Understanding Wireless Communications in Public Safety

A Guidebook to Technology, Issues, Planning, and Management

Written by:
Kathy J. Imel and James W. Hart, P.E.

Additional material for the second edition contributed by:
John Powell, Tom Tolman, and David Funk

For:
The National Law Enforcement and Corrections Technology Center
(Rocky Mountain Region)
A Program of the National Institute of Justice

First Edition: March 2000
Revised: August 2000
Second Edition: January 2003

Points of view are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice. This document is not intended to create, does not create, and may not be relied upon to create any rights, substantive or procedural, enforceable by any party in any matter civil or criminal.

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #96–MU–MU–K011 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

TABLE OF CONTENTS

The National Law Enforcement and Corrections Technology Center–Rocky Mountain ix

Acknowledgments ix

Introduction 1

Part 1. Planning and Managing a Communications Project 3

Chapter 1. What It Takes to Succeed 5
A Plan 5
Time, Money, and Resources 5
Getting Started 6
What Do You Have Now? 6
What Do You Need? 6
What Are Your Options? 7
How Much Will It Cost? 8
How Do You Implement the Project? 9
Getting Help 9
Other Agencies 9
Consultants 9
Vendors 10

Chapter 2. Planning the Project 11
Realistic Schedule 11
Project Team(s) 11
Project Manager 12
Responsibility 12
Authority 12
Time 12
Management Support 12
Physical Resources 12
Other Team Members 12
Budget 13

Chapter 3. Obtaining Funds 15
Types of Funds 15
Sources of Funds 15
Federal Sources 15

Motorola Solutions, Inc., Ex1017, p. 3

Block Grants 17
Discretionary Grants 17
Federal Asset Forfeiture Funds 17
State Sources 18
Local Sources 18
Single Agency Versus Multiple Agencies 19
"Selling" Your Need 19
Getting Help 20

Chapter 4. Buying What You Need 23
How to Buy 23
Competitive Procurement 23
Noncompetitive Procurement 23
Sole Source Procurement 24
Contract for Operational Services 24
Cooperative Purchasing 24
Western States Contracting Alliance 24
Leasing 25
Outsourcing 26
Request for Information (RFI) 26
Competitive Procurement (RFP) 26
Request for Proposal (RFP) 27
RFP Process 27
Develop the RFP 27
Issue the RFP 28
Evaluate Responses 29
Select Vendor 30
Negotiate Contract 30
Manage the Project 31
Acceptance Testing 32

Part 2. Wireless Communications Technology 33

Chapter 5. Voice Versus Data 35
Voice Versus Data 35
Analog Versus Digital 36
Analog Radio Systems 37
Digital Radio Systems 37
Transmission Differences 38
Encryption 39

Chapter 6. Characteristics of Radio Systems 41
Understanding Radio Terms 41
Wave 41
Wavelength 42

Motorola Solutions, Inc., Ex1017, p. 4

Cycle 42
Frequency 42
Spectrum and Bands 43
Public Safety Bands 44
Channels 44
Mobile Radio System Frequencies 46
Frequency Selection Considerations 46
Coverage 46
Building Penetration 46
Skip 47
Noise 47
Antenna Size 47
Transmitters and Receivers 47
Transmitters 47
Receivers 48
Antennas 50
Antenna Gain 50
Types of Antennas 52
Base Station Antennas 52
Directional Antennas 52
Mobile Antennas 53
Portable Antennas 53
Smart Antennas 54
Effective Radiated Power (ERP) 55
Interference 55
Radiation 56
Local Regulations Controlling Antennas 56
Radio Coverage 56
Duplexers, Combiners, Multicouplers 58
Duplexers 58
Combiners 59
Multicouplers 61
Multiple Access Systems 61
Frequency Division Multiple Access (FDMA) 61
Time Division Multiple Access (TDMA) 62
Code Division Multiple Access (CDMA) 62
Frequency Hopping 63
Direct Sequence 63
Packaging Data 63

Chapter 7. Current Public Safety Radio Systems 65
Paging Systems 65
Short Messaging Systems (SMS) 66
Two-Way Simplex Radio Systems 66
Two-Way Mobile Relay Systems 67

Motorola Solutions, Inc., Ex1017, p. 5

Repeater Innovations 68
Mobile Repeaters 69
Trunked Radio Systems 69
Specialized Mobile Radio (SMR) 71
APCO Project 16 Trunked Radio System 72
Project 25 Digital Trunked Radio System 72
TErrestrial TRunked RAdio (TETRA) 74
220 MHz Narrow Bandwidth Band 74
Cellular Radio/Telephone Systems 75
Personal Communications Systems (PCS) 77
Cellular Digital Packet Data 77
Point-To-Point Microwave Communications Systems 78
Microwave System Engineering and Licensing 79
Wireless Local Area Networks (WLAN) 80
802.11b Networks 81
Wireless Local Links - Bluetooth 83

Part 3. Wireless Communications Issues 85

Chapter 8. FCC Licensing, Rules, Regulations, and Related Issues 87
Licensing 87
FCC Rules and Regulations 88
Part 90 88
Docket 92-335 88
Part 22 88
Part 24 89
Part 101 89
Refarming 89
Frequency Reallocation 89
Computer Assisted Pre-coordination Resource and Database (CAPRAD) 91
4.9 GHz Band 92

Chapter 9. Tower Siting and Radio Frequency Electromagnetic Radiation Exposure 95
Towers 95
Radio Frequency Electromagnetic Radiation Exposure 96

Chapter 10. Federal Government and Other Initiatives 99
NCIC 2000 99
Public Safety Wireless Network (PSWN) 100
Program Overview 100
The National Institute of Justice and Its Interoperability Program 101
Advanced Generation of Interoperability for Law Enforcement (AGILE) Program 101
Developing Interoperability Standards for Public Safety 101
Integrating, Testing, and Evaluating Interoperability Technology 102
Raising Awareness of Interoperability 102

Motorola Solutions, Inc., Ex1017, p. 6

Mobile Broadband for Emergency and Safety Applications (MESA) 102

Chapter 11. Interoperability 105
Three Types of Interoperability 105
Interoperability Obstacles 108
Interoperability Solutions 108
Classes of Systems 108
Conventional Systems 108
Analog Trunked Systems 109
Project 25 Digital (Conventional or Trunked) 109
Infrastructure-Based Patching 109
Cost 109

Part 4. Wireless Communications Options 111

Chapter 12. Voice Systems 113
Dedicated Radio Systems 113
Sample Vendors 113
E.F. Johnson Division of EFJ, Inc.. 113
M/A-COM Division of Tyco International. 114
Motorola, Inc. 114
Advantages of Dedicated Systems 115
Disadvantages of Dedicated Systems 116
Cellular and PCS Radio 115
System Coverage 116
Pricing 116
Sample Vendors 117
AT&T Wireless Services. 117
Cingular Wireless. 117
Sprint. 117
Verizon Wireless. 117
Advantages of Cellular/PCS Radio 117
Disadvantages of Cellular/PCS Radio 118
Voice—SMR/ESMR 118
A Special Case: Conventional Radio System for the Township of Upper St. Clair, Pennsylvania 119
Sample Vendor—Nextel 119
System Coverage 120
Pricing 121
Sample Vendor—Lower Colorado River Authority 121
Advantages of an SMR/ESMR System 121
Disadvantages of an SMR/ESMR System 121

Chapter 13. Wireless Data Systems 123
Cellular Digital Packet Data (CDPD) 123

Motorola Solutions, Inc., Ex1017, p. 7

Sample Vendors 123
AT&T Wireless 124
Verizon Wireless 124
Advantages of CDPD 124
Disadvantages of CDPD 125
General Packet Radio Service (GPRS) 125
1XRTT Service 126
Private National Data Networks 127
Sample Vendors 127
Motient Wireless Data Network 127
Cingular Wireless (formerly RAM Network) 127
Advantages of Private National Data Networks 128
Disadvantages of Private National Data Networks 129
Regional Voice and Data Systems 129
Sample Vendor 129
RACOM 129
Advantages of Regional Voice and Data Systems 130
Disadvantages of Regional Voice and Data Systems 131

Chapter 14. Latest Developments 133
Mobile Satellites 133
Voice Communications Satellites 133
Example System—Iridium 133
Other Voice Satellite Systems 136
Data Communications Satellites 137
High Altitude Long Endurance (HALE) Platforms and High Altitude Platforms (HAPS) 138
Ultra Wide Band (UWB) Devices 139
Software Defined Radio (SDR) 140
Voice Over Internet Protocol (VoIP) 141
Motorola Greenhouse Project 143

Summary 145

Glossary and Acronyms 147
Glossary 149
Acronyms 153

Appendixes 157
Appendix A. State Agencies Administering Byrne Program Grants 159
Appendix B. Resources 163

Motorola Solutions, Inc., Ex1017, p. 8

The National Law Enforcement and Corrections Technology Center–Rocky Mountain

The National Law Enforcement and Corrections Technology Center (NLECTC) system was created in 1994 as a component of the National Institute of Justice's (NIJ's) Office of Science and Technology. NLECTC's goal, like that of NIJ, is to offer support, research findings, and technological expertise to help State and local public safety personnel do their jobs safely and efficiently.

NIJ's NLECTC system consists of facilities located across the country that are co-located with an organization or agency that specializes in one or more specific areas of research and development. Although each of the NLECTC facilities has a different technology focus, they work together to form a seamless web of support, technology development, and information to help the public safety community.

Located at the University of Denver, NLECTC–Rocky Mountain focuses on communications interoperability and the difficulties that often occur when different agencies and jurisdictions try to communicate with one another. This facility works with public safety agencies, private industry, and national organizations to implement projects that will identify and field test new technologies to help solve the problems of interoperability. NLECTC–Rocky Mountain also houses the newly created Crime Mapping Technology Center, the training and practical application arm of NIJ's Crime Mapping Research Center. The Rocky Mountain facility also conducts research into ballistics and weapons technology, as well as information systems.

Acknowledgments

The authors wish to acknowledge and thank the following individuals and organizations for their invaluable guidance and assistance in the preparation of this guidebook:

The staff at NLECTC–Rocky Mountain: Thomas Tolman, Robert Epper, Gene McGahey, David Funk, Joni Morris, Courtney Klug, Laura Lippman, and Sue Kaessner.

For providing background information and materials: Patrick Hobby and Barb May (Motorola), Stephen Ruskin (Ericsson), Robert Kuch (Nextel), Doug Daniels (AT&T Wireless), Larry Krenek (LCRA), Mark Minnick (San Marcos PD), and Gregg Miller (RACOM).

Our advisory panel, for the first edition: Scott Snyder (Longmont Fire Department), Terri Thornberry (Durango/La Plata Communications), Frank Bishop (Greeley/Weld Communications), Mary Moore (Fort Collins Communications), Mike Borrego (State of Colorado Telecommunications), Scott Morrill (Gunnison Communications), Ed Connors (Denver Police Department), and Emery Reynolds (Arapahoe County Sheriff's Department).

Our Advisory Committee, for the second edition: Steve Cooper (Denver Police Department), Tony Davidson (Atlanta Fire Communications), Doug Edmonds (Northwest Central Dispatch), Chris

Fischer (Valley Communications), Chris Hellewel (Spillman Technologies), Charlie Hoffman (NTIA), Ted Jacoby (Seattle Police Communications), Andy MacFarlane (Phoenix Fire Department), Rick Murphy (PSWN), Joe Peters (Sheriff's Association of Texas), Tom Raabe (Loveland Police Communications), Emery Reynolds (Arapahoe County Sheriff's Department), Tim Skalland (Shasta Area Safety Communications Agency), Ray Smith (Ohio Regional Planning Coordinator), Tim Walters (InfoTech Marketing).

Author Contacts:

Kathy J. Imel
La Loba International, Inc.
(p): 303–438–9565
(f): 303–438–1244
E-mail: kjimel@aol.com

James W. Hart, P.E.
Hartech, Inc.
(p): 303–795–2813
(f): 303–347–2652
E-mail: jhart@du.edu

NLECTC–RM Contacts:

Tom Tolman
(p): 303–871–4190
(f): 303–871–2500
E-mail: ttolman@du.edu

Gene McGahey
(p): 303–871–7453
(f): 303–871–2500
E-mail: gmcgahey@du.edu

To order additional copies of this document, please call NLECTC at 800–248–2742, or download a copy from the World Wide Web site at www.nlectc.org.

Motorola Solutions, Inc., Ex1017, p. 10

INTRODUCTION

The National Law Enforcement and Corrections Technology Center (NLECTC) system was conceived with the idea of helping public safety personnel understand and use new technology. In keeping with that goal, NLECTC–Rocky Mountain developed this guidebook to help unravel the confusing issues, terms, and options surrounding wireless communications, particularly as it involves commercially available communications services.

The target audience consists of those middle and upper managers who are responsible for funding and/or managing communications at their agencies, but who have little or no technical background in wireless technology.

This guidebook is divided into four parts:

Part 1. Planning and Managing a Communications Project: Discusses the overall scope of a project, including planning, funding, procurement, and management.

Part 2. Wireless Communications Technology: Discusses voice versus data, characteristics of radio systems (including terminology), and current types of public safety radio systems.

Part 3. Wireless Communications Issues: Discusses Federal Communications Commission (FCC) licensing, rules, regulations, and related issues; tower siting and radio frequency radiation exposure; various Federal and other group initiatives; and interoperability.

Part 4. Wireless Communications Options: Discusses voice system options, data system options, and some of the latest developments in communications technology.

Each section can be read separately from and independently of the others. If all you want to know is what your options are, go directly to part 4. However, if you are not familiar with how the various wireless options work and the terms used, you may first want to read part 2.

No one book can possibly cover everything you might ever need to know if you are planning a communications project. However, the authors will at least try to highlight the main issues and explain the terminology so that you can be an informed consumer. In addition, the authors have tried to point you toward other resources that will provide more detail about areas you want to understand better.

At various places in the document, you will find highlighted information and/or suggestions to make things go a little quicker or easier for you. Those tips are placed in boxes like the one to the right.

☞ Try this...

Find statistics about wireless carriers at CTIA's Web site:

http:/www.wow-com.com

Motorola Solutions, Inc., Ex1017, p. 11

At the end of the document is a glossary of common wireless terms, as well as a list of the acronyms you may run into. (Note: The number of terms and acronyms used in this industry is *huge*. For the sake of brevity, only the most common are included.)

If, after you have read this guidebook, you still have questions or need help, contact NLECTC–Rocky Mountain by phone at 800–416–8086 or 303–871–2522 in the Denver area or via the Internet at nlectc@du.edu.

PART 1

PLANNING AND MANAGING A COMMUNICATIONS PROJECT

Part 1 gives an overview of the steps involved in a communications project. Chapter 1 discusses the steps needed to be successful. Chapter 2 covers the planning process. Chapter 3 identifies various potential sources of funding for projects of this type. Chapter 4 goes through the procurement process itself, with details for those who have never been involved in a large-scale competitive procurement.

For those who have managed projects before, who already have identified funding, or who are familiar with purchasing requirements, you may want to skip part 1 and go directly to part 2.

Motorola Solutions, Inc., Ex1017, p. 13

Chapter 1

What It Takes to Succeed

Successful projects are usually the result of careful planning. Planning helps to create a disciplined, businesslike approach to the project and fosters communication among groups, often resulting in partnerships.

A Plan

The first step in planning is to gather information about agency needs, available assets and resources, existing communications infrastructure, end-user requirements, and other related issues.

A plan is important because it defines the project's goals, describes the specific problems or needs that are being addressed, lists any potential partners and their roles, identifies staffing requirements, outlines a marketing strategy, proposes a detailed budget and time line, and includes an operational plan that addresses how the project will be funded now and into the future.

A good plan should list all tasks, including flowcharts, schedules, and task budgets. A number of software programs, particularly project management software tools, are available that help make creating and maintaining these much easier.

Time, Money, and Resources

No project can succeed without adequate amounts of time, money, and other resources. Thus, to be successful, time must be allocated to:

- ➡ Identify, recruit, and assign or hire necessary staff.
- ➡ Identify potential project partners and create formal relationships.
- ➡ Identify potential sources of funding and apply for funds.
- ➡ Identify and procure appropriate communications technologies.
- ➡ Implement the project.

The following sections in part 1 will discuss the issues of time, money, and resources in more detail.

Motorola Solutions, Inc., Ex1017, p. 15

Getting Started

Before going forward on a communications project, you will need to answer a number of questions. While collecting the information may seem tedious, you will be well rewarded down the line when you find that you are asked to provide this same information to potential funding sources, management, and others.

What Do You Have Now?

One of the first things you need to identify are your existing business functions. In other words, answer the questions:

- What do we do?
- How do we do it?
- What are our core functions?
- How does or will technology support those functions?
- What are your interoperability needs with other agencies?

Plus, you should try to identify the benefits of such a project, both the tangible, measurable benefits (decreased maintenance costs, improved coverage, etc.) and the intangible benefits (improved morale, better customer service, etc.).

In addition, you should make an inventory of all of your existing communications hardware and software and FCC-issued radio licenses. The inventory should include as many of the following as possible:

- Quantity.
- Manufacturer, make, model (or version number of software).
- Year of installation/purchase.
- Year last upgraded.
- Frequency of use.
- Purpose (what it is used for).
- Location.
- Owner (for example, radio towers may be leased rather than owned by the agency, but should still be included in the inventory).
- User (the type of agency and/or personnel, not necessarily the specific individual).
- Original cost.
- Estimated remaining useful life (in years).

In addition, you should identify the human resources that are potentially available to work on the project, including their skills and current assignment.

What Do You Need?

Identifying what you need is not simply making a list of equipment. You should start at a much higher level and try to determine the kinds of functions/tasks you want to be able to perform. Are you wanting to add

new capabilities to your existing system? What are they? Who will use them, and how often? Will the existing system support those new capabilities?

For example, if you want to be able to put mobile data computers into your vehicles, you will need to ask yourself a series of questions, such as: What will the computers be used for? Will they need to communicate with computers in other locations? What locations? What kind of data will be passed over the radio system (dispatch messages, wants and warrants, field reports, a combination)? How much data? How much growth do you expect over the next 5 to 10 years? What kind of software applications will need interfaces (computer-aided dispatch, records management systems, automatic vehicle location system, geographical information system, etc.)?

It is extremely important to include the users of your system(s) in this evaluation process. Users, including dispatchers, are often the most aware of shortcomings and ongoing problems with your current equipment and can often recommend procedural changes that will improve performance without a major outlay of capital. Remember that, even though there may be numerous technical solutions to your communications needs, most have equally important operational considerations in order to make those solutions effective.

Knowing what you hope to accomplish in the long term will also help you identify the solution that will best fit your needs. Use documents such as your agency's strategic plan (perhaps you call it a 5-year plan or some other similar name) to help determine your needs. For example, if your agency is planning to consolidate with another nearby agency within the next 5 years, your combined communications needs may be dramatically different from those required for just your agency alone. In addition, review the strategic plan(s) for the government entity you are part of (city, county, State) to see if its plans might provide you with some assistance. Review the plans of other government entities that have wireless communications needs (information systems, telecommunications, and various utility departments are often good sources of information).

Review your inventory to see how much, if any, of your existing equipment should be retained. What equipment will need to be replaced because it is obsolete or too expensive to maintain?

What Are Your Options?

Now that you know what you have and what you need (at a functional level), you are ready to start reviewing your options. Essentially you will be faced with two choices: purchasing a dedicated system or contracting with a commercial service provider.

In certain rural areas of the United States with small populations, there may not be any commercial service providers. In that case, the only option will be purchasing a dedicated system. Chapter 3 discusses different funding sources, as well as partnering with other agencies as a means to obtain more "bang for the buck." If you are in an area of the country that has access to commercial services, you will have to research the available services providers for cost, coverage, services, level of support, etc., to determine how well their services meet your needs (see part 4 for a complete discussion of your options).

Motorola Solutions, Inc., Ex1017, p. 17

How Much Will It Cost?

Cost is one of the most difficult items to accurately predict because certain critical items are often left out. The purchase price of the equipment or service alone is not sufficient to understand how much a system will cost you over a 10-year period (the average lifespan of a communications system). You need to look at the full life cycle cost of the system, including such things as maintenance, personnel, and license costs.

In addition to identifying the costs, you should also try to identify any cost savings that will result from implementing your project. What will you not have to pay for anymore once your project is installed? The cost savings will help offset the costs, thus reducing your overall life cycle cost.

Table 1-1 below compares a hypothetical agency's costs to operate a purchased, dedicated, mobile data system with its costs to operate a commercially provided system. (Note: These numbers should not be interpreted as examples of what actual costs would be to operate your system. Every agency is different, and vendor prices for equipment and services vary widely.)

Table 1-1. Ten-Year Life Cycle Costs—Mobile Data System

Agency Costs[1]	**Purchase**	**Service Agreement**
Infrastructure Cost (controller, base station, install)	$125,000[2]	$0
RF equipment (radio or PC cards: 25 cars)	$37,500	$5,000
Mobile equipment (25 cars @ $5,000 each)	$125,000	$125,000
Mobile software (25 cars @ $800 each)	$20,000	$20,000
Airtime (25 cars @ $50/month/car)	$0	$150,000
High speed data circuit to service provider ($300/mo)	$0	$36,000
Infrastructure maintenance (approximately 10% of purchase price/year)	$125,000	$0
RF equipment maintenance (10% of cost per year)	$37,500	$5,000
TOTAL	$470,000	$341,000

[1] Not every cost that would be involved in the creation of a complete mobile data system is included in the above table. Other items could include: CAD and/or message switch interface costs; interface maintenance; and mobile equipment maintenance. Typically, the mobile equipment would be replaced every three to five years, but for simplicity, they are shown as a one time purchase only.

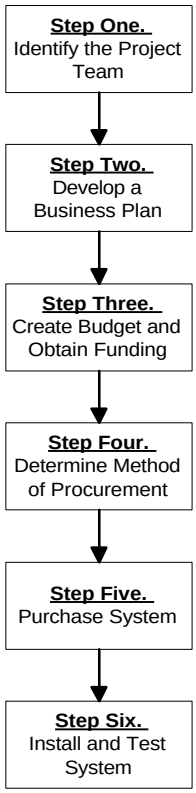
[2] The cost to purchase the infrastructure could vary higher or lower than the cost given above, depending upon a number of factors (e.g., terrain, size of coverage area, cost to acquire radio site if none exists, etc).

Most commercial vendors or service providers will be happy to provide you with budgetary information to help you plan your project. The information you gathered in your inventory and during your needs analysis should be provided to them to allow them to estimate their costs as accurately as possible.

How Do You Implement the Project?

The overall steps needed to implement a project like this are identified in figure 1-1. Each is important. Additional details regarding planning of the project (part of steps one and two), obtaining of funds (step three), and the procurement process (steps four through six) are given in subsequent chapters.

Figure 1-1. Project Steps



Getting Help

At this point you may be starting to feel a little overwhelmed with the size and complexity of the project you have taken on. Don't. Many agencies, both large and small, have successfully undertaken radio projects over the years. However, if you still feel that this task is beyond your ability to handle or will take more time than you can reasonably provide, you can get help from a number of sources (also see resources in appendix B).

Other Agencies

Other agencies near you have done this before. If you do not know who to call, contact your local chapters of organizations such as the Association of Public-Safety Communications Officials (APCO), National Emergency Number Association (NENA), International Association of Chiefs of Police (IACP), or International Association of Fire Chiefs. Those who have local/state chapters, such as APCO or NENA, will be the most help. Ask them for a list of agencies that have recently completed a project similar to yours. Ask those agencies for help. They are usually glad to send you copies of requests for proposals (RFPs), contracts, coverage requirements, system test plans, or any other type of sample documentation you may need. They may even be willing to sit down and discuss how they managed their project and make suggestions for yours.

Remember that, like you, these people also have a full-time job working for their own agency. They won't be able to do the project for you. But, if what you need is a sounding board for ideas, most people are happy to do what they can.

Consultants

If you decide that you need more dedicated and expert help than can be obtained from your neighbor agencies, you may want to consider hiring a consultant. A consultant can perform a number of the project tasks for you, from conducting the inventory and needs analysis to developing budgetary cost estimates to creating an RFP to assisting you with the project management. You determine the level and extent of services you wish to purchase.

Many consultants will perform your work as a fixed-price contract, provided you can clearly identify the scope of work you wish them to perform. Otherwise, you can hire a consultant on a time and materials basis. In the latter case, your risk is higher, since you may not have any cap on the amount of money spent or any guarantee that your project will be finished when you run out of money to pay the consultant. The authors recommend, whenever possible, that you create a clear scope of work and have the consultant give you a firm quote. Have proposers provide you with unit costs (hourly rate) for additional work and set "not to exceed" limits.

Depending on your agency's purchasing rules, you may need to create an RFP for consulting services. If you do, follow the same general steps that are outlined in chapter 4 for competitive procurements.

Again, your nearby agencies are a great source of information about consultants. They can tell you who they have used and tell you whether they were satisfied with the consulting firm's services. Make sure that when you are evaluating potential consultants they have completed similar projects.

Vendors

One of the most useful sources of information are the vendors of the products you are considering. Many have created libraries of articles (often called "white papers") written by industry experts, which explain the advantages and disadvantages of the various technologies. Most want to help educate you because they know that the better informed you are, the better buying decision you will make. Just remember that they are trying to sell you their product. So accept their information, but do the product comparisons yourself.

Motorola Solutions, Inc., Ex1017, p. 20

Chapter 2

Planning the Project

Realistic Schedule

One of the first things you need to develop when planning your project is an implementation schedule. The schedule should identify all major tasks and milestones and should allow enough time for the project to be developed, funded, and implemented. If you are applying for a grant, you may also need to add a period after implementation to comply with the grant's evaluation requirements.

A clear time line, identifying all of the milestones you expect to reach during the various phases of the project's implementation, is essential. Not only will it help all of your team to understand what has to be done and when, it will help reviewers get a much better perspective on what you are proposing.

Project Team(s)

Some projects are large enough that two project teams are needed and formed: a project *steering committee* and a project *implementation team.*

The *steering committee* is usually more involved with high-level planning and policy decisions, without getting actively involved in the details of the project. The steering committee often is composed of high-level representatives of the user agencies and/or departments, such as city/county managers, sheriffs, police and fire chiefs, finance directors, and sometimes elected officials. The purpose of the steering committee is to ensure support for the project at the highest levels of the organization. You need political, financial, and administrative support for your project to become a reality. Without that support, your project may never even get started, regardless of the need.

The other project team (or the only one in those cases where two teams are not needed or perhaps not possible) is the *implementation team*. The implementation team is the keystone upon which your project's success depends. This team must have the ability to effectively deal with both the technical complexity of a communications project and the organizational challenges associated with managing the project. The implementation team should include two components, one to manage the technical side of the project and the other to manage operational issues associated with the project. Both should consider the impact on, and coordination with, existing systems and users. And while the technical group must consider all of the technical issues involved, the operational group has equally important tasks that must include development of operational guidelines/procedures and the education and training of users. Training is a critical issue;

many advanced systems have not yielded their anticipated results because they are not being used effectively.

Project Manager

Like any other team, the person selected to lead the implementation group is critical. The key abilities needed in the project manager are organizational skills and people skills. Knowledge of the technical aspects of the project is helpful, but not critical. The project manager ensures that the team works smoothly together, makes sure that all tasks are completed on time and correctly, and solves the various problems that arise during the project. Pick someone who knows how to get things done.

Regardless of the skill of the project manager, that person will not be effective if he or she is not given the following:

Responsibility. The project manager must know that the ultimate success of the project is dependent on him or her and also that he or she will be held accountable for the project's success or failure.

Authority. No manager can succeed if given the responsibility but not the authority to make sure the necessary project tasks are carried out. The project manager must be empowered by the steering committee or other executive sponsor of the project to get and use whatever resources are needed to make the project a success.

Time. One of the most frequent causes for the delay or failure of a large project is not giving the project manager the time needed to do the job. Expecting to take someone who is currently doing one full-time job and assigning the project management tasks to him or her as well is just poor management. Estimate the time needed to effectively manage the project and then adjust the project manager's workload accordingly. Be sure to include time for unseen delays and for fine-tuning once the project is operational.

Management support. If a project manager's manager does not support the project, it is unlikely that the project manager will be successful. Make sure that the person selected has the backing of his or her management team.

Physical resources. It may seem obvious, but an adequate space within which to work is an absolute necessity. The project manager will spend hours on the telephone, in meetings, and reviewing detailed technical documents. Adequate space, privacy, and quiet are mandatory. Administrative support for tasks such as copying, filing, typing, and scheduling make the project manager more productive.

Other Team Members

Implementation team members should be selected to provide the project with the best chance for success. Each member should bring a unique perspective to the group. One could be technical. Others might be financial (including finance, budget, and purchasing) and legal. Still more might represent different aspects of the user community. (And don't forget to include your vendor on your team, once a vendor has been selected. Including the vendor on your team will minimize the chance of any last minute, unhappy surprises.)

Whatever their qualifications, team members should be willing to take on the assignment of certain tasks from the implementation schedule and have the time to accomplish those tasks. Like the project manager, team members must be willing to embrace the responsibility of performing their assignments and be allowed the time by the employing organizations to do those assignments well.

Budget

For funding administrators to evaluate your request for funds, you must be able to explain your budget in detail, particularly if you are applying for Federal funds. The budget must be reasonable for the tasks and equipment proposed, and the relationship of the budget to the project plan must be clearly identified and communicated.

Budgets should include all costs associated with the project. This could include costs for personnel, fringe benefits, computer hardware and software, other end-user equipment, telecommunications services and related equipment, furniture and space, supplies, and maintenance. If a new facility is needed to house personnel and/or equipment, construction costs may also be included.

If you are applying for a State or Federal grant, make sure you obtain a copy of the grant application guidelines (see resources in Appendix B). Most grants require detailed budget information and mandate that it follow a specific format. Failure to follow the rules often results in immediate disqualification of the grant application.

Motorola Solutions, Inc., Ex1017, p. 23

Chapter 3

Obtaining Funds

For many agencies, obtaining funds is the most difficult part of a communications project. Projects like this are expensive, and, as a result, funding may take months or even years to accomplish. Begin your efforts for obtaining funds far in advance of when you need the new system to be operational.

More detailed information about public safety funding can be found in the *Report on Funding Mechanisms for Public Safety Radio Communications*, published by the Public Safety Wireless Network (PSWN) Program (see resources in appendix B).

Types of Funds

For most local agencies, the types of funds available fall into two general categories: local revenue funds and grants. Local revenue funds are obtained by local governments through local taxes (e.g., sales tax, property tax), user fees, and other user charges, plus through the issuing of debt instruments, like bonds. Grants are funds made available to local agencies from State and Federal government agencies, as well as from private sources (like foundations). Grants usually require you to submit a formal application to justify your request for funding.

Sources of Funds

The process you must go through to obtain funding for your project will vary depending on who owns the funds you want. This section focuses primarily on government sources of funds, not private sources.

Remember, to fully fund your project, you may need to get money from several different entities. In fact, many of the Federal grants *require* a certain amount of matching funding. Learning as much as possible about all the possible sources is in your best interest.

Federal Sources

Local governments receive public safety funding from Federal sources primarily through grants and cooperative agreements. A third source of funds for law enforcement has been asset forfeiture funds. (Most of the Federal public safety funding in the last decade has been primarily for law enforcement, with little specifically earmarked for fire and emergency medical services.) Grants fall into two categories: *block* (or *formula*) grants and *discretionary* (or categorical) grants.

Motorola Solutions, Inc., Ex1017, p. 25

Most public safety funding has come through the U.S. Department of Justice (DOJ). However, funds for infrastructure projects like communications are also possibly available through the U.S. Department of Commerce [National Telecommunications and Information Administration (NTIA)], the U.S. Department of Transportation (DOT), and the Department of Homeland Security [through the Federal Emergency Management Agency (FEMA)].

A sample list of some of the programs that have provided funding recently, including the name of their funding and administering agency(s) and their matching funds requirements, is shown in table 3-1.

Table 3-1. Primary Federal Sources of Telecommunications/Technology Funding for Law Enforcement

Program Name	Type (Discre-tionary or Block)	Match Required?	Min. Match (%)	Fed. Source	Apply to	Contact
Local Law Enforcement Block Grants (LLEBG) Program	B	Yes	10%	DOJ-BJA	State	App.A
Edward Byrne Memorial State and Local Law Enforcement Assistance Program	B	Yes	15%	DOJ-BJA	State	App.A
State Identification Systems (SIS) Grants Program	B	No		DOJ-FBI/ BJA	State	Varies by State
Technology Opportunities Program (TOP, formerly TIIAP)	D	Yes	50%	DOC-NTIA	NTIA	App.B
Community Oriented Policing Services More (COPS MORE) Grant	D	Yes	15%	DOJ-COPS Office	COPS Office	COPS Office
Federal Emergency Management Agency (FEMA) Grants	D	Yes	50%	FEMA	FEMA	FEMA
State and Community Highway Safety Grants	B	Yes	20%	DOT	DOT	DOT

Block grants. Block grants are distributed by the Federal Government to States based on a statutory formula (which may take into account factors like population or crime rate). States then distribute their share of the block grant funds to local and State government agencies. The Federal Government issues broad guidelines about what type of things the funds can be used for, but the States process the actual applications.

The largest single formula grant source for law enforcement is the Edward Byrne Memorial State and Local Law Enforcement Assistance Program. Each State has an established office for assisting in the application for law enforcement-related block grants (at minimum to service the Byrne Program). The grant offices have various names within each State, although State planning agency is the most common. A list of the agency names and contact numbers for Byrne Program assistance in each State is given in appendix A.

In addition to administering the Byrne funds, these State agencies are often valuable resources for help in writing grants and for information about other funding sources.

A second block grant program, the Local Law Enforcement Block Grants (LLEBG) program, also has recently been a source of funds. If a jurisdiction is eligible for funding and completes an application, the Bureau of Justice Assistance (BJA) will make an award. The LLEBG program is not a competitive program.

Discretionary grants. Discretionary grants are usually focused on a specific purpose and are administered directly by agencies within the Federal Government. The rules for qualification, deadlines for application submittal, funds available, and format will be different for each type of grant and each agency administering the funds. Most require the local agency to provide some percentage of matching funds (see table 3-1).

The primary Federal funding agency for law enforcement grants is the Office of Justice Programs (OJP), within DOJ. The offices within OJP that make grants include BJA, Bureau of Justice Statistics (BJS), Corrections Program Office, Drug Courts Program Office, National Institute of Justice (NIJ), Office of Juvenile Justice and Delinquency Prevention (OJJDP), Office for Victims of Crime, and the Violence Against Women Office.

In recent years, a major source of law enforcement funding has been the Office of Community Oriented Policing Services (COPS), also within DOJ.

It is extremely important to follow all of the rules dictated by the funding agency regarding the application process. Each agency receives hundreds of applications for funding and will only consider applications that provide all of the necessary information and in the required format. Even if you have a great project idea, it will not get considered if you neglect to comply with the agency's application instructions.

Federal asset forfeiture funds. Asset forfeiture programs are administered by two different Federal agencies: DOJ and the Department of the Treasury. Funds for these programs are obtained from forfeitures

Motorola Solutions, Inc., Ex1017, p. 27

associated with the breaking of Federal law. Federal agencies have the authority to share fund revenues with any State and local law enforcement agencies that assisted in successful forfeiture cases.

If your agency has been involved in assisting a Federal agency and that case resulted in the seizing of assets, you should contact the Executive Office of Asset Forfeiture within either DOJ or Treasury for information about sharing of funds or property.

State Sources

The availability of State money to fund local public safety projects varies significantly from State to State (with the exception of the State-administered Federal block grants). Some States administer their own grant programs through a variety of different departments (e.g., Public Safety, Health, Human Services, Emergency Management, General Services, Business and Economic Development). The State planning agency administering the Byrne Program funds is the best place to start when inquiring into State sources of grant funding.

Sources other than traditional public safety-related State agencies are also worth exploring. For example, in Colorado, some police agencies have received Energy Impact Grants through the Division of Local Affairs. These are mitigation funds collected from oil and gas producers that are then returned to counties where petroleum extraction occurs. In this case, the funds are not public safety specific, but rather county specific.

Depending on the State, 9-1-1 and E9-1-1 surcharges are administered by the State and/or by the local government and may be available for communications projects. If you are unfamiliar with how 9-1-1 surcharges are administered in your State, contact either the national office or your State chapter of the National Emergency Number Association (NENA) (see resources in Appendix B). NENA should be able to tell you who administers the funds for your agency and provide you with a contact name and number.

A number of States are planning or implementing statewide wireless communications projects. In some instances, these projects include providing access for local public safety agencies in addition to State agencies. Each State has funded these large-scale projects in various ways, ranging from State tax revenues to bonds to user fees. Unfortunately, each State administers these projects differently and through different departments. To find out if a project like this is under way in your State, try contacting the department or division responsible for telecommunications or the State law enforcement agency.

Local Sources

Local governments spend the revenues they collect in several ways. The largest percentage is through the general fund, which pays for the overall operational budget for the government. Funding requests made to a general fund must usually follow the budget preparation rules of the local government and will be competing against all other departments within that government entity.

In addition, the local government may have decided to incur long-term debt by issuing bonds, certificates of participation, or similar instruments. The money raised in this manner is used to pay for many multiple-year or high-cost projects. In some cases, a specific tax may be levied (kept separate from the general fund)

that is earmarked to pay for certain capital improvement projects. (Remember, in some States, permission to issue debt or special taxes may require a vote of the citizens, which requires a ballot initiative and a significant amount of time and effort, with no guarantee of passage.)

Single agency versus multiple agencies. Over the past decade, increasingly agencies have been joining together to fund cooperative communications projects. The benefits of increased interoperability and reduced individual agency cost have overcome traditional resistance to sharing. Agencies have created intergovernmental agreements (IGAs), joint powers authorities (JPAs), nonprofit corporations, and other creative mechanisms for allowing the various agencies to contribute funds to a joint project.

Most agencies come up with some formula to determine the share of money that each must contribute. Formulas may be based on population, coverage area, number of transactions, number of units/officers, or any combination of these and other factors.

In addition to providing a mechanism for funneling local funds, a multiagency consortium often is able to obtain grant funds that a single agency might not. Many Federal grant programs look favorably on cooperative sharing of resources.

If you are considering creating a multiagency funding authority, contact several agencies that have participated in projects like this for suggestions on how to structure and fund your organization. They can give you valuable information on the time it takes to get all the various local governments to come to agreement, what has worked well for them, and what they would suggest you do differently.

"Selling" Your Need

Regardless of who you ask for funds, you must convince them that your project is necessary and that you will provide the most beneficial use of their dollars. The competition for funds is intense, and everyone believes that his or her needs are real. Getting the funds often depends more on your ability to present your needs in a businesslike and professional manner than on the need itself.

For example, the Technology Opportunities Program (TOP) of the Department of Commerce publishes extensive guidelines for preparing applications on its World Wide Web site (see resources in Appendix B). In addition to a detailed budget, a TOP applicant must be able to clearly answer the following questions:

- What are the goals of the project?
- What are the anticipated outcomes?
- How will the proposed solution make a difference in the community?
- How many sites are there and where are they located?
- Which communities are to be served?
- What organizations are participating as project partners?
- What technologies are to be employed?
- What will users do with the technology?

The review team needs to know that the project you propose is worth doing and that your team can actually do it. The feasibility of the project will be judged based on your technical approach, the skills of your team

Motorola Solutions, Inc., Ex1017, p. 29

members, your budget estimates, schedule, and time line, as well as the long-term operational costs of the project. Failure to clearly define any of these items could be cause for rejection of your request.

Involve as many people as possible in reviewing your project request **before** you submit it to the funding agency. Have someone who is not directly involved in your project read it for clarity and purpose. Have your financial staff person review the budget for completeness and accuracy. Have a technical editor proofread it for punctuation and grammar. Have another agency that has been successful applying for funds make suggestions for improvement. Above all, make sure the proposal tells a complete and cohesive story and that no questions are left unanswered.

Remember, if you miss your chance with this proposal, you may have to wait a year to submit another. In the case of Federal grants, if the appropriations for that program are cut off next year, you may never get another chance.

☞ Did you know?...

Data collected from TOP grantees show that a commonly reported problem is the under-estimation of the time and resources needed to complete particular project tasks. Grantees recommend that you develop a realistic time line that allows sufficient time to correct errors, troubleshoot problems, and deal with unexpected obstacles.

Getting Help

This section identifies some of the Federal resources that you may find useful when looking for funding. Many more resources exist than are listed below. Appendix B lists a number of additional contacts that may also be helpful.

For information about Federal grant programs in general:

- ➡ Get a copy of the *Catalog of Federal Domestic Assistance* through your local library for information on all Federal grant opportunities. The *Catalog* also can be ordered (for a fee) by calling 202–512–1800.
- ➡ Search the computerized database of grant programs, called FAPRS, maintained by the General Services Administration.

For information about DOJ programs specifically:

- ➡ Contact the DOJ Response Center (see appendix B).
- ➡ Contact the National Criminal Justice Reference Service (NCJRS) through its Web site at http://www.ncjrs.org or via e-mail at askncjrs@ncjrs.org.
- ➡ Contact the BJA Clearinghouse (see appendix B). (NCJRS, cited above, is the online version of the Clearinghouse.)

For information about DOJ block grant programs administered by each State:

Motorola Solutions, Inc., Ex1017, p. 30

➡ Contact the applicable State planning agency given in appendix A.

For information about TOP grant programs:

➡ Contact the NTIA TOP office given in appendix B.

To automatically receive notice about all solicitations sent out by DOJ:

➡ Ask NJCRS (see above for contact information) to put you on its mailing list for grant proposal solicitations.

➡ Check the postings on the BJA home page at http://www.ojp.usdoj.gov/BJA.

For help writing a grant:

➡ For law enforcement officials, the FBI's National Academy Program offers a noncredit course on grant program development and budgetary issues. Contact the FBI for more information.

➡ Contact other agencies that have successfully applied for the grant you are interested in. Ask them for copies of their grant proposals. Lists of successful applicants are found on many of the Federal Web sites, in particular at http://www.ncjrs.org

Additional information sources are identified in the resources in appendix B.

Motorola Solutions, Inc., Ex1017, p. 31

Chapter 4

Buying What You Need

Once funding has been secured, the purchasing process can begin. This section discusses the primary ways that communications systems have been purchased but does not attempt to itemize every variation that has been used.

How to Buy

Most government agencies have specific purchasing rules and regulations that must be followed for purchases to be legal. You should consult with the staff from your purchasing division or department to determine the rules that govern your agency.

Competitive Procurement

A competitive procurement usually involves the development of purchasing specifications by the local agency and then issuing of a Request for Quotation (RFQ) and/or a Request for Proposal (RFP). Multiple vendors respond to the RFQ with a bid (or to the RFP with a proposal) to provide what the agency has requested. A competitive procurement is designed to encourage competition among vendors to encourage fair pricing.

An RFQ is generally used to purchase commodities, which can be easily described and for which there are several suppliers. Most awards that result from RFQs are based on low bid.

An RFP is used for purchasing more complex items, like communications systems, for which a number of variables besides price may influence an award decision. For example, other variables could include maintenance hours, financial stability of the company, references from other clients, and ease of use.

Because it is the most common method for purchasing a communications system, the competitive procurement process using an RFP is detailed in a section below.

Noncompetitive Procurement

Local governments can contract for services in many cases without going out to bid. Check with your city/county purchasing department to see if there are any clauses in your policies and procedures that would work to your benefit. Two common examples that are used with communications are *sole source procurement* and *contract for operational services.*

Motorola Solutions, Inc., Ex1017, p. 33

Sole source procurement. In a sole source procurement, goods and/or services can be purchased from a vendor that has previously been awarded a contract, usually through a competitive bid process. The reasoning is that if that vendor is the "sole source" for additional items that are compatible with items already supplied, then another competitive procurement does not need to be conducted. For example, if you had purchased computer software from a vendor and now decide that you want to upgrade to a newer version of its software, and since it is the only one that makes that software, you could issue that vendor a purchase order without going to bid.

Each jurisdiction deals with the issue of sole source procurement differently. Some allow sole sourcing to vendors without a previous competitive procurement. Others do not allow it at all. If there is something you want to consider purchasing by sole source, you should check with your local purchasing manager *before* you issue any purchase orders to make sure you are in compliance with local ordinances.

Contract for operational services. Agencies contract for many types of operational services, like cellular telephone service and pager service. Many purchasing divisions treat service contracts differently than they treat contracts for purchase. You may only need to show that you have sufficient funds in your budget to pay for the service you want. In some cases, you may not even have to prove that since the belief is that you will cancel the service if you have no more money in your budget.

Some agencies have purchased mobile data cellular service [e.g., Cellular Digital Packet Data (CDPD) service] through noncompetitive service agreements and, thus, have completely avoided the competitive procurement of radio infrastructure equipment.

As always, you should confirm with purchasing that there are no restrictions to your contracting for services.

Cooperative Purchasing

Cooperative purchasing refers to the practice of buying from another agency's competitive procurement. The most common type is the ability of a local agency to buy from the State's price agreement list. State governments routinely solicit bids for thousands of commonly used items, like computers and printers, at fixed prices. Vendors promise to supply all of the items the State wants at that fixed price for a fixed period, frequently one year. Local governments can buy from these awards throughout the year at volume discount prices, usually without going through their own bidding process.

Check with your agency's purchasing manager to determine whether your State allows you to purchase items from its awards. Or contact the State purchasing division directly to see if it supports this type of cooperative purchasing.

Western States Contracting Alliance. The Western States Contracting Alliance (WSCA) was formed in October 1993 by the state purchasing directors from fifteen western states. The primary purpose of WSCA is to establish the means by which participating states may join together in cooperative multi-State contracting in order to achieve cost-effective and efficient acquisition of quality products and services.

Membership consists of the principal procurement official that heads the state central procurement organization, or designee for that state, from the states of Alaska, Arizona, California, Colorado, Hawaii, Idaho, Minnesota, Montana, Nevada, New Mexico, Oregon, South Dakota, Utah, Washington and Wyoming.

All governmental entities within WSCA states are welcome to use the approved agreements, as well as authorized governmental entities in non-WSCA states. Everyone benefits from cumulative volume discounts.

As of 2002, WSCA had negotiated purchasing agreements for the following goods and services:

- Data Communications Equipment and Associated Oem Maintenance & Training (including Routers, Switches, LAN/WAN Wireless, and CSU/DSU)
- Industrial Supplies And Equipment; Janitorial Supplies And Equipment; and Lamps And Light Fixtures
- Computer Equipment, Peripherals, Software And Related Services (current contracts are with: Hewlett Packard - Compaq Computer Corporation, Dell, Gateway, and IBM)
- Wireless Communication Services And Equipment (current contracts are with: AT&T Wireless, Verizon Wireless, Nextel Wireless Services, and Sprint PCS Wireless)
- Electronic and Satellite Monitoring Equipment (including continuous signaling electronic and alcohol monitoring services, random /scheduled tracking services, satellite monitoring with remote tracking services and support services)

As an example of the type of discounts that have been negotiated, the current Nextel contract offers a 10% discount off of Nextel's standard or government monthly access fee. The Sprint PCS contract offers a 15% discount.

For additional information about the WSCA program and your eligibility to participate, visit the WSCA web site (see resources in Appendix B).

Leasing

Leasing is not really a type of procurement, but rather is a way to pay once a procurement has been made. One of the above procurement methods would be used to select a vendor and determine a price. Once that was done, the local government could decide to finance the purchase and pay for it over a period of months or years, rather than purchase the equipment outright.

Leasing can be advantageous in those cases where you do not receive all of your funding at one time. For example, if sales tax revenues are funding your project, the revenues are spread out over a number of years. In that case, it might make sense to also spread your payments out over a similar number of years. The total cost of the purchase will be higher (because of interest charges), but you will get use of the system sooner than if you wait until all of the revenues are received.

With most government leases, the government owns the equipment upon contract completion. The equipment can then be traded or upgraded as technology improves or requirements change.

Motorola Solutions, Inc., Ex1017, p. 35

Leasing companies are generally willing to work with your agency to structure the lease to conform to your budget, tax, cash flow, delivery, or regulatory restraints. Because of the number of companies now offering leasing to government agencies, your purchasing agent may decide to ask a number of companies to bid on providing the lease, thus ensuring that you receive the most favorable finance rate.

Outsourcing

Outsourcing is one of the newer methods of procurement, at least at the local government level. Outsourcing refers to hiring an outside company to perform services traditionally performed by agency staff. The level of service can vary, from just providing the people to operate agency equipment to contracting for provision of people and equipment.

For example, an agency in Pennsylvania outsourced its entire emergency communications center. The vendor supplied the facility where the communications center was located, the people to manage and staff the center, the computer-aided dispatch system, the telephone equipment, and all other aspects of the center. The agency estimated that it would actually save money over the 10-year course of the contract by *not* operating the center itself.

Because relatively few governments have done this, you may want to talk to companies in your area that have outsourced services. While somewhat new to local government, it has been used for a number of years in corporate settings, with significant cost savings.

Request for Information (RFI)

Technically, this is not a procurement. However, it can allow you to gather information in a structured manner that will allow you to determine what products and services are currently on the market and their associated costs. Generally, the vendors provide only estimates of costs, but these are extremely useful in creating your budget.

An RFI usually describes the scope of the project, your projected time line, and any other descriptive information about the project. Vendors are asked to provide information about their suggested solution, with supporting product material and cost estimate information.

In some cases, vendors have been required to respond to an RFI in order to be eligible to move to the next step and receive the RFP.

Competitive Procurement (RFP)

The goal of this section is to provide additional details about competitive procurements using an RFP. It is not intended to cover every aspect of the procurement process, but rather is intended to give you an overview of what is involved. Specific requirements for the RFP should be requested from your local purchasing manager.

Request for Proposal (RFP)

As mentioned previously, an RFP is used for purchasing more complex items for which a number of variables besides price are important to the purchasing decision (see figure 4-1).

RFP Process

The following steps are involved in the RFP process (and are summarized in figure 4-1).

Develop the RFP. There are three main sections of an RFP: the instructions to proposers, the terms and conditions of purchase, and the technical specifications. Templates for the first two are generally provided to you by your purchasing agent. You may then need to add, delete, or modify portions of these as appropriate to the needs of your project.

The development of the technical specifications is usually the responsibility of the project team. The specification must be clear and comprehensive so that both you and the vendor know precisely what is wanted and what is expected of each party. Avoid over specifying, as it can limit the number of vendors that respond and, thus, limit your options. But do include sufficient detail to ensure that prospective bidders understand the precise goals, objectives, and constraints of your project.

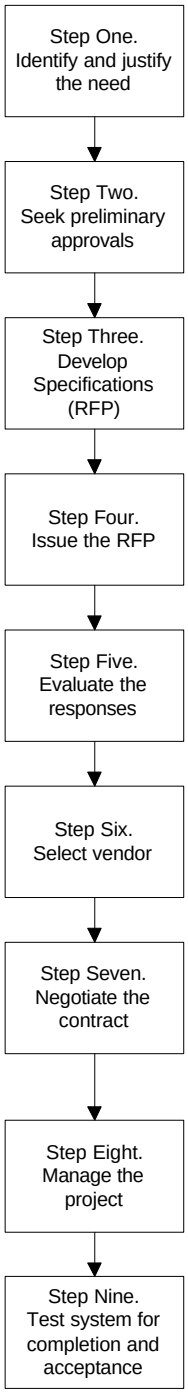
Examples of detail include:

> Are existing facilities/sites available to be used and/or will the vendor be able to use or recommend additional sites. Do added sites need to be on public property?
>
> Details on expected coverage of a radio system. Describe how coverage will be measured and by whom. Is coverage desired for portable use inside of buildings, or for mobile use from developed streets?
>
> Details on how equipment is to be installed/worn (for example, will a portable radio be belt-mounted with a remote microphone, or will it be held in the hand while being used – it can make a big difference in radio coverage).
>
> Environmental issues: Alert bidders to temperature/humidity/electrical issues (including threat of electrical storms) that may exist at proposed sites. Will air conditioning need to be added if equipment is installed as proposed by the vendor? Will proposed antenna or other structures require an environmental impact report (potentially causing major delays)?

You need to make sure that your RFP, at minimum, does each of the following:

- ➡ Describes the problem being addressed.
- ➡ Describes the existing environment (e.g., existing equipment, operational procedures, agency standards, constraints).

Figure 4-1. Steps in the RFP Process



- ➡ Describes how equipment will be installed and/or worn by the user.
- ➡ Describes the required project outcomes.
- ➡ Describes the scope and standard of service required in ALL areas (i.e., user functionality, system response times, delivery schedule, service levels, training).
- ➡ Identifies mandatory features and desirable features. Specifically highlight any mandatory requirements that would disqualify a proposal if they are not met.
- ➡ Identifies the key contractual terms and conditions (e.g., items that the agency is not willing to negotiate).
- ➡ Identifies criteria for acceptance and contract completion.

Obtain copies of RFPs for similar projects from other agencies and use these as a template for building your own specifications. However, never copy another agency's RFP verbatim. If you do not understand why certain terms or requirements were included by the agency in its RFP, ask the agency. It may have had certain requirements that do not apply to your project and that you should not include. You may have other requirements the agency did not need that you will want to add.

Remember, however, that a template is simply a starting point. It does not eliminate all of the work needed to create a thorough and complete RFP that best represents the needs of your project. If you are lucky, it just reduces the work somewhat and helps ensure that nothing is forgotten.

Once the RFP is written, have your team review it for completeness. Include members of your legal and purchasing departments as part of the review team. Make all necessary modifications before releasing the RFP. It is easier and better to delay issuing the RFP while you make corrections than to have to issue addenda during the procurement process.

Issue the RFP. Once the RFP has been completed and approved by your team, it is usually the responsibility of the purchasing department to issue it. The department has a standard set of procedures to follow that ensures that all of the legal mandates are met.

A period of time is often allowed within which potential vendors may submit questions. You need to be prepared to answer these questions in a timely manner and also to make sure that all potential vendors receive copies of the questions and responses to ensure impartiality. Many agencies host a vendors' conference to allow vendors to ask questions all at once and also to allow the vendors to inspect your site. This may reduce the number of written questions to which you are required to respond.

Allow vendors enough time to prepare a thorough response to your RFP. Depending on the complexity of the project, a period of from one to two months is common.

Proposals must be submitted by the date and time indicated in the RFP. Be sure to request enough copies for all evaluation team members. If a vendor submits a proposal after that time, its proposal should not be opened or included in the evaluation process.

Once the proposals are received and verified by purchasing, distribute copies to your evaluation team, which will include your implementation team as well as others with a vested interest in the project.

Evaluate responses. When evaluating the responses to the RFP, you must consider a number of items. Each item should have been clearly outlined in the RFP:

- **Compliance.** Does the proposal comply with the required specifications in the RFP? If it does not, eliminate the proposal from further consideration.

- **Value.** Value is more than just price. It may include all or some of the following: purchase price, quality, warranties, maintenance costs, training, service, response time, reliability, company stability, delivery time, and contract terms and conditions, among others.

- **Total Life Cycle Costs.** How much will the system cost over its expected life. In other words, if you expect the system to last 10 years, the life cycle cost would include the initial purchase price PLUS all operating and maintenance costs incurred over the entire 10 years. A system that has a low initial purchase price may have high maintenance costs that, over time, may cause its total life cycle cost to exceed that of a vendor with a higher initial purchase price.

- **Company References.** Talk to recent clients who have made similar purchases from the vendors for feedback on performance. Talking to several people from each client site will give you a more rounded impression of each vendor's performance.

☞ Did you know?

You can find more details about total life cycle costs in a PSWN book called "How2 Guide for Managing the Radio System Life-Cycle" which can be found in the Library at PSWN's Web site:

http://www.pswn.gov

Evaluate the proposals against evaluation criteria that were defined *before* the proposals were received. The goal is to select the proposal that best meets the defined needs and to determine whether the vendor has the ability to perform the work.

Read each proposal thoroughly. Use a standard evaluation format (e.g., a spreadsheet or written form) to help you compare responses of vendors more easily. Keep copies of the results.

Have your agency's purchasing and/or legal staff review the terms and conditions of the proposal to ensure that the vendor has not counter proposed any terms that would be unacceptable to your agency.

The entire evaluation process should be clear, fair, and equitable. Treating all vendors the same and keeping good records of the results of the evaluations will help ensure that there is no basis for a protest of your selection.

Select vendor. If a single best vendor emerges from the above evaluation process, you can move on to the contract negotiation phase of the process. However, it is more likely that there will be two or three vendors who appear comparable on paper (the "short list"). Before a clear winner can be selected, additional in-person demonstrations and/or interviews may be required with each of the short-listed vendors.

As a result of the demonstrations and/or interviews, each vendor may be asked to submit a best and final offer that allows an "apples to apples" comparison of the proposals and their value.

At this time, you should evaluate each company's financial stability as well, through bank references, credit reports, public financial records (if a public company), and other similar checks. Get help from experienced financial experts, either inside your agency or outside it, to ensure that you obtain the right information and that it is correctly interpreted.

Another important consideration is the company's ability to perform the work. In other words, does it have enough staff to do your project as well as the other projects to which it is already committed. Check to see how many concurrent projects the company is working on. Also check to see if it has adequate customer support staff to assist you with maintenance problems after the project has been installed.

Ultimately, the final selection should represent the best value for the money, from a financially stable, responsive, and well-respected company.

The unsuccessful vendors should be notified in writing once a selection has been made. However, the finalists should not be released from their obligation to perform until a final contract has been signed between the selected vendor and your agency. In the event that you are unable to successfully negotiate a contract with your selected vendor, you may wish to initiate negotiations with another of the finalists.

Negotiate contract. A written contract is mandatory. Both parties will benefit by having a document that clearly identifies each other's obligations.

The contract negotiation should begin as soon as possible after selection of the final vendor. The negotiations should be conducted between individuals from each of the parties who have the authority to make commitments on behalf of their agency or company. Otherwise, a great deal of time and effort can be expended during the negotiation process only to find out that the "powers that be" will not approve the resulting contract.

Your negotiators should have skills and experience in negotiating complex, high-technology contracts. If you do not have such expertise within your agency, seek help from recognized experts within other departments/agencies.

A copy of your agency's Standard Contract Terms and Conditions should have been included in the RFP and should serve as the basis for negotiating a final contract. (It is usually not in the best interests of the agency to use the vendor's standard contract terms and conditions; however, there may be circumstances when this is the best option available.)

In addition to legal terms and conditions, every contract should include a project schedule. This schedule should set clear, identifiable milestones for completion of each phase of the project. A milestone should be easy to measure and/or to determine that it has been completed.

The contract should also include a specific payment schedule, which clearly identifies when and under what circumstances payments will be made. As much as possible, payments should be tied to project milestones, with fixed-price amounts itemized. A certain percentage of the total contract price should be retained until the entire project is completed to ensure that all work has been completed to your agency's satisfaction.

The contract should specify how requests for changes in scope of work will be handled and who is authorized to request such changes. The contract should require that all changes to the scope of a contract be in writing (verbal authorization is not sufficient) to be binding. In addition, it is important to specify how any changes in the project cost, which may be associated with scope changes, will be handled.

Your agency's purchasing adviser and legal advisor should **always** be involved in reviewing any contract documents before they are finalized. Otherwise, the modifications made during the negotiation process may not be in compliance with existing governmental laws, rules, and regulations.

Ensure that the final contract is signed by the individuals from each party who are legally authorized to do so. Otherwise, the contract may be ruled invalid.

Manage the project. Managing the installation is one of the most important aspects of a successful project. Once the contract is signed, it is critical to monitor vendor performance, the contract terms, and the payments.

The project manager must ensure that the agency is getting what it asked for and that required milestones are met. Payments should only be made if milestones are completed as promised. However, payments should not be unreasonably withheld either. Ensure that payments are made on time for work properly performed.

One key to successful project management is open and frequent communications between the agency's project manager and the vendor's project manager. Raise questions or concerns as soon as they arise; don't wait for the next scheduled meeting. Waiting could cause a delay in your implementation.

Project management is a subject upon which numerous books have been written and for which many classes are taught. It is beyond the scope of this guidebook to cover all aspects of good project

Motorola Solutions, Inc., Ex1017, p. 41

management. A number of excellent project management software programs are available for helping with the planning, scheduling, and recording of the project tasks. Many include guidebooks on project management with the software.

Acceptance testing. The specifications should have indicated the system parameters to be tested and accepted. A thorough test plan should be submitted by the vendor. Tests should be run and witnessed by the agency *before* the system is turned over to the agency. All deficiencies should be corrected *before* final acceptance and final payment.

PART 2

WIRELESS COMMUNICATIONS TECHNOLOGY

Motorola Solutions, Inc., Ex1017, p. 43

Chapter 5

Voice Versus Data

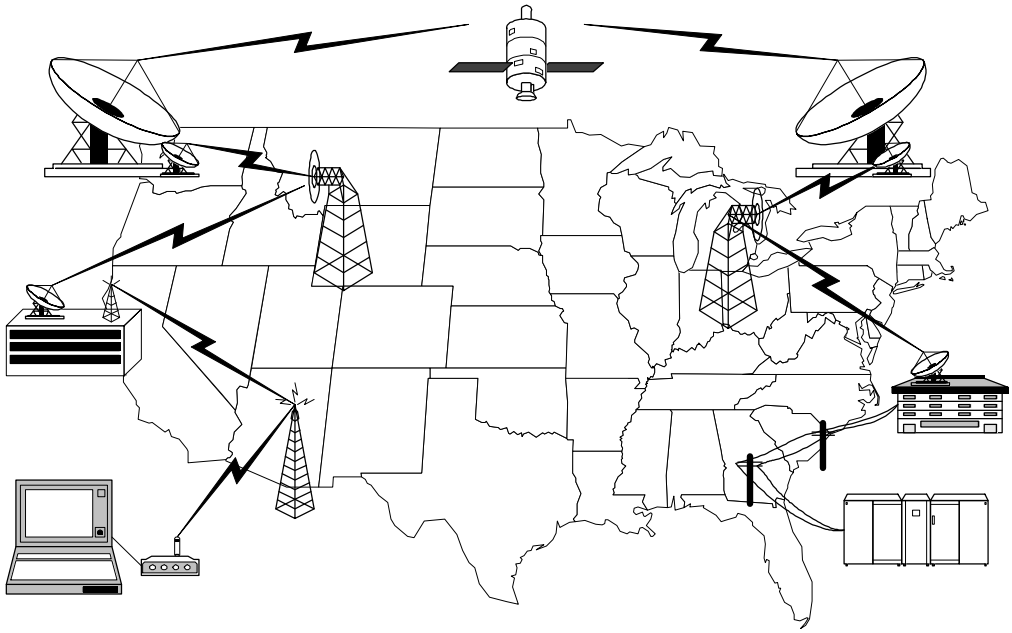
Voice Versus Data

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.

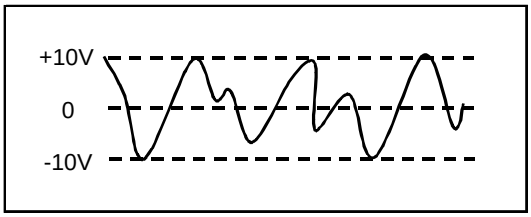
For example, figure 5-1 shows the various communications methods involved in sending data from an agency in California to an agency in Florida.

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.

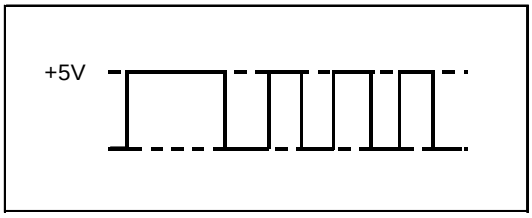
Figure 5-2. Analog Signal



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



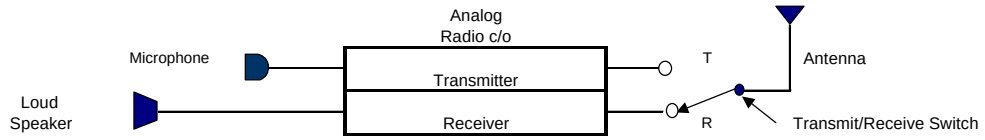
Analog Versus Digital

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

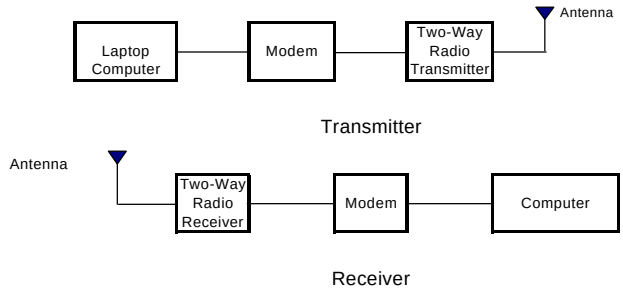


Figure 5-5 shows a laptop computer connection through a modem to a typical two-way FM radio. The laptop generates data as ones and zeros that are converted via the modem to analog tones that go into the radio transmitter. Once received, the detected tones pass through a second modem that converts the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

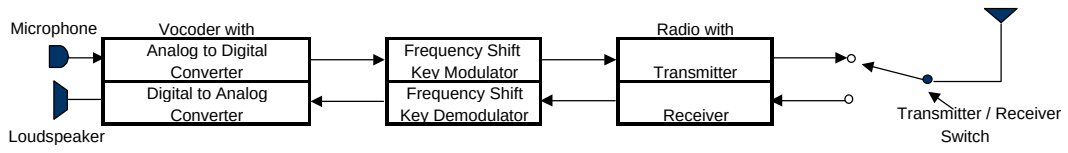
Digital Radio Systems

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.

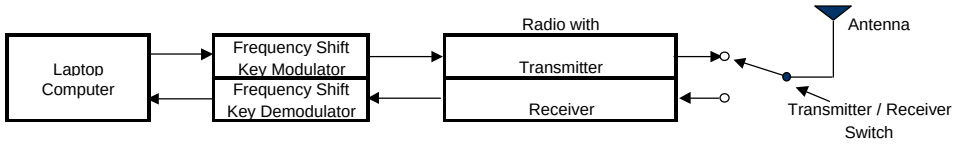
Figure 5-6. Block Diagram of a Voice Modulated Digital Radio System



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



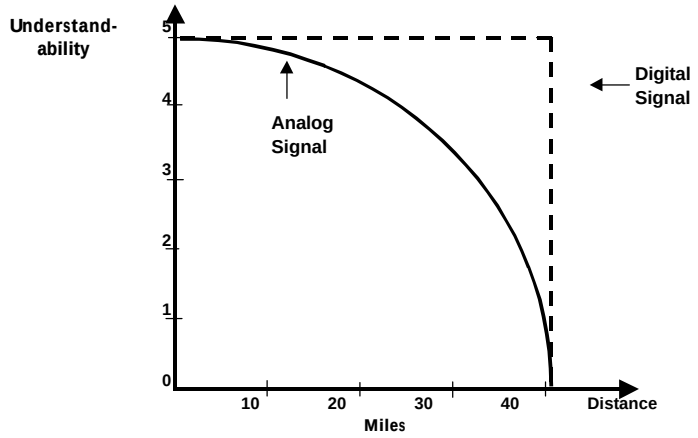
Transmission Differences

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.

Current digital encryption technology, when applied to digital radio systems such as Project 25, simply adds an encryption algorithm into the digital path. With reference to Figure 5-6, this "encryption box" is added between the Vocoder and the Modulator (for the transmitter) or Demodulator (for the receiver). The signal is already digital and the algorithm simply rearranges the bits so that a standard vocoder (for voice) or terminal (for data) can not regenerate a usable result. Because the system is already digital, the incremental cost to add a high level of encryption is usually low.

Encryption is used by more than just law enforcement agencies. Many fire departments transmit information such as alarm reset codes for businesses and private residences that could be unlawfully intercepted.

However, encryption is only as effective as the management of the "keys" used to protect the information. "Keys" are the data words (usually a group of random numbers or letters) used to control the encryption algorithm. All radios in an encrypted system must be loaded with the same key in order to understand the information being exchanged. These keys must be properly managed so that they do not fall into the possession of unauthorized personnel. They also need to be changed frequently in order to protect information. Given time, an unauthorized person can try many keys and eventually find the proper one to decode a transmission; if keys are not changed frequently, that person then has access to your information. Weekly re-keying with a random key is recommended for most local/state users.

When considering encryption, keep the following important issues in mind:

1. Legal requirements to protect information from eavesdropping. These typically vary by state and are especially important for criminal history information.

2. The time-sensitivity of information to be protected. This is the important property to be considered when determining the level of encryption needed. It is generally only necessary to protect information so that it cannot be used to undermine the operational aspects of an incident. Remember that most information, including actual radio transmissions, is available through the discovery process in court, or by Freedom of Information Act requests.

3. Media impact. The media can be your friend or foe when implementing encryption if they have always been able to monitor your voice radio system. Many agencies find that it is advantageous from the aspect of good media relations to encrypt voice transmissions on tactical channels and leave dispatch channels in "clear" mode.

Finally, all agencies employing more than a few (perhaps 10) encrypted field units on a digital radio system (such as a Project 25 system) should consider purchasing the Over-The-Air-Rekeying (OTAR) option. OTAR allows new keys to be effectively and securely loaded to field units from a central location, with assurance that all authorized units are re-keyed the next time they access the system. The incremental cost to add OTAR when compared with ongoing personnel costs to manually load keys usually makes this a cost-effective addition to an encrypted system.

Chapter 6

Characteristics of Radio Systems

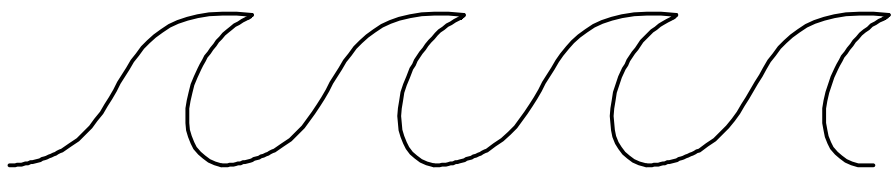
Understanding Radio Terms

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



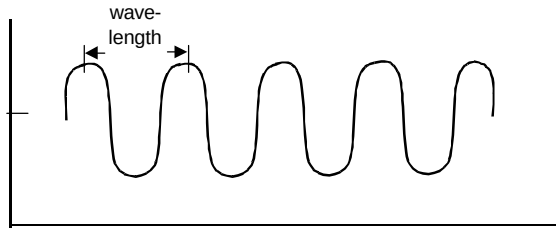
One big difference between ocean waves and radio waves is that ocean waves are visible, while radio waves are not. People can see how far apart or how high the peaks are on the ocean. Radio waves have those same characteristics; people just cannot see them.

Motorola Solutions, Inc., Ex1017, p. 51

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

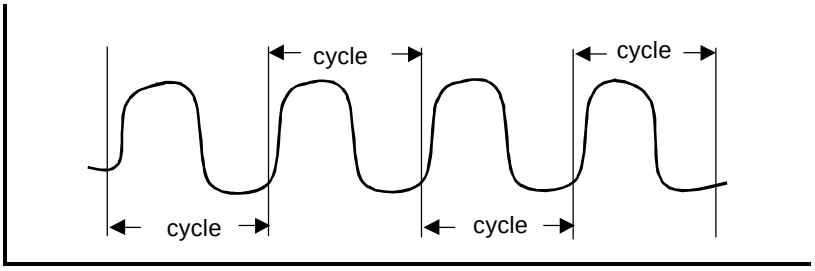


In radio terms, a *short* wavelength would mean that the peaks are relatively close together. A *long* wavelength would mean that the peaks are relatively far apart.

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.

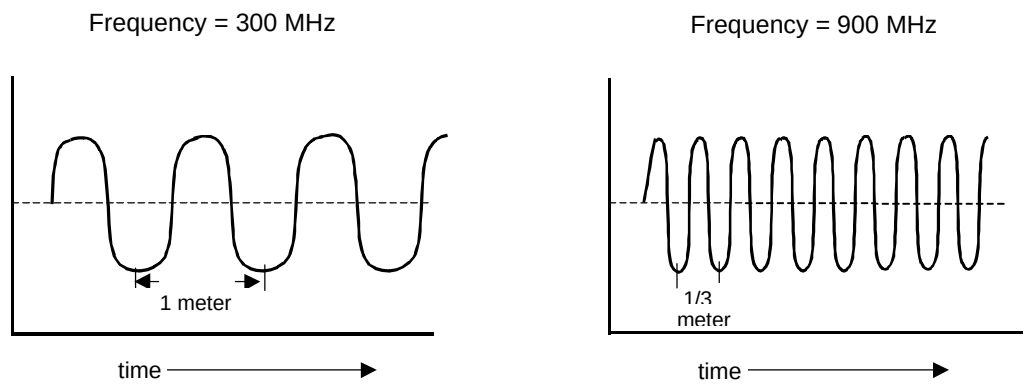
Motorola Solutions, Inc., Ex1017, p. 52

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).

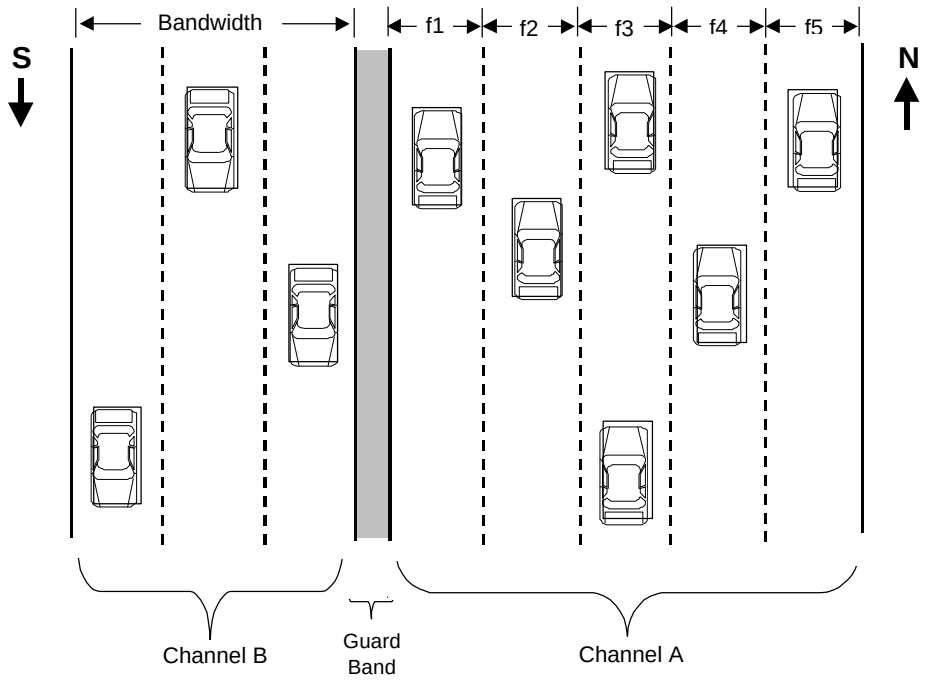
Channels

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.

Figure 6-5. Channels in a Wireless "Highway"



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

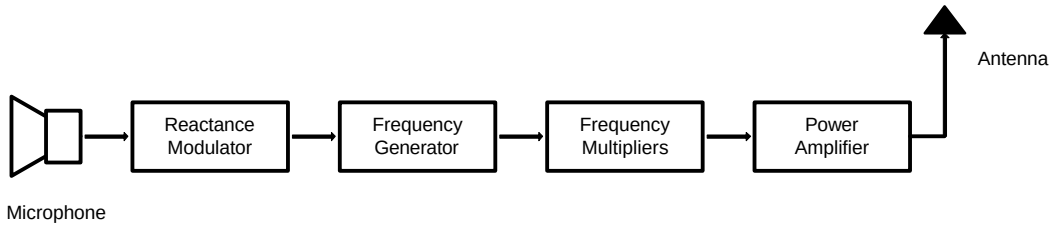
Base, mobiles, and handheld radios consist of components called *transmitters* and *receivers*. In most cases, some circuitry is used for both transmitting and receiving, so a radio is said to be a *transceiver*.

Transmitters

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

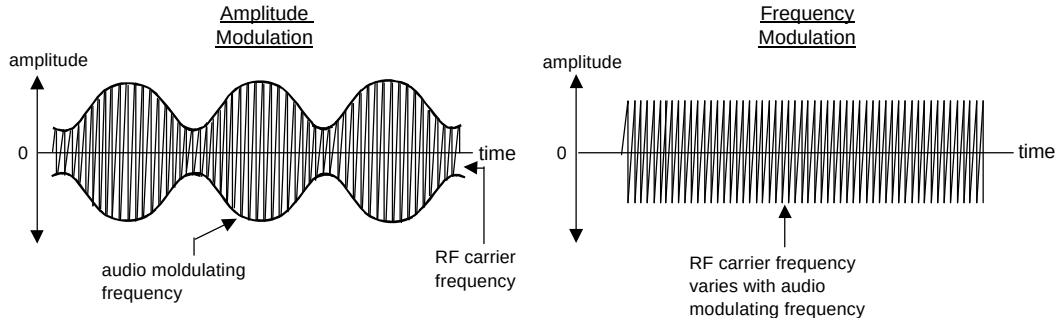
The frequency generating component is called an *oscillator*. *Frequency multipliers* multiply the frequency up to the final output frequency. A power *amplifier* increases the power of the signal to obtain the necessary power output to the antenna.

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.

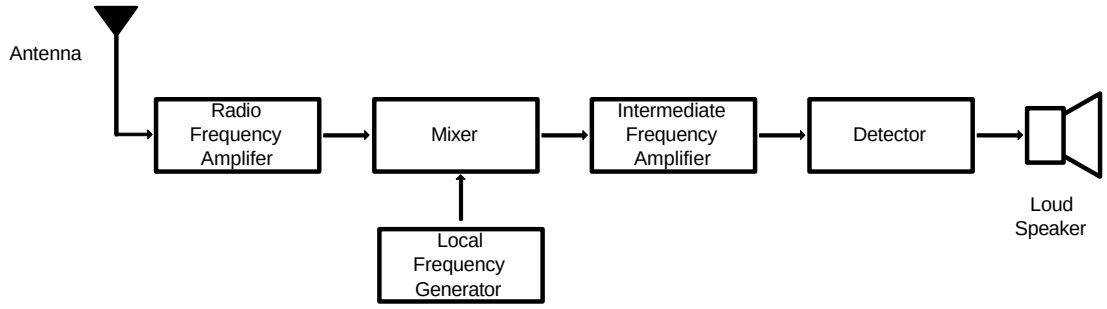
Figure 6-7. Comparison of Amplitude versus Frequency Modulation



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).

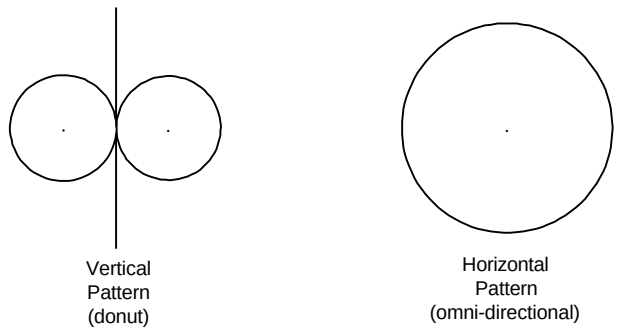
Antennas

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.

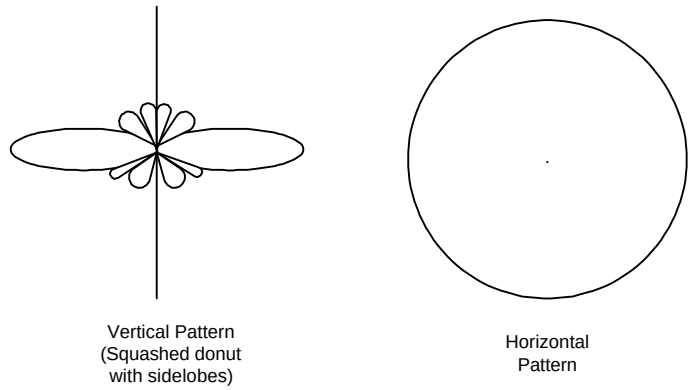
Suppose an antenna that radiates equally in all directions (an *isotropic radiator*) were represented by a perfectly round air-filled balloon with air as energy, then the energy per unit area (in watts/cm^2) on the surface of the sphere would be equal anywhere on the sphere.

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.

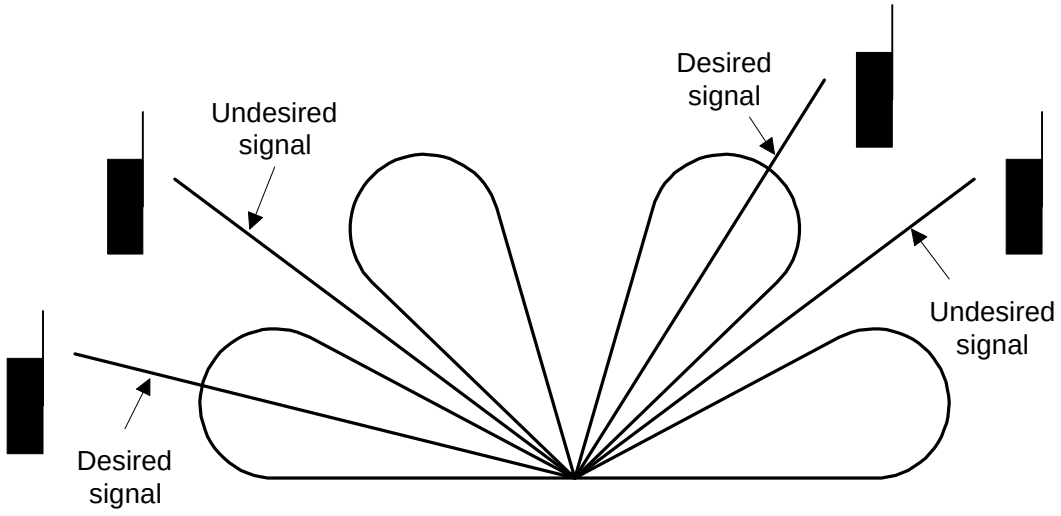
At VHF low band (50 MHz), a quarter wave monopole antenna is about 5 feet long. As the frequency is increased, the length of a monopole antenna is reduced. At 850 MHz, a monopole is only 3.5 inches long.

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:

$$\begin{aligned} P_{IN} &= 20 \text{ dBW} \\ L &= -3 \text{ dB} \\ G_{ANT} &= \underline{\ \ 6 \text{ dBd}} \\ ERP &= 23 \text{ dBW} \end{aligned}$$

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

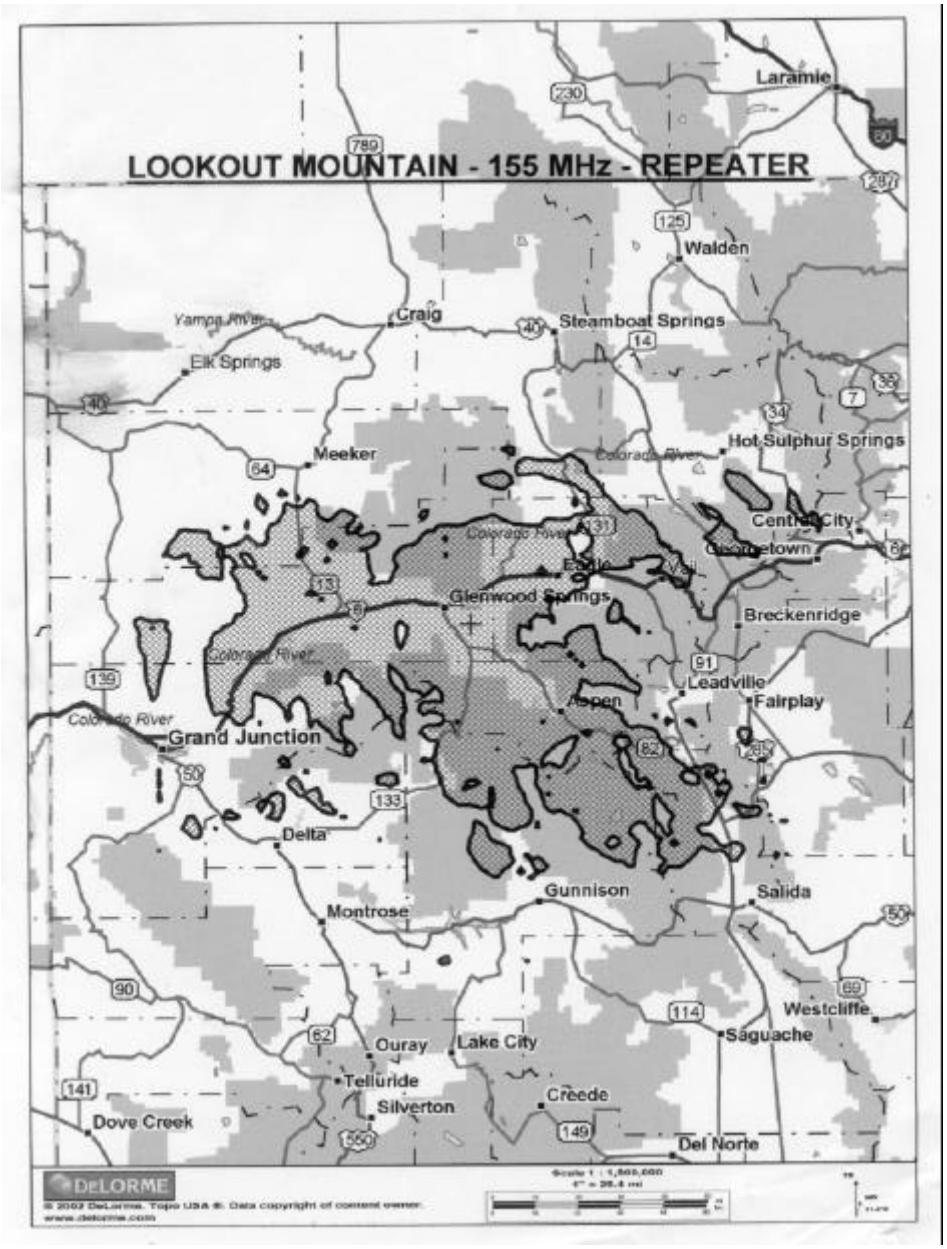
One of the most important characteristics of a radio system is its *coverage*. That is, it is important to know exactly where the base or repeater station signals may be received by mobile or handheld radios and exactly where mobile or handheld radio stations may be heard by a base or repeater station.

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

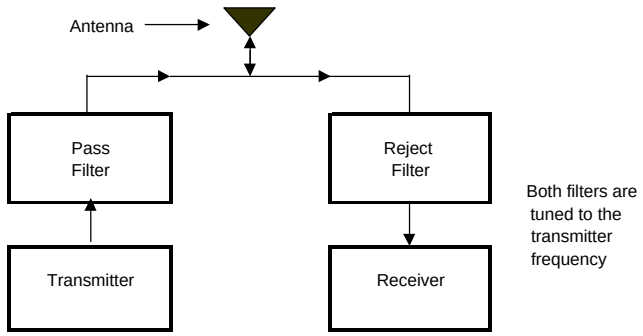


Figure 6-16. Typical Transmitter - Receiver Duplexer

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

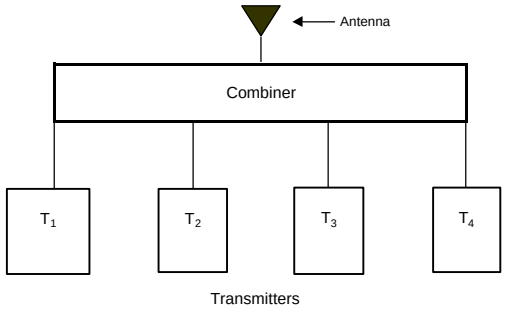
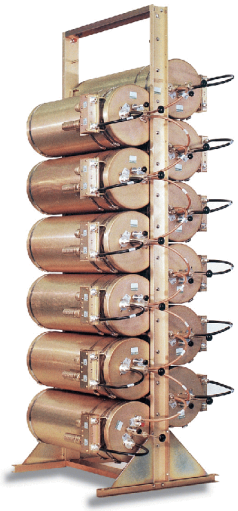
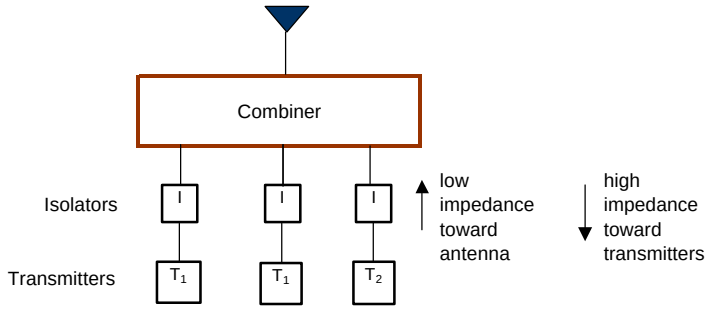


Figure 6-18. Typical Transmitter Combiner



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

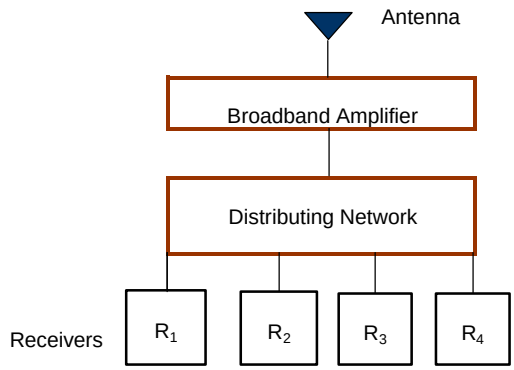


If there is inadequate isolation, the mixing of the transmitted signals can cause the generation of additional frequencies called intermodulation products, or IM products, which may cause interference to nearby receivers.

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

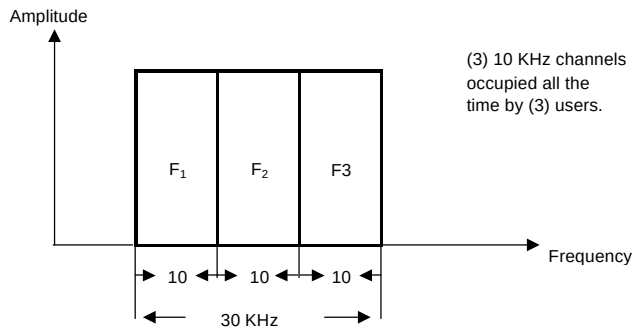
Several cellular radio systems are used to improve spectrum efficiency, allowing more users to employ a channel or frequency band. The primary technologies used today are frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). Public 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)

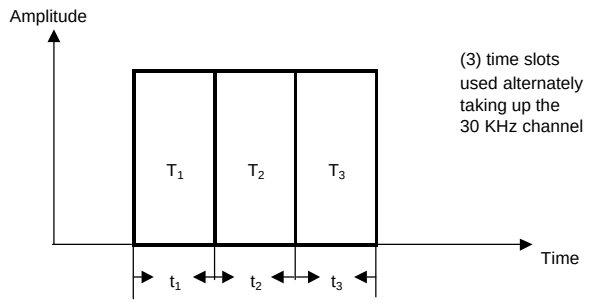


Time Division Multiple Access (TDMA)

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

Start Flag	Address	Message/ Information Data Field	Error Check	End Flag

[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.

Motorola Solutions, Inc., Ex1017, p. 74

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.

Motorola Solutions, Inc., Ex1017, p. 75

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.

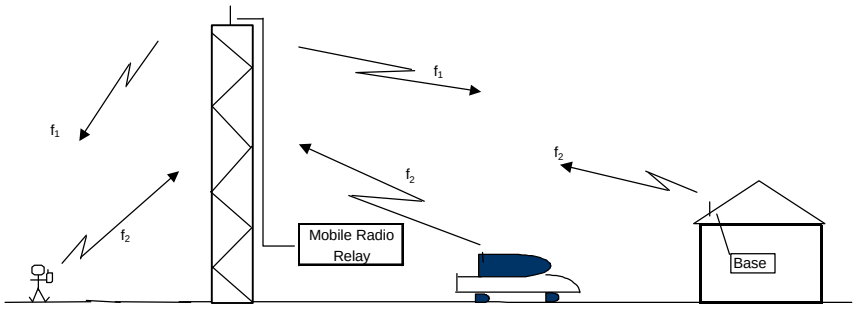
Base stations usually have high antenna installations to make sure that they can attain the desired radio coverage area. One problem with a simplex system is that handheld and mobile radios cannot communicate very far with each other because of their low antenna heights and are usually limited to just 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



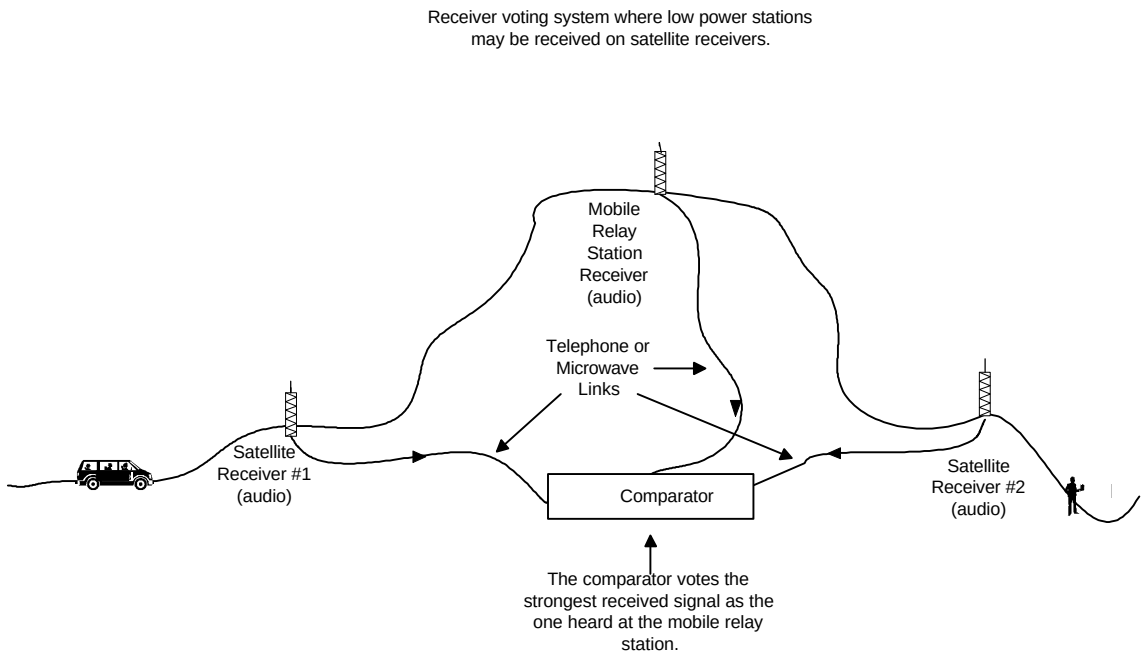
Mobiles, low power base and handheld radios transmit on frequency f_2. The signals are detected by the repeater and remodulate a transmitter on f_1 at the mobile relay site.

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

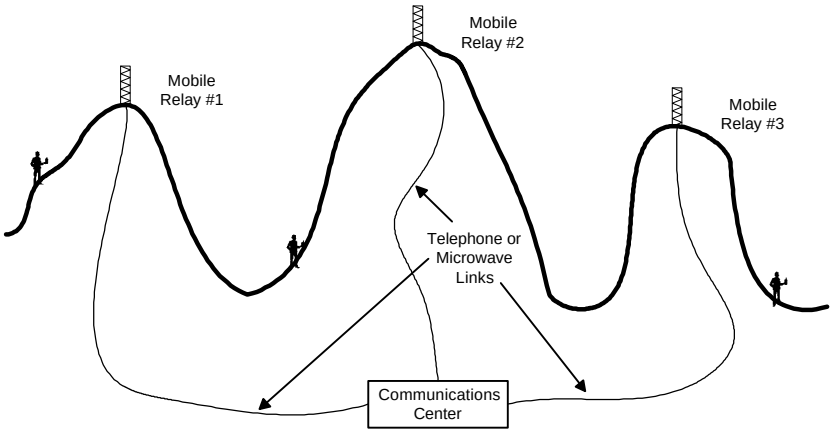


Another scheme used where there are problems transmitting to and receiving from mobiles and handheld radios due to large changes in topography requires several repeaters at different locations that may be switched at a central position, usually at the police communications dispatch center, to the repeater 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

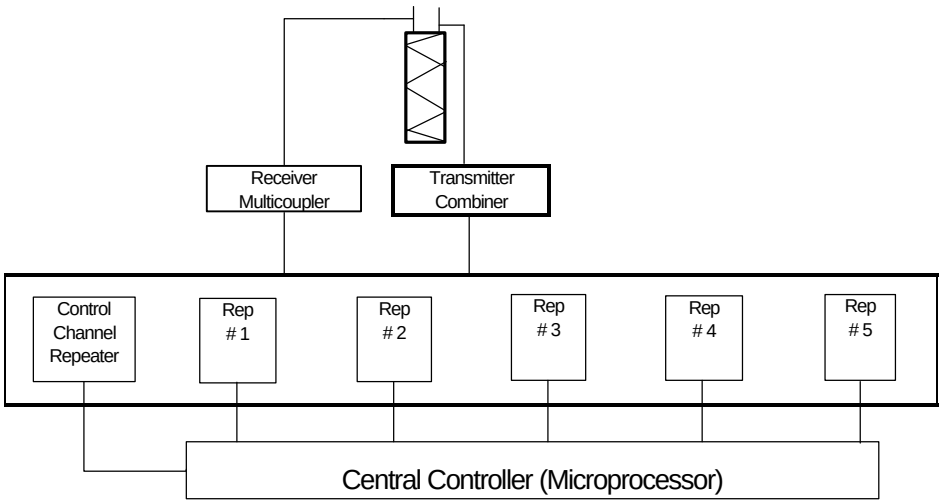
Public safety organizations have traditionally used dedicated repeaters. For example, in many communities, separate repeaters are used by the police department, the fire department, administrative departments, and road maintenance department, although the transmission loading is unequal for the departments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

Motorola Solutions, Inc., Ex1017, p. 81

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.

Motorola Solutions, Inc., Ex1017, p. 83

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.

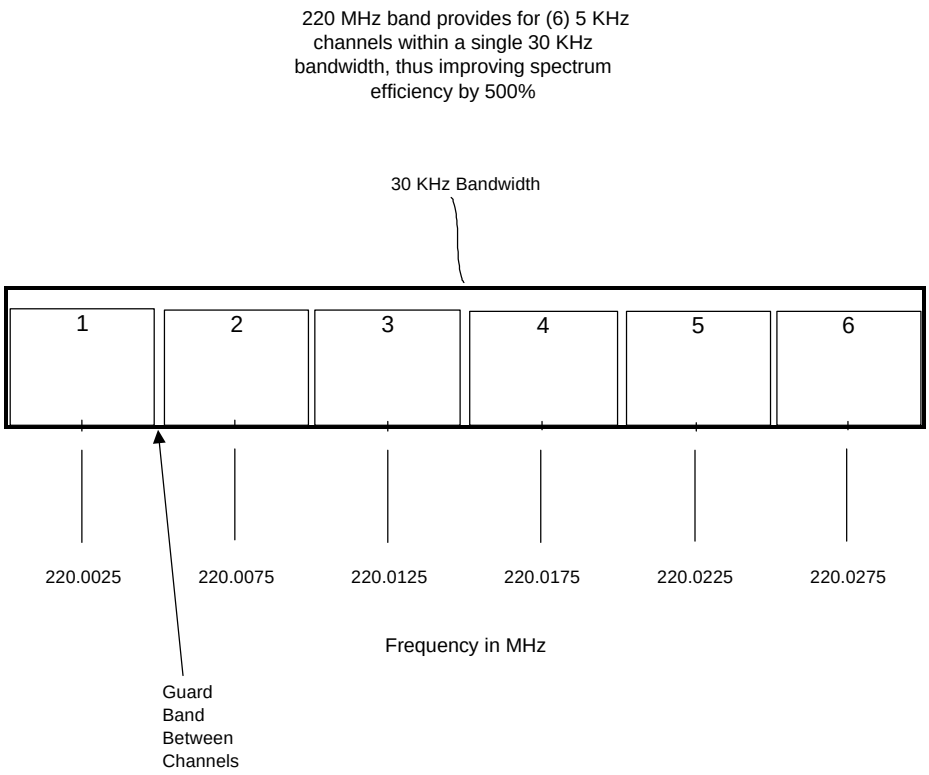
220 MHz Narrow Bandwidth Band

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



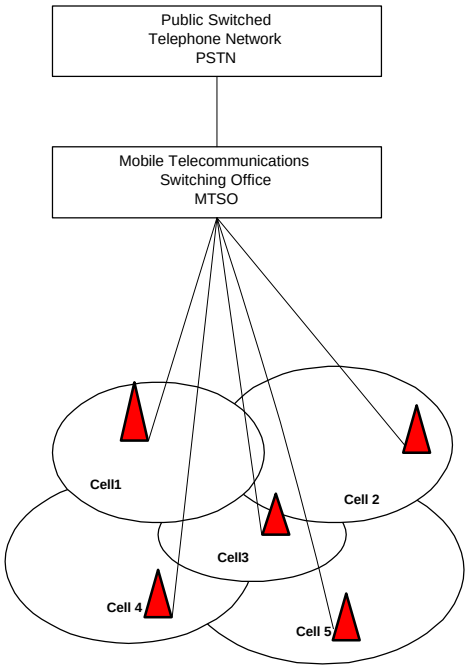
Cellular Radio/Telephone Systems

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.

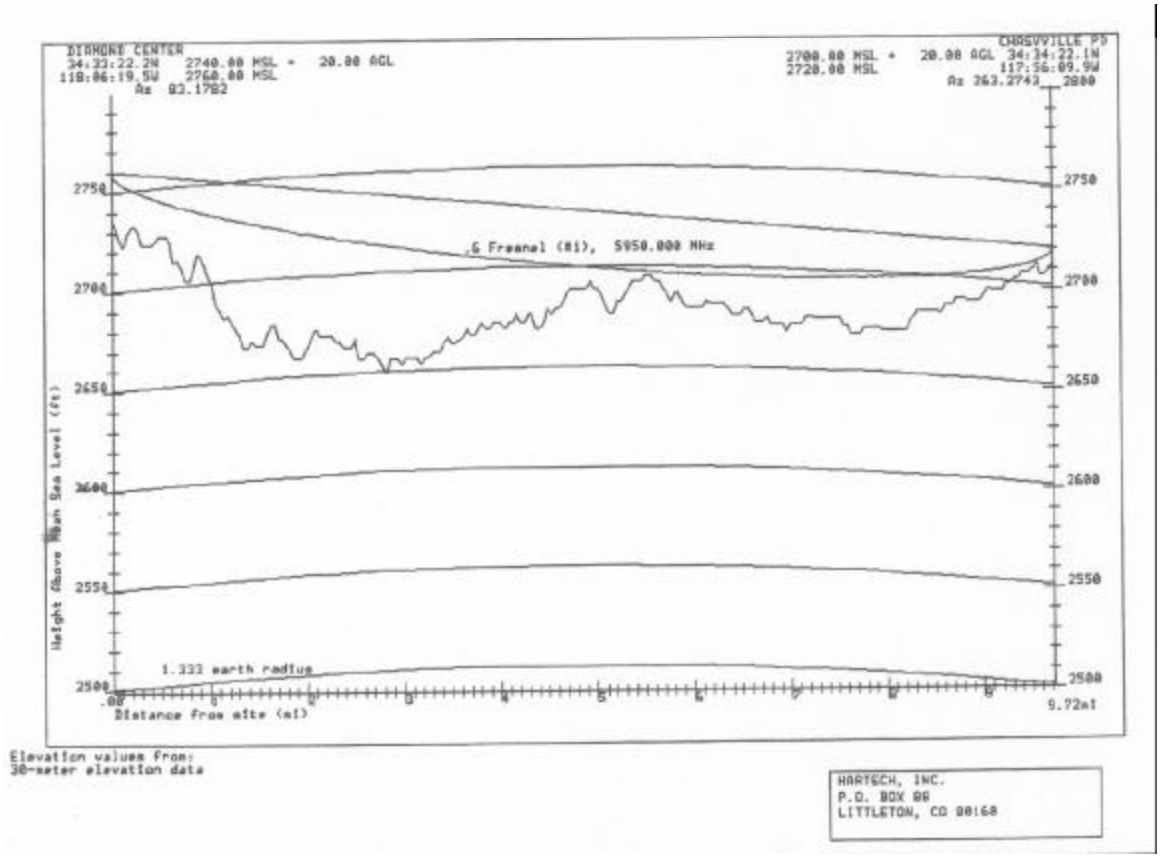
Most microwave communications systems require FCC licensing under Part 101 of the FCC Rules and Regulations. Frequency coordination is required and the applicant must utilize the FCC's Universal Licensing System (ULS) at the FCC website (see resources in appendix B) for all applications. There is a class 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.

Motorola Solutions, Inc., Ex1017, p. 89

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.

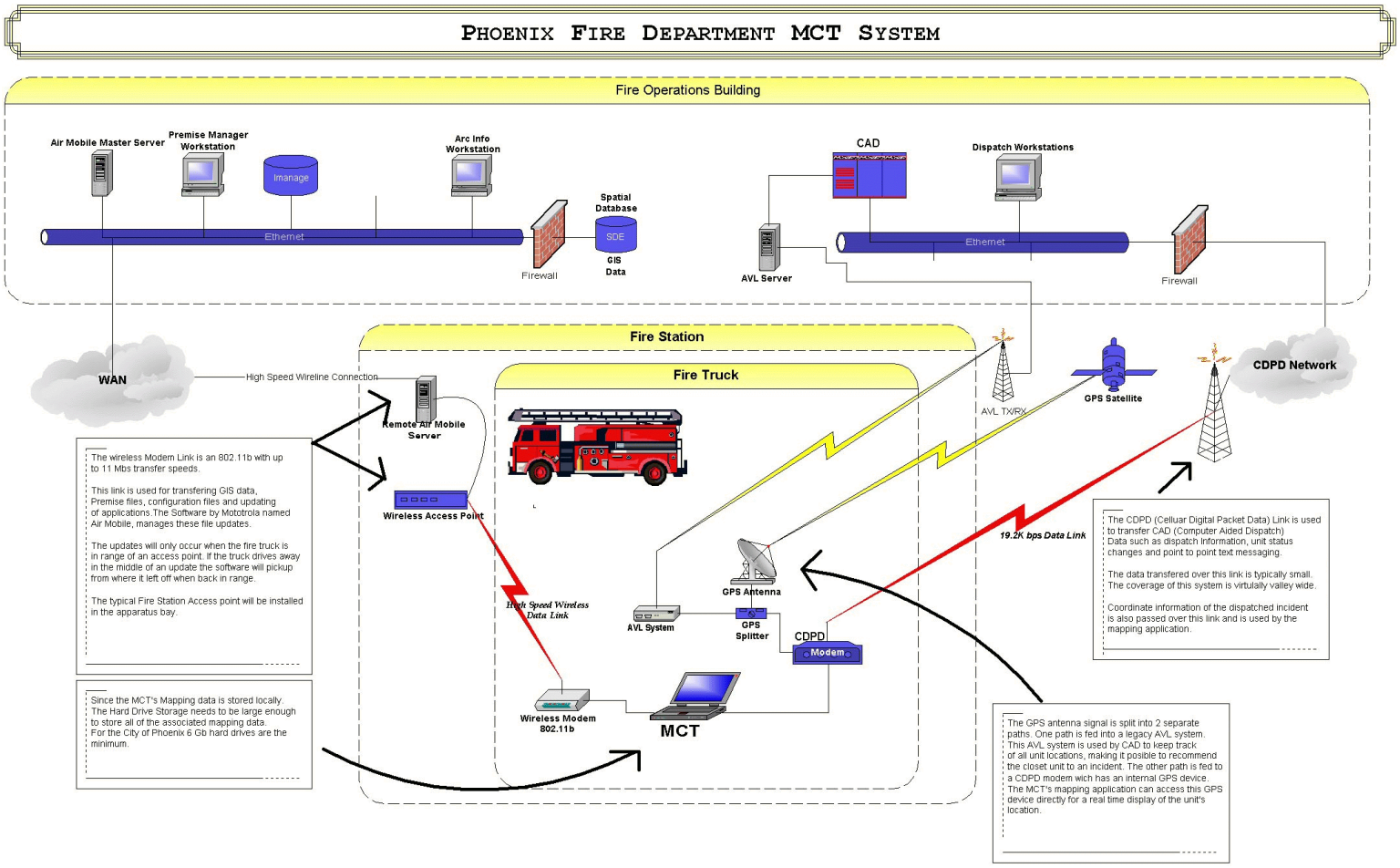
[3] 802.11h is being developed for the European market.

[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.

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.

☞ 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.

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.

Motorola Solutions, Inc., Ex1017, p. 94

PART 3

WIRELESS COMMUNICATIONS ISSUES

This portion of the handbook is a brief description of frequency licensing and pertinent FCC Rules, a description of the newly reallocated television channel frequencies for public safety, a discussion of the FCC's "refarming" policy, a discussion of tower siting and FCC radiation specifications (OET Bulletin 65), information on various Federal initiatives, and a discussion of the issues surrounding interoperability.

Motorola Solutions, Inc., Ex1017, p. 95

Chapter 8

FCC Licensing, Rules, Regulations, and Related Issues

The FCC Rules and Regulations are printed in the Code of Federal Regulations (CFR), Title 47. Copies of the rules may be purchased from the Government Printing Office (GPO) (see resources in Appendix B). The following parts of CFR 47 are of interest for mobile radio communications services:

Part 90 - Private Land Mobile Radio Services (PLMRS).
Part 22 - Public Mobile Services.
Part 24 - Personal Communications Services (PCS).
Part 101 - Fixed Microwave Services.

Copies of the Rules may be downloaded from the FCC Web site (see resources in appendix B) or purchased at GPO bookstores.

Licensing

If you are buying a system or constructing it yourself, you will need to apply for a license. However, before applying to the FCC, you must obtain specific frequencies of operation from a frequency coordinator. The coordinator will check to see if any frequencies are available in your area and assist you in evaluating your options.

There are four coordinating bodies responsible for public safety-related frequencies:

APCO - Association of Public-Safety Communications Officials.
IMSA - International Municipal Signal Association.
FCCA - Forestry Conservation Communication Association.
AASHTO - American Association of State Highway Transportation Officials.

In the past, the coordinator for most local public safety frequencies has been APCO. However, with the implementation of refarming (see the end of this chapter), applicants may use the services of any frequency coordinator certified to coordinate frequencies in its pool of eligibility. Contact numbers for all four coordinating bodies are given in resources, appendix B.

Motorola Solutions, Inc., Ex1017, p. 97

The application form for radio licenses is FCC Form 601 for two-way radio frequencies. For FCC microwave frequencies, the application is FCC Form 415. Forms are available from the FCC or may be downloaded from its Web site.

In addition, if one of your base, repeater, or microwave stations requires a tower or an antenna tip with a height of 200 feet or more, you will need to complete a Federal Aviation Administration (FAA) Form 7460-1. If your antenna is within 5 miles of an airport runway and its height (in feet) is greater than or equal to 40 times the distance to the runway (in miles), you will also need to complete the same form.

If you are purchasing communications services from a licensed vendor, you will not have to obtain licensing. If you are sharing a system with another agency, make sure that the other agency is licensed. Normally, a letter contract or a memorandum of understanding (MOU) is drawn up between the licensed agency and a user.

FCC Rules and Regulations

Part 90

Part 90 covers the Rules for a number of *private land mobile radio services* including those for public safety. This section specifies the frequencies available for the various private and public safety services, licensing information, and technical and operating requirements. Technical rules include types of modulation, bandwidths, interference criteria, power output, and antenna height data.

Licenses require frequency coordination. Public safety agencies generally must use APCO for coordination. No Federal fees are required for license applications from local government applicants.

Docket 92-235. In FCC Docket 92-235, adopted in February 1997, the FCC reduced the number of service pools for frequencies below 512 MHz to two:

1. *Public safety,* consisting of local government, police, fire, highway maintenance, forestry conservation, emergency medical, and special emergency.

2. *Industrial/business,* consisting of power, petroleum, forest products, film and video production, relay press, special industrial, business, manufacturers, telephone maintenance, motor carrier, railroad, taxicab, and automobile emergency.

Certified frequency coordinators for the particular services are still required to assign frequencies for these services. The FCC also authorized centralized trunking at allocated frequencies from 150 to 512 MHz, providing no harmful interference is caused to existing channels.

Part 22

Part 22 of the Rules covers the licensing and technical requirements for *common carrier mobile radio services,* including paging and radio telephone services, rural radio telephone service, and cellular radio.

Public safety agencies may use these services as subscribers only; the licenses are held by the service providers.

Part 24

Part 24 covers the Rules for personal communications services. This unique set of Rules deals with the auctioning of frequencies in the 900 MHz and 2 GHz bands. There is little technical detail, since winners of the auctions may provide many different types of service within the areas where they have won licenses.

At this time, the majority of 2 GHz PCS licensees are providing cellular voice services similar to those in the cellular radio frequency band.

Part 101

Part 101 covers microwave point-to-point radio frequencies. Frequency coordination, licensing, and technical standards are identified.

Refarming

The "Part 90 refarming" was officially adopted by the FCC in several dockets:

Docket 92-235 (6/15/1995).
Docket 92-935 (12/23/1996).
Docket 92-235 (2/20/1997).[8]

The purpose of this initiative is to reduce most of the bandwidths of Part 90 radio systems operating below 512 MHz, thus promoting an increased efficiency in use. The reduction is in two stages: first from 25/30 KHz to 12.5/15 KHz and then from 12.5/15 KHz to 6.25/7.5 KHz bandwidths over a period of time. Licensees will not be required to replace their equipment to meet the band reduction requirement.

Currently, manufacturers are required to supply new equipment meeting the 12.5/15 KHz bandwidth specification, allowing for a smooth changeover. The bandwidths must be halved by manufacturers again by January 1, 2005. More details regarding refarming may be found in the footnoted reference.

Frequency Reallocation

In July 1995 the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) established the Public Safety Wireless Advisory Committee (PSWAC) to evaluate the wireless communications needs of federal, state, and local public safety agencies through the year 2010 and recommend possible solutions to identified problems. In the PSWAC final report, published in September 1996, five primary areas of concern were documented: operational requirements, technology

[8] Ericisson, *Refarming - Truths and Myths* (brochure), February 1998.

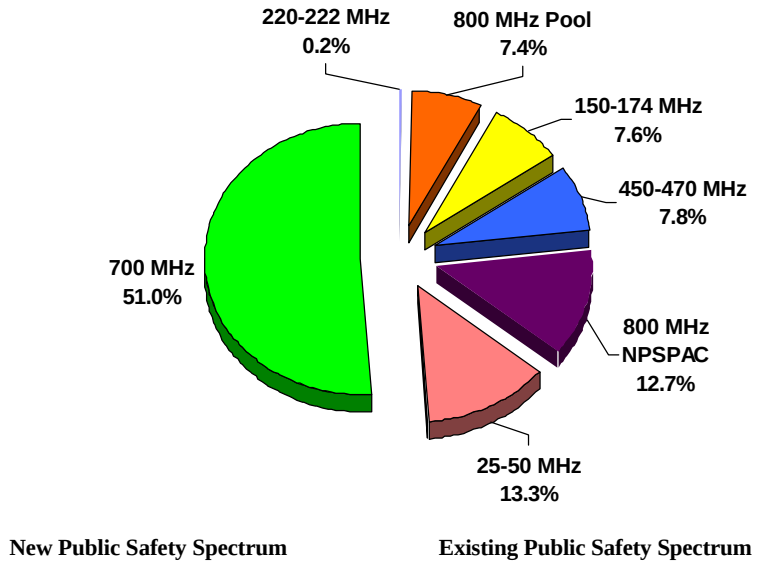
issues, technology transition, interoperability, and the need for additional spectrum. PSWAC recommended utilizing portions of the 746-806 MHz band (UHF TV channels 60-69).

When the FCC reallocated an additional 24 MHz of spectrum in the 700 MHz band for public safety use (specifically TV channels 63, 64, 68, and 69), the Public Safety National Coordination Committee was impaneled to establish plans for the use of the frequencies designated as interoperability channels. The net effect will be to double the amount of spectrum available for public safety communications (figure 8-1).[9]

The work of the NCC's Implementation Subcommittee identified the need for an information resource to support the planning and pre-coordination necessary for efficient and effective allocation of the 700 MHz public safety spectrum.

The National Public Safety Telecommunications Council (NPSTC), an ad hoc federation of federal, state and local associations and agencies, along with the Public Safety Communications Council (PSCC), an association of the four FCC certified public safety frequency coordinators, requested the development of a pre-coordination database designed to facilitate inter-regional coordination in the pre-allotment of frequencies, the development of state or regional plans, and the automation of initial and amended applications for frequency use.

Figure 8-1. Public Safety Spectrum Doubles



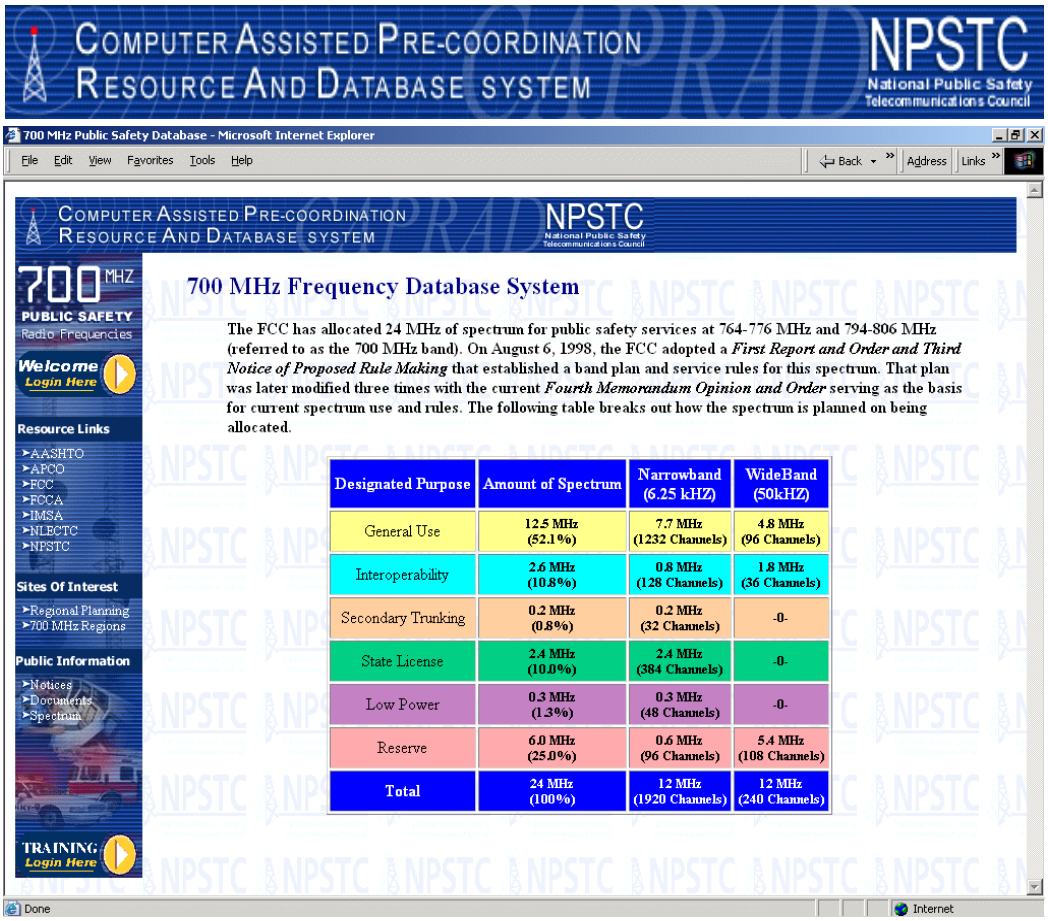
[9] "FCC Allocates More Spectrum to Public Safety," *Government Technology* (March 1998): 12.

Computer Assisted Pre-coordination Resource and Database (CAPRAD)

Originally envisioned as a notebook of available frequencies in the newly allocated 700 MHz public safety spectrum from which planners could formulate regional plans and select channels from for use within their regions, the Computer Assisted Pre-coordination Resource and Database (CAPRAD) has evolved into a suite of tools and resources which will assist regional planners, coordinators and users in managing the 700 MHz band from regional planning to consumer licensing.

The CAPRAD system features website access with a graphical user interface, an informational front page and secure access for registered users. The system is comprised of several interactive, relational databases which provide a frequency availability "notebook", search and report generating tools, interface to the PSCC's automated systems, and on-line help facilities, manuals and resources for planning, allotments and licensing applications (see figure 8-2). The system also serves as a repository for supplemental information such as completed regional and state plans, lists of broadcast television channels with potential impact, the final FCC report and order frequency table, contact information for RPC chairpersons and others as required, plus links to valuable sites and services available on-line.

Figure 8-2. Sample CAPRAD Screen



Designated Purpose	Amount of Spectrum	Narrowband (6.25 kHZ)	WideBand (50kHZ)
General Use	12.5 MHz (52.1%)	7.7 MHz (1232 Channels)	4.8 MHz (96 Channels)
Interoperability	2.6 MHz (10.8%)	0.8 MHz (128 Channels)	1.8 MHz (36 Channels)
Secondary Trunking	0.2 MHz (0.8%)	0.2 MHz (32 Channels)	-0-
State License	2.4 MHz (10.0%)	2.4 MHz (384 Channels)	-0-
Low Power	0.3 MHz (1.3%)	0.3 MHz (48 Channels)	-0-
Reserve	6.0 MHz (25.0%)	0.6 MHz (96 Channels)	5.4 MHz (108 Channels)
Total	24 MHz (100%)	12 MHz (1920 Channels)	12 MHz (240 Channels)

The CAPRAD system's state-of-the-art architecture, multi-level security protocols, and mirrored data management plan ensure both system integrity and system reliability. Fully integrated technical features of the hardware, software and support equipment provide exceptional system performance, availability, and security of information.

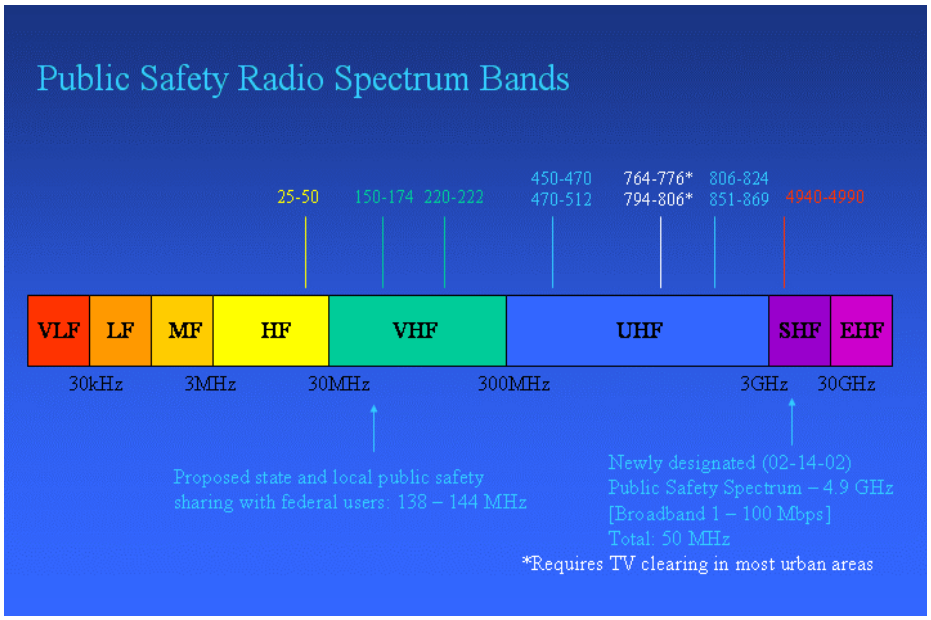
Years of planning by the NPSTC sponsored technical oversight working group, which included NPSTC technical membership, public safety frequency coordinator representatives and regional planners from across the country, and many months of development by the NPSTC Support Office and TEQ Services, Inc., a database and information systems firm in Englewood, Colorado, resulted in a database which will transform the regional planning process nation-wide.

Planning for and operation of the CAPRAD system is administered by the National Law Enforcement and Corrections Technology Center-Rocky Mountain Region, NPSTC Support Office. The NLECTC-RM is a program of the National Institute of Justice and is sponsored by the University of Denver through the Denver Research Institute (DRI). Special Federal funding supported the development of this database, as well as the outreach and training efforts required to assist the frequency coordinators and 55 regional planning committees (RPCs) in the use of the database and regional planning efforts.

4.9 GHz Band

Further FCC reallocations of the available spectrum occurred in February 2002. The 4.9 GHz band (4940-4990 MHz), originally transferred from Federal Government to private sector use in 2000 as substitute spectrum for the 4635-4685 MHz band which was reclaimed for Federal Government use, was reallocated to public safety use. This reallocation is now the largest ever to be made in the interest of public safety nationwide encompassing 50 MHz of spectrum.

Figure 8-3. Public Safety Radio Spectrum Bands With Newly Allocated 4.9 Ghz Band



The 4.9 GHz band is designated for fixed and mobile wireless services use in support of public safety. The FCC's actions align with new national priorities focusing on homeland security and are intended to ensure that entities involved in the protection of life and property possess the communications resources needed to successfully carry out their mission. This allocation and designation will provide public safety users with additional spectrum to support new broadband applications such as high-speed digital technologies and wireless local area networks for incident scene management. The spectrum can also support dispatch operations and vehicular or personal communications.

Proceedings are underway which will establish the 4.9 GHz band licensing and service rules; define eligibility to use the band, including the scope of the public safety designation; delineate specific band segmentation and channeling plans; identify the interference impact on 4.9 GHz band operations from the adjacent U.S. Navy operations band; classify utilization of the band in a manner that will not interfere with the adjacent astronomy operations radio band; implement technical standards for both fixed and mobile operations on the band; and characterize innovative licensing approaches to serve public safety.

Chapter 9

Tower Siting and Radio Frequency Electromagnetic Radiation Exposure

Towers

All radio systems require towers to hold the antennas that transmit and receive radio energy. The higher the tower, the larger the coverage area for a given antenna. And, in general, as the capacity of radio systems is increased, more towers are required to attain necessary reliable area coverage.

Tower permits are issued by local zoning departments which require applicants to submit proposals for their approval. A portion of the local zoning ordinances is related to Federal requirements. These requirements include compliance with the National Environmental Policy Act (NEPA), the National Historic Preservation Act (NHPA), the Migratory Bird Treaty Act (MBTA), and the Endangered Species Act (ESA). Included in the NHPA are protections of certain Native American and Native Hawaiian tribal properties. Historic properties getting special treatment are those listed in the National Register, which is kept by the U.S. Department of Interior.

These acts are described in detail in the FCC Rules and Regulations, Sections 1.1301 through 1.1319. To meet the requirements of these acts, it may be necessary to complete an Environmental Assessment (EA) or an Environmental Impact Statement (EIS) to demonstrate tower installation compliance. There are other federal environmental requirements including meeting the FCC standards for hazardous radiation described below.

Although application processes vary from one governmental body to another, public hearings are usually required to receive input from those supporting or objecting to proposals. Unfortunately, the "not in my backyard syndrome" has been a powerful influence on the results of these hearings. The public often wants better public safety services but is not willing to accommodate new towers in their neighborhood without a battle.

Many local zoning ordinance policies are written to maximize the number of users on existing and new towers in order to minimize the total number of towers. In addition, the ordinances are written to maximize the number of "stealth" towers where appropriate. Stealth towers take advantage of existing natural and man-made structures such as high building roofs, church steeples, mountain sites and imitation trees. Anything that can be done to make towers less aesthetically imposing helps with the approval

Motorola Solutions, Inc., Ex1017, p. 105

process. For example, monopoles are often less obtrusive then lattice towers. However, most antennas need to be high, and it is difficult to put up beautiful towers at a reasonable cost.

Fortunately, public safety agencies have a bit more clout than private entities. Where possible, negotiating with private applicants for antenna space is often beneficial for both the private and public entities. The Communications Act of 1996 contains language which requires communities to accommodate "reasonable tower heights," which is often useful in applying for tower permits. If permits are not approved, suing under the Act is possible but can take a very long time, so it is better to work carefully with and educate the public before and during the permit process.

Many tower leasing companies have space available for public safety organizations' antennas on an annual fee basis providing the new user does not cause interference to current users. Some of the larger tower companies are American Tower, SBA, Signal Tower, and Pinnacle Tower.

Towers near airports require special consideration. If a tower will be 200 feet or more high or is to be located within five miles from an airport runway (above a height slope of 40 feet per mile from a runway), a radio license applicant must also file a Federal Aviation Administration (FAA) Form 7260-1 with a copy to the FCC. The FCC will not issue a license without prior approval of the FAA.

When communications towers are constructed, the owner must register the antenna structure by filing FCC Form 854 either electronically or via paper. The registered tower is given a number and inventoried by the FCC. The criteria for FCC registration are identical to those of the FAA above.

Radio Frequency Electromagnetic Radiation Exposure

All licenses and renewals filed after September 1, 2000, require that the applicant certify that the environmental regulations of Section 1.1307(b)(1) of the FCC Rules concerning RF exposure will be (or are being) met. The hazardous radiation calculations especially for multiple transmitters at a site can be complex and may require the services of a Registered Professional Engineer who practices in this area to perform the calculations.

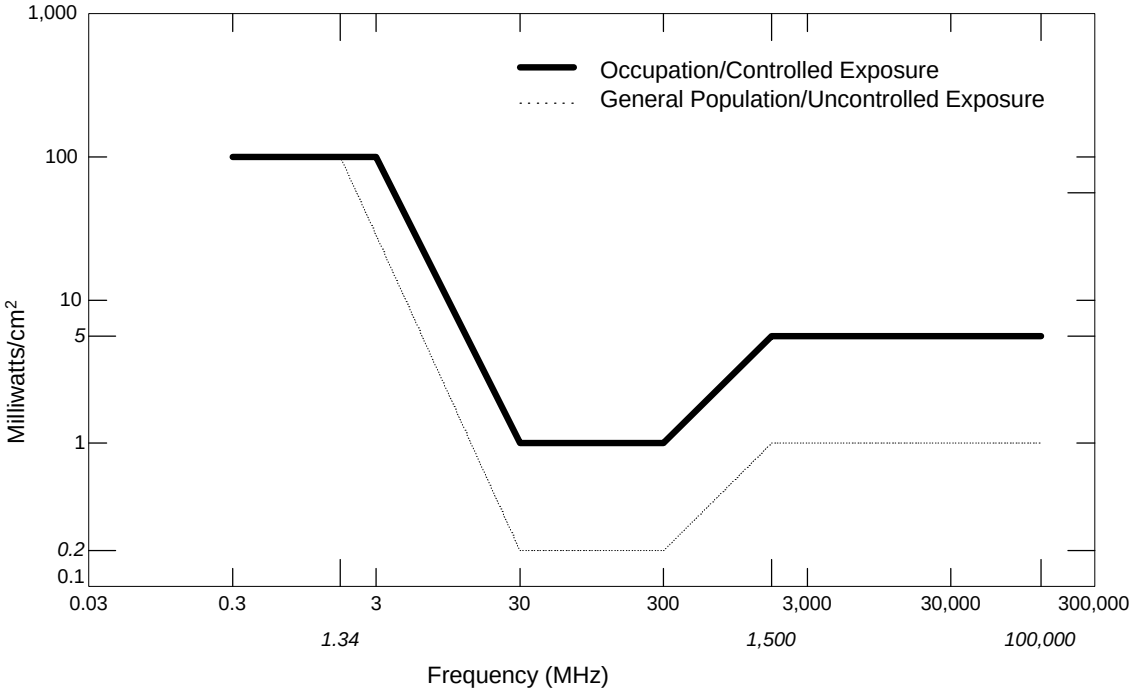
(Note: The methodology for making calculations is outlined in the FCC Office of Engineering and Technology Bulletin #65, "*Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Electromagnetic Fields*" upgraded in August, 1997, by a mandate from the 1996 Communications Act. The document may be downloaded at www.fcc.gov/oet/rfsafety.)

Before upgrading the bulletin in 1997, the FCC held extensive meetings with health and safety agencies, the medical community and universities working in RF non-ionized radiation research and confirmed there is no credible research showing any hazardous effects to human beings other than exceeding thermal dissipation rates within our bodies. This is analogous to a microwave oven where one places food into a known RF radiation field for a time period to heat it up. If you are exposed to RF radiation at too high a power and for too long, you will also "cook." Consequently, transmitter output powers may have to be reduced or transmitters be turned off while technicians work near transmitters or climb towers.

There are two standards listed in OET Bulletin #65, one for personnel who work on radio systems considered "occupational" and the other is the "general public". The standards vary with frequency bands because the human body is resonant and therefore can absorb more energy in the 30 to 300 MHz range than at other frequencies. Guidelines concerning fencing and signage where hazardous radiation may exist are also spelled out in the bulletin.

Figure 9-1 shows a graph of the standards for radiation densities. The worst frequency for RF absorption is in the 100 to 300 MHz range. At that frequency, the highest permissible RF level in controlled areas is 1 mW/cm^2 for 6 minutes of exposure time and 200$\mu W/cm^2$ in uncontrolled areas for 30 minutes of exposure time.

Figure 9-1. FCC Limits for Maximum Permissible Exposure (MPE)
Plane-wave Equivalent Power Density



Chapter 10

Federal Government and Other Initiatives

In addition to the FCC, the Federal government has a number of other initiatives that impact agencies at the State and local level. Some of the more obvious ones are discussed here.

NCIC 2000

The FBI's National Crime Information Center (NCIC) computer provides all 50 States with access to the records in the databases. Currently, more than half a million users in some 80,000 agencies make 1.7 million inquiries per day to NCIC.[10] Harris Corporation has been awarded a contract to upgrade the NCIC system, which includes replacement of the old computers with new IBM® 390 mainframes and operating systems. Projections call for up to 2 million transactions per day.

The NCIC 2000 project expects to support communication with mobile-imaging units in patrol cars.[11] The upgraded system will require that communicating units use TCP/IP over X.25 protocol before the system is placed online. After many users' requests, the FBI is considering other protocols such as TCP/IP over point-to-point protocol (PPP), Ethernet, and additional options. The FBI has conducted tests using various communications technologies, including CDPD, 800 MHz alone, and 800 MHz in conjunction with microwave.

An NCIC 2000 workstation has been developed for mobile-imaging units to transmit and receive mug shots and fingerprints. Plans call for high-quality imaging, including mug shot field imaging with high- quality field cameras so that officers may simply point and click. A quick check of a right index fingerprint will be possible with the fingerprint-matching subunit planned for use in the system. When the system is complete and operational, a field officer will be able to:

- ➡ Enter a wanted person's fingerprint, mug shot, and identifying images.
- ➡ Identify a wanted person using a fingerprint.
- ➡ Modify a fingerprint entered into NCIC 2000 with a new fingerprint.
- ➡ Link a wanted person's fingerprint to one entered by another organization.

---

[10] "FBI Readies New Crime Information Network," *Government Technology Reseller* (March 1998): 30.

[11] Ibid.

- ➡ Cancel a wanted person's fingerprint.
- ➡ Receive ownership of a linked fingerprint when the original owner cancels the entry.

The NCIC workstation and the MIU (mobile imaging unit) are be based on Intel's Pentium technology. In addition, the FBI has published requirements for peripheral equipment (printers, scanners, data radio modems, etc.), commercial off-the-shelf software (COTS), and NCIC 2000 workstation applications software (to be provided by the FBI to the States at no cost). All of these specifications, as well as the latest status on the testing and implementation of the NCIC 2000 project, may be found by contacting the FBI directly (see resources in appendix B).

Public Safety Wireless Network (PSWN)

The Public Safety Wireless Network (PSWN) was created in 1996 through the National Partnership for Reinventing Government as an effort to re-engineer how government provides services to citizens through more effective use of information technology, among other approaches.

PSWN was specifically created as a jointly sponsored endeavor between the Department of Justice and Department of the Treasury to plan a nationwide wireless communications network for providing interoperability among federal, state, and local public safety entities. The Federal Law Enforcement Wireless Users Group (FLEWUG), which represents the interests of federal agencies with public safety missions, helped establish PSWN. In addition to oversight from the Departments of Justice and Treasury, the PSWN Program reports to the Government Information Technology Services Board (GITSB) .

The PSWN program is funded annually by the Departments of Justice and Treasury, with annual funding levels based on appropriations made by Congress. The program is a 10-year initiative.

Program Overview

The overall mission of the PSWN program has been to formulate a comprehensive plan for interoperability among wireless networks so local, state and federal public safety requirements can be met. PSWN is pursuing a number of system development support activities, analytical studies and outreach efforts which may be viewed on their website (see resources in Appendix B). The program is working to achieve a vision it shares with the public safety community -seamless, coordinated and integrated public safety communications for the safety and efficient protection of life and property. The program's primary objective is to develop a national implementation plan for interoperability based on an information and experience baseline developed during the course of the program.

The PSWN program is pursuing technical assistance, case studies, and analysis efforts throughout the country, including San Diego , the Mexican border area, Alaska, Arizona, Idaho, Mississippi, Tennessee, West Virginia, and Wyoming. Through these efforts, the program hopes to develop a better understanding of existing public safety interoperability problems. The field data is helping leaders understand public safety communications limitations because the information is comprehensive rather than anecdotal.

Motorola Solutions, Inc., Ex1017, p. 110

Near- and long- term recommendations for solutions to improve interoperability will be based on this analysis. These efforts have evolved into pilot projects sponsored by PSWN which are being used as test-beds for demonstrating interoperability technical, policy, and piloted solutions. In addition, the PSWN program participates in test-beds, demonstrations and special events sponsored by other organizations such as the National Institute of Justice (NIJ).

PSWN has completed an effort to develop a Wireless Interoperability National Strategy called Public Safety WINS. Public Safety WINS serves as the PSWN program's key mechanism to synthesize and apply the data the program has gathered into a coherent solution - oriented strategy for improving interoperability.

PSWN is also pursuing a number of directed and special studies in the areas of coordination/partnerships, funding, spectrum, and standards. The program is trying to help the public safety community better understand various aspects of spectrum policy, legislation, management and regulation through a number of reports that can be found on the PSWN website library.

The National Institute of Justice and Its Interoperability Program

Created by the Omnibus Crime Control Act of 1968, the National Institute of Justice (NIJ) is the research and development arm of the U.S. Department of Justice. With one of its primary mission elements aimed at developing new technologies to fight and improve criminal justice, NIJ (through its Office of Science and Technology (OST)) is addressing the issue of interoperability among criminal justice and other public safety agencies. The concept of interoperability is discussed further in Chapter 11 below.

Advanced Generation of Interoperability for Law Enforcement (AGILE) Program

The National Institute of Justice (NIJ) has developed a focused, comprehensive program to address interoperability - the Advanced Generation of Interoperability for Law Enforcement (AGILE) Program. The AGILE program was created in 1998 to pull together all of the interoperability projects currently underway at the National Institute of Justice. AGILE's strategy addresses both short- and long-term interoperability solutions involving wireless telecommunications and information technology applications through three program elements:

- Standards
- Research, Development, Testing, and Evaluation
- Outreach

Developing Interoperability Standards for Public Safety

NIJ is identifying, adopting, and when necessary, developing open architecture standards for voice, data, image, and video communications systems for the public safety community. It is doing this in partnership with NIJ's Office of Law Enforcement Standards (OLES), located within the National Institute of

Motorola Solutions, Inc., Ex1017, p. 111

Standards and Technology (NIST); the National Telecommunication and Information Administration (NTIA); and other key organizations. AGILE is also working with the Global Advisory Committee.

Integrating, Testing, and Evaluating Interoperability Technology

The AGILE program will use operational test beds to integrate, test, and evaluate technologies that can contribute to addressing interoperability needs. AGILE is developing new technology solutions when shortfalls of existing technologies are identified. Results of operational evaluations will be shared with State and local public safety agencies.

Raising Awareness of Interoperability

AGILE aims to raise the awareness of interoperability issues through an outreach program so that policy makers and public safety leaders can make informed and cost-effective decisions. Through technology assistance to State and local agencies, AGILE helps disseminate short-term interoperability solutions, lessons learned or best practices, and NIJ's standards for interoperability as they are established.

Up to date information on the AGILE program, as well as other developments in interoperability, can be found on the AGILE website (see Resources).

Mobile Broadband for Emergency and Safety Applications (MESA)

Project MESA is a collaborative partnership made up of the European Telecommunications Standards Institute (ETSI) and the Telecommunications Industry Association (TIA) in the United States to generate the specifications for a suite of wireless technologies requiring the mobile and fixed radio transmission of data rates of up to 2 MB per second for emergency services, law enforcement, medical services and civil defense entities. The activity of this partnership devoted to public safety is called the Public Safety Partnership Project (PSPP) which constitutes the legal and operational framework for the standards developments. Accomplishments may be checked out on the Project MESA website, www.projectmesa.org.

Specific aims of the group are to provide common European and U.S. standards for:

* The communications management at crisis and disaster centers by public safety officials to minimize the loss of personnel and assets.

* The delivery of fire information communicated by sensors attached to fire fighters in burning structures to the fire management team to optimize fire fighting activities. Also video and sensor communications from planes over forest fires to better aid the protection of fire fighters and maximize the use of fire equipment.

* Front line medical assistance for injured citizens including the monitoring of vital medical signs, two-way communications of EMS technicians to a medical facility, and streamed video.

Motorola Solutions, Inc., Ex1017, p. 112

* Interconnection of broadband satellite constellations to ensure stable communications from remote areas where terrestrial infrastructures have been seized during natural disasters.

* Coordination of military requirements for a wide variety of applications. For example, with terrorist activities possible and the potential for small military conflicts, the standards could be applied to NATO or U.S. Army "commercial procurement of off-the-shelf (COTS)" equipment.

* Communications from mobile robotics used by public safety and the military to inspect and report video and audio information via wireless communications from inside dangerous territories. This includes the discovery of injured people in hazardous areas due to earthquakes or fires, narcotics undercover investigations, SWAT team actions, automated inspections in inaccessible regions etc. and military operations including the discovery of mine locations.

*Interoperability with existing and future broadband LEO and MEO communications satellites and High Altitude Platform Systems (HAPS). The Project MESA team believes satellite and HAPS communications will accomplish the interoperability out of small cell regions when necessary.

* Quickly establish "ad hoc" networking to deploy broadband communications integrated with terrestrial networks in both the public safety and military sectors.

Additional applications may include:

* Airport security by transmitting suspect identification for fast broadcast to the public safety staff.

* Remote evidence gathering by law enforcement and peacekeeping operations.

* Airplane or helicopter surveillance communications of video, audio and data.

* Mobile surveillance for transmission of camera video to public safety teams.

* Electronic news gathering for radio and TV stations.

The Project MESA specification will complement, in terms of bandwidth positioning, existing and planned narrow band and broadband wireless standards. The project genesis was due to the APCO activities in their pursuit of Project 34 and the ETSI DAWS (Digital Advanced Wireless Services) program. A resolution to support Project MESA by making new spectrum available is slated to be discussed at the 2003 World Radio Conference (WRC 2003).

Motorola Solutions, Inc., Ex1017, p. 113

Chapter 11

Interoperability

"Lack of radio interoperability" is usually highlighted as one of the major problems following any large-scale public safety event, be it a bombing such as Oklahoma City, a hostage incident such as Columbine, wildland fires, or hurricanes such as Andrew. The events of September 11 again underscored the need for improvements in our ability to talk to one another, a capability hampered for years by technical, operational and political barriers, and by a lack of funding to make needed changes. Too often, interoperability is the forgotten stepchild as systems are improved or replaced.

Three Types of Interoperability

Interoperability falls into one of three categories. The PSWAC Final Report provides the following general descriptions of each:

- Day-to-Day

  1. Commonly used in areas of concurrent jurisdiction

     a. Agencies need to monitor routine traffic
     b. Minimizes need for dispatcher-to-dispatcher interaction

  2. If agencies are on different bands, may involve multiple radios in each vehicle

     a. Difficult for personnel using portable radios

  3. Infrastructure based interoperability is not efficient due to continuous use of an extra RF channel by each participant on a different band or system

- Task Force

  1. Usually involves several layers of government (fed/state/local)

  2. Opportunity for prior planning usually is present

3. Generally involves use of portable and/or covert equipment

4. Often requires extensive close-range communications

5. Nature of traffic is such that wide area broadcast is usually undesirable

6. May rove in and out of infrastructure coverage (metro to rural, in and out of buildings, etc)

7. Often implemented by exchanging equipment

- Mutual Aid

1. Can involve many agencies with little opportunity for prior detailed planning (e.g. riots or wild land fires)

2. Often requires assignment of several to many small groups, each on it's own talk group or frequency (tactical communications)

3. Once on-scene, generally involves use of portable radios

4. Many incidents are in rural areas out of infrastructure range

A detailed study by the PSWAC Interoperability Subcommittee found that 95% of all interoperability requirements fall into the "day-to-day" category. Good local communications must be promoted first. As an example, "automatic aid" where the closest unit(s) to an incident respond, regardless of jurisdiction, has been embraced by the fire services for many years, and is starting to make its way into the law enforcement community. Local interoperability is a must for automatic aid to work. It is the first, largest, and most important piece of the interoperability puzzle.

☞ Did you know?

"Interoperability is the ability to talk to who you need to talk to when you need to talk to them. It is not the ability to talk with everyone all of the time."

-- Chief Harlin McEwen (Ret), Chair, IACP Communications & Technology Committee

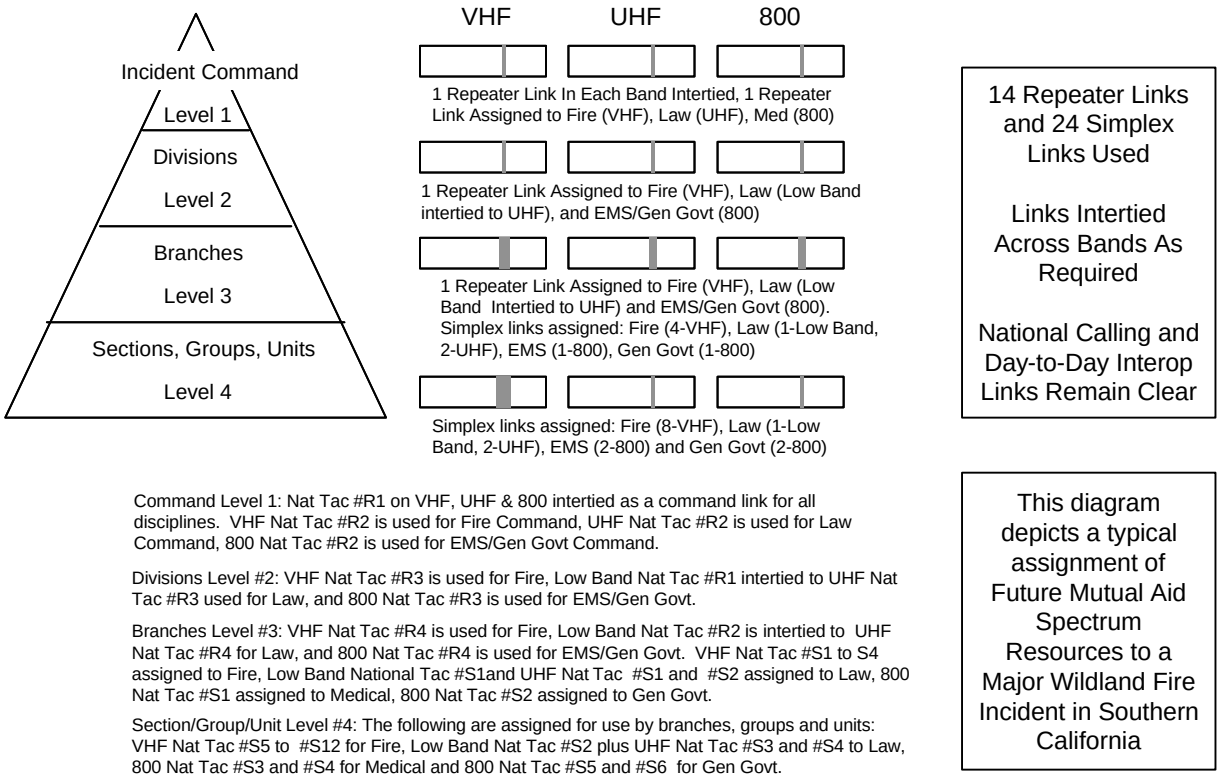
Task Force interoperability is more regional in nature. Once agencies have local interoperability, their next priority for communications is with other public safety agencies in their region/state. This is the second, and mid-sized piece of the interoperability puzzle.

Finally, mutual aid, typified by the massive multi-agency, multi-state responses seen in New York City and at the Pentagon on September 11, and experienced across the country each year for earthquakes, wild land fires, floods, hurricanes and other large-scale events, is the third type of interoperability. This is the national component of the interoperability puzzle. Mutual aid is usually tied to compacts implemented by state statute, thus the states must play an important role in interoperability as it expands to their boarders and beyond.

The FCC's National Coordination Committee for the 700 MHz band recognized this requirement, and the FCC embraced their recommendations when it recently incorporated the concept of State Interoperability Executive Committees (SIECs) into its regulations for the new 700 MHz band. That is not to say that States must control interoperability, rather that operational and technical requirements are best defined at the state level. SIECs will be most effective with broad representation from local, regional and state agencies within their boundaries. Proposals to expand the role of the SIECs beyond the 700 MHz band to include all spectrum assigned to local and State public safety agencies, as well as a number of Federal mutual aid channels, are now receiving wide support.

The following diagram provides the reader with an example of the interoperability links required to manage a major incident, in this case a large wildland fire similar to those that impact the western United States each year. This example was developed by the PSWAC after analyzing an actual incident in Southern California in the mid-1990s.

Figure 11-1. Interoperability for A Major Wildland Fire



Motorola Solutions, Inc., Ex1017, p. 117

Interoperability Obstacles

In the technology arena, local, state and federal agencies are split across nine major frequency bands. At best, public safety radios fielded today can cover two or three of these bands. Even if your system shares the same band with your neighbors, systems are implemented in different incompatible technologies by different manufacturers; this is particularly true for trunked radio systems.

In the operational arena, we choose to use different protocols and naming conventions. While the fire service has generally standardized nationally on the Incident Command System (ICS), law enforcement still "does its own thing" in different areas of the country. They install compatible channels in their radios and then agencies name them different names; the field officer doesn't know the technical details and just assumes they won't talk to each other! Finally, agencies rarely train together using the interoperability channels and so, when a major event occurs, must start from scratch on how to make it work.

Perhaps the most difficult obstacles to overcome are in the political arena. Fire and police agencies often don't see a need to intercommunicate. There are turf differences between agencies, and not just at the agency head level, but between field officers as well… between police officers and sheriff's deputies, between park police and highway patrol, and the list goes on. However, when a major incident happens, everyone works together and works together well - they get the job done to the best of all their abilities - and the rivalries disappear. Just think how much better and more efficient they could do that job if they could intercommunicate and did it often enough that it was second nature.

But the politics list goes further. It goes to long-standing friendships between agency heads and/or purchasing managers and radio suppliers that lead to the purchase of an incompatible system, even though all of your neighbors share a common technology. And it goes to local control… it has to be "my system" even though a regional system may be more effective and efficient, both operationally and financially.

Interoperability Solutions

The key to successfully implementing interoperability is to carefully examine current systems and communications links, and identify where additional links need to be established and what the technical and operational parameters are that apply in each instance.

Classes of Systems

There are several major classes of systems. The characteristics, requirements and limitations of each are generally summarized as follows:

Conventional Systems:

1. Can make use of simplex and/or repeater-based operations.

2. All subscriber units must be in same RF band.

3. Secure communications usually requires equipment from same vendor.

Analog Trunked Systems:

1. Currently available only in 400 MHz band for Federal agencies and 800 MHz band for State/local agencies.

2. Proprietary systems require subscriber equipment from the same manufacturer (or a licensed second-source provider).

3. Secure communications usually requires equipment from the same vendor.

Project 25 Digital (Conventional or Trunked):

1. Vendor independent (including secure mode).

2. Infrastructure not required for conventional operation.

3. Some advanced features may be proprietary to a particular manufacturer.

Infrastructure-Based Patching:

1. Necessary only in following cases:
    a. Non-compatible (generally trunked or secure) systems
    b. Subscriber units on different RF bands

2. Requires one RF channel on each participating system, but can waste spectrum, especially for day-to-day operations.

3. Not usable when out of range of infrastructure (remote areas, etc).

4. "Interoperability" radio coverage is only available in the coverage area that is common to all participating systems.

5. Provides control that may not be present with other technologies.

Cost

Even if the previously described barriers can be overcome, the issue of funding often overshadows the others. Changes are often expensive and must be planned far in advance. Government funding cycles are long and the processes arduous. It is not uncommon that, by the time a budget is approved, the proposed equipment is old technology. Fortunately, the events of September 11 have highlighted the need for federal assistance to local and State first responders. There will be financial relief, at least for the next few years, and public safety agencies must take advantage of this opportunity.

As a national priority, the ultimate goal for interoperability must be that the field officer has it "on the belt" and knows how to use it when an event occurs. There should be no delay in their ability to talk with whom they need to talk to when they need to talk to them.

That said, getting there is a difficult and expensive road to follow. Estimates place the interoperability price tag at about $18 billion for local and State agencies. And, the road is different for each of the over 45,000 first responder agencies in the United States. Interoperability is hampered by the diversity of public safety spectrum and differences in the technology each agency has chosen to implement.

General consensus is that, until an affordable all-band, multi-mode subscriber radio is available, the best solutions to interoperability will be (1) regional harmonization of RF band and chosen technology - the preferred method, and (2) a system of cross-band patching of infrastructure. Though typically much less expensive (a 12-channel any-band patch system can be implemented for about $75,000), this latter choice is less desirable because of the large amount of spectrum required in a major event and because patching systems are only effective within the common coverage area of all participating users, as highlighted above.

Ultimately, the most successful technical solution to interoperability, even if affordable, will not be effective without appropriate operational procedures and regular training and/or use.

PART 4

WIRELESS COMMUNICATIONS OPTIONS

This section looks at the options public safety agencies have for wireless communications, including the purchase of their own radio components and systems. The authors also have included examples in which local governments have used commercial services.

One special case is described in which a tower and radio supplier provided radio communications to a town by entering into an agreement to use some of the town's high-elevation real estate for commercial radio development in return for dedicated government radio systems.

Examined are the many commercial voice and data services available to public safety, including cellular and PCS, CDPD, GPRS, SMR/ESMR, and data networks.

Networks are complicated. They consist of three generic components—hardware, software, and middleware. Hardware consists of radios, modems, and laptop computers; software is the programming that runs the radio controllers, modems, and laptop computers; and middleware is the (software) glue that interconnects all the components together. Middleware must be selected that supports the required hardware and software protocols.

A reminder: All radio systems should be carefully checked to make sure they have the coverage you need. If you are purchasing a new system, make sure that the supplier gives you written assurances that the system meets your needs. If you need to communicate with handheld radios in reinforced concrete buildings, make sure the supplier knows and makes calculations taking that into account. There are independent consultants who also can perform these calculations if you need a verification check. If the radio network is already constructed, borrow or rent equipment from the supplier and make sure the coverage satisfies your requirements.

Motorola Solutions, Inc., Ex1017, p. 121

Chapter 12

Voice Systems

Dedicated Radio Systems

Dedicated public safety radio systems include all radio technologies, ranging from conventional FM simplex and repeater systems to very complex and expensive trunked wide-area analog and digital radio systems at all of the two-way frequencies.

There are many suppliers for public safety radio systems. Three companies, however, have supplied and continue to supply the majority of public safety conventional and trunked radio systems: the EFJohnson division of EFJ, Incorporated, the M/A-COM division of Tyco International, and Motorola Incorporated.

The three major companies had representatives on the Project 25 Committee, which selected the first phase digital trunked system technology standard to carry public safety communications into the next century. The Motorola protocol was selected for the first phase, and Motorola has offered its intellectual properties, royalty free, to other suppliers to allow competition. A large number of suppliers are developing systems using the new standard.

There are many other smaller suppliers of FM equipment, and some are supplying narrow band systems for the 220 MHz frequency band.

Sample Vendors

EFJohnson Division of EFJ, Inc. EFJ, Incorporated (formerly Transcrypt International, Inc.) was founded in 1978 to manufacture embedded voice privacy and specialized signaling add-on devices for land mobile radio. In later years, the company diversified its product line and began developing digital products. EFJ, Inc. bought EFJohnson Company, a manufacturer of two-way radios to support communication of public safety and commercial users, in 1997. The EFJohnson Company, founded in 1923, was one of the early pioneers in radio technology.

EFJohnson offers both conventional and trunked analog and digital radio systems. Its Multi-Net II trunked platform provides single-site, multisite, and wide-area simulcast solutions that are APCO Project 16 compliant. In addition, it offers digital Project 25-compliant radios, as well as analog portable equipment that is compatible with Motorola's SMARTNET II and SmartZone® systems. EFJohnson has also been a leader in introducing Voice Over IP (VoIP) technology to the public safety network environment.

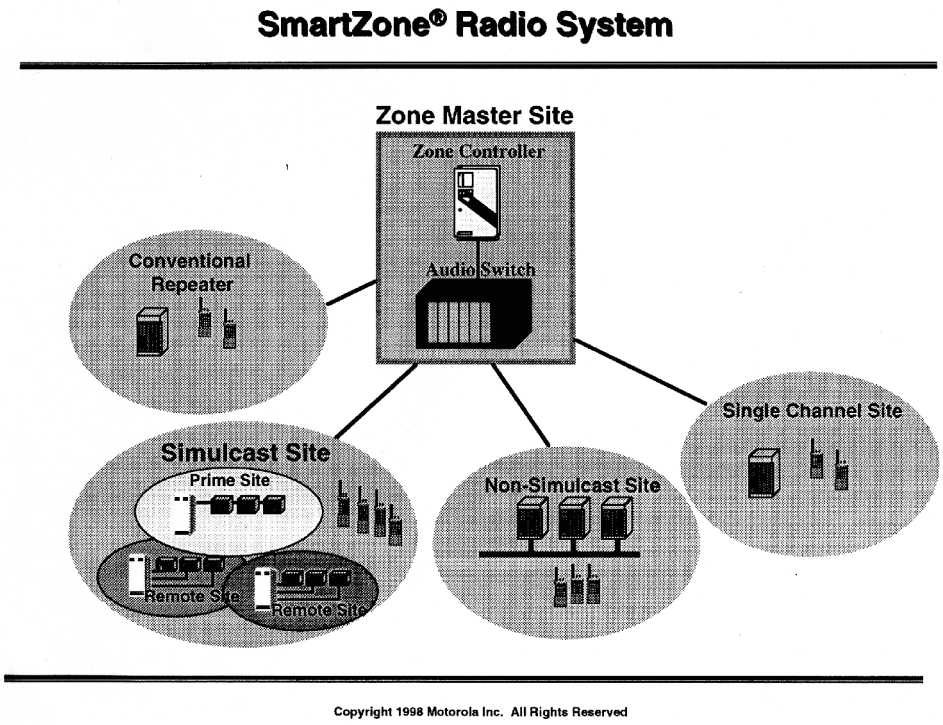
M/A-COM Division of Tyco International. The M/A-COM Division of Tyco International began as General Electric Mobile Radio. Through buyouts and mergers, it subsequently became Ericsson-GE, then ComNet Ericsson Critical Radio Systems. ComNet Ericsson was subsequently purchased by Tyco International and merged into its M/A-COM division. The result is the consolidation of two major public safety product lines

The main line of equipment acquired from ComNet Ericsson was its enhanced digital access communications system (EDACS), used by public safety agencies worldwide in trunked repeater systems (including wide-area simulcast coverage). M/A-COM brought its TDMA technology in a network configuration linked by VoIP. (Initially developed for the United Parcel Service, this technology has been upgraded for the public safety environment.) The initial rollout of the merged M/A-COM product line was for the State of Pennsylvania public safety system.

Motorola, Inc. Motorola was founded in 1928 as the Galvin Manufacturing Corporation. In the 1930s, the company commercialized car radios under the brand name "Motorola," a word selected because it suggested “sound in motion.” During this period, the company also established its police radio department. The name of the company was changed to Motorola, Inc., in 1947. Today Motorola provides software-enhanced wireless telephone and messaging, two-way radio products and systems, as well as networking and Internet-access products, for consumers, network operators, and commercial, government and industrial customers.

Motorola’s product line includes conventional and trunked wireless radio, integrated wireless voice and data radio, as well as dedicated wireless data. Its ASTRO 25 systems provide wireless voice and data solutions that meet the Project 25 standard. Its digital radio networks, as evidenced by its SmartZone® system, can be configured for conventional repeaters, single or multiple site trunked repeaters, and/or simulcast trunked repeaters, as shown in figure 12-1.

Figure 12-1. Motorola SmartZone® Radio System Configuration



Advantages of Dedicated Systems

1. Public safety entities may generate specifications to meet their exact system needs. They have complete control of the design and operations.

2. As part of the tailoring, the priority of use may be established within the entity.

3. Combined dedicated radio systems (i.e., shared with other communities) may save considerable investment and still preserve the tailoring at a more reasonable cost per agency.

4. Feature sets are chosen to meet public safety agency needs, not simply "what is available" from a commercial provider.

5. Proper design of a system ensures interoperability with other local, regional and national systems.

6. Priorities for expansion, operational issues, and restorability following an outage are set by the agency, not a commercial provider.

Disadvantages of Dedicated Systems

1. The capital outlay for an advanced digital systems may be quite high and prohibitive for a small to medium size community.

2. The owner of the system must pay for all maintenance and improvements.

3. Agencies need a certain level of in-house expertise for optimum operation.

Cellular and PCS Radio

The cellular and PCS industry has three major components: the manufacturers; the carriers, or service providers; and third-party agents. Manufacturers make the cellular and PCS equipment. Carriers provide the actual cellular and/or PCS telephone service. Third-party agents re-sell the equipment or services, but are generally not affiliated with either the manufacturers or the carriers. In this section, we limit our discussion to the carriers, as they are the ones dealing directly with the wireless networks.

Many law enforcement agencies are already using cellular radio systems in addition to their dedicated radio systems for the transmission of voice messages. Almost all urban and suburban areas in the United States are covered by one or more cellular providers, although in sparsely populated areas, coverage may not be available. Both analog and digital cellular service is provided by many carriers, but analog is being phased out by many.

In addition, the construction of personal communications systems (PCS), most of which are cellular systems in the 2 GHz band, has proliferated in higher density areas, and these systems are competing directly with 800 MHz cellular communications systems. There are as many as nine different technologies being used by different suppliers of cellular and PCS radio, so, once a user has chosen a company and handsets, it may be stuck with that supplier until the end of the contract.

System Coverage

System coverage is a major consideration in selecting a cellular system or PCS. The first thing to do when you think you want cellular or PCS service is identify the suppliers in your area. Contact them or go to the Internet and obtain a coverage map for your area for each supplier as well as its prices and terms. Borrow phones from suppliers and test different systems, where available, to determine which one covers your needs best.

Pricing

With the advent of increasing competition in many areas of the United States, the pricing packages are constantly changing, so you will need to get the latest information at the time of purchase. Law enforcement may have some leverage in negotiating with suppliers since it is a highly visible public agency.

Motorola Solutions, Inc., Ex1017, p. 126

Sample Vendors

The following list is not comprehensive, but is intended to provide examples of the types of national companies that provide this type of service. In addition to national providers, many urban areas also have local service providers (check your local telephone directory for contact information).

AT&T Wireless Services. AT&T has cellular and PCS licenses for most of the United States, originally using analog and then migrating to digital technology. They have begun to deploy GSM technology in the same areas where they currently provide TDMA coverage and expect to complete the deployment by the end of 2002. To determine if they provide coverage in your area, it is best to get the actual current coverage maps showing the specific area of interest (most can be obtained from the AT&T Wireless Services web site).

☞ Try this...

Find statistics about wireless carriers at CTIA's Web site:

http://www.wow-com.com

Cingular Wireless. Cingular Wireless is a joint venture between the U.S. wireless divisions of SBC and BellSouth. They have both TDMA and GSM nationwide voice coverage in most urban and many rural areas providing both cellular and/or PCS service. To determine if they provide coverage in your area, contact the company (their web site only provides calling rate area maps, not coverage areas).

Sprint PCS. Sprint PCS has almost all the U.S. licensed for PCS coverage. The network is an all-digital, all-CDMA, single frequency network., They claim 100% coverage for U.S. cities with populations of 100,000 or more. To determine if they provide coverage in your area, you can check the current coverage maps showing the specific state or zip code of interest by going to the Sprint web site.

Verizon Wireless. Similarly, Verizon Wireless has Nationwide coverage using CDMA technology. Their coverage footprint includes nearly 90% of the U.S. population, with 49 of the top 50 and 97 of the top 100 U.S. markets based upon population. Verizon Communications, the parent company of Verizon Wireless, was formed by the merger of Bell Atlantic and GTE. To determine if they provide coverage in your area, contact the company (their web site only provides calling rate area maps, not coverage areas).

Advantages of Cellular/PCS Radio

1. Where there is coverage, subscribers should be able to contact any field or fixed personnel, regardless of agency or jurisdiction (i.e., supports a high level of interoperability).

2. Pricing is competitive in most areas.

3. Service can supplement dedicated radio communications.

4. With digital protocols used by many cellular/PCS radios, listening by unauthorized scanners is limited or eliminated.

Motorola Solutions, Inc., Ex1017, p. 127

5. Under certain emergency conditions, some vendors can supply portable cell sites to the scene of emergencies to provide for increased cellular radio traffic.

6. Cellular radio systems tend to be reliable even under bad environmental conditions.

Disadvantages of Cellular/PCS Radio

1. Coverage is dependent upon a subscriber base to support service, thus may be limited or nonexistent in sparsely populated areas.

2. There is no priority of service for public safety users over other users of the cellular system. Consequently, in some locations, cellular/PCS systems may be subject to overload in emergency situations or at peak times of the day.

3. Cellular/PCS systems only provide one-to-one communications capability.

4. Cellular/PCS systems require infrastructure for operation; there is no unit-to-unit direct communications capability.

5. There is no interoperability between cellular/PCS systems and dedicated public safety radio systems.

6. Most systems competing in local areas use different modulation techniques so that a particular handheld phone may not work with any other system, other than in analog mode with a limited feature set.

☞ Buyer Beware...

Before purchasing any commercial system, you should "try before you buy." Test to ensure you have coverage in the places you need it and accessibility at the times you need it (e.g., test it during rush hour or other peak times in your area).

Voice—SMR/ESMR

When the FCC wrote the trunked radio Rules, it provided for licensing specialized mobile (trunked) radio service companies (SMRs) to provide leased two-way mobile radio service. As time passed, with the development of digital radio trunking systems called "enhanced specialized mobile radio" (ESMR), greater spectrum efficiency was achieved. These systems use the 800 and 900 MHz portions of the radio spectrum.

Many SMR/ESMR systems are extremely reliable and are well suited for use by public safety agencies. SMR/ESMR systems work well for radio dispatch and for interconnection to the public telephone system. Offerings are usually competitive with other available mobile radio services.

The following list is not comprehensive, but is intended to provide examples of the types of companies that provide this service.

Motorola Solutions, Inc., Ex1017, p. 128

A Special Case:
Conventional Radio System for the Township of Upper St. Clair, Pennsylvania

Upper St. Clair, a Pittsburgh suburb, has a unique problem of having deep narrow ravines throughout the township, making full radio coverage with its 460 MHz law enforcement system impossible. Patrol cars were unable to communicate with headquarters on roads at the bottom of some of these ravines. Also, the radios were installed years before, required excessive servicing, and were overdue for replacement.

The town did have one asset. The town's communications tower was in a high city park, overlooking much of Pittsburgh, making it an attractive site for other radio systems. The township was approached by Crown Communications, a commercial radio enterprise, to enter into a contract to install a new radio system and tower for the town's law enforcement communications, providing Crown could use the tower for commercial communications.

Crown used a computer propagation model to predict that, by replacing the present police system, with its antenna at 180 feet above the ground, with a new antenna with a down-tilt radiation pattern at 350 feet above the ground at the same location, a 460 MHz communications system would have practically full township coverage.

St. Clair officials recognized a good offer when they saw one. At no cost, Crown provided St. Clair with a new 350-foot tower (with police repeater antenna and room for expansion), a new base station, new mobile units, and new handheld radios. In addition, St. Clair got a zero-cost radio unit maintenance plan, as well as a small monthly lease income for making the site available and for allowing the company to construct a communications facilities building and install a number of commercial systems.

In a single "win-win" contract, St. Clair solved both its obsolete equipment problem (at no cost) and its coverage problem (tests showed the new system had excellent coverage, even at the bottom of the ravines).

Although deals as sweet as St. Clair's may not come along every day, your community may have assets that could lead to a similar "horse-trade" for equipment or commercial services.

Motorola Solutions, Inc., Ex1017, p. 129

Sample Vendor—Nextel

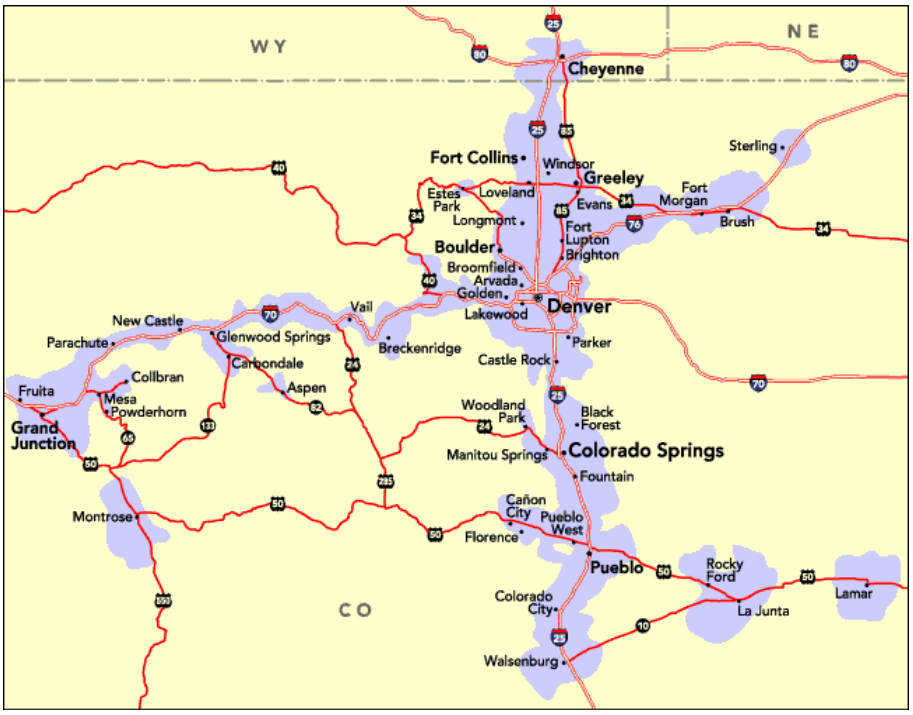
One ESMR provider with national coverage is Nextel (although, like the cellular/PCS providers, its presence is spotty in small-population areas). The Nextel system uses Motorola's iDEN equipment.

The system is quite similar to that of cellular radio; however, in addition to making phone calls, Nextel offers paging and dispatching services whereby a subscriber may call another mobile station or a group of stations on company-owned repeaters. The service allows for full duplex communications. Thus, one device gives you the capabilities of both a cellular phone and a handheld radio.

Nextel has several models of handsets, but you must use one made by the company. Five types of dispatch calls may be available with the Nextel system: private calls, call alerts, local service area group calls, selected service area group calls, and wide-area group calls.[12]

System coverage. Coverage of the nationwide Nextel system is restricted. As an example, figure 12-2 provides a typical coverage diagram for Colorado. You can see the system covers the major cities in Colorado, as well as major arteries in the State, but rural areas are virtually uncovered.

Figure 12-2. Sample Diagram for Colorado



Nextel Coverage the State of (2002)

[12] Nextel, *Overview of iDEN*, R01.04.02, April 24, 1997, p. 3.

(Diagram courtesy of Nextel)

Information on the coverage in this and other areas can be obtained at Nextel's Web site. However, remember that the areas shown give the outside perimeters of coverage; they do not show the "holes" that may exist within the coverage area. As with all other types of service, test the coverage yourself before making a purchase.

Pricing. The prices can vary from location to location and are subject to change. Pricing is usage based, so it will vary by the anticipated and/or actual time used. Generally, there will be a monthly charge with a certain number of minutes included. Minutes over that amount are then charged per minute. Up-to-date information may be obtained from the Nextel web site or directly from the company.

Sample Vendor— Lower Colorado River Authority

The Lower Colorado River Authority (LCRA) is a conservation and reclamation district in Texas that monitors and controls portions of the Colorado River. LCRA has a very extensive M/A-COM EDACS digital radio system with extra capacity available for leasing to other utilities and, most recently, to public safety organizations.

When the San Marcos, Texas, Police Department's proposal for a $3.5 million upgrade for its radio system was rejected by the city council, the department needed to find a less costly alternative. LCRA provided a convenient option. The Authority supplied a new communications tower and a seven-channel trunked (EDACS) 900 MHz radio system within San Marcos. The city council approved $700,000 for the purchase of about 300 new mobile and portable radios, plus four new dispatch consoles. It also arranged for the installation of a T1 circuit to link the city communications center to the trunked repeaters.

San Marcos currently uses the radio system for voice transmissions. However, it will be installing laptop computers in squad cars in the near future. The city is evaluating new software for the dispatch center, which will allow laptops to communicate directly with NCIC.

San Marcos is paying LCRA a flat channel fee of $19.95 per month per mobile unit and $9.99 per month for each portable. LCRA takes care of all maintenance at its trunked facility.

Although LCRA will not prioritize public safety traffic along the network, when the first San Marcos emergency (27 inches of rain fell in October 1998) pushed the number of radio transmissions up from a normal average of 16,000 per day to 41,000 per day, the system operated well, with only a few minor hitches.

Advantages of an SMR/ESMR System

1. Capital expenses are amortized monthly and spread over the total customer base of the company.

2. Many modes of operation are available by using this service, as discussed above.

Motorola Solutions, Inc., Ex1017, p. 131

Disadvantages of an SMR/ESMR System

1. The agency must purchase special telephone/radio units.

2. Prioritizing transmissions for public safety agencies is generally not provided at this time. Consequently, in some locations, SMR/ESMR systems may be subject to overload in emergency situations or at peak times of the day.

3. Flat rate billing may not be provided. Rates are commonly based upon a fixed fee plus usage.

4. Coverage is dependent upon a subscriber base to support service, thus may be limited or nonexistent in sparsely populated areas.

5. There is no wire line interface between dispatch centers and infrastructure to ensure priority access to a channel for dispatching.

6. There is no interoperability between the SMR/ESMR systems and other dedicated public safety radio systems.

Chapter 13

Wireless Data Systems

Data transmission requirements of local public safety agencies continue to increase as computer-to-computer communications needs spread. Today, agencies need rapid radio access to governmental databases to obtain relevant information about vehicles, drivers, histories, hazardous material storage areas, and so forth.

Laptop computers are becoming standard equipment in vehicles to allow for accurate and quick inquiries. These computers may be connected to almost any radio system, with the proper modem. Agencies have used and continue to use dedicated, agency-owned radio systems for data, both conventional and trunked. However, increasingly commercial options have appeared in the marketplace. One such system (described below), which has become more and more popular, is cellular digital packet data, with expanded offerings in many parts of the country.

Regardless of the type of radio system used for data transmission, software also is required for these systems to work properly. Software on the laptop (usually licensed on a per-PC basis) and software back at the main computer site must both be present and be able to talk to each other over whatever backbone you select. The effective speed of your data network will depend heavily on the efficiency of the software used to pass the data back and forth.

Cellular Digital Packet Data (CDPD)

If you are planning on transmitting data for dispatching, for license and criminal record information, or for writing accident reports, CDPD may be the technology to use. CDPD uses packet radio hardware and software and is regularly used with laptop computers or mobile data terminals. CDPD may be available from a cellular supplier in your area. Some CDPD suppliers with interesting offerings are described in the following section.

Sample Vendors

The following list is not comprehensive, but is intended to provide examples of companies that provide this type of service.

Motorola Solutions, Inc., Ex1017, p. 133

AT&T Wireless. AT&T Wireless Services developed a white paper in 1997 titled "CDPD for Public Safety," outlining the use of CDPD by law enforcement agencies. The document includes information on the wireless environment applicable to public safety dispatch users and the economics for CDPD usage. It compares CDPD with the other options available to public safety organizations for the transmission of wireless mobile data, including government-owned voice- and data-dedicated private mobile radio systems, specialized mobile radio (SMR) trunked radio systems, and public networks.[13] Note that the document is a marketing piece and, thus, tends to downplay the disadvantages of CDPD, but not unfairly.

AT&T is offering CDPD service for public safety use on a fixed-price per vehicle per month schedule; some other providers have followed suit (see below). However, AT&T is in the process of migrating its customers from CDPD to GPRS (see below for more information on GPRS), which may use a completely different pricing model.

The McKinney Police Department (near Dallas, Texas) is using AT&T CDPD and claims to have saved close to $500,000 by using AT&T's wireless network. The department equipped its patrol cars with laptops, modems, and other necessary equipment. The city is using the network to obtain history reports on domestic violence and to perform criminal and vehicle checks.[14]

Verizon Wireless. Verizon offers their CDPD service (now called Mobile IP) for vertical market solutions and Web-based applications such as browsing and e-mail. The service is flat rate based. (In 2002, the access fee was $55 per month for a one year contract with unlimited usage. Discounts were available for 2-yr plans with 50 or more IP addresses.).

Advantages of CDPD

1. The service is available in many areas in the United States and is ideal for applications involving short rapid data exchange. Police officers can readily access local, State, and national databases from their patrol cars.

2. The capital expenses are only for computers, modems, and software. The communications network is provided by the cellular service provider, so entry costs for agencies are quite low.

3. Information may be obtained quickly from database resources, including NCIC, without the need to extend time to go through a dispatcher.

4. The accuracy of the information may be better if it is directly obtained from a law enforcement database without any voice involved.

5. Industry standard TCP/IP protocols make the connection with standard databases.

---

[13] Vlcek, Charles, "CDPD for Public Safety," AT&T White Paper, May 29, 1997.

[14] *Wireless Week* (June 1, 1998): 28.

6. Some service providers are willing to prioritize traffic on their CDPD networks so that law enforcement may be able to displace noncritical traffic during emergencies.

7. Hardware and software are available from multiple sources, allowing for competitive bids in a community where there is more than one source.

8. CDPD can act as a backup communications network if the primary law enforcement radio communications network goes down.

Disadvantages of CDPD

1. CDPD cell coverage may be limited or not available in sparsely populated communities or rural areas.

2. There may not be enough capacity to handle public safety requirements during peak periods (such as rush hour traffic).

3. The maximum data rate is 19,200 bps, which may not be satisfactory for obtaining high-quality fingerprints or complex mug shots quickly.

4. In large agencies with a large number of vehicles, the cumulative cost of CDPD service could exceed the cost of a dedicated radio infrastructure.

5. Some service providers will not prioritize traffic for public safety users.

6. Some CDPD providers do not have dedicated CDPD channels and may give priority to voice users.

7. With the recent FCC decision to allow cellular carriers to drop analog service in 2005, CDPD may no longer be available after that time.

8. With the advent of use of GPRS, some CDPD providers have already begun notifying their users that CDPD service will no longer be available after a vendor designated cutoff date.

General Packet Radio Service (GPRS)

One of the new network carrier methods which will eventually replace CDPD is General Packet Radio Service, or GPRS, the 2.5G packet data extension to GSM. Some of the national wireless carriers, including AT&T Wireless and Verizon Wireless, are already well along in migrating their TDMA networks to new GSM/GPRS networks,

The largest advantage of GPRS will be its greatly enhanced data carrying capacity. The GPRS systems can support peak network speeds of wireless data transmissions up to 115KB/second, with actual data rates of 30-50 kbps in practice. Further enhancements to software will boost data transmission rates to as

much as 384KB/second, with an effective rate of 75 to 100 kpbs. The ultimate goal is to achieve third generation (3G) capabilities, which could allow vendors to support data speeds of up to 2MB/second.

In addition, GPRS can offer "always-on" connectivity to the Internet, which means you could receive voice calls while in data mode, thus blurring the line between what is a “voice”system and what is a “data” system.

However, one significant concern for law enforcement, which has yet to be overcome in every State, is the change in the way that devices are identified in a GPRS network. With CDPD, each individual mobile device has its own unique IP (Internet protocol) address. This IP address is used in many State criminal database systems to ensure that mobile access to the database is secure and is only coming from an authorized user (e.g., a police officer’s laptop would need to have an IP address registered with the State before being able to perform a wants and warrants check wirelessly).

Instead of using a unique IP address per device, GPRS dynamically assigns IP addresses (using the Dynamic Host Control Protocol (DHCP)) each time a user connects to the system. As a result this address may be different each time the user connects to the network. Some carriers offer the option of purchasing static (fixed) IP addresses as part of their GPRS service (this may have an extra cost), while others only offer dynamic IP addressing. Many State criminal information system applications are set up to validate only against a unique IP address, in addition to a user login and password. Before moving to this new technology, make sure you check with your State system administrator about their security IP addressing requirements and with the carriers in your area to know your options.

☞ Did you know?

Throughput on a data network is often expressed in terms of the **peak** network speed. However, the actual effective rate that you experience could be much lower, as much as 50% to 70% lower.

1XRTT Service

1XRTT is short for single carrier (1x) radio transmission technology, a third-generation (3G) wireless technology based on the CDMA platform. 1xRTT is also referred to as CDMA2000. 1xRTT has the capability of providing ISDN-like speeds of up to 144 kbps, with an average practical rate of 40 to 60 kbps. Like GPRS, the system uses a packet based transmission over the cellular network, where the user pays for the amount of data transferred and not for time of connection to the network.

Verizon Wireless began offering 1XRTT service in a limited number of markets in early 2002, making it the first carrier to introduce 3G networks in the United States. Sprint PCS began offering its 1XRTT service later the same year.

While 1XRTT’s peak speeds of 144 kbps appears faster compared to 115 kbps for GPRS, both standards are expected to offer consumers an average of between 30 and 60 kbps, making the discrepancy in data rates less of a differentiator than might have originally been thought.

Since the introduction of packet-based networks based on both GPRS and CDMA2000 1xRTT technologies, uptake among subscribers has been slow, possibly due to the lack of fixed pricing plans similar to those applying to fixed line Internet connections. Sprint PCS has now begun offering unlimited data use for its PCS Vision at a fixed rate per month, when purchased as part of a total PCS plan. Others are likely to follow.

Private National Data Networks

At this time, there are two private national data networks: ARDIS and Mobitex. Both networks offer data communications services within urban areas and between many cities across the continental United States, Alaska, and Hawaii.

Sample Vendors

Motient Wireless Data Network. Motient Corporation was founded in 1988 as American Mobile Satellite Corporation. The company completed its acquisition of the ARDIS mobile data network in March 1988. The company name was changed to Motient in April 2000. Motient has had its financial difficulties, but successfully emerged from Chapter 11 bankruptcy protection in May 2002.

Motient has an extensive data network in more than 500 U.S. cities (including cities in Alaska, Hawaii, Puerto Rico, and U.S. Virgin Islands), providing services for in-building, on-street, and in-vehicle locations. Some 2,200 base stations are tied together to form a national backbone. PC, LAN, and mainframe systems can be connected to the Motient network via radio modems, dial-up, or dedicated leased lines.

The company now claims to provide services to many rural areas (90 percent of the U.S. area containing 80 percent of the population), much of which is not well covered by other wireless services. As a result, small public safety entities in remote areas may have a commercial option for obtaining database information from far-flung databases or for other computer or voice communications.

Packet data network technology is employed by the system. According to the company, the combined satellite/terrestrial network allows the company to optimize the transmission of data by using both terrestrial and satellite paths, thus minimizing their costs.

The system can employ a number of different hardware configurations, including laptop and palmtop computers with appropriate wireless modems. The system is software and middleware driven. Compatible software and hardware are supplied by a number of vendors. Motient has nationwide contracts with organizations such as AT&T, Pitney Bowes, IBM, Avis, Sears, and Otis Elevator Company.

Cingular® Wireless (formerly RAM Network). BellSouth Mobile Data Corporation took over RAM Mobile Data in early 1998 and began expanding the number of base stations in metropolitan areas across the United States. The network is now operated by Cingular, the joint venture between SBC and

BellSouth. As visualized by BellSouth, "the primary objective of the RAM network is to send and receive messages and data from anywhere at anytime."[15]

According to Cingular, the network now covers more than 93 percent of the business population located in 492 Metropolitan Statistical Areas (MSAs) and non-MSAs with a total population of 200 million people and over 130 of the top airports in the nation. In addition, it is the network backbone behind Xpress Mail GoodLink Edition, Xpress Mail BlackBerry Edition, Interactive Messaging PLUS, and Wireless Internet PLUS.

The service is based upon M/A-COM's Mobitex® standard used throughout Europe. The network supports many data communications protocols including UDP/IP, TCP/IP, SNA/3270, X.25, asynchronous, and MPT/1 transport protocol.[16]

The system is a data-only, packet-switched network and uses packets of 512 bytes transmitted at an 8 Kbps rate. Efficient addressing, automatic repeat requests, and forward error correction are used in the network making it 99.99 percent reliable, according to the company.

The base stations use transmitters with 200 watts ERP, and mobiles transmit with up to 2 watts. A multitude of trunked base stations are used throughout all the metropolitan areas in the United States. UHF SMR channels are used to transmit the data. The data are encrypted by scrambling the packets to provide privacy to customers and may be further encrypted by customers, if required.

To operate on the Mobitex network, an agency needs laptop or palmtop computers, application software supported by appropriate middleware, a wireless modem, and Cingular's Mobitex wireless two-way data transmission service. Cingular provides open interfaces that enable many vendors to supply hardware, software, and system integration services.

Coverage information may be obtained by calling Cingular or from the company's web site. As stated previously, an agency is encouraged to perform its own coverage testing before making a commitment for the use of the network.

Advantages of Private National Data Networks

1. Network store and forward. Packets may be stored for sending at a later time.

2. Companies guarantee fast network response and delivery of data, within seconds of being transmitted.

3. Both companies provide encrypted service, if desired.

4. Costs are proportional to usage.

---

[15]"RAM Mobile System Overview," Executive Summary, August 1995.

[16]"MOBITEX Features and Services," RAM Mobile Data White Paper, February 1997.

Disadvantages of Private National Data Networks

1. The two national data networks do not yet support data rates in excess of 8 kbps.

2. Because these are packet networks, with 200 to 1000 bits per packet, they are not very efficient for long messages. They need to be used for files of less than 10,000 bits.

Regional Voice and Data Systems

A number of ESMRs provide digital radio systems for both voice and data traffic. One is discussed below. Other communications and utility companies across the country have offerings for the provision of regional communications.

Sample Vendor

RACOM. RACOM, headquartered in Marshalltown, Iowa, operates a large 800 MHz trunked digital wireless network and boasts of some 6,000 customers in Iowa, Minnesota, Nebraska, South Dakota, Wisconsin, and Illinois with some 4,000 contiguous channels (see figure 13-1). The company's core business consists of wireless voice and data services for public safety, utility, and industrial customers. By combining the needs of many entities on a common network and providing a high level of network maintenance, RACOM claims that users can avoid substantial cash outlays while experiencing a high degree of system reliability and flexibility.

The backbone network consists of M/A-COM's EDACS system; however, the company is now constructing an additional network using Motorola's iDEN technology. One major advantage of RACOM's network for public safety is that it provides interoperability to governmental customers.

For example, the cities of Moline and East Moline, Illinois, put out bid requests for dispatch centers and radio equipment for their police, fire, emergency medical, and public works departments. Two bidders responded. One proposed two dispatch centers; the other, RACOM, proposed a combined center. The RACOM proposal offered each department in each city separate frequencies for specific talk groups and offered clear channels for intra-city communications when required.[17] The cities went with the RACOM plan, thus saving the money to be spent on a second center.

RACOM provided the Fort Dodge (Iowa) Correction Facility with the capability for transmitting voice, data, dispatch, and vehicle-tracking signals. Of special concern was the plausibility of being able to transmit and receive signals within all areas of the prison. RACOM established a transmitting facility within a half mile of the prison, and, as a result, there are no dead spots within the prison facility.[18]

---

[17]SMR/Private Radio, "Agencies to Operate RACOM System," *Wireless Week* (March 30, 1998).

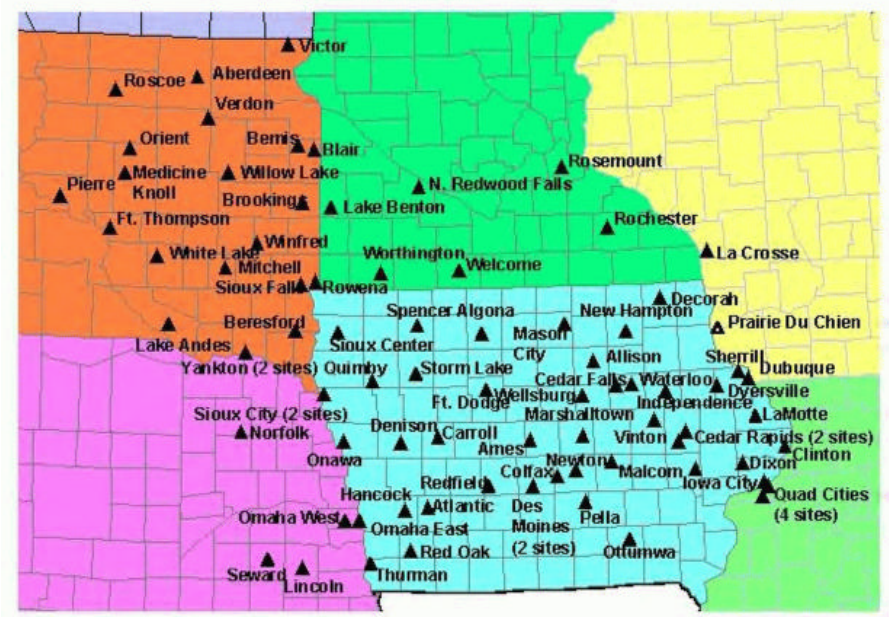
[18] Ibid.

Motorola Solutions, Inc., Ex1017, p. 139

Besides those mentioned above, as of 2002, RACOM's other public service clients included Polk County, Iowa; Sioux City, Iowa; the US Army Corp of Engineers; Illini Hospital; Blackhawk County/Waterloo, Iowa; Bettendorf, Iowa; Nobles County Hwy Dept, MN; Dubuque, Iowa; Polk County Public Works, Iowa; Grundy County, Iowa; Scott County, Iowa; Coralville, Iowa; US Dept. of Transportation; Cheyenne County, NE; Buchanan County, Iowa; Div of Alcohol Tobacco & Firearm (ATF); Lincoln, Nebraska; United States Coast Guard; Dept. of Natural Resources; Marshall County, Iowa; the Federal Aviation Administration; Worthington, Minnesota; the US Army Reserves; Davenport, Iowa; Norfolk, NE; Iowa City, Iowa; Illinois Dept of Transportation; and Lucas County, Iowa. Additionally, RACOM had commercial customers including John Deere & Co., General Mills, Rockwell International, MidAmerican Energy, Utilicorp, AAA Travel of Nebraska, Pfizer, GTE, Central Iowa Rural Water, and Qwest Communications.

Figure 13-1. RACOM Network in Six Midwestern States (diagram courtesy of RACOM)

South Dakota Minnesota Wisconsin



Nebraska Iowa Illinois

Advantages of Regional Voice and Data Systems

1. Lower capital outlay by sharing existing system.

2. Maintenance is taken care of by the system supplier.

3. Capital expenses are amortized in monthly invoices and spread over the total customer base of the company.

4. Many modes of operation are available by using this service, as discussed previously.

5. There is usually a wire line interface between the dispatch center and the infrastructure to ensure priority access to a channel for dispatching.

Disadvantages of Regional Voice and Data Systems

1. Law enforcement agency does not have complete control over the system.

2. The agency must purchase or lease special telephone/radio units.

3. Prioritizing transmissions for public safety may not be provided, depending upon the vendor. In case of an emergency, public safety agencies may not be preferred customers.

4. Flat rate billing may not be provided by companies. Rates are commonly based upon a fixed fee plus usage.

5. The service may not be available in your area.

Motorola Solutions, Inc., Ex1017, p. 141

Chapter 14

Latest Developments

Mobile Satellites

Although it is uncertain as to when satellite communications will be practical and economical for use by public safety agencies, it is critical to discuss these important emerging technologies in this handbook.

The United States has a fleet of geosynchronous earth orbit (GEO) satellites at approximately 22,500 miles above the equator providing wideband transponders to connect telephone and television circuits around the world. There are several GEO systems used for general mobile services available today. However, they require a briefcase full of equipment, including a highly directional antenna. In addition, there is a delay of about 1/4 second for the transmission, which slows down interactive voice and data transmissions considerably. Because of this, the service is not yet appropriate for the use of simple handsets as used for cellular or PCS radio.

☞ Did you know?

LEO = low earth orbit

MEO = medium earth orbit

GEO =geosynchronous earth orbit

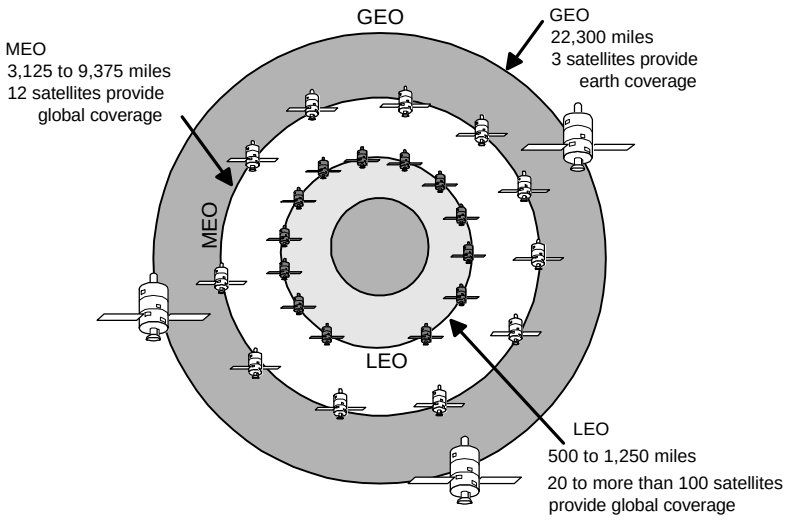
Voice Communications Satellites

Besides GEOs, medium earth orbit (MEO) and low earth orbit (LEO) satellites have been proposed for relaying radio transmissions. MEO and LEO satellites require less output power from phones and have less time delay than GEO systems. The relationship of GEO, MEO, and LEO satellites is shown in figure 14-1.

Example system—Iridium®. In 1987, Motorola engineers proposed their Iridium satellite system for wireless communications to allow a person with a small handset anywhere on the earth's surface to communicate with another person's handset anywhere else on the earth's surface. This satellite system was the first of a number of systems that would not only receive signals from the earth (which are converted in frequency, amplified, and re-transmitted as commonly done in transponders) but would also contain switching and routing processors.

Motorola Solutions, Inc., Ex1017, p. 143

Figure 14-1. Mobile Satellite System Orbits



Reference: Public Safety Wireless Network, "Mobile Satellite Services (MSS) Report", p.8.

The Iridium system was constructed and functioned as planned; however, Iridium, LLC, filed for bankruptcy in February, 2000, because of a failure in their business plan. In December, 2000, Iridium Satellite, LLC was formed and acquired the operating assets of Iridium LLC including the satellite constellation, the terrestrial network, Iridium real property and the intellectual capital. A new management team was installed and the company sold their services in March, 2002, to the U.S. Department of Defense as a stable customer. The service according to the company is ideal for "heavy construction, defense/military, emergency services, maritime, mining, forestry, oil and gas and aviation and is actively seeking commercial and emergency service customers." The operation of the satellites has been taken over by the Boeing Corporation.

The Iridium system consists of 66 satellites placed in LEO orbits with seven spares to fill in should the company loose the service of a satellite. The system is composed of 6 planes of 11 satellites equally spaced

in a low-elevation orbit with an orbit altitude of 421.5 nautical miles, as shown in figure 14-2.[19] Each satellite provides a set of 48 separately controlled spot beams to cover the earth's surface so that (with the 66 satellites) there will be 3,168 cells covering the entire earth.

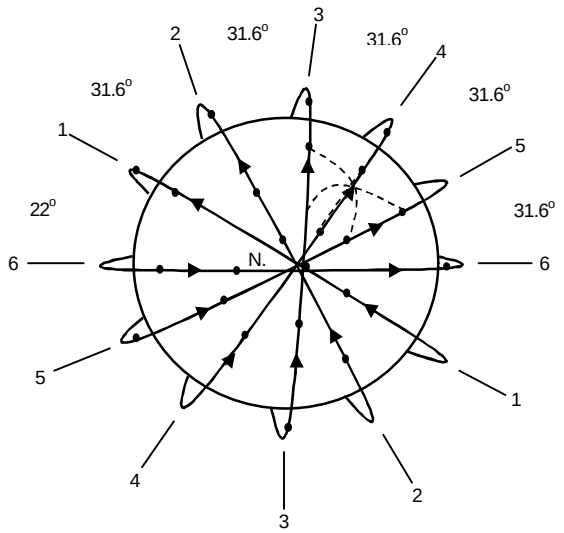


Figure 14-2. A polar view of the Iridium satellite orbits.

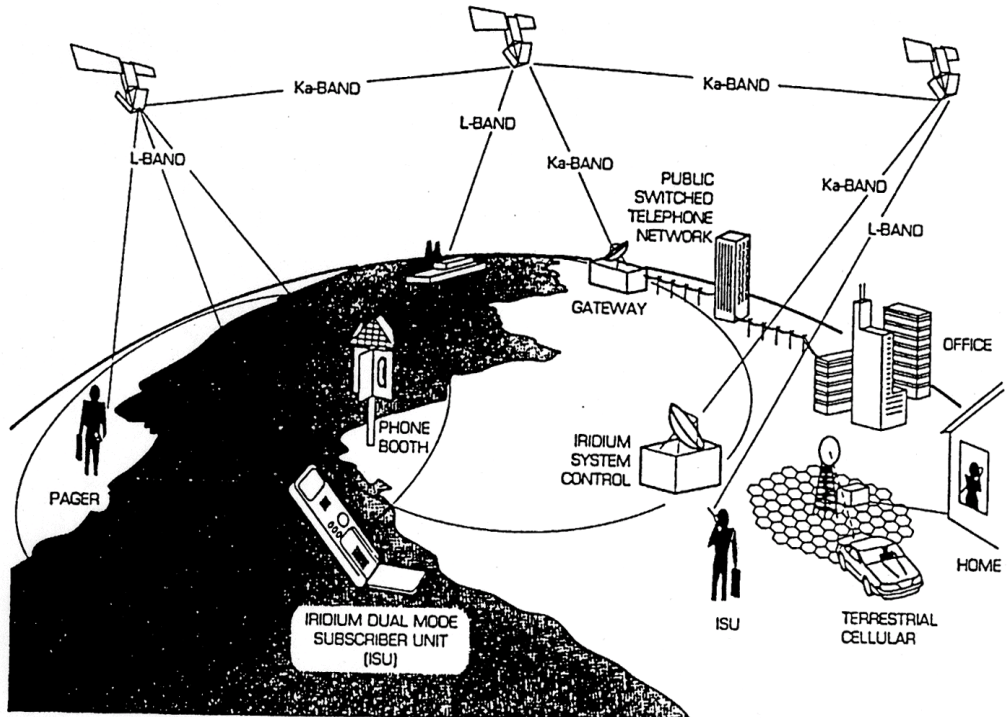
The system may be thought of as a type of cellular radio system where the "cellular base stations" and cells are constantly rotating so the earth signals are handed off from one satellite to another as they pass over an individual's handset.

L-band frequencies (1616 - 1626.5 MHz) are to be used for the communications between the earth and the satellites and the Ka-band frequencies (23.18 - 23.38 GHz) are used for intercommunications between the satellites. Ground segment frequencies to gateways and control facilities use Ka-band frequencies (downlinks,19.4 - 19.6 GHz, uplinks, 29.1 - 29.3 GHz). Figure 14-3 shows Motorola's concept of this system.[20] Iridium will support voice and data up to 4800 bps.

[19] Roddy, Dennis, *Satellite Communications*, 2nd Edition, New York: McGraw-Hill, 1989: 424.

[20] Ibid, p. 425.

Figure 14-3. Iridium® system overview *(Courtesy Motorola.)*



Other voice satellite systems. The other commercial LEO system in orbit is Globalstar, which is now a wholly owned subsidiary of Vodafone Group PLC. The system consists of 48 satellites allowing for seamless coverage anywhere on the earth. The system utilizes CDMA technology with path diversity and the company provides light weight, 12 oz. phones for voice communications.

Other companies have stated an interest in LEO and MEO narrow band systems. Mobile Communications Holdings' Ellipso™ and ICO Global Communications' ICO satellites are in MEOs, spaced at about 6,000 to 10,000 miles above the earth's surface.

The general characteristics of LEO and MEO satellite systems are shown in table 14-1.

Table 14-1. Narrow Band Voice and Data LEO's and MEO's General Characteristics					
Type	**Number of Satellites**	**Orbit Planes**	**Altitiude (Km)**	**Spot Beams Per Satellite**	**Estimated Cost**
LEO	46 to 66	6 to 8	700 to 1600	16 to 48	$3B to $5B
MEO	2 to 8	2 to 8	8K to 11K	60 to 170	$1B to $4B

There are tradeoffs between the LEOs and MEOs. Far fewer satellites are required in the MEO system than in the LEO system, but higher effective power is required for transmissions by the subscriber units, and time delays are greater. With the exception of Iridium, service offerings by these companies have not been described in detail.

Pricing of services has not yet been finalized, but it is estimated that prices will be in the range of $3 to $5 per minute. Almost all of the previously mentioned companies have Web sites. Visit those sites as the technologies develop to evaluate the use of satellite services as they become operational. Because of the large number of commercial providers for both voice and data systems, there will most likely be considerable competition when all of the systems are turned up.

Data Communications Satellites

Since 1992, American Mobile Satellite Corporation, now Motient Corporation, has offered satellite service employing geosynchronous satellites. Motient has recently transferred it's operating interest in satellite communications to a partnership called Mobile Satellite Ventures LLC (MSV). Motient retains approximately 25% interest in the partnership.

The MVS system provides coverage to North and Central America, parts of South America and the Carribean via a single geosynchronous satellite using "L-band" technology. Both voice and data may be handled on the same system, with communication of data up to 4800 bps. The equipment used includes both mobile and transportable units. The mobile units use a steerable antenna to allow use on a moving vehicle.

The system provides three different services. The first is a satellite telephone service that allows calls to be made to any phone through the PSTN and unit-to-unit calls to be made through the satellite without use of any ground stations.

The second service provided is a radio-like service that allows unit-to-unit calls via a talk group. Satellite units can have multiple talkgroups, and operate using the system as a satellite-based trunked radio system. Some rural fire and EMS agencies use this system for radio communications over very large areas. In addition, several local and US government agencies use these talk groups to coordinate task force disaster responses.

The final service is a packet data service. This service is relatively low speed and useful primarily for fleet tracking and equipment control.

Motient provides dual mode services allowing mobile units to use their terrestrial service when within their coverage area and to automatically switch over to the MVS satellite system when the terrestrial system is not available.

Wideband, data-oriented LEO and MEO PCS satellites are being studied and proposed at this time, as shown in table 14-2. These satellite systems will have the ability to carry high-speed data around the world at up to10 Gbps.

Table 14-2. Data Oriented Wideband Satellite Proposals[21]
General Characteristics

Type	Number of Satellites	Orbit Planes	Altitude (Km)	Capacity Per Satellite	Estimated Cost
LEO	288	12	1375	10 Gbps	$9B
MEO/GEO	36	4	10352/GEO	4.4 Gbps	$6B to $7B
GEO	3 to 9	Equatorial	GEO	0.5 to 9 Gbps	$1B to $7B

High Altitude Long Endurance (HALE) Platforms and High Altitude Platforms (HAPS)

In this proposed network, relay of signals would be accomplished using large blimp-like repeaters at several miles (20,000 meters) above the earth. The devices would cost less than the big satellite systems and could be recalled to earth for maintenance. Multibeam, phased array antennas would support both mobile two-way communications and broadband video. Although not considered HALE/HAPS, the U.S. is presently performing surveillance over the U.S.-Mexican boarder using low altitude tethered balloons carrying electronic equipment.

Four types of HALE platforms have been proposed,[22] which include helium-filled, robotically controlled dirigibles stabilized by ion engines; units powered by solar or fuel cells; piston-driven platforms; and jet engine-driven platforms. The biggest challenge faced by all of them will be power requirements versus

[21] Six high density data systems were spelled out in the last edition of this book. All have been delayed pending market conditions and capital availability.

[22] Pelton, Joseph N., "Telecommunications for the 21st Century," (278) 4 *Scientific American* (April 1998): 85.

refueling requirements. The first two types need little or no refueling but may not produce the transmit power needed, whereas the latter two types will have plenty of power but will need to be refueled every few days.

Sky Station International was the commercial initiator of this technology in the United States and filed with the FCC in March 1996 for use of the 47 GHz band. Sky Station claims a blimp repeater can offer many advantages over satellites, including less time delay and lower power at a considerably lower cost. The concept was also introduced at the 1997 World Administrative Radio Conference, and a portion of the 47 GHz band was tentatively allocated. The 47 GHz band is severely limited by rain, so space diversity ground circuits will most likely be required.

The basic concept is to have "very high antenna towers" allowing for very wide-area communications. This might be an alternative to backbone microwave terrestrial systems. Sky Station indicated that one could start with communications in local areas, expand to regional areas, and eventually cover the country. The FCC has made no decisions at this time. The concept has many technical and political challenges, and its development should be interesting to watch as it evolves.

Since the first edition of this book much greater consideration has been given to HALES/HAPS by many countries throughout the world. NASA has proposed a schedule for testing systems by 2003 using manned and unmanned aircraft and balloon type platforms[23]. The HALE/HAP systems at a height of 25 Km appears to have the least amount of wind speed and a coverage is about 200 Km.

Among the multitude of technical problems to be solved are:

1. Developing stability systems to hold the HALE/HAPS at station keeping locations and stabilize microwave antenna positions.

2. The testing of aerodynamics and aircraft structures.

3. The development of additional light weight, high strength materials.

4. Making sure the altitudes of HALE/HAPS will not interfere in any way with normal air or military air travel.

Ultra Wide Band (UWB) Devices

Microcircuit advances in the last year or so have made it possible to create ultra wideband (UWB) radio and radar equipment having very narrow digital pulses, in the nanosecond range, to transmit and receive very high rate data information. The bandwidths are very large and cover a great amount of the licensed frequency spectrum. The FCC and NTIA have studied and made tests to determine that the use of UWB at low power levels will not cause objectionable interference to those licensed services.

[23] NASA High Altitude Five Year Plan, dated March 25, 2002

Motorola Solutions, Inc., Ex1017, p. 149

In February, 2002, the FCC enacted rules under Part 15 to assign certain frequency ranges for UWB and to quickly allow for the development of commercial devices using this new technology. The UWB research has already yielded a number of new devices which will assist public safety groups as soon as the equipment is developed. These include:

* High Speed in Building Radio Communications - High speed digital transmission with rates in the gigabit range for computer networks using work stations or handheld devices within buildings. The transmissions must take place in the 3.1 - 10.6 GHz spectrum.

* Building Penetration Radar - Radar has been developed for firefighters to look into buildings through walls to find the position of people trapped during a fire. Similarly police surveillance may utilize this radar to determine the number and locations of people within buildings. Operation is limited to law enforcement and fire and rescue operation. The radar emissions must be kept within the 3.1 - 10.6 GHz frequency domain.

* Ground Penetrating Radar Systems - Public safety personnel may use ground penetrating radar (GPR) to determine the location of buried objects including the locations of people within the rubble of fallen buildings. Operation of the GPR is restricted to law enforcement, fire and rescue operations, scientific research institutions, commercial mining companies and construction companies. GPRs must be operated below 960 MHz or between 3.1 - 10.6 GHz.

* Surveillance Operations - Surveillance operations, as opposed to the wall penetration systems, are defined by the FCC operate as "security fences" to establish stationary RF perimeter fields to detect the intrusion of people or objects. Operation of these devices are limited to law enforcement, fire and rescue organizations, public utilities and industrial entities. The frequency band established is 1.99 - to 10.6 GHz.

* Vehicular Radar Systems - Licensed in the 24 GHz band, this UWB technology using directional antennas on road vehicles will detect and locate the movement of objects near the vehicle to enhance crash avoidance systems, improve airbag activation and suspension systems that will respond better to road conditions.

All the above uses of UWB are licensed under Part 15 of the FCC Rules and are subject to power restrictions as well as the frequency restriction discussed previously.

Software Defined Radio (SDR)

Public safety radio systems have changed over many years from simplex radios, to single repeaters, to trunked radio systems in both analog and digital configurations. Project 25 and other current radio systems make use of digital circuitry to emulate a number of these earlier configurations, allowing for efficient interoperability within single frequency bands.

However, the next big change in radio design is the use of software to dynamically change a radio's configuration to emulate a multitude of protocols and modulation waveforms using the same hardware.

Microprocessors are already used in today's radio systems at specific frequency bands to set up the transmitting and receiving frequencies, as well as for other functions including user configurations for different talk groups. Software Defined Radio (SDR) promises to integrate entire radio functions (including transmitting, receiving, signal processing and networking) to allow for specific hardware to be dynamically reconfigured to all types of public safety radio systems across multiple bands with a simple change of the "channel" switch. The resulting product will be the ultimate solution to the interoperability problem, giving the field officer a radio "on-the-belt" that can access many different systems on different bands, depending upon the configuration authorized by his agency. Additionally, this radio hardware platform should be easily upgradable to new technologies as they develop, reducing equipment obsolescence as new features, functions and systems are introduced.

An example of early software controlled radio is the use of multimode cell phones which allows a subscriber to automatically switch from the 800 to 2000 MHz frequency bands and emulate the present TDMA, FDMA, and CDMA standards without using several different cell phones. The third generation of cell phones are already utilizing as many as seven independent standards to automatically accommodate different transmission modes. Although the software for these technologies is embedded in chips, SDR promises to allow dynamically updated changes so that it will not be necessary to purchase new hardware every time an update to more efficient technology is made.

The first true SDR product to enter the public safety market (manufactured by Thales Corporation, formerly RACAL) supports a number of military and public safety waveforms, and covers the public safety bands from 30 MHz to 512 MHz. While the radio does not yet support Project 25 and trunking protocols, there is significant interest by the manufacturer and the Federal government to add these protocols to the radio. While this radio currently costs about twice as much as a similarly featured single band radio, if it replaces radios on three different bands (as it is capable of doing), it today provides significant savings. As with all new technologies, prices should drop significantly as market penetration increases.

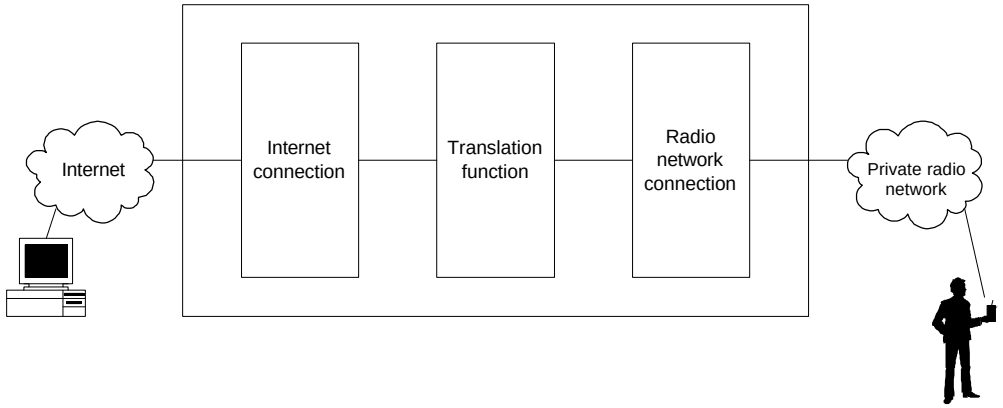
SDR is of sufficient importance to the public safety community that the AGILE program within the National Institute of Justice (see chapter 10) is funding significant participation in the SDR Forum, a voluntary group of industry and government representatives developing SDR standards. AGILE is also funding the development of specific SDR waveforms and protocols such as those used for Project 25.

Voice Over Internet Protocol (VoIP)

Using the Internet for wireless information applications is one of the latest technology developments to hit the telecommunication world. Voice delivered using the Internet Protocol, or IP, is simply a way of sending information from one device (a desktop computer, for example) to another (radio) over the Internet. To do this, voice information is converted into digital form and then sent in discrete packets over the internet to a receiving device on the other end (see figure 14-4). Changes in technology enable more information to be sent at higher speeds, including voice, fax, video and data through a single large pipeline.

Motorola Solutions, Inc., Ex1017, p. 151

Figure 14-4. Example Internet Radio Gateway



With the passage of IEEE's 802.11e standard, more network managers will be administering wireless voice over IP. This can mean private radio or cellular wireless or both. The standard is focused on supporting video on demand and audio on demand.

Multimode devices (such as NIC cards) are being developed that will work with a choice of 802.11e wireless LAN or cellular wireless LAN. Other researchers are working on multimode for 802.11 and CDPD. These multimode devices will likely be targeted towards users, such as business people in airports, who need to make cellular voice calls as well as send data over the Internet using a wireless IP link.

In public safety applications, portable radios could receive pager-like text messages, reducing the demand on voice traffic, mug shots could be sent from headquarters to the field officer, video footage can be sent from a crime scene to a dispatch center for assistance in resolving highly volatile situations, and GPS tracking is available for the added safety of officers in the field.

MOTOROLA GREENHOUSE PROJECT

The "Greenhouse Project" (Greenhouse) is the first Motorola private wireless wideband data system. A test bed was set up at Pinellas County, Florida for providing wide-area mobile video, voice and data transmissions simultaneously at a 460 kbps data rate. This experiment proved that applications conducted at one's personal computer may be accessed wirelessly in the field and teleconferencing may be conducted wirelessly from a field facility to another field or fixed facility. Tests were being conducted from patrol cruisers, surveillance vans, ambulances, fire engines and fire district vehicles equipped with Greenhouse equipment.

Greenhouse supports the following technologies and applications: [a]

* Video (Streaming IP video: 2-way video, 1-way video, video pull, video push)
* Voice (Voice over IP - Internet Protocol, Full Duplex - both users can talk at the same time)
* Data (high-speed mobile access to intranet and internet)

Some applications include:

* Automatic Vehicle Location (AVL) through GPS - vehicles locations appear on map
* Electronic Mail - instant messages including attachments
* Computer Aided Dispatch - facilitates quick deployment of public safety officials
* National and State Crime Database Access - ability to check drivers licenses, etc.
* The ability to distribute a picture of a missing child, or criminal suspect/sketch to all equipped vehicles in the field
* Robbery videotapes can be distributed shortly after an event
* Enable fire department access to building plans and hydrants
* Transmit fingerprints
* Transmit live video feeds for police officer pursuits
* Remote situation analysis

For example, at a crime scene, an officer may take a digital camera mug shot and crime scene pictures; digitize finger prints; select driver's license signature and picture information and send messages (wirelessly) over the Greenhouse system to obtain crime analysis data from NCIC as well as infrastructure information if required.

The project in Florida utilized a 150 KHz channel under an experimental license in the 700 MHz public safety band.

---

[a] Quoted from Motorola "Frequently Asked Questions" and news releases at www.motorola.com.

SUMMARY

At no time in the history of public safety communications have so many options been available. Technological advances and regulatory changes have combined to make selecting a communications system very complex. As we move into the future, it is unlikely to get any better.

NLECTC–Rocky Mountain and other groups [such as the Federal Public Safety Wireless Network program (PSWN)] are dedicated to helping you through the maze of technology jargon and bureaucratic rules as you proceed on your communications project.

We hope this guidebook has been useful to you. We welcome your comments and suggestions for improvement.

Motorola Solutions, Inc., Ex1017, p. 155

GLOSSARY AND ACRONYMS

Motorola Solutions, Inc., Ex1017, p. 157

Glossary

Amplifier: A device for obtaining an increase in voltage, current, or power.

Amplitude: Maximum departure of the value of an alternating current or radio wave from the zero point.

Analog: A signal that may vary continuously over a specific range of values.

Antenna: A device (usually metallic) for radiating or receiving radio waves.

Band: A well-defined range of wavelengths or frequencies.

Bandwidth: The range within a band of frequencies. A measure of the amount of information that can flow through a given point at any given time.

Bit: Abbreviation for binary digit (either a 0 or a 1), the basic unit for storing data in a computer.

Block grant: Federal grant funds that are allocated based on a predetermined statutory formula.

Cavity filter: A radio frequency device used to reduce interference to a receiver or from transmitter to other nearby radio frequency devices. Cavity filters are the primary component in a duplexer.

Channel: A band of frequencies of sufficient width to support a single radio communications path.

Combiner: A device used to combine the output signals from a number of transmitters into one antenna.

Coverage: The amount or percentage of area reached by a communications medium.

Cycle: One complete performance of a vibration, electrical oscillation, current alternation, or other periodic process.

Decibel: A unit for measuring the power of an electromagnetic signal; equal to the logarithm of the ratio of the measured signal to that of an arbitrary standard.

Digital: Information that can be represented by two discrete states (either 0 or 1). Most information in the speaking/seeing world is not digital, but must be converted into this form to be used by computers.

Dipole: A radio antenna consisting of two rods in line with each other, with their ends slightly separated.

Discretionary grant: Federal grant funds that are distributed at the discretion of the agency administering the funds.

Duplexer: A device that allows a radio transmitter and receiver to share the same radio antenna without interference to each other.

Effective Radiated Power: A term to describe radio system transmitted power that takes into account transmitter output power, combiner and feedline losses, and antenna gain.

Flowchart: A diagram showing the step-by-step progression through a complicated process or system.

Formula grant: Federal grant funds that are allocated based on a predetermined statutory formula.

Frequency: The number of repetitions of a periodic process in a unit of time.

Frequency multiplier: A device for multiplying the frequency up to a desired output frequency.

Gain: The effectiveness of a directional antenna, given as the ratio in decibels of standard antenna input power to the directional antenna input power producing the same field strength in the desired direction.

Guard band: A non-overlapping space between radio channels used to minimize interference.

Hertz: Alternate term for cycles per second, abbreviated as Hz.

Implementation team: A group of officials charged with ensuring that a project is planned, managed, and completed.

Infrastructure: The underlying permanent installations required for radio communications. Infrastructure includes antennas, base/repeater stations, consoles, links (fiber, microwave, radio and wire), towers, and support structures (such as buildings and towers).

Interference: Confusion of received radio signals due to strays or undesired signals.

Isolator: A device that may be added to the circuit between each transmitter and the combiner and used to increase the isolation to the other transmitter outputs.

Isotropic radiator: A theoretical antenna that radiates equally in all directions.

Modem: An acronym for modulator/demodulator, which is a device that translates digital signals coming from your computer or other digital device into analog signals that can be transmitted over standard telephone lines or radio circuits. The modem also translates the analog signal back into a digital signal.

Modulation: The process of implanting information onto a wave by varying the amplitude, frequency, or phase of a carrier or signal in telephone, radio, or television.

Multicoupler: A device used to connect a multitude of receivers to a single antenna.

Noise: An unwanted signal or disturbance (e.g., static) in a radio communications system.

Omnidirectional: Receiving or sending radio waves equally well in all directions.

Oscillator: A device for producing alternating current, specifically for producing radio frequencies.

Polarization: The action or process of affecting radiation so that the vibrations of the wave assume a definite form, usually horizontal or vertical as compared to the earth's surface.

Propagation: The action of traveling and spreading through space, in reference to wave energy.

Receiver: The portion of a radio device that converts the radio waves received over the air into a usable audible signal or data stream.

Refarming: An administrative process being conducted by the FCC to reduce channel bandwidths and, as a result, promote spectrum efficiency.

Repeater: A transmitter and a receiver operating on different frequencies and connected such that the signal received on one frequency is simultaneously retransmitted on the other frequency. Repeaters are often connected to a common antenna using a combiner.

Skip: The phenomenon by which a radio wave reflects from the ionosphere during the height of the sunspot cycle, often resulting in severe interference problems on frequencies below about 90 MHz.

Spectrum: The region of the electromagnetic spectrum in which radio transmission and detection techniques may be used.

Spectrum efficiency: Optimizing the amount of information sent over a given amount of bandwidth.

Steering Committee: A group of usually high-level officials charged with setting policy for a project.

Transmitter: The portion of a radio device that converts an audible signal or data stream into a radio wave and sends it out over the air.

Vocoder: Abbreviation for voice coder, a circuit that samples an analog voice frequency and then changes the sampled information into binary digits to modulate a digital transmitter.

Wave: A disturbance or variation that transfers energy progressively from point to point in a medium and that may take the form of a variation in electric or magnetic intensity or electric potential.

Wavelength: The distance from one point along the progression of a wave to the next point on the wave of corresponding amplitude and phase.

Motorola Solutions, Inc., Ex1017, p. 161

Acronyms

1XRTT	Single carrier (1x) Radio Transmission Technology
3G	Third generation wireless
AASHTO	American Association of State Highway Transportation Officials
ACSB	Amplitude Compandered Single Sideband
AGILE	Advanced Generation of Interoperability for Law Enforcement
AM	Amplitude Modulation
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Industry
APCO	Association of Public-Safety Communications Officials, International
AVL	Automatic Vehicle Location
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
CALEA	Commission on Accreditation for Law Enforcement Agencies
CALEA	Communications Assistance for Law Enforcement Act
CAPRAD	Computer Assisted Pre-coordination Resource and Database
CCITT	International Telegraph and Telephone Consultative Committee
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CFR	Code of Federal Regulations
COPS	Community Oriented Policing Services
COTS	Commercial Off-the-Shelf Software
CTCSS	Continuous Tone-Coded Squelch System
CDCSS	Continuous Digital-Coded Squelch System
DAWS	Digital Advanced Wireless Services
dB	Decibel
DOC	Department of Commerce
DoD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
DSP	Digital Signal Processing
EHF	Extremely High Frequency
EIS	Environmental Impact Statement
EMS	Emergency Medical Service
ERP	Effective Radiated Power
ESA	Endangered Species Act
ESMR	Enhanced Specialized Mobile Radio
ETSI	European Telecommunications Standards Institute
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission

FCCA	Forestry Conservation Communication Association
FDMA	Frequency Division Multiple Access
FEMA	Federal Emergency Management Agency
FLEWUG	Federal Law Enforcement Wireless Users Group
FM	Frequency Modulation
FSK	Frequency Shift Keying
GEO	Geosynchronous Earth Orbit
GHz	Gigahertz (1 billion cycles per second)
GITSB	Government Information Technology Services Board
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSA	General Services Administration
GSM	Global System for Mobile Communications
HALE	High Altitude Long Endurance
HAP	High Altitude Platform
HF	High Frequency
Hz	Hertz (cycles per second)
IACP	International Association of Chiefs of Police
IAFC	International Association of Fire Chiefs
ICS	Incident Command System
IEEE	Institute of Electrical and Electronic Engineers
IGA	Intergovernmental Agreement
IM	Intermodulation
IMSA	International Municipal Signal Association
ISP	Internet Service Provider
JPA	Joint Powers Authority
KHz	Kilohertz (1,000 cycles per second)
LAN	Local Area Network
LCRA	Lower Colorado River Authority
LEAA	Law Enforcement Assistance Administration
LEO	Low Earth Orbit
LLEBG	Local Law Enforcement Block Grants
LOS	Line of Sight
MBTA	Migratory Bird Treaty Act
MEO	Medium Earth Orbit
MESA	Mobile Broadband for Emergency and Safety Applications
MHz	Megahertz (1 million cycles per second)
MIU	Mobile Imaging Unit
MTSO	Mobile Telephone Switching Office
NAMPS	Narrowband Advanced Mobile Phone System
NASTD	National Association of State Telecommunications Directors
NATO	North Atlantic Treaty Organization
NCC	National Coordination Committee
NENA	National Emergency Number Association
NCIC	National Crime Information Center

Motorola Solutions, Inc., Ex1017, p. 164

NCJRS	National Criminal Justice Reference Service
NCS	National Communications Systems
NEPA	National Environmental Policy Act
NENA	National Emergency Number Association
NHPA	National Historic Preservation Act
NIC	Network Interface Card
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NLECTC	National Law Enforcement and Corrections Technology Center
NPSPAC	National Public Safety Planning Advisory Committee
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OET	Office of Engineering and Technology
OJJDP	Office of Juvenile Justice and Delinquency Prevention
OJP	Office of Justice Programs
OLES	Office of Law Enforcement Standards
OST	Office of Science and Technology
OTAR	Over-The-Air-Rekeying
PAN	Personal Area Network
PBX	Private Branch Exchange
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications System
PDA	Personal Digital Assistant
PLMRS	Private Land Mobile Radio Service
POCSAG	Post Office Code Standardization Advisory Group
PSCC	Public Safety Coordinating Council
PSPP	Public Safety Partnership Project
PSTN	Public Switched Telephone Network
PSWAC	Public Safety Wireless Advisory Committee
PSWN	Public Safety Wireless Network
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposals
RFQ	Request for Quotation
SDMA	Space Division Multiple Access
SDR	Software Defined Radio
SHF	Super High Frequency
SIEC	State Interoperability Executive Committee
SIS	State Identification Systems
SMR	Specialized Mobile Radio
SMS	Short Messaging System
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TETRA	TErrestrial TRunked Radio
TIA	Telecommunications Industry Association

TIIAP	Telecommunications and Information Infrastructure Assistance Program
TOP	Technology Opportunities Program (formerly TIIAP)
UART	Universal Receiver/Transmitter
UHF	Ultra High Frequency
ULS	Universal Licensing System
UWB	Ultra Wide Band
VHF	Very High Frequency
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network
WAP	Wireless Access Point
WLAN	Wireless Local Area Network
WRC	World Radio Conference
WSCA	Western States Contracting Alliance

APPENDICES

Motorola Solutions, Inc., Ex1017, p. 167

Appendix A
State Agencies Administering Byrne Program Grants

ALABAMA
Department of Economic and Community Affairs
http://www.adeca.state.al.us/index.html
334-242-5811

ALASKA
Alaska State Troopers
http://www.dps.state.ak.us/ast/
907–269–5641

AMERICAN SAMOA
Criminal Justice Planning Agency
http://www.government.as/gov.htm
011–684–633–5221

ARIZONA
Criminal Justice Commission
http://acjc.state.az.us/grant_programs.html
602–230–0252

ARKANSAS
Office of Intergovernmental Services
http://www.state.ar.us/dfa/intergovernmental/index.html
501–682–2579

CALIFORNIA
Office of Criminal Justice Planning
http://www.ocjp.ca.gov/
916–324–9140

COLORADO
Department of Public Safety
http://cdpsweb.state.co.us/dcj/dcj.htm
303–239–4400

CONNECTICUT
Office of Policy and Management
http://www.opm.state.ct.us/pdpd1/grants/DCSI.HTM
860–418–6416

DELAWARE
Criminal Justice Council
http://www.state.de.us/cjc/drugs.htm
302–577–8693

DISTRICT OF COLUMBIA
Office for Public Safety and Justice
202–727–9604

FLORIDA
Department of Law Enforcement
http://www.dca.state.fl.us/
850–410–7001

GEORGIA
Criminal Justice Coordinating Council
http://www.ganet.org/cjcc/byrne.html
404–559–4949

GUAM
Bureau of Planning
http://www.gov.gu/webtax/govoff.html
011–671–472–4201

HAWAII
Office of the Attorney General
http://www.cpja.ag.state.hi.us/gr/byrne98.shtml
808–586–1150

IDAHO
Department of Law Enforcement
http://164.165.67.76/dle/oldDle.htm
208–884–7042

ILLINOIS
Criminal Justice Information Authority
http://www.icjia.state.il.us
312–793–8550

INDIANA
Criminal Justice Institute
http://www.state.in.us/cji/home/index2.html
317–232–1230

IOWA
Office of Drug Control Policy
http://www.state.ia.us/odcp
515–281–3788

KANSAS
Criminal Justice Coordinating Council
http://www.ink.org/public/ksc/SiteMap.htm
785–296–0927

KENTUCKY
Criminal Justice Council
http://www.jus.state.ky.us/
502–564–7554

LOUISIANA
Commission on Law Enforcement
http://www.cole.state.la.us/
225–925–4422

MAINE
Department of Public Safety
http://janus.state.me.us/dps/homepage.htm
207–287–3619

MARYLAND
Governor's Office of Crime Control and Prevention
http://www.goccp.org/
410–321–3521

MASSACHUSETTS
Executive Office of Public Safety
http://www.state.ma.us/ccj/
617–727–6300

MICHIGAN
Office of Drug Control Policy
http://www.mdch.state.mi.us/ODCP/
517–241-0519

MINNESOTA
Office of Drug Policy and Violence Prevention
http://www.dps.state.mn.us/DrugPol/
651-284-3318

MISSISSIPPI
Division of Public Safety Planning
http://www.dps.state.ms.us/
601–359–7880

MISSOURI
Department of Public Safety
http://www.dps.state.mo.us/DPS/DIROFF/grants/narcotics.html#ncap
573–751–5997

MONTANA
Board of Crime Control
http://bccdoj.doj.state.mt.us/
406–444–3604

NEBRASKA
Commission on Law Enforcement and Criminal Justice
http://www.nol.org/home/crimecom/
402–471–3416

NEVADA
Department of Motor Vehicles and Public Safety
http://www.state.nv.us/dmv_ps/welcome.htm
775–687-5282

NEW HAMPSHIRE
Department of Justice
http://www.state.nh.us/nhdoj/
603–271–7987

NEW JERSEY
Division of Criminal Justice
http://www.state.nj.us/lps/dcj/index.htm
609–292–1502

NEW MEXICO
Department of Public Safety
http://www.dps.nm.org/
505–827–3424

NEW YORK
Division of Criminal Justice Services
http://criminaljustice.state.ny.us/
518–457–8462

NORTH CAROLINA
Governor's Crime Commission
http://www.nccrimecontrol.org
919–733-4564

NORTH DAKOTA
Bureau of Criminal Investigation
http://www.ag.state.nd.us/ndag/default.htm
701–328–5500

NORTHERN MARIANA ISLANDS
Criminal Justice Planning Agency
http://www.mariana-islands.gov.mp/cabinet.htm
011-670–664–4550

OHIO
Governor's Office of Criminal Justice Services
http://www.ocjs.state.oh.us/
614–466–4470

OKLAHOMA
District Attorneys Council
http://www.odawan.net
405–264-5008

OREGON
Department of State Police
http://www.osp.state.or.us/html/cjsd.html
503–378–3725

PENNSYLVANIA
Commission on Crime and Delinquency
http://www.pccd.state.pa.us/
717–787–8559, ext. 3064

PUERTO RICO
Department of Justice
http://fortaleza.govpr.org/
787–725-0335

RHODE ISLAND
Governor's Justice Commission
http://www.rijustice.state.ri.us
401–422–4493

SOUTH CAROLINA
Office of Safety and Grants
http://www.state.sc.us/dps/ojp/
803–896–9702

SOUTH DAKOTA
Office of the Governor
http://www.state.sd.us/attorney/attorney.html
605–773–3661

Motorola Solutions, Inc., Ex1017, p. 170

TENNESSEE
Department of Finance and Administration
http://www.state.tn.us/finance/rds/programs.html
615–741–8277

TEXAS
Office of the Governor
http://www.governor.state.tx.us/CJD/index.html
512–463–2285

UTAH
Commission on Criminal and Juvenile Justice
http://www.justice.state.ut.us/
801–538–1031

VERMONT
Department of Public Safety
http://www.dps.state.vt.us/
802–244–8718

VIRGINIA
Department of Criminal Justice Services
http://www.dcjs.state.va.us/
804–786–7840

VIRGIN ISLANDS
Law Enforcement Planning Commission
http://www.gov.vi/lepc/
340–774–6400

WASHINGTON
Department of Community, Trade and Economic Development
http://www.cted.wa.gov
360–586-8411

WEST VIRGINIA
Division of Criminal Justice Services
http://www.wvdcjs.com/
304–558–8814, ext. 206

WISCONSIN
Office of Justice Assistance
http://oja.state.wi.us/static/grants.htm
608–267-2116

WYOMING
Division of Criminal Investigation
http://www.state.wy.us/~ag/dci/grants.html
307–777–6608

Appendix B
Resources

Agency/Subagency	Web Address	Telephone
Federal Agencies/Programs:		
DOJ	www.usdoj.gov	800–421–6770
BJA	www.ojp.usdoj.gov/bja	800–688–4252
COPS	www.cops.usdoj.gov	800–421–6770
NCJRS	www.ncjrs.org	800–851–3420
NIJ	www.ojp.usdoj.gov/nij	800–851–3420
DOT	www.dot.gov	202-366-4000
TSA	www.tsa.dot.gov	866-289-9673
FAA	www.faa.gov	202–366–4000
FBI	www.fbi.gov	202–324–3000
CALEA	www.askcalea.net	800–551–0336
NCIC	www.fbi.gov/hq/cjisd/ncic.htm	304–625–2730
FCC	www.fcc.gov	888–225–5322
FEMA	www.fema.gov	202-556-1600
USFA	www.usfa.fema.gov	301-447-1000
GPO (for printed FCC rules)	www.gpo.gov	
NLECTC	www.nlectc.org	800–248–2742
NLECTC–RM	www.nlectc.org/nlectcrm	800–416–8086
NTIA	www.ntia.doc.gov	202–482–7002
TOP	www.ntia.doc.gov/top	202–482–2048
PSWN	www.pswn.gov	800–565–7796
Membership Organizations:		
AASHTO	www.aashto.org	202–624–5800

Motorola Solutions, Inc., Ex1017, p. 173

APCO	www.apco911.org	888–272–6911
FCCA	www.fcca.info	202–624–8474
IACP	www.theiacp.org	800-843-4227
IAFC	www.iafc.org	703-273-0911
IMSA	www.imsasafety.org	800–723–4672
NENA	www.nena9-1-1.org	800–332–3911

Motorola Solutions, Inc., Ex1017, p. 174