIICD cache equipment is used for standalone communications networks where needed to support large-scale emergency response, typically involving many agencies.

■ Beltway Sniper Incidents

Montgomery County (MD) had a supply of new, unused radios that was pressed into interagency service.

During a 3-week period in October 2002 two men terrorized the Washington, D.C., area through seemingly random sniping incidents that left 10 people dead. Each of the incidents brought local first responder agencies together, but more broadly, law enforcement agencies from across the region and all levels of government convened in pursuit of the attackers.

Montgomery County, Maryland was the location of the earliest and majority of the attacks. By coincidence, the county happened to be in the middle of deploying a new radio system for its public safety agencies. System infrastructure was largely in place and end-user equipment was warehoused for pending installation.

When joint task force operations involving many law enforcement agencies ensued, the new radio system was activated and the new radios distributed to provide interagency communications. In effect, cached equipment was used to provide a common communications environment, much as is done in the West during remote wildfires. Outside agencies used their own communications capabilities as well as they could considering varying coverage limitations, but the distribution of Montgomery County radios to cooperating responders and investigators provided simple, but much needed communications interoperability.

[63] For more information on the NIICD, see **http://www.fs.fed.us/fire/niicd/**.

Technology Approach: Gateways

Response to the Beltway sniper incidents involved another approach to interoperability: Connecting different systems or channels through a *gateway*. In order to provide communications between users of its old and new systems during the unanticipated activation, Montgomery County linked channels together across the two. The effect was to provide a common channel shared across each.

The term "gateway" is used for any of a number of means of patching transmitted and received audio from one source to another. Technically, it is a bit more complex, requiring controlling circuitry to initiate transmission on one side of the equation when something is received on the other. Whether involving radio channels, telephone calls, or another source of audio, channel patching is another age-old approach to connecting users from one system to those on another.

In its earliest form and still practiced today, a dispatcher at a communications console can literally patch the audio from one channel to another despite the fact that there might be huge technological differences between the individual systems. This is the same approach, technically speaking, that a dispatcher would use to patch a telephone call to a radio channel and vice versa. The effect is that the two communications channels are collapsed into one using bridges or gateways between different telecommunications systems.

Modern technology has made it possible to do this not only in increasingly complex ways from the dispatch console, but also via remotely operated gateways. The simplest gateway devices are no larger than a pack of cigarettes, limited in size physically more by the space needed for connecting cables than by the complexity of their internal electronics. This sort of portability allows for devices that can be fielded to patch together first responder channels. Though most commonly used to bridge radio channels in different frequency bands, many of the devices can also be used to link "push-to-talk" radios[64] to other two-way audio sources, such as landline, cellular, and satellite telephones.

Increasingly sophisticated networking technology allows gateways to be connected between dispatch consoles and other audio sources across data networks. Audio is digitized, addressed, and routed across networks just like any other form of data.

Gateways patch transmitted and received audio from one source to another.

[64] "Push-to-talk" radios are the standard type of radios used by public safety agencies. Whether portable, mobile, or installed at a fixed location, they're distinguished from other forms of radios by the fact that some sort of switch is manually or electronically actuated to initiate transmissions from the radio. The term "push-to-talk" has been used to distinguish the familiar two-way radio from other types of portable communications devices, such as cellular telephones.

VoIP is being used to connect systems across data networks using gateways.

As mentioned previously, Voice over Internet Protocol (VoIP) can be used for moving audio across data networks between radio systems. Those networks can even connect a gateway on one radio system to another that is geographically distant, providing radio end-users at either location with a means to talk to each other. This isn't 21st century James Bond wizardry, though. Amateur radio operators have been using the technology since the late 1990s and now have a worldwide network of more than a thousand Internet-connected radio nodes serving every continent, including Antarctica.

Whether as simple as a dispatcher's console patch or as complex as a worldwide VoIP network, gateways are widely used to connect distant and disparate channels of communications. While commonly used, this approach to interoperability has serious limitations and brings challenges of its own.

■ Gateway Issue: Capacity

By design, gateway devices linking together multiple channels of communications—radio or otherwise—end up repeating traffic from one channel to others. This reduces the original load-bearing capacity of each.

When two actively used channels are linked, the amount of traffic on each will increase significantly. Popular gateway devices allow many more than two channels to be linked, potentially multiplying the amount of traffic on each by the number of connected channels.

Obviously, any moderately used channel can be heavily taxed by patching together other, similarly used channels. This can result in serious contention for access to the channels, not to mention an increased level of traffic that may not be relevant to the original channel users.

Separate channels of communications are necessary during emergency response in order to segment responsibilities and account for the limited capacity of any individual channel. Indiscriminately used, gateway devices can disable the channels they interconnect by overwhelming them, literally or practically, with too much traffic.

■ Gateway Issue: Coverage

It might not be intuitively obvious, but gateways can only link first responders at an incident scene in areas of overlapping coverage between the linked systems. In other words, once outside the range of one's home system, the system user doesn't benefit by the gateway. The gateway doesn't extend the geographic range of the individual systems that are interconnected.

TMI: HOW MUCH DO YOU WANT TO COMMUNICATE?

In the wide world of communications, the term "signal-to-noise ratio" is used in talking about the eventual *intelligibility* of exchanges. The principle is that a signal has to be significantly stronger than any background noise for effective communications to occur. Anyone who has ever observed the volume level of conversation rise at a party as attendees increasingly struggle to be heard over one another has witnessed how the signal (conversation) can be lost amid background noise.

Back in the field, first responders often struggle to catch transmissions relevant to their jobs during incidents as radio transmissions multiply many times over. The challenge of too much information, of the signal being lost among "noise," is equally as disabling as not getting enough information.

Conversely, and somewhat perversely, linked systems can lead to too much, yet inadequate, coverage. For example, linking together Systems A, B, and C depicted in Figure 16-10 means that users of System C will be heard across the range of all systems, but still can't talk to any other system user when traveling outside of the range of their own. This can and does lead to systems interfering with others beyond their normal coverage areas. More critically, it also leads to communications failures in areas where responders were previously heard, but can't talk from once they get there.

Gateways can easily lead to *asymmetrical* radio coverage.

Radio coverage is a complex issue under the best of circumstances. It becomes even more so when multiple systems are linked together. Coverage becomes *asymmetrical*. That is, radio users can be heard in places where they can't talk from. Again referring to Figure 16-10, System A users can talk to users of both Systems B and C—as long as they are within the coverage footprint of System A. Once outside of it, they can't speak to anyone through the gateway *even though they are in the range of the other, linked systems.*

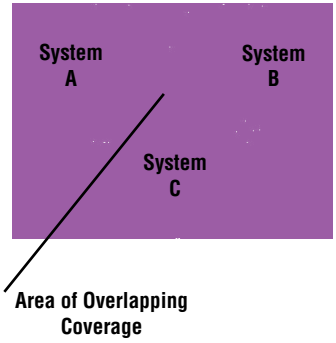


Figure 16-10: Overlapping Coverage of Systems

■ Gateway Issue: Transmitter Licensing

If the above technical complexities of gateways aren't daunting enough, their legal operation poses additional challenges. Unfortunately, a proliferation of gateway devices in recent years has led to some being used in operations outside the authority granted by the FCC for the respective interconnected systems. This is a rather obtuse and occasionally confusing subject, but we'll try our best to explain it here and provide reference to other sources.

Most transmitters are licensed for a limited area of operations.

Basically, FCC licenses are required for practically all radio transmitters used in public safety communications systems. Each portable, mobile, and fixed station radio is covered under a license that specifies, among other things, an area of operation—the area in which the radio can transmit. Most classes of fixed stations, such as base stations and repeaters, are licensed for a particular physical location, height above ground, and maximum power. Typically, end-user radios are licensed for operations only across the agency's jurisdiction or within a given distance from a fixed point.

Mutual aid and other types of interagency operations are often conducted outside of one or another agency's jurisdiction—by definition. While the visiting agency's radio system may provide incidental coverage outside its jurisdiction, it is illegal for end users to use any system outside of its licensed area of operation. This is done to protect other legitimate use of the licensed radio frequencies and to allow reuse of spectrum elsewhere.

When gateways are used to interconnect systems, the potential arises for radios to be operated outside their licensed area of operation. In addition, a portable or mobile radio connected to a gateway becomes a different class of radio station. In essence, it's no longer legally an end-user radio, but rather a type of fixed station. While the FCC can grant "Special Temporary Authority"[65] under emergency circumstances to operate an unlicensed transmitter, nothing beats preplanning and licensing.

The FCC-certified public safety frequency coordinators[66] are the best source of guidance in navigating the complexities of licensing transmitters used to interconnect radio systems through gateways.

FCC rules and regulations governing public safety radio systems (Part 90 – Private Land Mobile Radio Services) provide latitude for alternate use of licensed radio stations during emergencies that have disrupted communications facilities.

FCC Rules and Regulations
47 C.F.R. §90.407 Emergency Communications
The licensee of any station authorized under this part may, during a period of emergency in which the normal communication facilities are disrupted as a result of hurricane, flood, earthquake or similar disaster, utilize such station for emergency communications in a manner other than that specified in the station authorization or in the rules and regulations governing the operation of such stations. The Commission may at any time order the discontinuance of such special use of the authorized facilities.

■ Gateway Issue: The "Ping Pong" Effect and Other Complexities

Despite the relative simplicity with which gateways can be deployed to connect responders, they can have a negative impact on systems they interconnect. The National Institute of Justice (NIJ) CommTech Program[67] has worked for several years testing gateway devices and sharing lessons they have learned. Much of what we know about their use in the public safety environment comes from NIJ testing.

One technical complexity that has been described is referred to as the "ping pong" effect. It occurs when a gateway is used to connect users through two or more repeaters—fixed radio stations that receive transmissions from portable, mobile, or other fixed stations and repeat them for other radio users to hear more widely and clearly. Without careful tuning, gateways connecting repeaters can endlessly cause the other to transmit.

Similarly, multiple gateways on the scene of an incident or inappropriately configured ones can actually *dis*-able, rather than enable interagency communications. This can happen when uncoordinated use of multiple gateways leads to systems talking in an endless loop.

[67] CommTech was previously the Advanced Generation of Interoperability for Law Enforcement (AGILE) Program. Further information about the program can be found on its web site. See **http://www.ojp.usdoj.gov/nij/topics/commtech/**.

DUELING RADIOS

"By far the most challenging technical aspect of the deployment of the [gateway] was in interfacing with the repeater systems of the participating agencies. In systems in which a radio interfaced to the [gateway] is transmitting to a receiver site through a repeater, due to the length of the squelch tail, a repeater could stay up long enough to bring the radio connected to the [gateway] back up before the repeater goes down. Then because the radio is back up, the repeater could come back up, bringing the radio back up; and so on. This effect is referred to as the 'ping pong' effect."

Advanced Generation of Interoperability for Law Enforcement (AGILE)
Report No. TE-00-04, 23 July 2001
http://www.ojp.usdoj.gov/nij/topics/commtech/Gateway_Subsystem_Op_Test.pdf

Interoperability is promoted when agencies share a common frequency band and are able to agree on common channels. However, the general frequency congestion that exists across the United States typically places severe restrictions on the number of independent interoperability talk paths that are possible.

—SAFECOM
Interoperability Continuum

Despite the issues described here, gateways play an important part in many interagency communications systems today. They offer the portability and flexibility necessary to link various radio systems, frequency bands, and protocols existing across public safety agencies. Well used, they provide an important technological approach to interoperability.

Technology Approach: Shared Channels

Historically, the most common means of interagency communications by radio has been through the use of shared or common channels. As noted in the *Interoperability Continuum* excerpt, users of the same frequency band have the added option to share channels for interoperability. These channels may be for direct or unit-to-unit conversations within a limited range on scene or through repeaters programmed into their respective radios for greater range.

Although fragmented radio spectrum use reduces the potential, shared channels provide a low-cost and effective means of interagency communications in locales where users have the benefit of a common frequency band between their agencies. Commonly shared or formally designated interoperability channels now exist across all major public safety bands. In some jurisdictions, gateways are used to link designated shared channels between different bands, combining the use of multiple approaches to interoperability at the cost of duplicating transmissions across multiple channels.

PALMETTO 800 SYSTEM GATEWAY GUIDELINES

The state of South Carolina maintains guidelines for using gateways to interconnect other systems and users to the Palmetto 800 System. The purpose, objectives, and benefits of the guidelines are clearly stated:

Purpose: *To maintain the availability and functionally of the Palmetto 800 System for the primary system users.*

Objectives:
a) Ensure the integrity of the Palmetto 800 System
b) Provide interoperability options
c) Manage system loading
d) Establish a guideline for the use of interconnects.

Benefits:
a) Improve safety
b) Reduce interference and interconnect technical problems
c) Provide alternate 800 MHz service for special events and emergencies.

For more information, see: **http://www.cio.sc.gov/cioContent.asp?pageID=772**

Putting Shared Channels to Work
Use your radio technical resources and frequency coordinators to learn if there are FCC-designated shared channels available for use. There may be existing shared channel plans that you can take advantage of, but know the limitations and licensing requirements before putting them to use.

FCC Designation of Shared Channels

In addition to any specific frequency (or pair of frequencies for a repeater) adopted by convention by agencies for shared use, FCC rules and regulations designate specific frequencies for interagency communications. The number and availability of these frequencies vary considerably by band, as well as location.

Five VHF-high band (150 to 174 MHz) frequencies, ten UHF (450 to 470 MHz) frequency pairs, and five 800 MHz frequency pairs have been designated for more than a decade for interagency use. However, the VHF and UHF frequencies have been incorporated into interagency communications plans differently across the country, and often not at all. In many cases, the frequencies have been assigned for specific agency use. The 800 MHz pairs were designated solely for interagency use and provide key shared channels capability where this band[68] is well used.

[68] The FCC created the National Public Safety Planning Advisory Committee (NPSPAC) in the 1980s to guide rules for a segment of the 800 MHz band dedicated to public safety use. This spectrum is commonly referred to as the "NPSPAC band" or "800 MHz NPSPAC."

Regional shared systems are the optimal solution to interoperability. While proprietary systems limit the user's choice of product and manufacturer, standards-based shared systems promote competitive procurement and a wide selection of products to meet specific user needs. With proper planning of the talk group architecture, interoperability is provided as a byproduct of system design, creating an optimal technology solution.

—SAFECOM *Interoperability Continuum*

FCC narrowbanding rules and regulations split out additional channels from the traditional, 25 kHz ones, though they won't be wholly available until operations on adjacent channels migrate to narrowband. In 2000, the FCC designated five additional VHF frequencies and four UHF frequency pairs for interoperability use. These are narrowband (12.5 kHz) channels. Since January 1, 2005 their use under FCC rules for interagency communications has taken precedence over other licensed uses.

Many more channels specifically designated for interagency use are available in the 700 MHz band for regions of the country where this spectrum is clear of television broadcasters. As public safety systems are built in this frequency band, agencies will have access to more than 100 shared channels whose use is governed by state-level decision making bodies.[69]

Technology Approach: Shared Systems

The growing complexity and cost of radio systems have combined with serious needs for improved interoperability to push public safety agencies toward sharing of systems. Whether built of proprietary technology or based on accepted standards, shared radio systems offer economies of scale, less redundancy, and inherent interoperability of the chosen technologies. While sharing a radio system doesn't alone provide agencies with communications interoperability, it does provide core parts of the technical foundation.

Radio systems have been shared as long as public safety has been using the technology. In relatively recent history, however, technical innovation has followed their need to manage rising costs, crowded radio spectrum, and difficulties communicating with other agencies migrating to other frequency bands and technology. System sharing has come as a natural solution to each of these needs.

■ Proprietary Shared Systems

Trunking, as previously discussed, has been adopted as the primary means of sharing limited radio channels while still providing individual users with privacy and autonomy. The earliest trunked radio systems were built of proprietary technology, limiting the choice of system components and generally increasing costs through reduced competition and vendor lock-in. Many such systems are still in use today, both in single agency and shared use.

[69] The FCC maintains a web page explaining use of 700 MHz interoperability spectrum in greater detail. See **http://wireless.fcc.gov/publicsafety/700MHz/interop.html**.

Shared systems offer economies of scale, less redundancy, and inherent technological compatibility.

Proprietary or not, shared systems provide the technological compatibility necessary for interoperability between their users.

■ Standards-Based Shared Systems

The simplest shared system is where one or more channels is used conventionally (i.e., not trunked), either analog or P25 digital, between agencies. There is no proprietary aspect of such an approach and radios from various manufacturers can be mixed and matched to create the system. While channel efficiency of conventional systems can't approach that of trunked ones, they are a cost-effective option and provide opportunities for sharing of system infrastructure and backbone networks. Individual channels can be dedicated by agency with others shared for interagency communications.

P25 is the public safety standard for digital radio.

Because channel demand has overwhelmed available public safety spectrum, trunked systems provide the only alternative for shared systems in many areas of the country. As mentioned, trunking provides the means for many virtual channels, used privately between defined users, from a relatively few radio frequencies. This allows multiple agencies to come together on a shared system, use common channels (talkgroups), and still have private channels.

As public safety radio use migrated toward digital and trunked radio systems, the community saw a need—and an opportunity—to escape proprietary systems by setting future standards. Project 25 began in 1989 as a joint effort of the Association of Public-Safety Communications Officials – International (APCO) and the National Association of State Telecommunications Directors (NASTD) to ensure that public safety agencies would have an open, standards-based alternative for digital radio systems. Today, P25 provides that standard and is being extended to eliminate the lock-in that proprietary trunked systems face.

DEPARTMENT OF HOMELAND SECURITY TECHNICAL ASSISTANCE

The U.S. Department of Homeland Security offers help to recipients of its grants to improve interagency communications. As part of the Preparedness Directorate's Office of Grants and Training, the Interoperable Communications Technical Assistance Program (ICTAP) provides policy, operational, and technical help to projects funded under DHS programs.

See **http://www.ojp.usdoj.gov/odp/ta_ictap.htm**

Security

The security of public infrastructure, including information and communications systems, is of critical importance today. Security covers a much broader expanse than can be covered here, but we want to note issues that an interagency communications project manager may face. Particularly, there is a delicate balance between security and availability, which affects interoperability.

All radio system managers should follow established IT security practices.

Traditional information technology (IT) systems have long been guided by formal, well-defined security practices. Radio system managers increasingly face the same threats as their traditional IT counterparts. For example, denial of service attacks can affect and spread to all IP-based systems. The very flexibility that drives greater use of VoIP also increases vulnerabilities. All radio system managers seeking to secure their systems should follow established IT security practices.

The National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has published a series of documents on generally accepted security principles and practices,[70] recommended controls for securing federal IT systems,[71] and further principles addressing the subject from a systems perspective.[72] These documents describe the means of building a suitable foundation for secure voice radio systems.

SEARCH received funding from the COPS Office to produce a companion Tech Guide, *Law Enforcement Tech Guide on Information Technology Security: How to Assess Risk and Establish Effective Policies*. This guide provides more information on NIST security processes.

NIST addresses security throughout phases of the system lifecycle:

1. Project initiation.
2. Development and acquisition.
3. Implementation.
4. Operations and maintenance.
5. Disposition of systems.

---

[70] Swanson, Marianne, and Barbara Guttman, *Generally Accepted Principles and Practices for Security Information Technology Systems* (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, September 1996). See **http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf**.

[71] Ross, Ron, et al., *Recommended Security Controls for Federal Information Systems,* NIST SP 800-53 (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, February 2005, including updates to June 17, 2005). See **http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf**.

[72] Stoneburner, Gary, Clark Hayden, and Alexis Feringa, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* NIST SP 800-27 (Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology, June 2001). See **http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf**.

NIST points out that security is built into systems from the ground up.

The first four of these five phases of a system lifecycle should be familiar to the reader from Part II of this book. NIST principles point out that technology security isn't added onto systems, but rather built into them from the foundation up.

Advanced Radio Features for Physical Security

When most people think of radio systems security, they think of physically securing the infrastructure and logically securing the information that passes over the network. Conventional radio systems over the years have been plagued by the ease with which someone with malicious intent can disrupt communications by transmitting on the system. Lost and stolen radios are the biggest risk, but more than one system has been disrupted when a responder's young child wanted "to be like mommy or daddy" and spirited off a radio to the closet to talk.

Trunked radio systems control access to channels centrally, so offer an inherent ability to reject rogue radios with just a little effort on the system administrator's part. Better yet, modern radio systems, both conventional and trunked, offer the ability to disable the lost, stolen, or otherwise misappropriated radio remotely. That prevents the radio from requesting system access—or even transmitting at all!

While physical security is understandable as a fundamental to securing all systems, securing the information the system is built to transport is another matter.

Encryption and Key Management

Confidentiality, integrity, and availability are the three objectives of information security.

It's nearly impossible with current public safety technologies to prevent radio signals from being captured over the air. Military spread-spectrum techniques, where a signal is distributed across a wide swath of frequencies and thus made largely undetectable, haven't found their way to public safety voice systems. It's worthy to note that this technique is used with some cellular and wireless data systems, though.

Encryption is the traditional means of securing voice radio communications since they are so easily intercepted. The three objectives of information security—**confidentiality**, **integrity**, and **availability**—are served to different degrees by encryption.

- *Confidentiality* of the information is expected as long as the encryption system is uncompromised and the keys for unlocking its secrets are secured.
- *Integrity* of the information is the assurance that what was received is what was sent by the original sender. Encryption provides this, to a degree, simply by locking up the data, but other parts of the system contribute to its integrity by limiting access to the system to authorized users.
- *Availability* is a particularly difficult feature to secure in the radio environment because channel access can be denied simply by the presence of a rogue transmitter spewing RF noise across the frequencies in use (denial of service).

The great majority of public safety voice communications don't require great confidentiality. From an interoperability perspective, encryption brings additional challenges. Not only do all users that are expected to talk together on secure channels have to use the same encryption means and methods, but they must have current keys to lock and unlock transmissions. In effect, encryption adds technological junction points where interagency communications can be fractured. For example, most gateway approaches, such as console patches and other common audio bridges, require special care when moving traffic from one secure channel to another. There is the risk of originally encrypted traffic on one channel being decrypted at a gateway and broadcast unexpectedly on another channel unencrypted. Alternately, the encrypted traffic may be moved through a gateway to users of other channels who are unable to decrypt and use it, resulting in added noise and confusion for those users.

Encrypted interagency communications require greater efforts to ensure interoperability.

Despite these difficulties, the confidentiality and integrity of certain voice communications is of high value—high enough that availability risks are acceptable. Where needed, encrypted communications between multiple agencies require additional attention to technical compatibilities and their maintenance, to ensure interoperability.

■ The Digital Future of Encryption

Encryption of analog radio communications has a checkered past. Users have long been dissatisfied with the reduced range of encrypted communications and the lack of techniques to deal with a harsh RF environment that confuses the encryption systems. Analog encryption has been a necessary evil in most cases.

Digital communications naturally support encryption.

Digital radios bring a new day, though. The digital radio signal is, by nature, encoded, which reduces casual reception by common FM scanning receivers. As digital scanners become more prevalent, there's another arrow in the public safety radio quiver: The digital signal can be encrypted without effect on the system's basic functionality. That is, the transmitters, receivers, and radio environment keep on moving digital bits, not knowing whether they're scrambled one way or another.

■ Key Management

The big trick in dealing with encryption is managing the keys. Since encryption creates virtual private networks within the radio system, access to the keys allows users to be part of the network. There may be multiple sets of keys for different sets of users to limit access to only those with a predefined need for the "private" channel.

Like any other encryption system, those for radio are only as strong as their weakest link. That's usually the keys. Many an encryption system has been compromised because the secret decoder ring was stolen. Thankfully, this isn't a frequent occurrence with public safety radio systems, but all it takes is one radio to be lost or stolen for all others sharing the same keys to need re-keying.

OTAR is over-the-air re-keying, or updating encryption keys wirelessly.

First responder mobility challenges key management. If all users of an encrypted channel were in the same room, it would be easy to keep the keys up-to-date, switching them out as necessary to maintain security. Unfortunately for the radio system manager, users are rarely so easily contained. The need for "over-the-air re-keying" (OTAR) becomes apparent if you consider just the logistical challenge of maintaining encryption keys for potentially thousands of users on a large, modern radio system. OTAR is simply the process of encryption keys being passed from the system control point to affected radios, and then activated simultaneously.

OTAR makes it possible to load keys on the fly wherever the radios are, and then switch to the new set when they are all prepared.

Encryption is managed as a piece of the larger interoperability project.

Technology provides the means of key management in a shared radio system. The more difficult part is managing the people environment to gain concurrence about what will be encrypted, how the process and keys will be managed, and procedures for use of encrypted channels so users don't become stranded on yet another desert island lacking interagency communications. This aspect of the technology is managed as a piece of the larger puzzle that is addressed throughout this book.

■ Reports Available from SAFECOM

The Public Safety Wireless Network (PSWN) Program produced two reports on encryption key management. These reports are available from the SAFECOM library. The first is an introductory text explaining basic encryption concepts.[73] The second provides a key management plan template.[74]

[73] *Introduction to Encryption Key Management for Public Safety Radio Systems*, Public Safety Wireless Network Program, October 2001. See **http://www.safecomprogram.gov/SAFECOM/library/security/1113_securityissues.htm**.

[74] *Key Management Plan Template for Public Safety Land Mobile Radio Systems*, Public Safety Wireless Network Program, February 2002. See **http://www.safecomprogram.gov/SAFECOM/library/security/1114_keymanagement.htm**.

ON THE HORIZON – VOICE COMMUNICATIONS TECHNOLOGY

The most promising technology on the horizon for improving interoperability is ***software defined radios*** (SDR). Much like other electronics throughout the technology universe, radios are increasingly designed with internal functionality provided through software.

Thirty years ago, public safety radios were limited to just a few frequencies spread over a narrow slice of RF spectrum. Twenty years ago, early "programmable" radios were in use that allowed frequencies available in the radio to be changed electronically, rather than by substituting internal hardware. These radios also allowed use of a greater range of frequencies.

During the past 20 years, more and more radio functionality has been moved from hardware to software. Software defined radios are the next evolution that will allow even greater agility not only across bands, but also with varying channel bandwidths and across different modes of transmission. For example, the U.S. Department of Defense is developing the Joint Tactical Radio System that will operate across multiple bands, use various analog and digital transmission modes, and provide a combined platform to eliminate a plethora of different systems.

For public safety interoperability, the technology promises greater ability to span the chasm between different frequency bands in use. Today, radios using VHF aren't able to communicate with those using 800 MHz. In the future, this fundamental technical challenge to interoperability will be overcome.

Similarly, different means of getting information through radio channels will become more flexible. Narrow and wider bandwidths will be accommodated through software, as will analog and a variety of digital transmission modes.

Today, Project 25 radios provide analog and digital, narrow and wider band capabilities largely through software. SDR technologies will gradually be integrated into mainstream public safety radios, eliminating some of the technological barriers preventing direct interagency communications.

Much like artificial intelligence in computer systems, SDR techniques will be embedded in technology and largely unobserved by the end user. The effects will be significant, however.

Technology marches on, bringing new capabilities and overcoming the old.

Chapter 17: Data Communications

Voice communications over radio is accepted as the central interoperability challenge, but it's increasingly difficult to separate voice from data and wired from wireless networks. Data networks tie together public safety communications systems from beginning to end. From the automatic number identification/automatic location identification (ANI/ALI) data arriving with an initial 9-1-1 call for services through the responder's final status code transmission from a mobile data computer, data systems connect responders to the public they serve and beyond. Even at the core of modern radio systems, wired and wireless data networks connect dispatch consoles to central electronics banks, link complex subsystems in the radio room, and carry audio widely between distant transmitters.

Since the World Wide Web surfaced from the primordial Internet barely more than a decade ago, data networks have come to pervade our homes, our offices, and even our automobiles. In this chapter, we look first at the protocols and standards that fueled this explosive growth and then into the technologies of both wired and wireless data networks. We'll wrap up the chapter with an examination of how data networks are secured and close with a look at data communications developments on the horizon.

Common Protocols and Standards

Common protocols and standards are the building blocks for interoperability, technologically or otherwise. At technical and social levels, alike, the Internet has influenced the world of information sharing greatly, from civic and commercial realms, to government. Just as the World Wide Web evolved as the model of information sharing globally, the common protocols on which it was built have become the foundation for nearly all data communications.

Common protocols and standards are the building blocks of interoperability.

The Internetworking Effect

What suite of protocols powers the Internet and every private network that has arisen from it?

If the following section title didn't give it away, you might be surprised to know it's the *Transmission Control Protocol/Internet Protocol* best known as TCP/IP. Lest the term "suite" strike you as pretty fancy for just two protocols, understand that TCP/IP is commonly used to refer to dozens of protocols that lace the Internet together.

The Internet has become so ubiquitous and part of our daily lives that we may forget at times that it's a minor miracle that we can transfer a wide assortment of data around the world with little worry about how it happens. Electronic mail, files, video, music, and now voice telephony speed from point to point across increasingly faster and faster networks upon an amazingly standardized set of protocols.

Internationally, a body known as the Internet Engineering Task Force (IETF)[75] is central to the definition and formalization of these protocols. It's beyond the scope of this Guide to get very deep into the protocols, but we do want to note that they are many, varied, and built upon one another. The most basic, hidden services of wired and wireless networks connect physical components together in standardized ways, while increasingly complex protocols are built upon them to deliver information in a humanly digestible form.

■ At the Heart: TCP/IP and Friends

TCP/IP, its companions, and associated other protocols occupy the middle ground of a stack of open, standardized means of interconnecting information sources. The very term "Internet Protocol" describes the original purpose for the protocol: Connecting different networks.

Other key Internet protocols that have found their way into the heart of public safety communications include the following:

- **File Transfer Protocol (FTP) –** A venerable graybeard of the earliest days of internetworking and today underlying data transfer between many criminal records and other information sharing systems.
- **Simple Mail Transfer Protocol (SMTP)** and **Post Office Protocol Version 3 (POP3) –** Key pieces of today's e-mail, as well as automated fingerprint identification systems.
- **User Datagram Protocol (UDP) –** TCP's alter ego and the foundation for Voice over IP (VoIP) networking, including systems for interconnecting radios over data networks.
- **Session Initiation Protocol (SIP)** and **Real-time Transport Protocol (RTP) –** Doing yeoman's work for networking services as varied as peer-to-peer music sharing systems and VoIP telephony, beyond to the instant messaging capabilities of the Capital Wireless Integrated Network (CapWIN) around Washington, D.C.

[75] The IETF is an international community of industry, academia, and government. See **http://www.ietf.org/**.

- **Lightweight Directory Access Protocol (LDAP) –** Serving at the core of NASA's Integrated Services Environment just as it serves user authentication information to encryption engines securing Kansas' innovative Criminal Justice Information System.
- **Simple Network Management Protocol (SNMP) –** Giving technical staff a view into the core of the Internet, as well as the supervisory control and data acquisition systems of modern trunked radio systems.

These and many more standardized protocols have brought about a Golden Age for data sharing at a technical level, whether those data packets are carrying criminal history records, voice dispatch communications, or fingerprint images. As much as they contribute, these networking protocols alone don't make the data intelligible, though. It takes higher level application protocols and standards to transform data into information.

XML—Universal Language of the Internet

Broad adoption of Internet protocols has supported growth of a key tool for interoperable data communications: the Extensible Markup Language (XML). A project manager dealing with interagency data communications today will have a hard time avoiding XML. It is the universal language of data communications today, particularly for data that cross system and jurisdictional boundaries.

XML actually had its origin before widespread use of the Internet in something called Standardized General Markup Language (SGML). A markup language is basically simple, textual conventions for describing associated data and providing further details on how the data are used. SGML is actually an international standard; XML is a simplified subset of it.

XML's magic is in its extensibility—its innate capacity to describe and extend itself for wrapping data into ever more useful packages. It is structured text, making it both human and computer readable, but XML can wrap up and describe data of all types. Software capable of processing XML *documents*—packages of XML text and data payloads—are able to "learn" of the structure of the document, including associated nontextual data.

Applications that consume XML-based data can be structured to be very rigid or flexible in understanding the data. That is, the software can restrict itself to consuming only highly structured information or maintaining flexibility to learn how to deal with data in different forms. Not all systems can or should be so willing

to adapt to changing data forms, particularly in high-security and mission-critical environments, but XML provides the means for software to extend its understanding of the data it processes as designers see fit.

■ XML in the Justice System

As with consumer, business, and government systems worldwide in recent years, public safety information systems in the United States have become more open through the application of XML. Work by individuals and organizations involved with the justice system nationwide contributed a key, anchor tenant to the information sharing bazaar—the Global Justice XML Data Model, or GJXDM. (Don't even try to pronounce it; you'll be in lip splints for weeks.)

There's no shortage of acronyms in the world of Internet protocols—even ones with others embedded!

The U.S. Department of Justice (DOJ) Office of Justice Programs (OJP) released the GJXDM in early 2004 as the first comprehensive product to wrap together a **data dictionary**, a **data model**, and an **XML schema**.

A *data dictionary* is a set of standardized descriptions of data to provide a common definition and means of describing, for example, a person's name. A *data model* expands on a data dictionary by establishing how different data elements relate to each other. For example, a person has a birth date, height, and weight, while a vehicle has a make, model, and style. An *XML schema* defines how data elements make up documents and how documents are related to each other. Remember that in the worldwide web of information protocols and standards, XML documents can range from very simple to very complex sets of information.

GJXDM provides its own rich set of definitions that can be used outside the justice world. It and the use of XML, more broadly, are becoming requirements for public safety information systems funded with federal dollars in order to ensure interoperability between systems. In fact, the COPS Office now encourages police agencies engaged in technology projects to use XML whenever possible. For example, the Baltimore City Police Department was encouraged to use the GJXDM while working on a regional crime analysis project funded by a COPS Office grant. The department committed to incorporating GJXDM-compatible functionality into the regional database used in its Regional Crime Analysis Program and Regional Crime Analysis Geographic Information System. In doing so, the department has greatly enhanced the ability of police agencies participating in the Regional Crime Analysis System organization to share information about crimes and offenders.[76]

[76] Source: Baltimore City Police Department Progress Report, December 2005, submitted to the COPS Office.

Implementing Interoperable Systems using GJXDM

The standard reference for implementing GJXDM was produced by SEARCH for the Office of Justice Programs, Bureau of Justice Assistance. *Building Exchange Content Using the Global Justice XML Data Model: A User Guide for Practitioners and Developers* was published in June 2005. See **http://it.ojp.gov/documents/GJXDMUserGuide.pdf**.

The Global JXDM is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner. The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system to system, Global JXDM enables access from multiple sources and reuse in multiple applications.

—U.S. DOJ OJP web site, **http://www.it.ojp.gov/gjxdm**.

The COPS Office also funded SEARCH to convene a series of workshops and develop GJXDM Information Exchange Packages (IEP) for Law Enforcement.[77] The publication of law enforcement IEPs provided, for the first time, tangible models and GJXDM content that could be used by law enforcement agencies, whether large or small, urban or rural, federal, tribal, state, county or local, to begin on the path of data interoperability to support information sharing about crimes and offenders.[78]

GJXDM—and all the information-sharing capabilities it has spawned—contribute greatly to interoperability for data communications. It can be a complicated subject, so for our purposes we'll leave the topic here and move on to how it and other uses of XML are advancing emergency response.

[77] The workshop report is available online at **http://www.search.org/files/pdf/gjxdm-iep.pdf**. Documentation reports, such as Field Interview Report, Charging Document, Sentence Order, and Incident Report, are freely available from SEARCH at **http://www.search.org/programs/info/xml-iep.asp**.

[78] Elsewhere in federal grant programs, recipients of grants from the U.S. DOJ's Office of Justice Programs that are implementing XML are required to use GJXDM. See **http://it.ojp.gov/topic.jsp?topic_id=138**. Also, Fiscal Year 2005 grant guidelines from the Department of Homeland Security (DHS) required use of GJXDM specifications and guidelines regarding use of XML to support intersystem exchanges of information. "Fiscal Year 2005 Homeland Security Grant Program – Program Guidelines and Application Kit." See **http://www.ojp.usdoj.gov/odp/docs/fy05hsgp.pdf**.

■ XML in Emergency Response

The LEITSC web site offers emerging CAD/RMS standards information: **http://www.leitsc.org/.**

The beauty of XML standardization efforts is that, with proper coordination, different areas of interest or domains can leverage each other's efforts. For example, the Law Enforcement Information Technology Standards Council (LEITSC) has established priority objectives for development of functional standards for records management (RMS) and computer-aided dispatch (CAD) systems. XML and related standards are the primary focus of its technical committee.

The emergency management world is also seeing rapid growth of information sharing standards built around XML. For example, the Emergency Data Exchange Language (EDXL) is an effort to advance interoperability between data systems. EDXL is being developed through a practitioner-driven, public/private partnership between industry and the DHS's Disaster Management (DM) E-Gov (electronic government) initiative to advance U.S. disaster management response capabilities. One standard established before DM involvement was the Common Alerting Protocol (CAP). EDXL is a broad suite of draft standards to provide tools for information sharing, while CAP is a specific, standardized protocol for alerting and event notification.[79]

The Disaster Management Interoperability Services (DMIS) are part of a Presidential e-government initiative to advance U.S. disaster management response capabilities.

CAP has seen use in both government-funded and commercial applications. Disaster Management Interoperability Services (DMIS),[80] an interoperability software toolset providing real-time, secure sharing of incident information for public safety agencies, is an example of the former. DHS funded development of it as part of the Disaster Management initiative. DMIS uses the CAP standard, as well as other XML-based exchanges, to move information between users of either a no-cost DMIS client application or with other applications capable of using the protocol. The DMIS client application provides basic functionality using standard, web-based services to create, view, and exchange incident information.

Commercially, crisis information management systems (CIMS) are a rapidly developing breed of application built for information sharing. They commonly use XML to push data to and pull it from other information systems. Distinct from traditional RMS and CAD systems used by responder agencies, CIMS implementations are designed specifically to collect, distribute, and display

[79] For further information, see the web site of the Organization for the Advancement of Structured Information Standards (OASIS) at **http://www.oasis-open.org**. OASIS is a not-for-profit consortium of vendors and users developing guidelines for interoperable systems. For information on EDXL, see **http://xml.coverpages.org/edxl.html**.

[80] See the Disaster Management Interoperability Services web site at **http://www.cmi-services.org/**.

information from various sources—both from humans and machines. For example, popular commercial products allow integration of information from CAD and geographic information systems (GIS), while providing document sharing, video conferencing, and other collaboration tools.

Commercial CIMS products with XML capabilities are finding popular adoption among emergency management officials for noncrisis events, too. For example:

- **Football Championship Game – Jacksonville, Florida**
  In February 2005, the Jacksonville Sheriff's Office used a commercial, web-based collaboration product to help it and dozens of other agencies manage information flowing in all directions. It was found to be particularly useful in maintaining situational awareness, executing Incident Command System (ICS) incident action plans, and producing situation reports.
- **Presidential Inauguration – Washington, D.C.**
  A month earlier, the Metropolitan Police Department in Washington, D.C., made use of a different CIMS to push information to other homeland security and law enforcement information systems. It also helped the department document activities for subsequent federal reimbursement of expenses.
- **National Political Convention – Boston, Massachusetts**
  Boston was the site for a national political convention late in the summer of 2004. The Boston Emergency Management Agency implemented yet a different commercial CIMS for hundreds of users across dozens of agencies and organizations. It was used for incident information sharing between the agency and the U.S. Environmental Protection Agency during the convention.

There is great room for XML and similar technologies to advance interoperability of data communications. An October 2004 report on CIMS interoperability by Dartmouth College[81] noted the need to create a common vocabulary of technical terms, define data elements, promote public/private partnerships to advance standards, and overcome "cultural issues" affecting information sharing. Similarly, standards for open messaging between RMS and CAD systems are in their infancy.

[81] Institute for Security Technology Studies, *Crisis Information Management Software (CIMS) Interoperability: A Status Report,* (Hanover, New Hampshire: Dartmouth College, October 2004). See **http://www.ists.dartmouth.edu/TAG/cims1004.pdf**.

Building Blocks for Interoperability

The very process of standardizing, accepting, and implementing common protocols is endlessly challenging due to the rate of change in the world of information technology. Government, in general, and public safety, more specifically, faces these challenges in spades. It's impossible to adopt the power of standards without becoming part of the dynamic evolution of information sharing.

Challenges notwithstanding, the future looks bright for greater and greater technical capabilities to share data, make it intelligible, and, ultimately, make it into actionable information. Information sharing is the true measure of interoperability.

* * *

It's becoming increasingly difficult to separate wired and wireless modes of communications.

Common protocols and standards arising in conjunction with the Internet depend on physical networks to move data about. Increasingly, interagency communications capabilities are evolving simultaneously on both wired and wireless networks. In truth, it's becoming increasingly difficult to separate the two modes of communications. For the sake of discussing data communications technologies that use the protocols and standards mentioned, we'll take a look at wired and wireless networks separately.

Wired Data Networks

The term "network" is a very flexible one, something like "system." On the one hand, it's used formally to refer to technical assemblages of telecommunications hardware and software. On the other, it's used more broadly in reference to groups of people or functions linked by technology. Our use in this chapter is toward the technical side of that spread.

A Whole Lotta *AN Going On!

Most anyone who has been around an office computer environment more than about an hour has heard the term "local area network" (LAN). But have you heard about campus, metropolitan, and wide area networks (CAN, MAN, WAN)? Despite the obvious fun that can be had by use of the acronyms (in some quarters, at least), do these have anything to do with communications interoperability?

Well, yes they do. Thanks for asking! Just as common terminology is a key factor for interoperability, the design and operation of interagency communications systems is furthered by common use and understanding of terms. Data networking is easier to understand with a common, consistent vocabulary for network types.

■ Standard Network Types

Local area networks are typically constrained to an office or building environment. There are physical wiring limitations that have given rise to the term, but generally a LAN is considered a geographically and functionally constrained network connecting personal computers, and perhaps, servers and printers.

Multiple LANs may coexist in a single location to segregate use for functional or security purposes. For example, it's not uncommon in dispatch centers for separate connections to the state data network and to the city or county LAN to exist side-by-side—often connecting separate computers. The state connection provides access to the FBI's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and state systems, while the other provides access to local applications and data.

From an end user's point of view, CANs, MANs, and WANs may appear to be largely arbitrary distinctions in the geographic extent of data communications systems. To a large extent, that's true. Data networks are categorized in these geographic terms more for the sake of convenience in discussion rather than inherent technical limitations.

Groupings of networks to create the successively larger ones are defined at a technical level, of course, but widespread adoption of TCP/IP for data communications often makes them seem all as part of a larger whole. With the right agreements, technicians, and overarching applications—such as the Internet—they can easily serve as the technical means of data communications interoperability.

The FBI's CJIS WAN connects law enforcement agencies nationwide.

For example, the FBI's Criminal Justice Information Systems (CJIS) WAN connects to each state and some larger cities, providing the backbone for a wide array of NCIC, criminal history, and automated fingerprint identification services to agencies nationwide. Specialized networking equipment and circuits connect each of these pieces. And a whole lot of tuning and configuration makes it possible to pass data from one end to the other, but at the network level, there is interoperability.

■ Public Safety Network Types

Project MESA, an international effort to standardize broadband wireless access for emergency response, introduced several important networking concepts to public safety. We'll discuss Project MESA further in the final section of this chapter, but want to introduce the networking concepts here.

In the process of examining intra- and interagency needs, different type of networks were defined to address differing needs for high-speed data exchange. These aren't necessarily independent networks and may, indeed, be built of similar technology. Each amounts to a separate *functional* type of network.

The first is a personal area network (PAN). In public safety response, this is the networking environment that surrounds the individual responder. It may be short-range wireless means for microphones, location monitoring devices, and environmental sensors to be connected to a personal hub. From that hub, information may be made available to the individual responder, as it may be shared with team members, incident commanders, and beyond. The PAN will carry both data and voice communications within close proximity to the first responder.

How many acronyms can fit on the head of a PAN?

At a higher level, an incident area network (IAN) links multiple response elements responding to a particular incident. This is most easily seen as a network geographically limited to the scene of the incident, but the concept recognizes that outgoing and incoming communications from afar—such as from a central Emergency Operations Center (EOC)—may touch the incident area network as well.

Beyond individual incidents, the jurisdiction area network (JAN) describes functional and even technical networking requirements that span the general operational environment of one or more agencies. In essence, it serves to connect both widely dispersed resources and concentrated "hotspots."

The final networking type described by Project MESA is the extended area network (EAN). Multiple sub-networks linked across broad geographic expanses are most commonly known as WANs or extranets. The idea is that through use of common technical protocols, application-level interoperability, and shared security measures, data communications can span individual agency and jurisdictional networks.

Data Networking Evolution

For law enforcement, all this network connectivity isn't that unusual. NCIC, NLETS, and other collaborative data systems have allowed agencies to share wanted persons, stolen vehicle, and other information nationwide for almost 40 years. What has changed is that the networks have gotten smarter, faster, and more flexible. Dedicated circuits between systems that were more than adequate for decades have largely been relegated to the dust bin of history, as more and more data needs to be moved between agencies.

■ Speed Matters

Wired networks speeds have increased dramatically as the world has come to revolve more and more around access to information. Thirty years ago when ARPANET, the Internet's precursor, was the private domain of military facilities, defense contractors, and a few universities, LAN speeds were measured at just a few million binary digits (bits) per second—megabits per second or Mbps. WAN circuits speeds were orders of magnitude slower, running at what we would today consider good dial-up modem rates, measured in thousands of bits per second (kilobits/sec or Kbps).

Today, LANs are commonly built to transfer billions of bits per second (gigabits/sec or Gbps). Long-haul fiber optic circuits forming the backbones of modern WANs are measured in hundreds of Mbps, while even home access to the Internet is more often than not measured in broadband terms of megabits per second. In 2005, 60 percent of home Internet access in the U.S. was via broadband connections. [82]

■ Intelligent Networks

"The days of the fat, dumb pipe, are over."

According to industry sources,[83] increasing demand for TCP/IP networks to carry great volumes of data of various types brings a need for more smarts than raw bandwidth. Traditionally, demand for smarter networks arises as coworkers or collaborators get spread further apart geographically, depend more and more on web- and other server-based applications, and increasingly depend on IP networks for carrying voice and other multimedia traffic. Internetworking of government functions is at an all-time high and destined to be more critical as information sharing becomes not only expected by the public, but demanded.

Network intelligence has gradually come to the public safety world. Ten years ago essentially all access to NLETS and NCIC occurred over circuit-switched connections using specialized network protocols. Today, the majority occurs over packet-switched circuits, most typically using TCP/IP at the core. While private virtual circuits are used to protect traffic from prying, the circuits are still "virtual"; that is, they're passing through a larger cloud of intermingled bits and bytes.

■ Improving Quality of Service

VoIP applications need "fast" networks.

The greatest driving factor for increased network intelligence today for public safety purposes is to provide an improved *quality of service* (QoS) at a low networking level to applications, such as VoIP telephony, which suffer terribly from network delays.

[82] Source: **http://www.websiteoptimization.com/bw/0509/**.

[83] Erlanger, Leon, "Building the intelligent network," *InfoWorld*, July 18, 2005. See **http://www.infoworld.com/reports/29SRintelnet.html**.

Digitized and packetized audio from telephones or radios that is being sent and received in real time demands fast networks. Delays measured in fractions of a second can disable simultaneous two-way (duplex) voice communications, as we're used to with telephones.

And fast isn't the same as big, though the two have been intertwined since the earliest days of networking. That big, fat networking pipe connecting two points might, like a railroad, be capable of carrying huge amounts of data, but it can be slow to get up to speed and equally slow to decelerate, like a train. In the networking world—wired or wireless—delays between transmission and receipt of bits and bytes is referred to as *latency*.

Network latency affects duplex (simultaneous two-way) communications.

Have you ever noticed how hard it can be to carry on a cellular telephone conversation when there are network delays between you and the other party? Estimates are that delays of more than a quarter of a second (250 milliseconds) disrupt the normal flow of human conversations. Even that tiny amount of time serves as a cue for the wetware between our ears to switch from "receiving" to "transmitting" in a two-way conversation.

Wired data networks are more easily managed to maintain a set QoS level than are wireless networks.

Wired Networks Keep On Keeping On

Thankfully, the interoperability of data communications over wired connections isn't much of a technical challenge today. From the physical level of wiring through widely accepted and reliable networking protocols, there's little to prevent network architects from lacing together interagency communications systems.

The greater challenges probably come from *too* much connectivity, which brings security concerns, fosters the spread of viruses and other network pestilence, and generally threatens the manageability of segmented networks. We will address security issues and technologies associated with data communications later in this chapter.

Wireless Data Networks

Many protocols originally developed for wired data networks have migrated to wireless networks. While most originally arose for connecting independent data networks that were built at the time from coax cable and twisted pairs of copper wire, the rapidly evolving wireless world is pouring its own share of protocols into a spreading pool.

Higher level standards and protocols, such as IP, are equally as important in wireless networks as they are elsewhere. However, unlike in the wired world, there is great variance in low-level wireless standards. For example, Ethernet[84] in its various speeds is widely accepted and used for wiring together LANs using standard types of cabling. The wireless data world is much more in a state of transition, by comparison.

In this section, we'll look at wireless data communications technologies available to public safety agencies for their own networks and those used for commercial services. We'll tour the field in this order:

- Common principles
- Private radio technologies
- Commercial radio technologies
- Wireless local area networking
- Wireless metropolitan area networking.

We'll conclude this section with a look at how to evaluate options for building your own wireless data networks versus buying services from commercial providers.

Common Principles

In your own considerations of wireless data communications technology, work to avoid "Silver Bulletitis"—an affliction leading to the belief that there's a single, ideal technology awaiting discovery or deployment that will provide interoperability. Keep in mind a few common principles demonstrating the practical realities and tradeoffs facing network architects.

■ Speed, Capacity, and Throughput are Interrelated

Speed, capacity, and throughput (the effective amount of data passed) are all interrelated. All other factors being equal, more users on a network reduces total, practical capacity. This occurs because each user brings a certain amount of networking overhead. Theoretically, with enough users a network would reach capacity with overhead communications, alone and provide no useful capacity for practical applications. More users reduce the amount of network bandwidth available to all, reducing throughput and effective speed.

[84] *Ethernet* is the popular name given to wired networking technology that has grown dominant during the past 30 years. Technically, it is standardized by the Institute of Electrical and Electronic Engineers (IEEE) as IEEE 802.3. It has evolved in speed over the years, with good backwards compatibility.

■ Faster and Deeper Requires Smaller "Cells"

Recognize that basic networking theory maintains that more, smaller zones of coverage (e.g., cells, hotspots, etc.) provide greater speed and capacity. The tradeoff is complexity and cost. A side benefit is that smaller cells of coverage result in greater overlap, on a proportional basis, and thus redundancy.

Wireless WANs that depend on few fixed access points for bringing mobile users back home are relatively limited in capacity and speed. This applies to satellite networks, as well. Satellite data networking also demonstrates that the mere distance between users and central network components limits speed and capacity. That is, nature decrees that electromagnetic radiation is going to take a fixed amount of time to travel a given distance. Wireless networks of a few hundred feet in radius are faster and offer the potential for greater capacity than those connecting hundreds or thousands of miles into space.

■ Advanced Capabilities Cost Money

Speed, coverage, reliability, and security cost money. Compromises are made continuously in public and private sector data networking, as well as by commercial carriers, to provide the most for the best price. What constitutes an acceptable compromise and a good price varies widely, of course.

There's no free lunch, only relative compromises.

Private Radio Technologies

Early generation technologies available for wireless data systems were slow, providing speed only adequate for low-volume textual information. Very much like other data systems that relied on wide-area coverage by a relatively few transmitters, early mobile data systems ran at 4.8, 9.6, and 19.2 Kbps—rates considered painfully slow even by dial-up networking standards today. And recognize that those systems weren't dedicated to a single, point-to-point connection as a dial-up modem is, but shared each frequency among multiple users, just as voice radio channels were used.

Wideband standards for public safety use are rapidly developing. We'll take a look at the prognosis for them in the final section of this chapter, "On the Horizon."

As a matter of fact, the technologies for these systems operated in standard voice channels, encoding data as sounds just like a telephone modem does. Technological advancements allowed data speeds to double and then double again, but the result was still a network that ran a poor second compared to dial-up. Did we mention the data channel was shared by multiple users?

Slow technologies are still in wide use. The most common mobile data technologies in public safety use today still only run at 19.2 Kbps. And digital voice radios don't offer any immediate improvement. Project 25 (P25) radios, capable of passing voice and data digitally, have a maximum rate of 9.6 Kbps and effective throughput of half that.

MICROWAVE SUBSYSTEMS

Many public safety voice and data systems have private microwave backbones linking together facilities and radio sites. While unlicensed microwave technology is widely available, most agencies prefer to build backbone networks using microwave channels assigned by certified frequency coordinators and licensed through the Federal Communications Commission (FCC). As with voice frequencies, coordination and FCC licensing offers much better assurances that agencies won't suddenly find other users interfering with their operations.

Microwave backbone networks are popular because they offer high-speed, high-bandwidth connections without requirements for intervening infrastructure or recurring payments to network carriers for leased lines. Properly engineered, they are also considered more resilient to accidental and intentional disruptions.

(More than one public safety network has been subject to "backhoe fade," the tongue-in-cheek term for accidental breaks of buried wire and fiber circuits. Anyone involved in telecommunications for long has a horror story to tell of losing network access, receiving a call from a network carrier, and eventually gasping in awe at the sight of thousands of wires ripped apart by an errant backhoe operator.)

Shared microwave backbones are increasingly popular among public safety agencies looking to leverage funds and take advantage of the tremendous capacity of today's microwave systems. They are a natural adjunct to other shared systems, offering great potential to interconnect parts of participating agencies' data, voice radio, and telephone systems.

Mobile data systems built to operate across voice channels are inevitably constrained by the channel width of those frequencies. Greater bandwidth yields greater speed. Data systems built upon the narrow bandwidth of existing voice channels are limited to low speeds.

Commercial Radio Technologies

Industry sources estimate that 80 percent of the U.S. population is covered by carriers providing wireless data services at dial-up speeds or better. Nearly 50 percent of the population is covered by systems offering high-speed data transfer ranging from 10 to 30 times dial-up rates. The lure of such speed and implied capacity is understandable. Across the country, more and more agencies have turned to commercial services.

Commercial wireless services long ago outran technologies commonly available to public safety agencies for their own systems—at least in terms of raw speed and capacity. Recognizing that agency choices may value availability over raw performance, the attraction of commercial data rates is often a deciding factor.

■ Background: Generations of Commercial Wireless Services

Wireless data services provided by commercial carriers are commonly discussed in terms of which "generation" they're part of. There's some debate about what exactly splits the generations (sound familiar?), but we know that for wireless data communications, it tends to be based on transfer rates—or the amount of data measured in thousands or millions of bits per second (Kbps or Mbps).

At the time of this writing, second and third generation services—2G and 3G, respectively, in short—are being offered.

A brief taxonomy and short chronology of commercial wireless services may be useful.[85]

- **1G –** Defined only in retrospect, first generation wireless services included early analog cellular telephones and overlay data services, such as Cellular Digital Packet Data (CDPD). CDPD was popular among police and fire agencies as a commercial networking alternative. It ran at 19.2 kilobits/second (Kbps).
- **2G –** Digital cellular telephone systems are considered the second generation. Second generation systems include GSM, iDEN, and cdmaOne. Data rates for these technologies are around 20 Kbps.
- **2.5G –** Services running in the range of a few dozen to few hundred Kbps are considered to be in this transitional ground from dial-up speeds to wideband, 3G services. Examples include GPRS, 1xRTT, and EDGE technologies.
- **3G –** High-speed technologies that can compete with wired services, ranging in speed from a few hundred Kbps to more than 1 Mbps. Examples include EvDO and UMTS.

■ Growing Private and Public Sector Use

Use of commercial wireless services is growing. A 2004 report by the Yankee Group, a high technology market research firm, indicated that more than half of large U.S. businesses would be using wireless wide area networks by mid-2006, citing the growth of 3G networks and their capacity to bring enterprise-class application services to the mobile user. [86]

Figure 17-1 depicts real-world data throughput of different wireless technologies and likely dates for broad availability.

---

[85] The world of wireless data networking is full of acronyms. See Appendix F for a glossary of terms.

[86] Signorini, Eugene, *3G Represents an Inflection Point for Enterprise Mobility* (Boston, Massachusetts: Yankee Group Research, Inc., 2004).

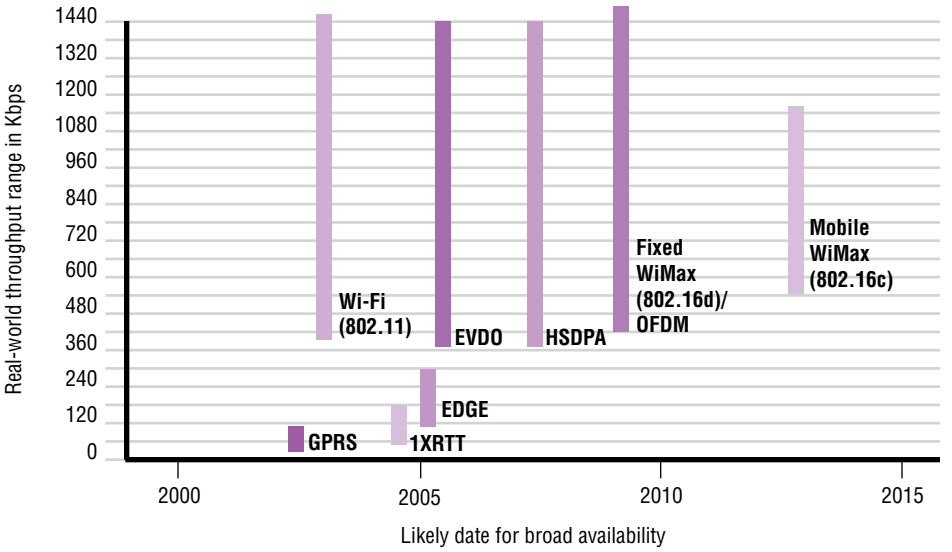


Figure 17-1: Wireless Data Rates and Availability

Source: InfoWorld, September 26, 2005

Satellite Services Commercial satellite services are the only means for U.S. public safety agencies to gain the advantages of space-based communications. As addressed in Chapter 16, **Voice Communications**, satellites have a definite niche for emergency response. They also have technical and cost drawbacks that keep terrestrial data networks as the first choice, where available.

Technologically, public safety tends to trail, but track, private data networking trends. We can look at those broader trends to project where public safety wireless is headed.

A late 2005 reader survey by *MissionCritical Communications*[87] showed that slightly more than half of respondents said that traditional, private radio networks were the primary means of wireless data access for their agencies' responders, while more than a third relied on commercial networks. Significantly, about half as many respondent agencies relied on high-speed wireless LAN (WLAN) technologies as relied on commercial services—16 percent versus 34 percent.

The use of popular WLAN technologies is an interesting parallel of public safety and private sector uses. The cited survey also indicated that 75 percent of respondent agencies planned to deploy WLANs at their facilities before the end of 2007. Of course, there's a difference between using the technology at facilities, such as offices and parking garages, and covering the wide, deep emergency response environ. Due to limited range of WLANs, most agencies using them rely on traditional private or commercial networks for more general coverage.

[87] "Public Safety Report: Snapshot Survey – Wireless Networking," *MissionCritical Communications*, September 2005, p. 64.

Wireless Local Area Networks

The growth and popularity of WLANs is indisputable. Various industry sources cite double-digit annual increase rates for the equipment market and triple-digit growth rates in the number of users worldwide. The value of mobile computing long recognized by public safety agencies has now been recognized in the consumer, industry, and general business sectors. Popularity has driven down the technology's price and spurred innovation in its use.

■ WLAN Technologies

As a matter of background, wireless LAN technologies are most often described in terms of the standards they use. The most common is the IEEE 802.11 family of standards,[88] which define wireless networks very similar to Ethernet (IEEE 802.3) in the wired world.

The Wi-Fi Alliance brought a standard implementation to 802.11 wireless networks.

Standardization has been key to WLAN growth. However, it wasn't until the thorny issue of interoperability was taken up that manufacturers adopted a common implementation of the standards, fueling an explosion in growth. The Wi-Fi Alliance, a nonprofit trade association established late in the 1990s, brought that common implementation well known today as *Wireless Fidelity* or Wi-Fi.[89] The term *Wi-Fi* has become such a standard part of the international wireless lexicon that it's well to remember it has a formal meaning.

High-speed wireless data networks are an increasingly important part of the interoperability equation. As agencies seek greater mobile access to information and weigh their options to rent or own networks providing it, the value of wireless data networking technologies is being factored in. We will address those technologies and evaluate privately owned versus commercially available options shortly.

■ Wi-Fi and Other 802.11 Networks

The IEEE 802.11 series of standards covers two incompatible types of technology: 802.11a and 802.11b. Though very similar technologically and both serving well in accurately described Wi-Fi networks, a key difference is in the frequency bands they use. Just like voice technology, WLANs using different frequency bands lack technical interoperability at a very low level. It's possible to include both 802.11a and b technologies in the same box, but they're still operating independently even if linked at a higher networking level.

---

[88] For further technical information on the IEEE 802.11 series of standards, see **http://www.ieee802.org/11/**.

[89] Wi-Fi® is a registered trademark of the Wi-Fi Alliance. Wi-Fi CERTIFIED™ equipment is the implementation standard for the vast majority of WLANs. See **http://www.wi-fi.org**.

802.11a networks use 5.8 GHz frequencies, while 802.11b networks use 2.4 GHz.

Both 802.11a and b technologies operate in the FCC's unlicensed frequency bands at 5.8 and 2.4 GHz, respectively. While use of these bands is unlicensed, it is regulated and every WLAN device has to comply. Antenna and power emission regulations limit what can be done with the devices.

Largely due to the more limited range of the frequencies used, 802.11a has not been as widely adopted as 802.11b, despite its higher data rates. As a matter of fact, common reference to Wi-Fi hotspots—local access points or base stations with broader network connections—in public transit areas and cyber cafés is usually referring to the slower, lower frequency equipment. Less range means that more access points are needed to cover the same area, leading to higher costs and greater complexity in linking all the devices to a common backbone.

Offering the lower frequency (2.4 GHz) and high data rates (up to 54 Mbps), 802.11g is a later standard now growing in popularity. It is also backwardly compatible to 802.11b. Real throughput is still less than half of the raw data rate and just like 802.11a and b, this latest Wi-Fi technology throttles itself back when faced with interference or weak signals in order to maintain connections.

Outside these factors, 802.11a, b, g networks are very similar in operation. Each uses a very few wideband channels in their respective bands. They move bits of data around the wide channel in a predetermined sequence to improve throughput and resistance to certain types of interference. This process of *direct-sequence spread spectrum* (DSSS) is common to Wi-Fi technologies.

By contrast, the basic 802.11 standard also provides for frequency hopping spread spectrum (FHSS) techniques that operate at lower data rates (1 or 2 Mbps), but which in application offer greater resistance to signal jamming and interference, unintentional or otherwise. Wireless network technologies using 802.11 FHSS are available for public safety use, though are eclipsed by the Wi-Fi juggernaut.

Hedy Lamarr

FREQUENCY HOPPING SPREAD SPECTRUM

In the midst of World War II, communications security was paramount. A little-known patent was filed in 1941 by "H. K. Markey et al"—Hedy K. Markey, better known to the world as the actress Hedy Lamarr—for a system using frequency hopping spread spectrum techniques to code transmissions for radio-guided torpedoes.

Now known to be a particularly robust transmission mode and effective encoding method, spread spectrum techniques never found popularity until long after Patent No. 2,292,387, "Secret Communications System," expired. Lamarr lived to see their popularization in military and commercial technologies.

WIRELESS DATA NETWORKING STANDARDS

The world of wireless standards is wide. Primary data networking standards are established by the IEEE in its 802 series, including:

802.11 – The ubiquitous wireless LAN standards. Wi-Fi equipment and networks are a particular, popular implementation of the IEEE 802.11 standards. Actual TCP/IP throughput is about half of the raw channel rate, which itself is stepped down to maintain connections in weaker coverage areas.

- **802.11a –** Operating at 5.8 GHz, offering up to 54 Mbps raw data rates
- **802.11b** – Operating at 2.4 GHz, offering up to 11 Mbps raw data rates
- **802.11g** – Operating at 2.4 GHz, offering up to 54 Mbps raw data rates and backwardly compatible with 802.11b.

Other 802.11 standards define further implementation details, such as:

- **802.11i** – A 2004 amendment correcting early security vulnerabilities in the Wired Equivalent Privacy (WEP) specification. A subset of this standard was adopted by industry and entitled Wi-Fi Protected Access™ (WPA™).

And next generation technologies are on the horizon here, as well.

- **802.11n** – A developing IEEE standard, occasionally referred to as Next-Gen Wi-Fi, promising higher data rates and greater range with 802.11 backwards compatibility.

802.15 – Standards under development for personal area networks (PANs).

802.16d and e – Developing wireless metropolitan area network (WMAN) standards for faster wireless networks promising greater range and security. Where 802.11 equipment is technically related to its Ethernet forebears, 802.16 is different at a low level, so fundamentally incompatible with WLAN technologies. 802.16e is intended to bring enhancements for mobile access to the networks. The interoperable standard for 802.16 implementations is referred to as WiMAX.

802.20 – Another WMAN standards effort intended to provide broadband wireless access for true vehicular speeds. Formally known as the Mobile Broadband Wireless Access, this standards process is in its early stages and it's expected to be years before compliant equipment is commercially available.

■ WLAN Interoperability

There's a remarkable degree of interoperability with Wi-Fi, making it such a popular technology. A combination of de jure (IEEE) and de facto (Wi-Fi Alliance) standards, openly accessible radio spectrum, and a receptive market caused it to boom. Manufacturers rushed to meet market demand, which in turn brought competitive prices for buyers. It's easy today to pick up a Wi-Fi network access card for less than the monthly cost of a cell phone and use it to connect to the Internet from public access points, often at no cost.

Some public safety WLAN needs can and have been met by no more sophisticated equipment than used by the average cyber café surfer. For example, "parking lot LANs" have been created and police vehicles suitably equipped so that reports, virus software updates, and other sizeable packages of data can be transferred in a reasonable amount of time when the officer gets within range of the station hotspot.

■ WLAN Weaknesses

The beauty of 802.11 wireless LANs is that the technology is readily available and highly developed due to its popularity. However, the technology does have a number of weaknesses.

- **Popularity.** Yep, the strength is also a weakness. Wi-Fi (IEEE 802.11b) hotspots today all compete for the same few slices of 2.4 GHz radio spectrum. Separate networks can operate in the same slice and over the same territory, but physics dictates that they will interfere with one another.
- **Use of unlicensed spectrum.** Popularity is one thing, but unlicensed use of the spectrum makes the WLAN ecosystem a bit of a jungle. Other widespread public, commercial, and industrial use of both 2.4 and 5.8 GHz unlicensed spectrum reduces its suitability for public safety purposes. For example, Wi-Fi networks share the band with cordless phones, microwave ovens, and nanny cams.
- **Security.** Wi-Fi networks have gotten a bit of a black eye for their hack-ability. While this has led public safety agencies toward proprietary adaptations of 802.11 standards, it seemingly hasn't dampened general enthusiasm elsewhere. Network security experts point out that all shared-medium networks, such as basic Ethernet and Wi-Fi, are inherently more vulnerable. Encryption and other security measures have been used for years with wired and wireless networks, alike, to at least protect the privacy of their communications.
- **Mobility.** The 802.11 standard suite wasn't designed for mobile devices that may be moving rapidly in and out of optimal coverage or in and out of range of different network access points. In essence, each Wi-Fi cell is a separate LAN unto itself, using separate network addresses. Even if the WLAN could manage

breaking and making connections each time a user moved from one cell to another, IP-based networks and applications don't deal well with addresses being switched on the fly, potentially several times a minute or more when users operate at cell boundaries. Proprietary extensions to 802.11 standards reduce this to a degree by making the access points "dumb" and moving most intelligence for managing mobility back to the network core. This comes at the cost of less standardization and, somewhat as a result, less interoperability.

■ WLAN Technology in Action

802.11b (Wi-Fi) technologies are preferred for citywide broadband wireless access projects.

Across the United States, municipalities are building wireless LANs to serve their residents, businesses, visitors, and agencies. Large and small cities, alike, see wireless as a means to bridge the "digital divide," keeping less advantaged citizens from the wealth of information and services available in our Connected Age, as well as the means to serve the community broadly. Almost exclusively, Wi-Fi technology is being used to deliver wireless access to users.

Examples are numerous. "Wireless Philadelphia" and San Francisco's "TechConnect" are two of the most expansive initiatives. The City of Philadelphia requested proposals in early 2005 looking for a network to cover its 135 square miles.[90] Later the same year, the City and County of San Francisco followed suit in efforts to cover its 49 square miles. Each specified Wi-Fi, specifically 802.11b or g, recognizing as put by San Francisco, "its ubiquity in user devices, standardization, low cost and ease of provisioning."[91]

Spokane, Newark, and many other jurisdictions across the country are using WLAN technologies to provide broadband data to emergency responders.

Large cities are not the only ones building wireless LAN systems. Police and other emergency agencies across the country are already making use of the technology, if at smaller scales, to connect field staff to information. Examples include Spokane, Washington, which has built a dual-use network with separate segments for public access and emergency agency use. The system covers a 100-block section of the downtown area, providing access for police and fire uses. Across the country, the Newark (New Jersey) Police Department is using a COPS Office Interoperable Communications Technology Program grant to install a broadband wireless network linking multiple policing partners and hospitals around the area.

[90] The Wireless Philadelphia web site has further information. See **http://www.phila.gov/wireless**.

[91] The San Francisco TechConnect web site has further information. See **http://www.sfgov.org/site/tech_connect_page.asp?id=33899**.

Multiagency Wi-Fi networks provide standards-based, shared data communications systems.

In essence and practice, these are standards-based, shared systems. Widely available and compatible technology provides agencies using Wi-Fi networks with a competitive market to keep prices down and service quality up. Broad use outside the public safety market brings innovation and further economies of scale through sharing of infrastructure. Police, fire, and EMS agencies are leveraging the commercial popularity of Wi-Fi technology.

■ Mesh Networking Technologies

Many of the networks mentioned above will be built in the form of *mesh networks*, a form of networking that links together individual nodes to blanket part or all of a jurisdiction with broadband wireless access while providing high reliability and system throughput. According to ABI Research, implementation of citywide wireless networks are expected to be the largest factor in the growth of mesh networks between 2005 and 2010.[92]

The term "mesh network" has come to be used rather loosely in recent years, but properly refers to a network of many nodes, each of which communicates with two or more of its neighboring nodes. End-user network devices, such as a mobile data computer, can access a mesh network and thereby become part of it, but rarely are designed to be part of the mesh fabric itself.

Figure 17-2 depicts a simple mesh network of four access points (AP) that communicate with each other and mobile computers. Each AP maintains a line of communications with all other APs. Traffic received at one AP is passed to the station and, potentially, on to a WAN either directly or through another access point.

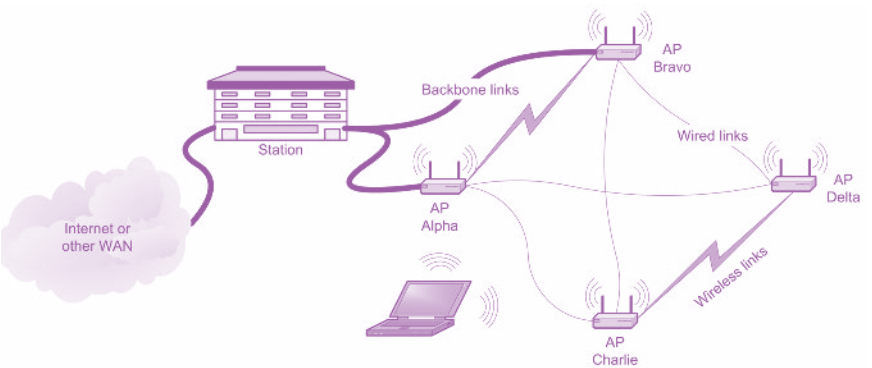


Figure 17-2: Mesh Networking of WLAN Access Points

[92] "Mesh Network Market May See Tenfold Growth in Five Years," ABI Research press release, November 16, 2005. See also **http://www.abiresearch.com/abiprdisplay.jsp?pressid=556**.

Wired or wireless links separate from the WLAN channels provide alternative paths for the traffic to follow. This helps in balancing traffic on the mesh links and provides resiliency in case one of the intermediate APs is lost. Circuits or links that carry masses of traffic from one point to another are referred to as backbone links.

Consider an example. The laptop in Figure 17-2 is depicted as being able to communicate with either AP Alpha or Charlie. This assumes the APs have some share of overlapping coverage, which is common in real-world networks. Under normal conditions, Alpha would serve as the AP of choice since it's closer to the station, network-wise. If it went down for some reason, communications from the laptop could continue through Charlie to Bravo and onto the backbone.

This is a classic, full mesh network. If the individual APs weren't connected to all others, it would be considered a partial mesh. If each was linked directly back to the station, it wouldn't properly be called a mesh, but rather would be said to have a star network topology.

Mesh networking is becoming the rule rather than the exception when multitudes of WLAN access points are used in concert across a jurisdiction. For example, the City of Tempe (Arizona) is building tandem Wi-Fi mesh networks over a 40-square-mile area to serve the public and municipal agencies, independently. Approximately 400 access points will be used to communicate with mobile wireless devices, as well as to route network traffic to backbone networks. Emergency responder vehicles capable of operating on either the mesh network or the city's pre-existing mobile data network will use in-vehicle routers to dynamically choose the optimal network path back to agency servers.

WLANs linked together to MANs today require proprietary technologies to make them appear to users on both the wireless and wired sides as part of a single network. Not to draw too fine a point, but wireless mesh networking is a bit of a frontier itself. As of late 2005, there were no fewer than six companies offering different technologies to bridge WLANs into a common mesh.

Mesh networks commonly use proprietary technologies to link Wi-Fi access points into a common network.

While a lack of standards in this realm may cause interoperability concerns, it should be pointed out that the mesh technology is linking together parts in the background, not at the network level the user sees. In the networks discussed here, any common Wi-Fi-enabled laptop computer could, with appropriate authorization, roam onto the mesh network, find the appropriate channel, and operate regardless of who manufactured the computer or its wireless card.

Wireless local area networks are an increasingly important means of interagency communications. The standardization, popularization, and widespread availability of

Wi-Fi technology, in particular, has opened many broadband wireless opportunities for public safety agencies.

Rent or Own?

WLAN technology is one of several choices available for interagency data communications. Where public safety agencies had only one practical means of connecting mobile users to data sources—building their own networks—an explosion in commercial services has provided viable alternatives for many. With the popularization of consumer wireless data technologies, agencies now have a third, hybrid alternative to build their own networks from technology broadly available outside of the public safety environment.

We've heard heated debates about why one approach to wireless data for public safety agencies is preferable. There are many strong points to be made on either side, but ultimately, the best decision is made by agencies that put technological debates to simmer on the back burner while letting their own *business needs* drive the decision. Those needs and all compromises made will only then properly include consideration of system lifecycle costs, security needs, and operational priorities.

There's no single right choice of wireless technologies. The techniques recommended in this Guide for managing interagency communications projects will lead to the best choice between wireless data technologies for your agencies' particular needs.

The following chart (Figure 17-3) will be useful in balancing needs. Three alternatives are examined:

1. **Build Using Specialized Public Safety Technologies –** Traditionally, wireless data networks used by public safety agencies have been built by the agencies themselves, using niche technologies. Broad consumer and business use of the technologies never existed. Traditional, low-speed mobile data networks are included in this category.
2. **Lease Commercial Services –** Data network services are leased through a wireless carrier.
3. **Build Using Broadly Available Technologies –** Use of widespread wireless data technologies brings a hybrid option to build agency-owned networks from commonly available parts. Wireless LAN technologies are included in this category.

Pros and cons for decision factors and alternatives are provided. The "ratings" indicators include a minus sign (-) for detracting factors, a plus sign (+) for attractive factors, and a check mark (✓) for acceptable compromises.

Wireless Data Communications Rent or Own Decision Factors

	SPEED			AVAILABILITY			RELIABILITY		
	Rating	Pro	Con	Rating	Pro	Con	Rating	Pro	Con
Build Using Specialized Public Safety Technologies	–	No nosebleeds	Data speeds at 1% to 5% of alternatives; improved coding techniques and software yield little relative improvement	+	Coverage designed for agency requirements	Design, construction, and implementation of networks takes time	+	Stable, dependable technologies built for the rigors of public safety use	Capacity is very low relative to alternatives and difficult to increase significantly
Lease Commercial Services	+	The fastest wide-area alternatives are available soonest	Technology turnover brings new user equipment and installation costs	–	Existing networks means systems can be brought up more quickly	Coverage is designed for broader market needs; reduced coverage in rural and isolated urban areas	–	Highest capacity, typically, due to sharing with other users	Capacity is designed for broader market needs; reduced capacity in rural and isolated urban areas; ruggedized user equipment may be required at higher cost
Build Using Broadly Available Technologies	✓	Much faster than traditional, specialized public safety technologies	Turnover of consumer and industry technologies is faster than specialized technologies traditionally used by public safety	✓	Coverage designed for agency requirements	Design, construction, and implementation of networks takes time; coverage is typically spotty compared to traditional networks; wide area coverage is expensive	✓	Capacity designed for agency requirements that can be increased relatively easily	High capacity to meet surge needs requires overbuilding; ruggedized user equipment may be required at higher cost

Figure 17-3: Rent or Own Alternatives and Factors

– = Detracting Factors + = Attractive Factors ✓ = Acceptable Compromises

SECURITY			SUPPORT			COSTS		
Rating	Pro	Con	Rating	Pro	Con	Rating	Pro	Con
✓	Relatively obscure technologies lead to a bit more security	Staples of modern network security, such as Virtual Private Networks (VPNs) and advanced authentication, are difficult or impossible to use	–	Relative reliability of equipment leads to reduced support needs	Heavy reliance on vendors for information, even with internal support		Easily predictable initial costs; long product lifecycles	Limited market for the technology increases initial costs; ongoing maintenance costs can be high, mainly for vendor maintenance contracts, licenses, internal labor, and contracted services
✓	Broadband provides IP and other standards supporting modern network security measures	Common use and widely available information on technologies used increases vulnerabilities	+	Least amount of internal support required; broad usage means there is widely available community support	Lack of internal expertise and support leads to vendor dependence		Predictable costs that may be negotiated and contracted; lowest internal labor costs; other markets find wide-area commercial services cost-effective	Recurring costs, typically monthly; shortest lifecycles for user equipment; most rapid migration of technologies, adding to costs
✓	Broadband provides IP and other standards supporting modern network security measures	Widely available information on technologies used increases vulnerabilities	✓	Wide range of community support	Internal expertise requires continuous study; commercial user technologies are less rugged		Wide availability of technology reduces purchase, operations, and maintenance costs	Ongoing maintenance costs can be high, mainly for labor or services; relatively rapid equipment lifecycles

Figure 17-3, continued

Cost factors vary by implementation. Initial and ongoing costs should be evaluated over comparable system lifecycles and assessed based on requirements met. Absolute dependence on any one or more requirements may lead to acceptance of higher costs.

You'll note that the third alternative, building agency-owned networks from widely used technologies, is considered here a good compromise across the board. It is an increasingly attractive alternative buoyed by a boom in wireless data usage by consumers, business, and industry. Public safety usage was once a large share of the wireless data market, but today is miniscule by comparison. The advantages of long product lifecycles and security through obscurity of traditional mobile data technologies are fading.

■ Leveraging Advantages: Layered Networks

Modern networking technology makes it possible, at a price, to combine the advantages of each of these approaches. The Tempe, Arizona system mentioned earlier is such an example. The ideal is the coverage availability and reliability of traditional public safety wireless data networks combined with the speed, capacity, and suitability for advanced security measures that are supported by commercial services—and, of course, ideally available at the lowest cost over all systems' lifecycles.

Ubiquitous, broadband wireless coverage is economically unfeasible in many jurisdictions. Narrowband, slow-speed data is often the only means to fill in gaps left in higher speed, higher bandwidth, shorter range WLANs.

It is possible to build user devices making use of high-speed WLANs or hotspots, when available, switching to broader coverage, slower MANs between hotspots, and eventually resorting to low-speed WANs as the lowest common denominator. Practically speaking, this requires different radio technology at the lowest levels for each type of network, plus mobile equipment that dynamically chooses the ideal route for each packet of data. That route not only varies by location, but by the speed of the mobile device and other service demands on the broader networks.

The technology to do this is available today. Its use in supporting interagency communications needs is evolving. Networks upon networks are built to serve different needs and practical realities. Since the data networking is almost always provided through core infrastructure—as opposed to directly between units—the wider network, itself, serves as an ever-present gateway to other networks. With adoption of standard wireless and higher-level protocols, such as IP, security and our ability to manage it to serve interagency communications needs becomes a key factor.

Security

Security for data communications networks, wired and wireless alike, necessarily evolves at least as rapidly as the connecting technologies themselves. Threats have grown in direct proportion to the capacity and extent of networks stretching across the globe and deep into societies worldwide. Not only has access to networks by those with malicious and criminal intent grown tremendously, but every insecure networked computer can serve as a naïve accomplice in attacks. Growth in high-speed, always-on connections to homes and small businesses has magnified the risk.

It's easy to maintain secure data communications. Just lock up all computers networked together into a single room, building, or compound, secured electromagnetically to TEMPEST standards,[93] and then control physical access by their users. It's done all the time. It just isn't very practical for the public safety environment, particularly where interagency collaboration is the rule rather than the exception.

Police, fire, and EMS agencies maintaining their own physical or logical networks within or connected to others necessarily have security interests that must be maintained. Some, such as the FBI's Criminal Justice Information Systems (CJIS) Security Policy, are conditions of connecting to other networks. The boundaries between networks, physical and logical, are secured to control access, determine authorities, and provide means of auditing use. Interoperability requires the technical capability to share information within the legitimate constraints of each partner's security needs.

Whether to guard against criminal, terrorist, or nuisance attacks, network security tools continue to grow in sophistication and availability. We will examine some of those tools and their relations to interoperability in a moment. First, let's take a look at a key federal policy shaping law enforcement information systems.

FBI Criminal Justice Information Systems Security Policy

The CJIS Security Policy covers a number of security areas. Those related to interagency data communications are addressed here.

The FBI's National Crime Information Center (NCIC), the original information sharing system for law enforcement agencies, has brought changing needs for data communications security during the past 40 years. As central information repositories, NCIC and its younger siblings such as the Integrated Automated Fingerprint Identification System (IAFIS) originally operated over dedicated, point-to-point communications networks. These systems still connect state and local law enforcement agencies over commercial circuits segregated electronically and logically from other users, but today connect to other networks that are, themselves, widely connected elsewhere. Growing internetworking of all forms has shaped the FBI's CJIS Security Policy.

[93] TEMPEST is a national standard defining limits of unintentional electromagnetic emissions from electronics for security purposes. Endorsed TEMPEST products are required for the most secure telecommunications networks, but are rarely specified for public safety purposes. See also **http://www.nsa.gov/ia/government/index.cfm**.

■ Scope

Established in 1999, the CJIS Security Policy affects all agencies using FBI systems managed by its Criminal Justice Information Services (CJIS) Division. Because the policy is considered *Sensitive But Unclassified*, we'll only cite a couple of elements in passing. State and local agency systems connected to CJIS Division systems are required to adhere to the policy, so affected agencies should have ready access to it through official channels.

Most law enforcement agencies access NCIC and other similar systems through state-level proxies. *CJIS System Agencies* are those agencies with direct connections to CJIS Division systems. Most operate both as primary users of the systems and intermediaries. For example, a state police computer center may be the termination point for a CJIS Division network circuit and, from a relative perspective, the start of a statewide data network for access by its own users and those of other agencies.

For both network and information security purposes, the CJIS Security Policy applies to all users of CJIS Division systems and information from them. Systems and networks not connected to the FBI aren't subject to the policy, but combined networks carrying CJIS, CAD, internal records, and radio system control traffic are increasingly common in law enforcement agencies.

■ Technical Security Requirements

The CJIS Security Policy establishes standard requirements for technical security of connected systems. They include the following:

- Documentation of network configurations
- Use and maintenance of physically secure facilities
- Use of advanced authentication means
- Unique identifiers for all authenticated users
- Standards for network security, including
  - Encryption and its management
  - Internet, wireless, and dial-up access
  - Firewalls
  - Audit trails
  - Virus protection
  - Penetration testing

A full treatment of these subjects is beyond the scope of this Guide; CJIS Security Policy, itself, is the definitive statement. The FBI CJIS Division and each CJIS System Agency has a designated Information Security Officer (ISO). Check with the ISO

responsible for your agency with questions about requirements for data networks carrying CJIS Division information.

Since interagency communications can be affected by these requirements, we want to address a few from the standpoint of interoperability. A couple of basic principles of the CJIS Security Policy should be kept in mind for that discussion.

1. Different technical security requirements exist for public or shared networks than for those entirely under the control of a criminal justice agency. Networks with components in nonsecure locations or which pass through public network segments require special authentication and encryption measures.
2. The 5 years from September 30, 2005 to September 30, 2010 is a transitional period for CJIS security requirements. Systems purchased or upgraded after the earlier date are subject to higher user authentication and encryption requirements. After the later date, all systems accessed from nonsecure locations or across public network segments must meet the higher requirements.

In essence, the distinction between secure and nonsecure locations and networks revolves around management control. Systems and networks entirely under the control of a criminal justice agency are considered secure. General governmental networks, the Internet, and telephone dial-up access are all examples of nonsecure networks presumed more susceptible to compromise by unauthorized individuals.

■ Interoperability

New connections between, for example, two local agency systems already subject to the policy don't necessarily bring added security requirements. However, interconnections made across networks managed by others likely do need additional security measures.

For example, consider a county sheriff's office and a municipal police department that are independent users of a state criminal justice network that provides their NCIC access. Each is subject to relevant parts of the CJIS Security Policy. If the two agencies chose to connect their internal, secure networks to share CJIS information over a general-use municipal or county government network, that connection would be subject to the same CJIS security requirements. This might occur if the two agencies wanted to exchange calls for service between their respective CAD systems that contain NCIC records information. The solution would be to secure the connection across the noncriminal justice network according to CJIS Security Policy, for example, by using a *virtual private network* (VPN) "tunnel" between the agencies.

Wireless data networks are given special treatment by the CJIS Security Policy.

Wireless data networks are given special treatment by the policy due to the ease by which RF signals can be intercepted. While encryption and security requirements are significant and must be observed on wireless networks of affected agencies, the practical effect of the policy on interagency data communications is the same, whether wired or wireless. This is because the interconnection of two wireless networks operated under the policy is handled just like the example above. Similarly, a single wireless network shared by multiple agencies, some CJIS users and some not (e.g., by police, fire, and EMS), must have its CJIS traffic encrypted and authenticated just as it would have to be over the Internet or other common-use network—say through the use of a VPN.

Securing interagency data networks is more of a management than a technical challenge.

The process of operating interagency data networks brings challenges due, in large part, to the added coordination needed between agencies for common management of encryption and advanced authentication. It's simply harder for multiple agencies to coordinate management of the complex technologies, sharing control and authority. This is true in any multiagency security process; it's not a unique effect of the CJIS Security Policy.

* * *

If information sharing is the product of interoperability, then FBI CJIS Division systems are a cornerstone of the process. From a data communications standpoint, the common need of criminal justice agencies nationwide to uphold the CJIS Security Policy means its provisions are a de facto standard. The FBI's longstanding Advisory Policy Board (APB) guides policy, assuring it meets federal, state, and local security requirements.

Common conventions, standards, and means of interfacing systems provide for interoperability of data communications. However, greater security requires more coordination and planning to assure interoperability, otherwise mechanisms to prevent unauthorized access can be barriers between those who would otherwise cooperate. For example, encryption will deny information access to anyone without the keys, seeking to use it illegitimately or just without adequate prior coordination.

Fortunately, the CJIS Security Policy is maintained and managed in part to provide this very coordination.

Securing Data Networks

Standard technologies for securing data networks are equally applicable to public safety. The primary tools of the trade are virtual private networks and firewalls. Both bring interoperability implications since their whole purpose is to restrict access.

■ Virtual Private Networks

Virtual private networks (VPNs) are a workhorse of modern data communications security because they provide the means to secure a substream of data across a more broadly used network. The name alone pretty well describes their purpose.

VPNs can be implemented in hardware, in software, or most commonly through a combination of both.

VPNs can be implemented in software, hardware, or most commonly through a combination of both. They are used over many different types of data networks, too. Physically, all types of wired and wireless networks are supported, most typically using Internet Protocol (IP) standards that are largely oblivious by design at this level to the type of physical connection or media over which they're running.

The important issue from an interagency data communications standpoint (the topic of this chapter!) is mainly the "V" part of VPN—their virtual nature. Much as with trunked radio systems and their talkgroups, a VPN is a virtual channel within a larger network. Granted, the "P" part (private) may be important or even critical to the virtual channel (network) users, but if so, that's probably true whether or not interagency communications are being carried.

In attempting to understand VPNs, it's useful to picture a tunnel between two networks through a third. For our simple purposes, picture two relatively secure, agency-operated networks using the Internet or common-use municipal network to hook up. Properly implemented, the secured border crossing points between each agency and the common network can be connected by a tunnel that looks open from either end, but inaccessible from the middle. See Figure 17-4.

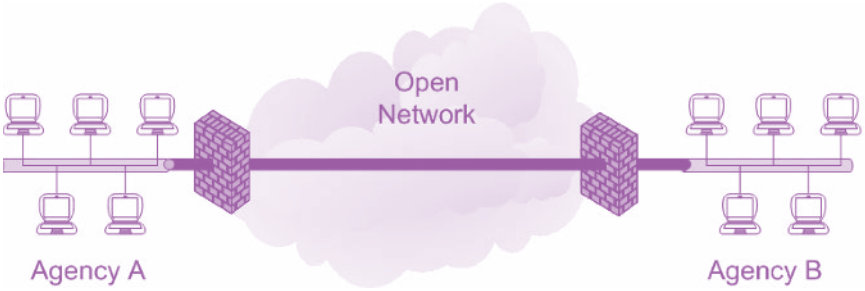


Figure 17-4: VPN Tunnel Between Agency LANs.

Advanced authentication techniques are generally used with VPNs. The techniques assure that the VPN only gets connected for authenticated users. Typically, a combination of a password and encryption certificate stored on the computer or in a device that can be connected to the computer serve to prove that a legitimate access attempt is being made. As with the VPN software, hardware configurations, and system permissions, user authentication has to be managed to provide interoperability across jointly connected data networks. The alternatives are undesirable: Either no access or networks with big security holes in them.

■ Firewalls

The device at each network border depicted in Figure 17-4 is a firewall. A firewall is simply a device that sits at the junction point between two or more networks. This diagram is a bit of a simplification because there is typically more networking equipment, but recognize that the firewalls are the means to control traffic crossing network borders.

Firewalls can vary greatly in complexity and cost. They also can provide an end point for VPN connections.

The simplest firewall is a small computer with two network interfaces and software controlling what passes in which direction. Firewalls grow in complexity, up to enterprise-grade devices that may have dozens of physical networks attached and allow tens of thousands of individually encrypted VPN sessions.

And this brings us back to the point of interoperability. For purposes of interagency communications, firewalls can be an impediment. Most assuredly, they are a basic building block for secure data networks, but they can and do impede interagency communications if not managed to provide the capability.

An example of how firewalls are used may be helpful in understanding the interoperability impact. Consider the two agency LANs in Figure 17-4, each with its own firewalls. The firewalls are configured to block LAN file server and printer traffic from passing, while allowing Simple Mail Transfer Protocol (SMTP) connections to pass packaged fingerprint images.

Firewalls are typically configured to deny all traffic passing from the "untrusted" outside network to the "trusted" inside.

Before being activated, firewalls are loaded with rules defining what data may pass in which direction. For security purposes, they are typically configured to deny everything by default from the "untrusted" outside network to the "trusted" network inside. Akin to Mikey in a classic breakfast cereal commercial, they don't like anything and refuse to pass it. One-by-one, specific rules are added to customize the firewall. As may be imagined, the firewall has to be configured accordingly to provide the needed interagency communications, in our case, without opening up the connected networks to all forms of virulence and pestilence.

Obviously, this takes coordination between network uses on either side, and a degree of trust. It's not uncommon for two secure networks to be connected with firewalls back-to-back—one being managed by each of the agencies and likely sharing similar security profiles and traffic rules (in reverse). While this may seem like a waste of a good firewall, the fact of the matter is that it allows each party in the arrangement to control its own border, just like nations do with their own physical borders.

■ Other Network Security Devices

Network security is an important, dynamic field. A multitude of techniques and tools are used to protect individual and multiagency networks. Other tools include active *intrusion prevention systems* and more passive *intrusion detection systems*.

Security has to be carefully managed to avoid it acting as a barrier to interoperability.

Any network subsystem that has the potential to shut down communications has an interoperability dimension. Whether through the security of VPNs, firewalls, or other subsystems, the intended communications can only proceed reliably if agency needs are clearly identified, articulated, and documented to assure the technology serves its purposes. Security doesn't need to be compromised to allow agencies to share information, but it has to be carefully managed to avoid it acting as a barrier.

On The Horizon

Rapidly developing technologies and standards mean that public safety agencies have greater and greater data networking capabilities to look forward to. The most exciting developments (and interest) has been in wireless networking.

Wireless Metropolitan Area Networks

WiMAX is the popular name for 802.16 wireless metropolitan area network implementations standards.

Standards development organizations in the United States and worldwide are working to tame the latest wireless frontier: High-speed data networks spanning greater distance, supporting truly mobile users who may move through and across cells of coverage at vehicular speeds consuming bandwidth at rates unseen today. Wireless Metropolitan Area Networks (WMANs) are the current frontlines in standards development.

The term "WMAN" implies more expansive networks and this is, indeed, the intent of standards developed for them. In 1999, the IEEE formed its 802.16 Working Group on Broadband Wireless Access Standards. The evolving series of standards, known as WiMax, are expected to define faster, more robust broadband wireless access techniques that will extend current wireless LAN technologies. [94]

[94] For further information, see **http://www.ieee802.org/16/**.

The first WiMAX standard is for fixed point-to-point wireless networks.

The first WMAN standards released defined how fixed points are linked together with compliant technology. Others in the series that are under development provide definition for mobile uses, particularly intending to overcome Wi-Fi limitations.

In 2001, the WiMAX Forum was created by interested industry parties to bring common implementations of the diverse set of options within 802.16 standards, commonly known today as WiMAX.[95]

Broadband Wireless Access for Public Safety

The 4.9 GHz frequency band was allocated by the FCC for exclusive public safety use.

Public safety agencies have had to adapt to commercial and popular use technologies to get broadband (multimegabit per second) wireless networking in the past. Increasing availability of spectrum in the vicinity of that used for 802.11a Wi-Fi promises to bring the power of mass markets and broad standards to bear on police, fire, and EMS needs for broadband wireless access.

In 2002, the FCC allocated 50 MHz of spectrum in the 4.9 GHz band for public safety use.[96] The amount and location of the spectrum were important because they allow for the development of broadband wireless equipment to meet public safety needs for ruggedness and reliability, but which could be largely based on more popular commercial technologies, bringing economies of scale to keep costs low. For example, 802.11a Wi-Fi operates in the nearby 5.8 GHz band. With minor changes, popular consumer and industrial technology can be adapted to operate in the exclusive public safety band, offering greater security and reducing competition for the airwaves.

WLANs in the 4.9 GHz band will require more access points for the same coverage as 802.11b Wi-Fi networks.

In practice, 802.11a-based WLANs require much more infrastructure, such as wireless access points, than do 802.11b/g ones. This is due to the transmission characteristics of the different frequency bands used—5.8 versus 2.4 GHz.

How much of a difference in coverage is there? Studies show that the lower frequency signals are 100 to 1,000 times stronger in foliage, 10 to 100 times stronger through common building materials, and 5 to 10 times stronger filling in gaps in the open

[95] The WiMAX Forum is a nonprofit association formed by manufacturers to ensure interoperability of IEEE 802.16-compliant equipment and networks. See **http://www.wimaxforum.org**.

[96] For further information on the FCC's actions, see "Public Safety's New Allocation – Answering Users' Questions on the 4.9 Gigahertz Band," available from SAFECOM at **http://www.safecomprogram.gov/SAFECOM/library/spectrum/1088_publicsafetys.htm**.

beyond the line-of-site of transmitters.[97] Optimistic estimates are that twice as many access points are needed at the higher frequencies to provide the same level of coverage, while less optimistic ones suggest 5 to 10 times as many are needed

Public safety agencies will build jurisdiction area networks (JANs) in the 4.9 GHz band using mesh and other networking topologies, but it's likely the technology will be used mostly for campus and incident area networks in the near term.

Wideband Wireless Standards for Public Safety

The public safety 700 MHz band will have 120 paired wideband channels and another 18 designated exclusively for interoperability.

Outside the traditional VHF, UHF, and 800 MHz bands with their narrow voice channels, the 700 MHz band offers some hope for high-speed data. The band is to be transitioned to public safety use as incumbent broadcasters move to digital television (DTV) technologies. FCC regulations[98] provide 120 paired channels (base and mobile), each 50 kHz wide, that can be combined for greater bandwidth.

An additional 18 paired channels in the 700 MHz band are designated specifically as *wideband interoperability channels* that can be combined in groups of three for up to 150 kHz of bandwidth—the equivalent of a dozen Project 25 channels. Thus combined, six wideband interoperability channels will be available as the spectrum is cleared and 700 MHz Regional Planning Committees[99] complete their work.

Tests have shown the potential of high-speed technologies built specifically for public safety use. Technologies used in a 2001 experimental pilot conducted by Pinellas County, Florida yielded raw data rates pushing 460 Kbps in 150 kHz channels.[100] Following these tests, the Telecommunications Industry Association (TIA) published TIA-902, a standard since recommended to the FCC by its Public Safety National Coordination Committee (NCC) and the National Public Safety Telecommunications Council (NPSTC).

At the time of this writing (late 2005), FCC action on recommended standards for wideband use of 700 MHz channels was pending and considered imminent. A decision was anxiously awaited because FCC rules prevent licensing and use of wideband interoperability channels until it has adopted a standard for their use.

---

[97] Dobkin, Daniel M., *RF Engineering for Wireless Networks: Hardware, Antennas, and Propagation* (Burlington, MA: Newnes, 2004).

[98] 47 CFR Chapter I, § 90.533(c).

[99] The FCC maintains a web page addressing public safety 700 MHz public safety spectrum and the regional planning process. See **http://wireless.fcc.gov/publicsafety/700MHz/**.

[100] See the Public Safety Wireless Network report available from SAFECOM, **http://www.safecomprogram.gov/SAFECOM/library/technology/1033_GreenhouseProject.htm**.

NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL (NPSTC)

The NPSTC is a federation of public safety organizations. It is very active in wireless regulatory matters, standards development, and support for statewide interoperability committees.

Project MESA

Project MESA seeks to address both operability and interoperability aspects of broadband wireless data for public safety.

Project MESA, also known as the Public Safety Partnership, began as another in the Association of Public-Safety Communications Officials – International, Inc.'s (APCO) respected series of projects shaping the world of public safety communications. As Project 25 proceeded to define the standard for public safety digital voice communications, an ambitious project to do the same for data began life as APCO Project 34 in 1995. Interest in the effort grew, eventually becoming international in scope. During a series of meetings in Mesa, Arizona it was adopted as a joint project of the North American-based TIA and the European Telecommunications Standards Institute (ETSI). It has been known as Project MESA since.[101]

Project MESA seeks to address both operability and interoperability aspects of broadband wireless data for public safety. That is, much like Project 25, resultant standards will affect communications within and between agencies. It will most likely not result in the production of new types of electronics and low-level engineering protocols as did P25.

Where public safety makes up a sizeable share of the two-way wireless voice world, its use of wireless data is increasingly insubstantial as a share of the total. Public safety agencies will increasingly use more generalized commercial technologies for wireless data networking due to relatively gigantic leaps in capabilities being made available and dramatically dropping costs of equipment sold in great volumes. Broadband public safety networks will be built of generally commercialized electronics, customized at high network protocol layers for its unique needs.

Project MESA will most likely provide standard implementation profiles for public safety use of commercially available broadband wireless technology, much as the Wi-Fi Alliance and WiMAX Forum serve, rather than technology standards.

[101] See **http://www.projectmesa.org**.

Standards: A Necessary, But Insufficient Condition

Rich technical standards provide enough options that divergent implementations can preclude interoperability.

Late into this Guide, it probably comes as no surprise that we're advocates of standards for everything from training to technology. The wireless communications world has demonstrated particularly well how standards—particularly complex technological standards—are the first step toward interoperability. However, we've learned with Project 25, as well as the broader world has learned through WLAN implementations, that the plethora of options available under reasonable standards leads to divergent implementations of the technologies—and a lack of interoperability.

The Wi-Fi Alliance and WiMAX Forum previously mentioned were formed expressly to bring interoperability for implementations of IEEE 802.11 and 802.16 standard technologies, respectively. Early WLAN products operating well within IEEE 802.11 standards were not interoperable between manufacturers.

Wireless LANs didn't take off until a subset of 802.11 standards was settled on.

The WLAN market didn't take off until the Wi-Fi Alliance created a "meta-standard" narrowing the range of implementation options for 802.11 technologies and a process to certify Wi-Fi compatible products. As expected, this process brought critical mass to the market. Today, Wi-Fi, with all its compromises that reduce options across a well-considered standard, is being used around the world from coffee shop hotspots to public safety mesh networks.

The WiMAX Forum was created with forethought to assure interoperability. The success of those efforts in bringing broad standardization to WMAN implementations is yet to be seen, but the market is bound to be further advanced through them than it would have been otherwise.

P25 (TIA/EIA-102) is a rich set of standards that can be interpreted and implemented in different ways.

In the public safety arena, debate continues in the digital voice realm about which elements of the broad set of standards known as P25 (TIA/EIA-102) must be implemented for interoperability. And because P25 is frequency-band agnostic, even use of its fundamental standard—the Common Air Interface—doesn't guarantee that radios can talk to each other if they're operating in different bands. We expect similar interoperability questions to be raised in implementation of TIA-902 wideband standards for public safety data communications. Development of conformance tests is key to the practical use of both voice and data standards.

This important debate can't be done adequate justice here, but suffice it to say that broad standards alone are not sufficient to guarantee interoperability in the technical realm. Further implementation standards are inevitable.

Epilogue

Through wired and wireless networks, carrying voice and data, communications interoperability is built as a complex system of systems. While technology is an inescapable piece of the interoperability puzzle, it alone cannot solve the problem, for it will be forever impossible to build a complete system without human management, operations, and procedural subsystems being integrated far in advance.

SEARCH has been privileged to work with agencies large and small across the country under U.S. Departments of Justice and Homeland Security programs that provide assistance to improve interagency communications among first responders. We've seen great need for resources—human, financial, and technological—to solve this puzzle, but we've also seen growing cooperation among responders from all disciplines and levels of government.

Our intention in creating this *Communications Interoperability Tech Guide* was to share best practices in project planning, procurement, and implementation, as we've come to understand them through agencies making a difference in their own jurisdictions. We're confident that the best practices in this Guide will improve the odds of your project's success.

And, if you need help along the way, we'll be there to support you with technical assistance resources.