Wireless Technology in Government

Intergovernmental Advisory Board
Federation of Government Information Processing Councils
in Cooperation With the
Office of Intergovernmental Solutions
Office of Governmentwide Policy
U.S. General Services Administration

November 2001

New wireless technologies will help spread broadband Internet access to rural areas.
"Hopefully, high-speed access will come over the air as opposed to fiber optics."

President George W. Bush

Wireless Technology in Government

Intergovernmental Advisory Board
Federation of Government Information Processing Councils
in Cooperation With the
Office of Intergovernmental Solutions
Office of Governmentwide Policy
U.S. General Services Administration

November 2001

Table of Contents

For more information about this report, please contact:

John Clark at 202.501.4362 or via e-mail at john.clark@gsa.gov.

This document is available on-line at http://gsa.gov/intergov under the Intergovernmental Advisory Board section and Reports and Presentations.

Acknowledgments

This report is based on the discussions and recommendations of the Intergovernmental Advisory Board (IAB) of the Federation of Government Information Processing Councils. The IAB recommended this research study on wireless technology in government.

The IAB consists of nine members three members each representing federal, state, and local government. The IAB is chaired by Frank McDonough, Deputy Associate Administrator for the Office of Intergovernmental Solutions, an office in the General Services Administration 's (GSA's) Office of Governmentwide Policy.

Members of the IAB:

FEDERAL

Brian P. Burns
Deputy Chief Information Officer
Department of Health and Human Services

Linda Burek
Deputy Chief Information Officer
Department of Justice

Richard Friedman
Chief Information Officer
Centers for Medicare and Medicaid Services
Department of Health and Human Services

STATE

Aldona K. Valicenti
Chief Information Officer
Office of the Governor
Commonwealth of Kentucky

Carolyn Purcell
Executive Director
Department of Information Resources
State of Texas

Wendy Rayner
Chief Information Officer
Office of the Governor
State of New Jersey

LOCAL

F. Russell Doupnik
Information Systems Director
Howard County Government
Howard County, MD

David J. Molchany
Chief Information Officer
Department of Information Technology
Fairfax County Government
Fairfax County, VA

Randall Murphy
Administrator
Department of Management Services
Lake County Government
Lake County, IL

John Clark of the Office of Intergovernmental Solutions, GSA, prepared the report. Comments on the content of this report may be sent to John Clark at john.clark@gsa.gov.

Copies of this report are available from Ms. Renee Hughes, GSA, at (202) 501-0291 or by e-mail at renee.hughes@gsa.gov. The report is also posted on the Office of Intergovernmental Solutions' home page under publications at http://gsa.gov/intergov.

Executive Summary

Wireless communication has advanced rapidly in a short time as worldwide interest in the technology fuels speedy innovation. Increasingly, personal digital assistants (PDAs) and wireless handsets can connect to back-office, agency-wide and even corporate information systems. The power and finesse of these devices is making them look more and more like mini personal computers (PCs). Many industry experts believe these mobile communicators represent not only the next generation of mobile phones, but also the next generation of the Internet.

The Yankee Group speculates that by the end of 2001, 25 million data subscribers on Internet-enabled wireless devices in the United States will generate $3 billion a year in subscription revenue to content providers. And that's just the start. Market research firm Ovum predicts that by 2005, about 484 million people worldwide will make wireless connections to the Internet.

Government users are no different. The U.S. Navy, for example, is using mobile devices onboard ships to reduce inspection errors and keep sailors connected. Several civilian agencies, such as the U.S. Department of Energy, the U. S. Department of Justice, and the U.S. Department of the Treasury, are using, or considering using, wireless devices to perform remote inspection functions. Universities such as the University of Texas at El Paso, Valdosta State University, Georgia, and other institutions of higher learning are leaders in deploying wireless networks. Additionally, state and local governments have embraced the technology to provide remote connectivity to building inspectors and electrical and water system managers.

It is important to understand that although wireless is in its third generation, it is a developing technology in the government marketplace. Wireless bandwidth speeds, costs, services and applications have only become practical in this sector in the past two years. Traditionally, wireless data services have been targeted at,

[1] The Intergovernmental Advisory Board (IAB), chartered as an advisory board under the Federation of Government Information Processing Councils (FGIPC) in May 1997, was established in recognition of the need for increased intergovernmental collaboration and education. The IAB bridges the gap between federal, state and local governments and educates IT professionals nationwide on new solutions to intergovernmental challenges.

The U.S. General Services Administration (GSA) in conjunction with the IAB is publishing this report. A total of 16 case studies were submitted from the public and private sectors. Each provides a point of contact for obtaining further information that may assist other government entities in their own efforts to implement wireless technology. Some of the major findings from these case studies are highlighted in this executive summary.

Executive Summary

and created for, the consumer. However, as wireless devices mature, needs change and expectations are set, it has become apparent that vertical markets, such as financial, legal, medical and government, will drive the wireless market and ultimately sustain its growth.

Privacy & Security

The U.S. Air Force believes that wireless local area networks (WLANs) provide a capability that could contribute significantly to improve agile combat support in the future. The advantages of wireless Ethernet are ease of installation and user mobility within a work area. However, there are many factors to consider when implementing a wireless solution in a government environment. The first and foremost consideration is data security and privacy.

A concern in the U.S. Air Force is the multitude of systems, both on and off base, that may interfere, intercept, jam, etc. another wireless transmission. The Air Force is awaiting National Institute of Standards and Technology approval of equipment that will both encrypt transmissions and enable the Air Force to use non-commercial radio frequencies.

Just as hard-wired LANs have security considerations and concerns, so do WLANs. Some that should be evaluated when planning and deploying such a network include:

1) Security features are not turned on by default—vendors want their products to work out of the box, and security is not necessarily a convenient feature.

2) Radio Frequency is a broadcast medium, susceptible to interception. 802.11 wireless LANs operate in the 2.4 GHz frequency range using spread spectrum technologies. The spread spectrum implementation reduces interference, but since everyone knows the spreading sequence, little security is gained and interception is not difficult.

3) Unlike wired networks, it is difficult to limit availability of the wireless network to a defined area; the range of the network accessibility may extend beyond your perimeter of control. Without encryption and/or authentication, a nearby wireless network card can join a wireless network, either accidentally or intentionally.

4) The Wired Equivalent Protocol (WEP), which can be used to encrypt communications between the access point (AP) and the client, suffers from some security flaws that can lead to attacks.

This does not mean that WLANs are not practical and should not be implemented. But a risk assessment should be a prerequisite to development and deployment of any information system or application. The vulnerabilities of wireless technology are different than the wired networks and should be identified and appropriate action taken to minimize the risks associated with the particular application and technology. It is important for an organization to weigh the security risks versus the business requirements. Like most decisions regarding security, it is important to understand the technical and business risks of a solution in order to determine what security is appropriate and what risk level is acceptable.

The Status of Wireless Standards

The most popular wireless transmission standards for moving forward into a 3G world are Code Division Multiple Access (CDMA) 2000 and Wideband CDMA (WCDMA). The choice of a standard will depend on the wireless carriers' existing technology. If they use Time-Division Multiple Access or the Global Systems for Mobile Communications standard—the two main standards outside the United States—then upgrading to WCDMA is the choice. But if the carrier uses CDMA, which is the most popular U.S. standard, then the move will be to CDMA 2000. The choice of a standard will depend on the wireless carriers' existing technology.

The vendor community believes there has never been a better time to create and implement a wireless strategy. The technology industry is in the best position ever to provide operational

Executive Summary

wireless products and services that will provide maximum benefit today, while preparing users for the technology that is on the way. For the first time in history, there are truly open wireless standards to facilitate widespread development of services and applications. For example, the Wireless Application Protocol (WAP) is utilized in over 95 percent of wireless devices and is used for development at hundreds of thousands of companies every day. Seventy percent of the world's network operators have deployed a service based on WAP, and banking institutions, ISPs and wireless portals around the globe have launched mobile products and services based on the WAP standard.

There are thousands of development resources editors, emulators, testing programs and out-of-the-box solutions available to the government entity that wishes to beat the curve and deploy wireless services today. Wireless technology can provide a complete and secure wireless strategy for any office that will fully utilize existing standards and protocols, while preparing users for GPRS, 3G, and beyond.

Wireless Applications in the Public Sector

The U.S. Department of Energy (DOE) has replaced an outdated paging system at a Nevada test site with a two-way messaging system linked to the national network of WebLink Wireless Inc., Dallas, Texas. The Nevada Operations Office (NEVOO) has broken new ground in contractor/government relationships by forming a partnership with a commercial wireless service provider to offer paging services to a remote area on a government installation where coverage by a commercial operator would not normally be cost effective.

In the area of health care, the National Institute of Allergies and Infectious Diseases (NIAID) implemented an interesting wireless application. Imagine what it would be like to conduct biomedical research with no Internet connection, no e-mail communication, no local area network, and no reliable phone system to communicate with colleagues. Until a few months ago, this was the situation for U.S. sponsored scientists at the University of Mali in West Africa. For the Malaria Research and Training Center (MRTC), information technology (IT) staff used wireless technology to change and solve all these problems. NIAID chose a WLAN solution and installed WLAN cards in the remaining MRTC computers using the new 802.11b technology. The total cost was a few hundred dollars per computer rather than thousands, and there were no cables to buy or maintain. The job was completed in weeks, rather than months or a year.

The Public Safety Wireless Network (PSWN) Program, co-sponsored by the U.S. Department of Justice and the U.S. Department of the Treasury, works with the public safety community to realize a shared vision of interoperability—seamless, coordinated, integrated public safety communications for the safe, efficient protection of life and property. The program has achieved success in developing solutions that allow users of disparate land mobile radio (LMR) systems to communicate. These solutions typically involve resolving problems associated with differing frequency bands or LMR technologies. The PSWN case study reviews three of these solutions.

A recent wireless application developed for the City of Edmonton, Alberta, is a good example of how a mobile database system can increase productivity while improving working conditions for the employees who use it. Building inspectors in Edmonton are now spending more time completing inspections and less time on paperwork, thanks to the mobile database application.

The Town of Enfield, Connecticut, deployed a wireless solution to connect several buildings to the town network. This initiative saved money, shared resources and preserved a historic landmark. The local government used the town's wireless network to deliver a wide range of services including education, public safety and public works, tax assessment, planning and development, social services, attendance, payroll, insurance and Internet access.

Executive Summary

Graham County, Arizona, implemented a wireless network and shares its innovative approach to using wireless technology to connect. In its case study, Graham County discusses the challenges of going wireless, the planning process in building a wireless network and the steps taken in solving each problem in the process.

In Salt Lake City, Utah where preparation is underway for the 2002 Winter Olympics, a utility company crew working downtown in the early morning hours severed a fiber optic line. The accident left a third of the city's campus without access to its network, e-mail or the Internet. The utility company estimated that the line could be fixed within ten days, but being without network access for this length of time would have severely impacted a number of city operations. Keith Barlow, the city's network administrator, restored communications in "down" locations using a WLAN. By late morning, access points had been delivered, and by early afternoon (just six hours after the accident), network operations in all sites were up and running again. A WLAN had enabled the city to meet disaster-recovery requirements within a few hours instead of days.

The Public Buildings Service (PBS) of the U.S. General Services Administration is the largest real estate organization in the United States, maintaining more than 339 million square feet of workspace for more than a million federal employees in over 1,600 communities. In the Great Lakes Region, PBS offers workspace for federal employees in Minnesota, Wisconsin, Michigan, Illinois, Indiana and Ohio. The PBS Network Team provides IT support for the nearly 1,200 Public Buildings Service employees in the region, who depend on the network for important day-to-day operations and national applications, in addition to communications such as e-mail and the Internet. PBS deployed its first WLAN to connect two of the three buildings that make up the Detroit field office. "Implementation was simple, literally plug-and-play," comments Charles Pierce, Network Team Leader in GSA's Great Lakes Region, "and, since we've eliminated the monthly cost associated with two 56K leased lines, the network will literally pay for itself in no time."

Wireless Technology on Campus

Part of the University System of Georgia, Valdosta State University (VSU) strives to provide an educational environment that fosters special concern for individual student needs, while providing the best instruction at both the undergraduate and graduate levels. Valdosta's diverse and comprehensive curriculum includes the humanities, education, nursing, sciences, business and the arts. VSU looked to wireless technology to bring connectivity only to those rooms in which students have a computer, currently about one third of the on-campus population. The cost of installing a wireless infrastructure was less than $50,000, compared to a much higher cost for the hard-wired alternative.

All of the examples cited illustrate that WLAN technology has many features that may help meet the requirements of a constantly evolving government IT infrastructure:

- Data rates up to 11 Mbps (54 Mbps soon to be released according to the 802.11b IEEE standard)
- Flexible and convenient local area networking infrastructure
- Long-range (radio line-of-sight) bridging for connectivity between sites
- Encryption and access control features
- A variety of products and vendors to choose from
- Affordability
- Ease of implementation
- Standard 40Mb WEP encryption and 128 Mb encryption

We conclude that:

- Wireless technology, beyond cellular phone usage, is a developing technology in the government marketplace.
- Wireless technology is quick to deploy and easy to scale.
- Privacy and security issues are major barriers, but are being addressed.

Executive Summary

- Wireless standards are maturing.
- Wireless applications in the areas of building inspection, education, public safety and access to Internet are beginning to appear.
- The military, state and local governments and the educational community are among the leaders in deploying wireless technology.
- Wireless technology complements, and in some instances replaces, the robust wired infrastructure in the United States.

After the recent terrorist attack on the Pentagon on September 11, 2001, Arlington County, with private sector assistance, finished building a WLAN and provided Internet access in two days. This system helped the firefighters, emergency management personnel and the police and security personnel in the search, rescue and cleanup effort. The system gave officials and rescue workers access to e-mail, networked printers, and federal, state and local databases.

.

Introduction

During the Intergovernmental Advisory Board (IAB) teleconference on April 11, 2001, several topics for possible exploration in 2001 were discussed. In particular, there was strong support for an IAB report regarding Wireless Technology in Government. This subject is topical because little is published, and we expect tremendous growth in the use of the technology to further the goals of electronic government.

This report was compiled by soliciting input from international, federal, state and local governments and their industry partners regarding how they are using or plan to use wireless technology for advancing electronic government. In particular, we solicited input in the following areas related to the use of wireless technology to deliver government information and services:

- Approaches to create wireless applications
- Advantages and/or benefits of wireless technology
- Development of government wireless applications
- Tools available to assist in the development of wireless applications
- Addressing personal privacy and security in the use of wireless technology
- Barriers to creating wireless applications
- Private industry's ability to provide mature wireless products and services
- Status of wireless technology standards

A total of 16 case studies were submitted by the public and private sectors. Each case study provides a point of contact for obtaining further information that may assist other government entities in their own efforts to implement wireless technology. Some of the major findings from these case studies are highlighted in the Executive Summary section of this report.

PUBLIC SECTOR

City of Edmonton, Alberta, Shares a Wireless Success Story

City of Edmonton, Alberta, Shares a Wireless Success Story

By Joni Mines

City of Edmonton, Alberta

Business Challenge

To put the full resources of the organization at the front line employee's fingertips and do it in a reliable way using limited capacity laptops or handheld computers.

Results

Improved customer service, increased employee satisfaction and better use of an organization's data resources, as well as increased productivity while improving working conditions for employees.

Success Story

Mobile computing is becoming a vital tool for many businesses. Arming staff with the information they need, when and where they need it, is now seen as a competitive key advantage. For public organizations, mobile computing solutions are providing efficient ways to provide improved service in the face of restricted budgets.

A recent application developed for the City of Edmonton is a good example of how a mobile database system can increase productivity while improving working conditions for the employees who use it. Building inspectors in Edmonton are now spending more time completing inspections and less time on paperwork, due to the mobile database application developed by a local value added reseller (VAR) Computronix using Sybase SQL Anywhere. Equipped with handheld tablet computers, the inspectors download their work assignments for the day from home each morning and head directly to the first site. By eliminating the need to drive to the office and organize paper-based inspection requests, the inspectors estimate they can dedicate about two hours more each day to serving their customers, the taxpayers of Edmonton.

The application, called POSSE, helps to guide inspectors through each inspection, prompting them to input certain data. That information is downloaded to the central server simply by plugging the computer into a cellular phone. That means when a customer calls the head office to check on the status of an inspection, the results are right there, minutes after the inspection has been completed.

Jim den Otter, POSSE system architect at Computronix, says, "A key advantage of SQL Anywhere is its small footprint, which allows the developer to bring a quality, relational database to a portable computer. SQL Anywhere enables the developer to build an 'elegant' application on the handheld computer for an affordable price. Computronix found the product's toolkit so easy to use, it took them only five months to build the application from scratch."

For more information, contact Joni Mines, City of Edmonton, at (780) 496-6001.

Department of Energy Partners With Weblink to Solve Paging Problems

Department of Energy Partners With Weblink to Solve Paging Problems

By Michael Tiemann

U.S. Department of Energy

The U.S. Department of Energy (DOE) has replaced an outdated paging system at a Nevada test site with a two-way messaging system linked to the national network of WebLink Wireless Inc., Dallas, Texas. The Nevada Operations Office (NEVOO) has broken new ground in contractor/government relationships by forming a partnership with a commercial wireless service provider to offer paging services to a remote area on a government installation where coverage by a commercial operator would not normally be cost effective. DOE has purchased WebLink equipment for additional sites that will be needed to cover southern Nevada. NEVOO employs 2,800 people, primarily at the test site, which is roughly the size of Rhode Island. Management and operation of the DOE-owned Weblink equipment is provided by NEVOO personnel.

The deal is worth about $3.7 million to WebLink, whose commercial coverage area has gained more than 1,000 square miles. WebLink's national wireless network covers about 90 percent of the U.S. population, and the company acts as a carrier for other wireless service providers.

In order to provide paging coverage in the past, NEVOO personnel had to wear two pagers. SkyTel Communications Inc., a subsidiary of MCI WorldCom Inc., has provided national paging services. Local service has been provided by an obsolete, 20-year-old, DOE-owned ultra-high-frequency (UHF) system. But even with the dual coverage, service has been unsatisfactory. Skytel's single transmitter in Las Vegas could not provide coverage to the test site, and the local paging system provided only one-way paging with no guaranteed delivery.

When the Commerce Department's National Telecommunications and Information Administration mandated that federal agencies convert all wide-band (25KHz) UHF radio systems to narrow-band (12.5KHz) operation, the decision was made to utilize commercial services for all paging requirements in lieu of replacing all existing government-owned paging equipment.

WebLink's extensive network gives the test site workers local and national coverage with a single device. The system uses a network of transceivers that receive signals from a satellite linked through the master controller. WebLink is adding14 transceivers to its Nevada network, and DOE is installing dedicated switch and e-mail routers for their traffic. DOE's purchase of the equipment makes the expansion economically viable for WebLink. Although DOE owns and manages the transceivers covering the test site, that portion of the network will still be open to commercial traffic, expanding WebLink's coverage along the corridor between Las Vegas and Reno.

Department of Energy Partners With Weblink to Solve Paging Problems

Energy users have three choices for service, depending on their equipment. So-called 1.5-way paging lets the caller send and receive an acknowledgment of alphanumeric messages. With 1.7-way paging, callers can send messages, and users acknowledge them from a preset list of replies. With full two-way paging, they are capable of using a keyboard to send and respond to messages.

Concerns over control issues in the event of national emergency situations prompted NEVOO to demand the ability to have signals routed to a controller located on their premises and under their immediate control. In addition, availability clauses were inserted into the Weblink contract that stipulated a maximum downtime of no more than four hours per year.

Over the last year of operation, the Weblink service has performed within the availability standard. However, problems associated with government-owned infrastructure and equipment that interface the Weblink equipment have caused most of the errors, delays and downtime. In hindsight, control of the system should have been left entirely to the professionals at Weblink. System availability would be much higher, while the cost (both capital and recurring) to DOE would be lower.

For more information, contact Michael Tiemann, Acting Associate CIO for Architecture, Standards and Planning, Department of Energy, by e-mail at michael.tiemann@hq.doe.gov .

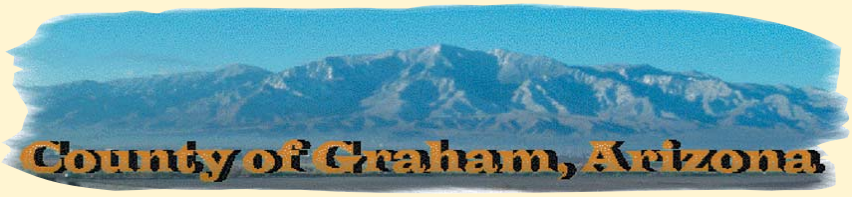
Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach

Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach

By John C. Lucas

Information Technology Director

Graham County, Safford, Arizona



Limitations and Challenges

Rural Arizona. It's your western movie backdrop: big sky, long horizon and large landscapes. Graham County is 160 miles east of Phoenix, Arizona—a rural county lining the banks of the Gila River and resting at the base of Mount Graham. The major challenge is finding a cost-effective solution to bring technology and better government services to all communities. Graham County implemented a wireless network and shares its innovative approach to using wireless technology to connect. In this article, Graham County discusses the challenges of going wireless, the planning process in building a wireless network and the steps taken in solving each problem in the process.

Background

Graham County, Arizona, is primarily made up of three communities—Safford, Thatcher and Pima—and has a population of just over 34,000, covering an area of approximately 4,630 square miles.

In general, small communities face many problems as a result of their size and the limited financial resources available for public services. In Arizona, the small communities are often spread over large physical and geographic regions. When considering telecommunications, this disproportion of area and size creates a barrier to entry, especially to provide access to telecommunications. Initially, the investment to service a large physical area with new communications technology cannot be regained from the revenues from such a small population. As a result, small communities such as Graham County typically suffer in connectivity. Technologies, such as T1 lines, DSL, ISDN and other services that are common in larger communities, are often just a dream in a rural county. Everyone told us what we could not do because of our limitations, yet it was time to find a way to just do it.

Wireless: Where and How to Connect

Graham County wanted wireless technology. Specifically, we wanted wireless connectivity for patrol cars in law enforcement. The response: "You want what in your patrol car?" Our response: "Yes, we want wireless networking. Where do we go to find it?"

For most law enforcement agencies throughout the U.S., computers in patrol cars are the direction where agencies want to head. The only problem is where to go to make it all happen when you have no digital cellular service, no data communications between agencies, limited high-speed phone services and a limited budget.

Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach

Centralizing services makes sense. As in many small communities, the county provides dispatching services for all law enforcement agencies in the county. In Graham County's situation, this structure did create a natural central point of data communications if a Wide Area Network (WAN) could be established between each city, town, county and state agency.

We found that we had three basic problems. First, how to effectively cover such a large area? Second, how to create a WAN connecting all of the communities to share common data communications and resources? Third, how to extend our communication to mobile and remote residential locations?

Our main objective was placing computers in the patrol cars, thus moving many of the duties of dispatch out to the field officer and decreasing response time. As with many projects, this proved that meeting one objective leads to developing another problem in order to accomplish the end goal.

Evaluating our Wireless Options

Before we could accomplish our goal of wireless networking, we had to answer two questions. First, what did we want to do with the connection once we had it? And second, what type of wireless technology were we going to use?

First, Graham County wanted the ability to run standard network based applications, real-time access to our law enforcement database, Internet and e-mail access for remote units and access to network resources such as our document imaging system. These requirements all translate to transfer speed in excess of 2Mbs-11Mbs.

For our second item, we found there were basically three solutions available:

1) ***Cellular or CDPD:*** This service is provided by a local cellular company that offers voice cellular. It is a form of digital cellular and bills on a per packet basis rather than time. At least this was what was explained to us. This service generally offers speeds of 14Kbs, much like a slow home modem. Since we were looking for something that would allow us to send graphic and run network applications, this was unacceptable. Also this was not available in our area at the time and is not projected to be available for several more years.

2) ***Satellite:*** Based on cost, availability and again speed of 14Kbs, this option was quickly tabled as well.

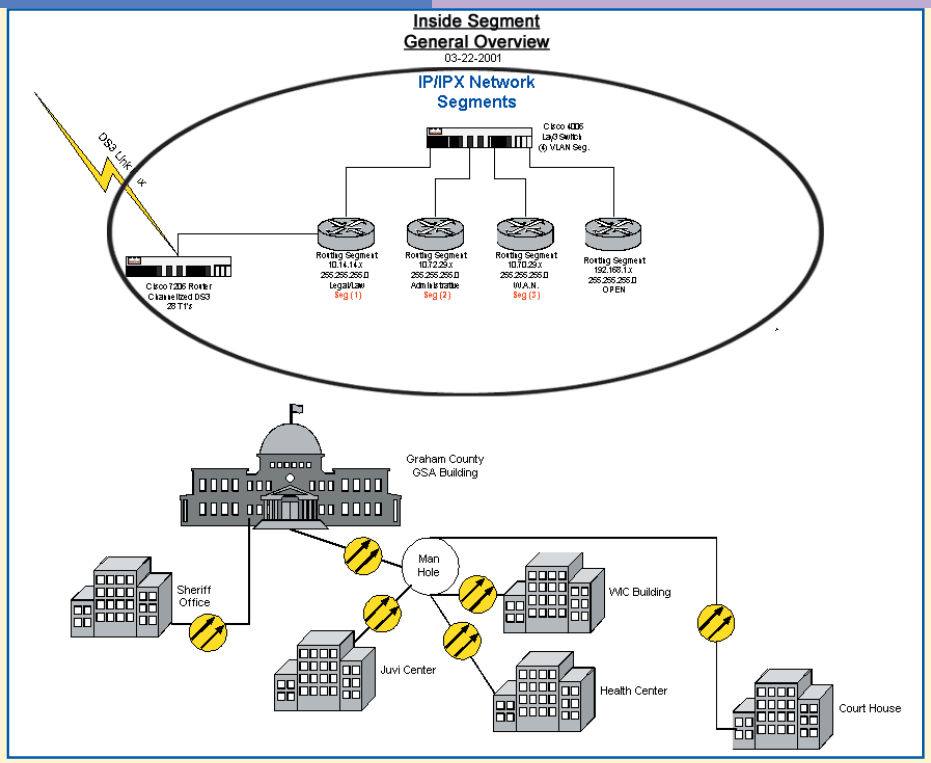
3) ***2.4Ghz Spread Spectrum:*** This system required establishing our own radio infrastructure to support access points from which the mobile units would receive their signals. Each access point would cover a radius of approximately 2.5 square miles. In examining our topography, we felt it would take approximately 25 access points to cover the majority of our population area, at a cost of about $3,500 per access point with amplifiers. It was determined that with an initial site count of ten access points, we could begin deploying mobile units, with the remaining sites installed over the next few years. Total mobile costs were in the range of $3,000 to $3,500 per unit, including laptop and 2.4Ghz radio units with amplifiers. The features that came with this solution were transfer rates of 11Mbs, 128 Bit encryption, Mac Address Isolation at access points and both IP and IPX bridge/routing.

The 2.4Ghz spectrum was selected. On the negative side, the 2.4Ghz is a public band and is used by many Internet Service Providers (ISPs). We found that it was necessary to form a frequency coordination group with all the local ISPs in the county to insure everyone played nice. Even though this initially created some additional obstacles, in the end it solved many problems.

Building a Backbone

Our first objective was connecting agencies and creating what is called a communication **"BackBone"** to drive our WAN. In looking at the best communication options available, we found that fiber optics, although expensive, was the best long-term solution. Graham County began by connecting our

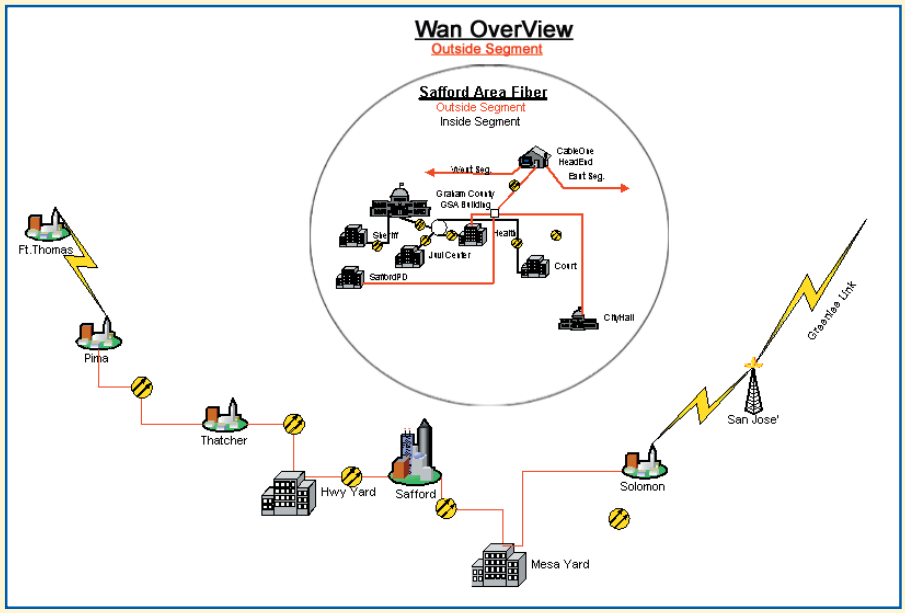
Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach



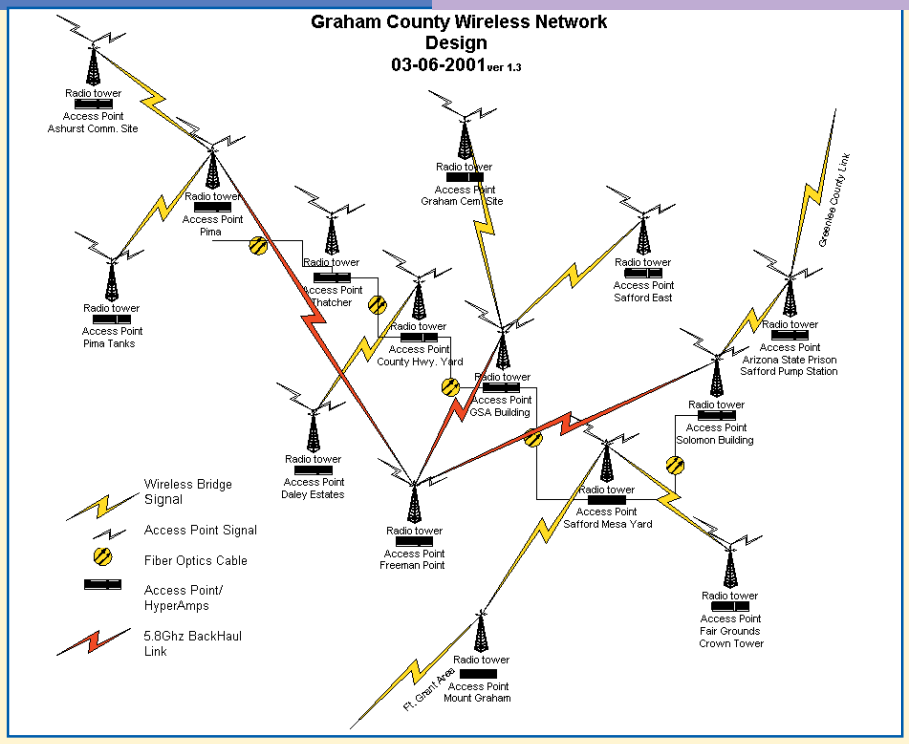
local offices and buildings within the county complex of one city block using Multi-Mode fiber optics. As we began to expand our Local Area Network (LAN) to include additional offices and departments, we partitioned (split up) our network into multiple TCP/IP segments and used a Cisco 4006 Switch to manage routing between segments. This was done based on services required and security needed. We have established three main segments: Administrative, Legal and Outside Services (WAN). By doing this, we were able to isolate and secure by using not only passwords, but also TCP/IP routing and services needed.

Connect One, Connect All

Once we had established our internal "BackBone" throughout all county departments, we looked at connecting other agencies such as cities, towns and state agencies. While reading a magazine, I came across an article on cities and counties working with utility companies, such as phone and cable, to obtain fiber links. We contacted our local cable company, CableOne, and opened discussions with them to obtain some of their dark fiber. Generally, when a company lays fiber, they overbuild for future expansion and to mitigate bad lines. This means that often times they have extra fiber they are not using or do not intend to use for quite some time. After some negotiation, we were able to obtain two strands of Single-Mode fiber optics connecting Solomon (east end of county), Safford, Thatcher and Pima (west end of county) creating our "BackBone". Each of these connections were Daisy Chained together to create a 100Mb fiber link. This link currently is being upgraded to 1Gb.



Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach



Going Mobile with Wireless

Once we had created a "BackBone" link to all of our agencies, we began the next step of going wireless. From each of the agency links to our fiber optic "BackBone," we established a broadcast point for the 2.4Ghz wireless network. These locations are referred to as access points and bridges. An access point is the radio unit that each mobile client connects with to attach to the WAN. A bridge is a link to a remote access point not on the main "BackBone" that broadcasts to mobile clients. During our test, we found that it is possible to go from one bridge to another several levels out, but we found that transfer rates from a bridged environment were reduced over those that where connected directly to the fiber "BackBone". We do use bridge-to-bridge links in several situations to reach remote areas, but we don't expect the same performance as those connected directly to the main land-based "BackBone" connection.

In a separate project, we connected all the high school districts in Graham County using bridge-to-bridge links. This is being done to provide high speed Internet to our schools and to implement a Distance Learning program from school to school and to a local community college. These bridge-to-bridge links work quite well, even though we suffer transfer speed loss at each jump.

What Have We Learned About Wireless Networking?

After almost four years of working with wireless communications and a community network, Graham County, Arizona, has learned several critical lessons:

1) To obtain any distance, you must amplify signals beyond the default radio specifications.

2) We have found that some brands do better in a bridge-to-bridge environment and some do better in the mobile roaming mode.

3) Communication rates are better from access points connected directly to land base network connects rather than those over bridged ones.

4) Establishing a frequency coordination committee within the community can resolve a lot of potential problems and result in better community relations and radio communications.

Wireless Security

Security for 2.4Ghz wireless comes in four levels. A general level of radio security is established with Spread Spectrum, since it requires similar equipment to intercept signals. On most of the models we have worked with for both bridging and roaming, we have had the ability to engage 128Bit data encryption between units. On the models we use for our mobile roaming client, we are able to secure each access point

Go Wireless: Lots of Land, Few Lines Lead to Graham County, Arizona's Innovative Approach

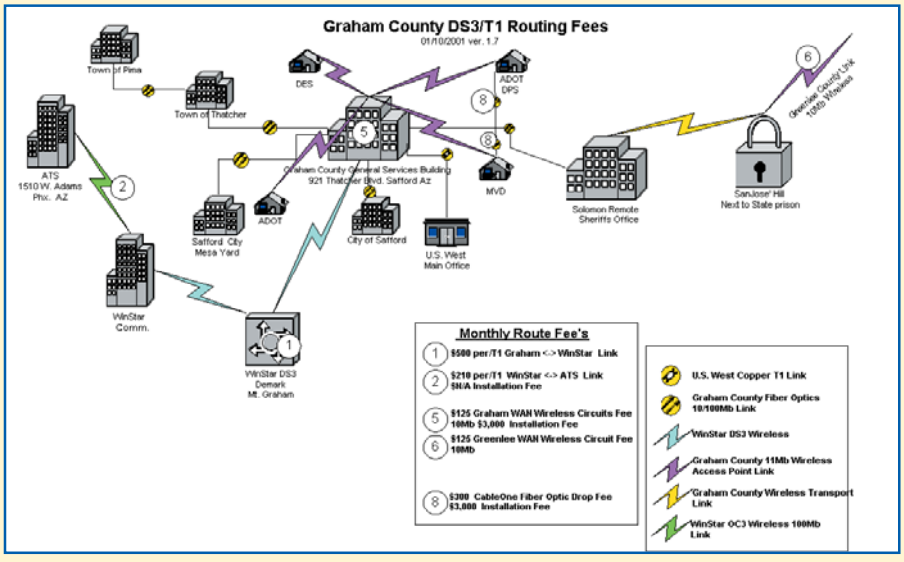
from a client, based on the client's unique Mac Address assigned to the radio card. In addition to the security found in the radio system, the network security employed by each server operating system should be the final gate to keep unwanted signals out and protect your system. If additional security is required for remote office connection via the wireless network, a PIX firewall can be installed. We have found the Cisco PIX506 to work quite well for this.

You Are Wireless: Collaboration and Success

Graham County has placed mobile units in over 30 police cars and expects to install 30 additional units by 2002. Collaborating with the State of Arizona, Graham County will link these units directly into the state's criminal database through a high-speed DS3 microwave link at the county building in Safford, Arizona.

The DS3 link provides the equivalent of 28 T1's directly into the State of Arizona Department of Administration and to the office of the Supreme Court.

We have connected all the county supervisors and the county manager via the wireless link directly into the county network to provide e-mail, Internet and county resources. Several information technology personnel have links through the wireless network to maintain network function from their homes. In the next fiscal year, Graham County will begin to deploy wireless technology to county engineering and service groups such as Assessors and Health Services. Not only have we expanded our WAN to include Graham County, we have also extended our resources to our neighboring county of Greenlee. Because of the speed that is now available to our personnel in the field, we have moved many office functions, such as document image retrieval, into the mobile units. We are using Axis Web cams to connect to remote radio to place monitoring cameras in locations where only power is available. Both the mobile units and desktops in offices can monitor these cameras. We intend to place cameras in each patrol car to allow dispatch to monitor the patrol unit and determine its status. It is also our intent to place mobile radio cameras inside local schools, so that a police unit outside in a car or at its office can monitor situations as they arise inside our schools.



We feel that only a small part of the ability of our WAN has been utilized at this point. It is important to look at the system as a whole. In fiscal years 2001 and 2002, the county of Graham is installing a 5.8Ghz wireless back-haul link to tie both ends of the fiber "BackBone" together to create a redundant path should the fiber link fail. A great deal of cooperation is required by all agencies involved, and there is an ongoing battle to keep everyone heading in the same direction. Even though a project such as this might seem extreme or beyond your ability, remember that "those who never try, never succeed".

John C. Lucas has been the Information Technology Director for Graham County in Safford, Arizona, since 1996, with over 20 years experience in software development and networking. For more information, contact John C. Lucas at www.graham.az.gov/.

Making Wireless Technology Work For Biomedical Research In Mali, West Africa

Making Wireless Technology Work For Biomedical Research In Mali, West Africa

By Dr. Laurence Wolfe

Chief Information Officer

National Institute of Allergy and Infectious Diseases

Imagine what it would be like to conduct biomedical research with no Internet connection, no e-mail communication, no local area network and no reliable phone system to communicate with your colleagues. Until a few months ago, this was the situation for U.S. sponsored scientists in the Malaria Research and Training Center (MRTC) at the University of Mali in West Africa. For ten years, the MRTC has been a primary center of collaborative malaria research in Africa for the U.S. National Institute of Allergy and Infectious Diseases (NIAID's) laboratory of parasitic diseases. NIAID, an Institute at the U.S. National Institutes of Health, leads worldwide biomedical research efforts in HIV/AIDS, malaria and other diseases.

For the MRTC, NIAID's information technology (IT) staff is using wireless technology to change and solve the MRTC's communications problems. NIAID began late last year by wiring the MRTC for connection to the Internet. Initially, they wired the MRTC for connection to the local Internet Service Provider (ISP) in Bamako, Mali. Although an improvement, the solution proved only temporary because the phone lines in Mali are expensive to use, unreliable and experience frequent outages.

To solve this problem, NIAID's IT staff switched the Internet access from phone lines to a NIAID microwave radio communication system. The microwave transmitter uses radio waves to communicate directly to the ISP in downtown Bamako, which then connects to the Internet via a satellite dish shared by the entire country. NIAID's experience is that microwave radio communication is less expensive in developing countries and more reliable than phone-line connections. But microwaves need to have "line-of-sight" to communicate. This means that the antennas at the MRTC needed to have a direct, unobstructed view of the tower located on top of the ISP building in Bamako. Fortunately, the MRTC is located on a plateau above the city, providing a perfect "line-of-sight" view of most of Bamako, including the ISP.

When setting up the microwave connection, NIAID's IT staff configured the computers so that when a person connects to the Internet, they are actually connecting via the local area network (LAN) to a microwave transmitter on top of the building. This led to a second problem, the tremendously high cost of installing a LAN in Mali. At the time of the microwave project, only a few computers were set up as a LAN due to cost and maintenance issues. To do the job for the rest of the biomedical researchers' computers in a traditional LAN wiring arrangement would have been too expensive to be feasible. Computer hardware, cabling and skilled IT help are scarce in developing countries like Mali. Equipment is frequently nonstandard, and even the most common computer parts that are readily available in the United States are often not available anywhere in Mali. Consequently, NIAID would have needed to import all of the LAN cabling and much of

Making Wireless Technology Work For Biomedical Research In Mali, West Africa

the technology labor, a very expensive and time-consuming proposition. NIAID estimated it would have cost upwards of $4,000 per computer just for the cabling and installation and taken over a year for installation.

Wireless technology again came to the rescue. NIAID chose a wireless LAN solution and installed wireless LAN cards in the remaining MRTC computers, using the new IEEE 802.11b technology. Instead of installing cables between all computers in all the laboratories, NIAID IT staff visited Mali and installed wireless 802.11b cards that allow researchers' computers to function as a LAN and communicate with speeds up to 11Mbps, using a special range of radio waves. Total cost: a few hundred dollars per computer rather than thousands and no cables to buy or maintain. The job was completed in weeks, rather than months or a year.

The wireless LAN has been a great success. However, while the microwave connection to the ISP has proved to be a great improvement over phone-line connections, it is still not an ideal solution. A few months ago, the satellite connection the country uses to connect to the Internet went down. Then, a few days later, the state telephone company, which maintains the system, went on strike, essentially leaving the entire country offline with no Internet service. International phone lines were down for several days as well. Mali scientists had no communications with NIAID in the United States or elsewhere.

NIAID's IT staff then developed a plan to provide the MRTC with its own satellite system, not dependent on the local Bamako ISP or telephone company. In addition to improved reliability, the new satellite system was targeted to address another problem, an explosion in growth in the number of people using the Internet in Mali. While it is great that more Mali citizens can be connected, Mali still has only the one and same size "pipe" or satellite link for the entire country. The connection is becoming so congested that it is sometimes almost unusable. For those reasons, NIAID chose to get the MRTC its own satellite communications system.

NIAID is implementing the plan and has already installed its own satellite dish in one of its Bethesda, Maryland, facilities. The Mali dish installation was completed in the first week of November 2001. Once operational, the new NIAID/MRTC satellite system will provide greater Internet connectivity at higher speeds. NIAID and the MRTC will use the new satellite connection to conduct collaborative research projects. The satellite will also enable communication between researchers at NIAID in Bethesda, Maryland, the main MRTC lab facility in Mali, and a remote field laboratory and clinic in Bandiagarra, which will also be equipped with a satellite dish. The satellite connection is especially important for maintaining research databases at all three sites, ensuring fault tolerance of the data.

NIAID's IT staff is already planning to extend the capabilities of the new satellite. NIAID envisions the use of voice over Internet (VOIP) and dynamic video conferencing technologies. These features will provide more capabilities at lower cost and greater reliability for MRTC scientific researchers in communicating with their colleagues in the United States and other countries.

NIAID is now working on a new challenge to support the Institute's biomedical research efforts in Africa. Again, wireless technology will be the solution of choice and necessity. The problem comes from one of NIAID's primary missions in Mali—providing and facilitating biomedical research on malaria. Each year the challenge becomes more crucial once the malaria season begins. Researchers traveling to villages must keep patient records in the village clinics. Therefore, they need to be able to access and transmit data on site, instead of sending floppy disks by truck to the Bamako facility. NIAID needs to provide a way for researchers to send and receive data and e-mail from field sites and make updates to the vaccine research databases in real time. The challenge becomes more complex because remote field locations don't always have telephone lines or electricity, and what they have is not always reliable.

NIAID plans to install a packet radio system to connect field sites that have unreliable or no power sources. A packet radio

Making Wireless Technology Work For Biomedical Research In Mali, West Africa

antenna has already been constructed at the MRTC, and the first packet radios are scheduled for installation in the fall of 2001. The plan is to install packet radios in Jeep-like vehicles already in use by researchers. The packet radios will allow voice, fax, e-mail communication and database updates from any location within several hundred to as much as a thousand kilometers of Bamako, but at lower speeds.

For researchers, it will be like using a slow modem connected at 2,400 bits per second as compared with today's standard modem speed that operates at 56,000 bits per second. However, the advantage for researchers will be tremendous, since they will have real time e-mail and database access where now they have none. Since packet radios don't require much electricity, NIAID's IT staff plans to hook up the packet radios to laptop computers and configure them to run from car batteries. NIAID's IT staff will visit Mali this fall to install and test the first packet radios.

Helping the MRTC staff and Malians become accustomed to the new technologies has been a great and rewarding experience for NIAID's IT staff. A first introduction to computers, followed by the change to wireless LAN, microwave, satellite and now packet radio technologies has been a real challenge for many.

The response from the MRTC and the Malians has been superlative. In several visits, NIAID IT staff members trained MRTC personnel on topics ranging from introductory computer use and word processing to accessing the Internet. NIAID showed MRTC staff how to set up computers and servers, how to install the operating system and how to configure and network them.

The new wireless technologies have helped the MRTC and Malian staff make a dramatic transformation to IT. They now see the Internet as a communications tool they can really use to help their biomedical research. They've never had the capability to reach the outside world electronically via the Internet or to use computer networks to accomplish their work. Wireless technology helped make it happen.

For more information, contact Dr. Laurence Wolfe, Chief Information Officer and Director of IT, U.S. NIAID, via e-mail at lwolfe@niaid.nih.gov

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

By Bob Lee, U.S. Department of Justice

Rick Murphy, U.S. Department of the Treasury

The Public Safety Wireless Network (PSWN) Program is a joint initiative of the U.S. Department of Justice and the U.S. Department of the Treasury. The program is dedicated to saving lives and protecting property by improving wireless communications interoperability among public safety organizations. In support of this objective, the program is working to promote interoperability as a national priority. While establishing itself as the leader in providing comprehensive solutions to wireless interoperability, the program seeks to ensure that no person will ever lose his or her life because public safety officials could not talk to one another.

Every day, incidents that require a coordinated public safety response occur throughout the Nation. For the most part, local agencies in a given community achieve interoperable communications among themselves through small-scale measures that address the situation on a very localized level. However, in extreme cases, such as the acts of terrorism on September 11th, where multiple jurisdictions are involved, lack of interoperable communications could become a major impediment to the success of the operation. The inability of organizations to communicate effectively on demand stems from several issues. They include inadequate funding for shared public safety networks, insufficient spectrum for interoperable communications or technical incompatibility of equipment.

To address these issues, the PSWN Program has undertaken a multifaceted approach to resolving wireless interoperability. The program is actively conducting interoperability assistance projects, developing and sharing solutions to interoperability problems and engaging public safety agencies at all government levels to address the key issues related to improving interoperability (i.e., coordination and partnerships, funding, spectrum, standards and technology and security). Through these efforts, the program works with the public safety community to realize a shared vision of interoperability—seamless, coordinated, integrated public safety communications for the safe, efficient protection of life and property.

Many of the program's activities to date have focused on building the baseline of information needed to resolve interoperability issues, developing partnerships with the public safety community and developing a national strategy for improving interoperability among wireless networks. The program is actively engaged in several areas across the country to implement proven approaches to interoperability. The public safety community relies heavily on private land mobile radio (LMR) systems for mission-critical communications in emergency situations. The infrastructure of an LMR system is typically characterized by one or more base stations, each providing coverage for several square miles, and numerous mobile radios that provide two-way voice and possibly data connectivity for the public safety personnel. Each mobile radio can be mounted in a vehicle or carried

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

by a public safety officer. LMR systems operate in several frequency bands and use a wide range of technologies, some of them proprietary. While some public safety agencies are using systems with cutting-edge digital technology, others still employ systems designed several decades ago.

Historically, LMR systems were designed and built to meet the needs of individual agencies and departments in a limited geographic region. This limited design has often led to difficulties in joint operations because of poor interoperability between the various LMR systems. To improve communications and operations among public safety personnel, a variety of technical solutions must be developed to integrate the disparate systems. Therefore, one of the PSWN Program's main areas of activity is the development and implementation, for proof-of-concept purposes, of technical solutions for interoperability among public safety networks. The program focuses on repeatable technical concepts that address common interoperability shortfalls among public safety agencies throughout the Nation. The program develops these solutions in partnership with state and local agencies in the region. This approach allows the PSWN Program to leverage the solution beyond the pilot region and, more broadly, to benefit the public safety community as a whole. The following sections provide an overview of three innovative solutions the program has developed.

The Transportable Public Safety Radio Interoperability Unit (TPSRIU)

The TPSRIU is one of the technical interoperability solutions the PSWN Program has developed and implemented in several locations. The TPSRIU was designed based on lessons learned from the program's San Diego case study and pilot test project. The San Diego case study focused on an assessment of interoperability in San Diego and Imperial Counties. The primary recommendation from the case study was to implement a pilot test targeting the need for a transportable interoperability solution supporting public safety agencies responding to emergency situations. To support this effort, the PSWN Program, working with local officials, developed the Transportable Communications System (TCS). Features of the TCS include:

- Providing first response communications interoperability during the initial 24 to 48 hours of an emergency situation
- Supplementing or extending the reach of fixed infrastructure coverage
- Providing transportable communications backup with flexible system configuration
- Enhancing federal, state, and local interoperability during emergency operations and special events.

Due to the success of the TCS in improving interoperability in San Diego, the program developed the TPSRIU, a transportable interoperability solution that can be implemented anywhere in the country. The TPSRIU consists of three basic building blocks: radios, an audio switch to provide the interconnections and interface hardware (e.g., custom cables, terminal strips) to provide the physical connectivity supporting system operation. The TPSRIU was designed for mounting into transit cases that could be transported to any location that could provide the necessary power. The TPSRIU was integrated from commercially available hardware and software and was fully tested prior to shipment to the required locations. The following radios are integrated into the TPSRIU and provide interoperability with the majority of LMR systems used by the public safety community:

- Very high frequency (VHF) programmable (146–174 megahertz [MHz]) Motorola ASTRO Spectra mid-power mobile radio with a W4 radio control head designed with the Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA)-102 (Project 25) Common Air Interface (CAI) and configured for conventional operation
- Department of Justice (DOJ) Justice Wireless Network (JWN), VHF (146–174 MHz) Motorola ASTRO Spectra high-power mobile radio with a W4

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

remote mount radio control head designed with the TIA/EIA-102 CAI and configured for conventional operation, encryption, over the-air re-keying (OTAR) and multikeying

- 800 MHz (806–870 MHz) Motorola ASTRO Spectra high-power mobile radio with a W4 control head designed with the TIA/EIA-102 CAI and configured for Motorola SmartZone trunking and conventional operation
- Ultra high frequency (UHF) programmable (403–433 MHz) Motorola ASTRO Spectra mid-power mobile radio with a W4 control head designed with the TIA/EIA-102 CAI, and configured for Motorola SmartNet trunking and conventional operation.

TPSRIU systems are now on station at the following locations:

- Albuquerque, New Mexico
- Denver, Colorado
- Phoenix, Arizona
- Quantico, Virginia
- Salt Lake City, Utah
- San Diego, California

The program selected these locations because these jurisdictions needed this type of interoperability solution and because of their geographic separation. The TPSRIU has been used successfully during critical joint-agency emergency operations. During the rescue and recovery operations at the Pentagon after the September 11th terrorist attacks, the Quantico, Virginia, TPSRIU was successfully deployed at the scene. It facilitated interoperability between the Federal Emergency Management Agency (FEMA) and urban search and rescue teams from Virginia, Maryland, Tennessee and New Mexico. The TPSRIU allowed personnel to communicate directly using their own equipment. Without the TPSRIU, rescue personnel would have had to employ runners or carry extra radios to communicate. Either of these alternatives would have certainly inhibited the response effort.

Interconnection of Incompatible Radio Systems in South Florida

The PSWN Program employed a technological solution in the south Florida region to solve an interoperability problem identified by the Attorney General of the United States. Because of south Florida's proximity to the island of Cuba, that area's public safety agencies must prepare for a unique challenge, a mass migration incident. Such an incident would require highly coordinated radio communications between all responding agencies. Because the responding agencies in the south Florida area have a variety of incompatible radio systems, it is typically not possible for them to communicate directly with each other using their own mobile and portable radio units. The agencies responsible for responding to such an incident are the Florida Highway Patrol (FHP), Florida Department of Law Enforcement (FDLE), Broward County Sheriff's Office, Miami-Dade Police Department, Monroe County Sheriff's Office, U.S. Coast Guard (USCG), Federal Bureau of Investigation (FBI), U.S. Immigration and Naturalization Service (INS) and the Border Patrol.

The agencies in this area have LMR systems on the VHF band, the UHF band, and the 800 MHz frequency band. Agencies in the same frequency band that have conventional, non-trunked radio systems can have direct interoperability if they share frequencies and squelch codes. Agencies in the same frequency band that have compatible trunked radio systems can share talk groups for interoperability. Agencies using radio systems with incompatible, proprietary trunking protocols, such as those offered by Motorola and M/A-Com Private Radio Systems (formerly ComNet Ericsson), cannot share talk groups and must find another method to achieve interoperability. Agencies that do not conduct operations in the same frequency band cannot share frequencies to achieve interoperability and must also find another method to achieve interoperability. The agencies participating in this pilot operate in the UHF, VHF high and 800 MHz frequency bands, and they also use incompatible trunked radio systems.

The complexity of the interoperability problem in the region required a two-part

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

solution. The PSWN Program solution included a console-to-console link and mobile audio switches. To provide a link between agencies with disparate radio systems and overlapping coverage, the program developed a console-to-console link. The console electronics switches are linked together via the leased telephone circuit and treat each other as though they were connected to conventional base stations. A standard base interface module (BIM) (manufactured by Motorola) or conventional interface card (CIC) (manufactured by M/A-Com) is used to interface with the interconnecting four-wire telephone circuit. The consoles are typically set for voice operated transmit (VOX) operation. Voice audio supplied by one of the consoles to the telephone circuit activates the corresponding console at the other end of the circuit. This configuration creates a "patch" between the two consoles to connect users on one system with users on the other system, thereby allowing field-unit-to-field-unit interoperability.

Although the console-to-console interoperability solution works very well, its usefulness is limited to the overlapping coverage areas of the LMR systems that are patched together. Therefore, the PSWN Program provided mobile audio switches that could be used to link subscriber portable or mobile radio units together in these areas. Each mobile switch can interface with up to 12 different portable and mobile radio units and patch them together to provide interoperability between the various agencies. The PSWN Program provided one mobile audio switch and a corresponding VHF conventional mobile radio unit to each of the three selected counties in south Florida—Broward, Miami-Dade and Monroe. The three counties own, manage and maintain the audio switches to ensure that they are operational and available whenever they are needed. The PSWN Program provided the appropriate radio interface cables for each audio switch. When needed, each agency supplies the appropriate mobile and/or portable radio unit(s) to be connected to the audio switch at the scene of an incident. With the audio switches and the console-to-console links, the public safety agencies of the south Florida region now have a complete technical solution to meet the interoperability needs that might arise from any public safety incident.

Consolidation of Multiple Radio Sites in Red Lodge, Montana

Throughout the Nation, a major impediment to interoperability is the accepted practice of each agency building its own separate LMR system. It is much more difficult to achieve interoperability if the systems involved are designed and built separately. To avoid these difficulties, one of the PSWN Program's goals is to encourage the public safety community to build shared systems that will spread the cost of construction and maintenance and ultimately improve the service provided and interoperability. While shared system development is a superior method for building new LMR systems, it is very difficult to coordinate, especially among federal, state, and local public safety entities. Therefore, the PSWN Program sponsored the upgrade and consolidation of a radio site at Red Lodge, Montana.

With this site consolidation project, the State of Montana will be able to launch a repeatable site collocation and consolidation effort. Through this effort, the Montana Department of Transportation, Montana Department of Justice (Highway Patrol), Carbon County, the Bureau of Land Management, the U.S. Forest Service and the FBI are consolidating their radio resources within a single facility. In addition, after all federal, state, and local public safety agencies are migrated to the new tower and shelter, two aging, adjacent radio sites will be removed. The consolidated site will provide significant cost savings for the individual public safety agencies and improve the overall quality and reliability of the radio communications service provided.

The PSWN Program supported the site consolidation project by providing technical assistance (e.g., site surveys, antenna subsystem design and intermodulation analysis) and surveying potential site users to determine the site requirements

The Public Safety Wireless Network Program Pilots Wireless Technology That Improves Public Safety Interoperability

(e.g., shelter capacity, layout, backup power, heating, ventilation, air conditioning and future requirements). Analysts used this information to create a statement of work and specifications for the site tower, shelter and the tower and shelter installation. The assistance the PSWN Program provided throughout all phases of the project can be used as a model for consolidating other sites throughout Montana. This project proved that federal, state, and local public safety agencies can effectively collocate their LMR resources to the benefit of all users.

More information on these solutions and other means for achieving interoperability is available from the PSWN Program. The PSWN Program can be contacted by e-mail at information@pswn.gov or by telephone at 1-800-565-PSWN. The program's Web site, at www.pswn.gov, provides a wealth of information regarding public safety wireless interoperability.

U.S. Air Force Addresses Privacy and Security Concerns

U.S. Air Force Addresses Privacy and Security Concerns

By
Colonel
Thomas J. Zuzack

US Air Force

Addressing Personal Privacy and Security Issues With Use of Wireless Technology

Wireless cannot be thought of as just cellular phones and pagers that require protection against fraudulent use and eavesdropping. Future security requirements will include all of those currently associated with wire network information systems, plus all needs arising from wireless mobile communications by individuals in and away from the office. Addressing security requirements will be a major priority due to the additional exposure and vulnerability associated with wireless technology.

Assessing the Ability of Industry to Provide Operational Wireless Products and Services

A concern that has been identified within the Air Force for some time is the multitude of systems, both on and off base, that may interfere, intercept, jam, etc. another wireless transmission. We have developed interim policy, waivers, etc. All have acted as stopgaps or band-aids, but we need to get out of the commercial bands to finally fix this problem for military systems wishing to use Radio Frequency (RF) Wireless Local Area Network (WLAN) products. We are awaiting the National Institute of Standards and Technology (NIST) approval of equipment that will both encrypt transmissions and get us out of those commercial bands.

Barriers to Creating Wireless Applications

The lack of accepted international operating standards and adequate international spectrum allocations effectively prohibits deployment of single-instrument, worldwide secure cellular telephone (CT)/Personal Communications Systems (PCS) technology at this time. Although multi-band CT/PCS devices are spreading rapidly, this technology is by no means close to providing the secure, universal service required for global military connectivity.

Passive and Active Attacks Against IT Infrastructure Using Wireless Technology

One or more of the following examples of the type of attacks against modern wireless systems have been encountered at Air Force installations: Attacks against the security management infrastructure that provides user authentication data, passwords, keys, authentication algorithms, etc., include:

- Passive intercept attacks against control signals
- Passive intercept attacks against user signals
- Active attacks against wireless network, including those network functions involved in:
  - o Security service management

U.S. Air Force Addresses Privacy and Security Concerns

- o Security mechanism management
- o Security audit
- o Security recovery
- o Coordination of network security services
- o Intersystem messaging security
- o Physical attacks against the mobile unit
- o Geo-location
- o Jamming
- o Spoofing
- o Denial of Service

Developing Government Wireless Applications

Recent decisions in Congress and by the Federal Communications Commission (FCC) have redirected the development and deployment of dedicated federal wireless services using federal spectrum to commercial leased systems. The Congressional actions include the Clinger-Cohen Act (also known as the Information Technology Reform Act) and the Telecommunications Act of 1996.

These two Acts have had a significant impact in the areas of telecommunications and information technology. Specifically, these acts encourage the procurement of commercial-off-the-shelf (COTS) products and services instead of custom products and government unique developments.

Identifying Advantages/Disadvantages and/or Benefits of Wireless Technology

Wireless LANs provide a capability that could contribute significantly to improved agile combat support in the future. The advantages of wireless Ethernet are ease of installation and user mobility within a work area.

The two major disadvantages of wireless technology are vulnerabilities to accidental interference and malicious activity. 802.11b operates at 2.4 GHz, in the unlicensed Industrial, Scientific, Medical (ISM) band. Thus, there may be interference with devices such as medical instruments and the new generation of cordless telephones.

Identifying Tools Used to Assist in the Development of Wireless Applications

Soon to be available as a COTS product is a biometrics device that uses unique physical identifiers such as voiceprints, fingerprints or retina images to positively identify the user. By combining third-generation wireless with smart cards and biometrics, organizations will finally have a unified security system that works for both the wireless and wired worlds.

Identifying Wireless Technology Standards Used

The most popular wireless transmission standards for moving forward into a 3G world are Code Division Multiple Access (CDMA) 2000 and Wideband CDMA (WCDMA). The choice of a standard will depend on the wireless carriers' existing technology. If they use Time-Division Multiple Access or the Global Systems for Mobile Communications standard—the two main standards outside the United States—then upgrading to WCDMA is the choice. But if the carrier uses CDMA, which is the most popular U.S. standard, then the move will be to CDMA 2000. The choice of a standard will depend on the wireless carriers' existing technology.

For more information, contact Carlson Wiltshire (ANSER), HQ USAF/SCMNT, Directorate of Mission Systems, Mobile & Wireless Technology/Applications Systems Lead, at DSN 425-2559 or Commercial (703) 588-2559.

Wireless Education Takes a Leap

Wireless Education Takes a Leap

By Anna Hines

Chief Information Officer

University of Texas at El Paso

Consider the Following Scenarios:

- On a joint field trip to a rich geological area south of Juarez, Mexico, geology students from the University of Texas at El Paso (UTEP) and from the Universidad Autonoma de Ciudad Juarez (UACJ) witness the discovery of an unusual strata formation. Not wanting to waste a valuable learning opportunity, the graduate assistant opens his laptop and accesses a database via the Internet and finds the information he needs to teach the students about the formation.
- Students in five different El Paso high school anatomy classes are glued to the projection screens in their classrooms watching heart surgery performed at Johns Hopkins teaching hospital.
- A UTEP senior lies in a hospital bed convalescing from an accident listening via his laptop to an important biology lecture and slide presentation of a class occurring in the UTEP Undergraduate Learning Center.
- A student who has forgotten an important paper at home rushes to the UTEP Student Union building to check out a laptop so she can access her computer at home and download and print the paper while sipping a latte on a couch with her friends.
- Students viewing an art exhibit at the El Paso Museum of Art use their laptops to access the Internet to research and view other paintings by the same artist as the docent explains the progression of the artist's work.
- An assistant UTEP basketball coach opens his laptop and sends a video e-mail to a star recruit during a basketball game, telling him about UTEP and how the coach was thinking of the recruit's three point shooting ability during the last trip down the court.

All of these scenarios are about to become reality at UTEP.

Internet2's Wireless Gateway to Mexico

UTEP sits at the corner of Texas, bordering the State of New Mexico to the north and overlooking the Rio Grande River and Juarez, Mexico, El Paso's sister city, to the south. Due to El Paso's geographical and cultural proximity to Mexico and the city of Juarez, UTEP has always worked closely with educational institutions in Mexico in searching for ways to solve common problems together as neighbors.

In 1999, Mexico founded Corporación Universitaria para el Desarrollo de Internet (CUDI) to begin an initiative to interconnect Mexican universities into a research network similar to Internet2 in the United States. In 2000, the two networks were connected with a single high-speed link in California. The Universidad Autonoma de Ciudad Juarez (UACJ), though paying membership dues to CUDI, did not have a dedicated physical link to the rest of the CUDI community because of its distance from other major Mexican metropolitan areas. Since UTEP is a member of Internet2, UACJ could be connected to both Internet2 and CUDI if it had a direct connection with UTEP.

Wireless Education Takes a Leap

Connecting by fiber optic cable proved cost prohibitive, as the fiber provider wanted $35,000 per month to use its fiber network, so UTEP began to explore wireless alternatives. UTEP applied to the Federal Communications Commission (FCC) for a license to transmit on specific frequencies imposed by the equipment that was to be used. Obtaining an FCC license turned into a bureaucratic nightmare that resulted in cancellation of the application by the FCC. In spite of these setbacks, UTEP decided to implement a temporary 11 Mbps (megabits per second) IEEE 802.11b solution, which operates in the unlicensed radio frequency spectrum and does not require FCC approval.

Although there is a direct line-of-sight between UACJ and a tower on UTEP's campus where the antenna is mounted, the distance of 4.7 miles was close to the limits of this technology, so amplifiers were installed to cope with potential signal loss. The entire installation process was accomplished in several days and required only a few border crossings. Measurements after installation showed good signal-to-noise ratio and transmission has been trouble free during the six months of its operation.

While discussing ways to provide UTEP's students, faculty and staff with a high-speed, citywide wireless link to the campus network, the Internet and Internet2, Western Multiplex suggested using a 100 Mbps Tsunami wireless bridge that operates in the unlicensed part of the spectrum. Quickly realizing its usefulness in solving the CUDI-Internet2 problem, UTEP asked Western Multiplex to partner with them on the project. Western Multiplex graciously agreed to drastically reduce the cost of the equipment and also enlisted the assistance of Integrated System Group, an El Paso-based company with a great deal of experience in both the United States and Mexico, who agreed to perform the site survey and installation free of charge. The new 100 Mbps link was installed and was operational at the end of July 2001. Should traffic warrant a higher capacity link, Western Multiplex offers another product in the Tsunami line that operates at 720 Mbps, above the OC-12 level commonly used for Internet2 connections. UACJ has also informed UTEP that it would have a new direct link to the main CUDI network installed by the end of July. This will provide Mexico with an additional link to Internet2, enabling redundancy and load balancing.

Campus Wireless Projects

The involvement with wireless networking technologies at UTEP began when the University Bookstore was looking for ways to enable network connectivity for outdoor book fair events in popular places, such as in front of major campus buildings. The temporary nature of these events and the outdoor ambient made wiring very impractical. Wireless LAN seemed to be the perfect solution.

To evaluate this technology, UTEP launched a pilot program with the help of Enterasys Networks, who donated a RoamAbout 802.11b wireless LAN access point, ten laptop computers, and a larger number of wireless PC cards. The access point was placed in the Student Union, a popular building that houses the University Bookstore, along with several eateries, lounging areas and other facilities. The computers and the wireless PC cards were used in a checkout program in which students could borrow the laptops and use them to access network resources and services from anywhere within the Student Union building.

The program was very successful, and there was demand to expand the area covered with wireless LAN signal to other major buildings. Currently, several buildings are covered with signal including the Library, the flagship Undergraduate Learning

Wireless Education Takes a Leap

Center, the Information Technology department, and the Union Plaza, an outdoor area between the two wings of the Student Union. Beside students, faculty and staff have also embraced this network and become regular users.

The Student Union building and its surrounding area will soon be upgraded with new access points based on the 802.11a standard that will enable data rates of up to 54 Mbps. These access points will be downward compatible with existing 802.11b based 11 Mbps data rates. New 802.11a PC cards will be required to take advantage of the faster rates.

There are many requests from various departments and individuals for further expansion of this network. An interesting suggestion is that the one entire campus street where several already covered major buildings are located should be covered with signal, enabling users to walk from one building to another without breaking a connection. The goal is to cover the entire campus with wireless LAN.

Point to Point Wireless Links

The university recently acquired a small off-campus building. The building was to house the Center for Inter-American and Border Studies with less than ten employees. The applications in use are e-mail, access to the student information system and other information services, and Web access, similar to the majority of other campus offices. In addition, the office hosts a Web server that is accessed mostly from outside campus.

The building is located only a few blocks from the main campus, but too far for the local area network to reach. Installing fiber optic cable was not an economical option, and besides, there was no time for such a solution—the building had to be equipped in a very short period of time. Another option considered was leasing one or more T1 or ISDN lines from an Internet service provider (ISP), a solution that is currently used with some other off-campus buildings. It was ruled out because the monthly charges would soon have surpassed the cost of a wireless solution while offering a fraction of the bandwidth.

Cable modem and DSL services were also considered because of their acceptable bandwidth, but were rejected for similar reasons. In addition, they would require the traffic to go through the ISP's network, as well as through the university's already saturated commercial Internet connection. There would also be privacy issues, requiring the use of virtual private networks (VPN). It was clear that a wireless connection would provide much better performance than any other solution except fiber, while avoiding all their disadvantages. Higher bandwidth, more control, no monthly charges, no expensive and time consuming installation and no adverse impact on the university's commercial Internet connection made wireless an obvious choice.

Enterasys RoamAbout 802.11b wireless bridges were installed on both ends, operating at 11 Mbps in a point-to-point configuration. A directional antenna was mounted on the roof of the building, pointing to another antenna on the main campus with a clear line-of-sight. The wireless bridge in the building is hooked up to a 24-port Fast Ethernet switch that delivers network connectivity to individual desktops. Because of the relatively short distance, no exhaustive site survey was conducted other than making sure there was a clear line-of-sight between the two antennas. Signal strength measurements were taken after installation to ensure that the link was in stable operating condition.

For the time being, the 11 Mbps connection is adequate for the number of users and the mix of applications they are running. Currently the utilization on the link is below ten percent on average, which shows that there is enough

Wireless Education Takes a Leap

bandwidth for current and future applications. This would not be the case with a T1 line whose bandwidth is only approximately 1.5 Mbps. If the link becomes saturated in the future, it can be easily upgraded to a faster 54 Mbps solution. For data rates of 100 Mbps and higher, more expensive proprietary solutions are available, as well as a fiber connection, although at the moment that seems unlikely.

Users in the building are pleased with the quality of the wireless link, both in terms of capacity and availability. Any difference between this connection and fiber connections to other campus buildings is not noticeable to the users. From an individual user's perspective, this 11 Mbps wireless link provides network throughput that is comparable to wired 10 Mbps feeds to several other buildings of similar or larger size on the campus periphery or most larger buildings with 100 Mbps feeds.

The success of this connection served as a model for connecting two much larger off-campus buildings, a project that is underway as of this writing. The College of Health Sciences and the Stanton building are located on adjacent blocks about a mile away from the main campus. The two buildings are connected with a fiber link, and a T1 line connects the College of Health Sciences with the main campus. Upgraded in 1995 from two 56 kbps links, this line is currently inadequate for the amount of traffic being generated, especially since only about a third of the bandwidth is used for data traffic, while the rest of the line capacity is reserved for video conferencing. The data portion of the T1 line is therefore almost constantly utilized at 100 percent during business hours. This has been a problem even for low bandwidth services like e-mail and completely prevents the use of high bandwidth application, especially on Internet2 both on and off campus.

To alleviate the situation, an 802.11b wireless link is being installed, in addition to the T1 link, which will boost network throughput more than tenfold. The T1 line is still necessary for the other services, but if they can be migrated to the data network, it would allow UTEP to discontinue the use of the costly T1 line.

Although the new wireless link will provide superior service compared to the existing one, it is considered only a temporary solution. With the rest of the campus upgrading to Gigabit Ethernet, it will probably be necessary to install a very high speed wireless connection such as the 720 Mbps Tsunami by Western Multiplex to take full advantage of new bandwidth intensive applications on Internet2.

Future Plans

UTEP is planning to expand its wireless capabilities to include the citywide area of El Paso. Since El Paso basically surrounds the Franklin Mountains, this can be achieved by setting up several wireless bridges and antennas on the mountains so the entire city is within line-of-sight of at least one antenna. This will not only provide UTEP's students, faculty and staff with a high-speed wireless link to UTEP and the Internet, but will also facilitate UTEP connection to local school districts. This connection will enable teachers to connect to Internet2 for educational purposes, as well as allow UTEP to conduct teacher training by videoconferencing. The UTEP community is excited about the emergence of the wireless network that has generated a greater sense of pride in the university and interest in the new educational opportunities.

For more information, contact Anna Hines, Chief Information Officer, University of Texas at El Paso, by e-mail at ahines@utep.edu

Wireless Technology Keeps the City of Richmond, British Columbia, Above Water

Wireless Technology Keeps the City of Richmond, British Columbia, Above Water

By Edward Hung

Manager of Advanced Research and Technologies Team

City of Richmond, British Columbia

The City of Richmond in British Columbia on Canada's west coast would be under water at times during the year if the drainage pumps operated by the city weren't constantly pumping water into the broad Fraser River, which encloses the city on three sides. On the fourth side, the salt waters of Georgia Strait lap the city's shores. The city has an average elevation of only one meter (three feet) above sea level.

Obviously, careful planning is essential. A leaky main or burst pipes spell trouble in a city where water can't drain downhill. Entire neighborhoods could be flooded if drainage systems are unable to meet the demands of new development or a heavy downpour. But where should new pumps be located? Which pumps are most vulnerable to breakdown? How much impact does a new shopping center, office building or residential development have on drainage or water usage? When Richmond planners went to answer these questions, they discovered that they had millions of lines of data, but very little useful intelligence.

Data Into Intelligence

The data comes from one of North America's largest supervisory control and data acquisition (SCADA) systems. Radio transmitters at 180 pumps, temperature sensors, and river level monitors send status reports to a receiver on the top of a high hotel, which feeds it to a control room where alarm conditions such as failed pumps or power outages can be identified. Each week, the system collects more than 2 million records, which are stored in a proprietary database on a PC server running a real-time operating system.

To gain intelligence about this data, Richmond turned to WebFOCUS from Information Builders. WebFOCUS had two outstanding features that attracted Richmond: First, it was capable of tapping into the proprietary database in which all that data was stored and, unlike that database, it had powerful reporting and analysis capabilities. Second, its ability to publish reports on the Web means the city can put that intelligence in the hands of anyone, including users of wireless devices. Today, public works crews in the field or engineers in planning meetings can pull down useful intelligence about the city's infrastructure on PDAs.

That's a far cry from Richmond's earliest alert systems. In those days, a siren would sound and a red light would flash until someone—usually a nearby resident—would call and report the alarm. The SCADA system improved the quality and timeliness of alerts by sending data about pump activity to a central dispatch station, but city planners still had no way to analyze most of the data the system collected. The new system allows any city official with access to the Web site to view recent alerts, such as pumps experiencing mechanical failures, sanitary sewage tanks getting too full or city streets approaching freezing temperatures. They also can view trend

Wireless Technology Keeps the City of Richmond Above Water

information, including how hard each pump is working, how often it has failed in the past and how its load or activity changes after a downpour drenches the city or a new parking lot is paved in an area.

The Wireless Connection

The WebFOCUS system quickly demonstrated that it could make sense of the data that the city collected. But Information Builders went well beyond the original scope of the project by advising city planners to make smart decisions about the future. Information Builders first raised the possibility of linking the data to handheld devices, such as Palm Pilots, so that managers could take the data with them or access it over wireless networks. That, in turn, led to the vision of any city official or public works service crew having comprehensive data about the city's public works system, whether they were sitting in council chambers during a budget meeting or in a truck responding to a midnight alert in the dead of winter.

Considering the dramatic increase in the quality and availability of information it delivered, the new system was relatively inexpensive. The new database reporting system required only six weeks of development. The Web site has been in production since the fall of 2000, and wireless capabilities were offered in early 2001. Wireless PDAs get the data off the Web site by using AvantGo®, a service that converts Web data into simple forms that can be easily displayed on the small screens of PDAs.

The WebFOCUS solution has opened the city's eyes to the potential of a system that can deliver detailed information on all public facilities, using open networks and Web standards. The city, which has won national and international awards for its beautiful boulevards, parks and neighborhoods, wants to combine an intelligent database with an inventory of trees on city property. The city plans to implement this database with Information Builders' WebFOCUS.

Built for the Future

The city acquired a system that lends itself to future development because of its adherence to open standards and use of widely available hardware. Because the data is available on the Web, and the only client software required is a Web browser, city departments can access data in a number of ways. They can choose desktop or PDA, wired or wireless.

For more information, contact Edward Hung at EHung@city.richmond.bc.ca.

Private Sector

Automating the Mobile Worker: Applying Mobile and Wireless Technologies

Automating the Mobile Worker: Applying Mobile and Wireless Technologies

By Anthony Meadow

President

Bear River Associates, Inc.

Oakland, California

The Gartner Group recently estimated that there are 35 million mobile workers in the United States. Many of them work in the public sector. Mobile workers are the last people in this country to be computerized, because the technology was not available until recently. In the last five years, mobile and wireless technologies have developed to the level where they are both practical to use and reasonable in cost and are now capable of generating significant benefits to the public sector in particular. This case study examines some of the challenges and benefits of applying these technologies to government agencies.

Mobile and wireless technologies are distinct, and their benefits are different. Mobile computers are handheld computers that today might run the Palm OS, Windows CE, Symbian or some other operating system. More recently, there are Slate computers running Windows that can be used by mobile workers. Laptop computers are movable, but not really mobile. They are difficult to use while standing or moving, especially since they require the user to type on a keyboard. Mobile computers are especially useful when information is needed in the field.

Wireless technology comes in several flavors: wide area networks (including service providers such as Cingular, CDPD, Qualcomm, Metricom, etc.), local area networks (such as 802.11) and personal area networks (Bluetooth). Wireless communication is especially useful when the timeliness of information is important or critical (as in public safety).

Today, mobile computing is of great value in automating many processes that are fundamental to the missions of many government agencies, especially those that involve inspections. Inspections of construction projects, trucks, ships, locomotives, cars, hospitals, laboratories, nursing homes and child care facilities, as well as much of the work performed by police officers, parole agents, social workers and healthcare professionals can be computerized with today's mobile computers.

Mobile computers used alone have some value to an individual, but they are considerably more valuable to an organization when integrated into an enterprise mobile information system (EMS). Such an information system includes mobile computers, middleware, databases and desktop-accessible applications (Web-hosted applications in some cases). Generally, an EMS is integrated with other information systems and databases.

Before looking at some of the challenges and benefits of mobile computing, let's look at two examples of EMS that are in use today: the first used to track the progress of construction projects, the other used to automate parole agents.

Automating the Mobile Worker: Applying Mobile and Wireless Technologies

ePeg Construction Diary

This EMS is used to track the progress of construction projects on a day-by-day basis. The information collected includes which employees of which contractor did how many hours of work in what capacity with what equipment and what materials on which task of which project. This information has traditionally been collected on forms known as "Daily Construction Diaries," and a large project may generate tens of thousands of them. This set of forms is the only detailed record of all work performed on a project from the owner's perspective. This information is used to pay vendors and to provide the financial status of projects.

Caltrans has been using ePeg since 1996, when its first installation was funded by the Federal Highway Administration (FHWA). It has been used on many projects at Caltrans where there are almost 400 users. Caltrans has found that diaries are now more complete and more detailed. Project managers have all of the diary information at their fingertips and are better able to manage their projects on a day-by-day basis. Project information can be shared throughout the organization as required. A significant financial benefit is that there are remarkably few claims filed against Caltrans on projects where ePeg has been used. Project managers are able to quickly resolve issues that might otherwise enter into a legal process, and these issues are resolved at a lower cost than would otherwise be the case.

Mobile Fieldbook

The Mobile Fieldbook is an EMS used to automate parole agents of the California Youth Authority. Most parole agents' use a three-ring binder filled with several inches of forms. Almost all of the information in the binder is not available to anyone but the parole agent. The Mobile Fieldbook means that a parole agent enters his/her information into a mobile computer. When synchronized with the central database, the information can be viewed by the supervising parole agent.

Benefits of Enterprise Mobile Computing

Mobile computers are on an adoption path similar to what personal computers went through. Initially, individual users benefit from improvements in their personal productivity. In many cases, the computers are purchased by individuals with personal funds. The next stage is when work groups begin to adopt the technology, purchasing the computers and assigning them to workers in the group. The benefits from using this technology increase considerably, because the group is able to share information with considerably greater ease than before. The boundaries that separate workers in time and space are diminished. The next stage occurs when the organization as a whole makes a commitment to the technology, involving the IT department with the new technology. The organization benefits further as information can now be shared across all parts of the organization. Processes that involve multiple parts of the organization can be integrated and simplified. In this way, mobile computers are bringing about significant changes to organizations, just as personal computers did over the previous two decades. The changes brought by mobile technology will have a very significant impact on government agencies.

The benefits of mobile computing increase dramatically in proportion to the level in the organization that they are connected. Some benefits are readily quantifiable and should be examined in detail when preparing a financial justification for a new EMS. Other benefits may be harder to quantify, but these should also be examined. In some cases there may be benefits that, while non-quantifiable, significantly enhance one or more of the agency's capabilities.

Here are some examples of benefits that we've seen over the last five years with a variety of enterprise mobile solutions in use in both the public and private sectors:

- Increased accountability (time, money, items)
- Improved ability to manage workers
- Reduction of cycle time in processes

Automating the Mobile Worker: Applying Mobile and Wireless Technologies

- Increased efficiency
- More complete inspection reports
- Increased consistency of reports
- Elimination or reduction of paper-based forms. In some cases, there is a significant ROI in eliminating the creation, production, and storage of the forms, and collection, transportation, data entry and storage of the completed forms.
- Elimination of data entry processes
- Increased morale. There's nothing like replacing a clipboard and form with the latest technology!
- Reduction in staff size (in some cases)
- Reduced employee turnover, since they're able to focus more on their jobs and less on the paperwork.

Challenges of Enterprise Mobile Computing

We have seen a variety of challenges arise when organizations have started using enterprise mobile solutions. Many of them are common to any new information system or information technology. Others are more commonly seen with EMS than with other information technologies. Each is listed with the lesson learned from the challenge.

- ***Re-examine the process being automated.*** When automating any process it is important to re-examine the functions and goals of the process. This is especially true when automating a process that has not previously been automated. Automating without examination can lead to information systems that codify the existing inefficiencies of paper-based processes.
- ***Mobile computing technology is still rapidly evolving.*** Expect that the mobile computers purchased today will be obsolete in three years. Develop the EMS so that the majority of the system is isolated from the mobile technology. Using middleware (COTS or custom developed) can help a great deal to enforce a logical separation between the mobile technology and the other components of the information system.
- ***Expect the first version of an EMS to generate a lot of change requests.*** People always have an easier time reacting to a concrete implementation of an information system than to an abstract description of one. Given that an EMS is often replacing a paper-based process, expect that your users will have a lot of complaints and suggestions for improvement. Plan ahead for this in your budget and schedule.
- ***Provide good support and training for EMS users.*** Changing a work process is not easy; people often resist change. It is especially important to provide good training and support for users in this situation. Provide refresher/review sessions for users within 30 to 90 days of their initial use of the EMS.
- ***Implementing and supporting an EMS requires a broader range of skills than other information systems.*** There are often more tools, technologies and platforms needed in an EMS than most information systems. Any new technology has a learning curve. Using outside resources to help with EMS projects until the skill sets have been transferred into your agency can sometimes reduce project schedules and budgets.
- ***Go for a phased approach, not a "big bang" project.*** There are always risks with any IT project. Manage your risks by using a phased approach. Get a basic EMS in operation and then add functionality. Separate features into "must have," "nice to have" and "future."
- ***Mobile computers, when integrated into an EMS, are often single-function devices.*** Some of the usual concerns about compatibility with desktop platforms are less relevant than with other information systems. Laptop and desktop computers are

Automating the Mobile Worker: Applying Mobile and Wireless Technologies

primarily used as general-purpose computers. Mobile computers in an EMS are often used to automate a single work process.

- ***Look after the privacy of users.*** Users don't want to use any information system that unnecessarily invades their privacy. Users have a right to know about the data that is collected by an information system, especially any information collected about their own behavior. Enterprise mobile systems, because they integrate mobile technology, can be invasive of privacy.
- ***Use a staging database to separate the EMS from other information systems***. Keeping information systems clearly separated can help reduce the overall fragility of the information ecosystem. Changes in one information system can ripple through other interconnected information systems. A good design principle is to use a clearly defined interface to separate information systems.

Conclusion

Mobile technology is readily usable in numerous governmental applications today. Since so many government workers are mobile workers, mobile and wireless technologies have great potential to improve the internal operations of agencies. Replacing forms, clipboard and filing cabinets with mobile computers, wireless communications and databases will finally enable changes that can bring about great improvements in effectiveness and efficiency.

For more information, contact Anthony Meadow at (510) 834 5300 or by e-mail at tmeadow@bearriver.com; or Dennis Dulay, California Youth Authority, at (916) 262-1382 or by e-mail at ddulay@cya.ca.gov; or Yader Bermudez, Caltrans, at (510) 286-5205 or by e-mail at yader_a_bermudez@dot.ca.gov.

Blackbird Technologies: Lessons Learned in Wireless Technology and Security

Blackbird Technologies: Lessons Learned in Wireless Technology and Security

By Roger Edmiston

Senior Consultant

Blackbird Technologies, Inc.

Blackbird Technologies is an information security professional services company based in Herndon, Virginia. With a diverse client base that includes commercial and government organizations, we have reviewed several implementations of wireless networking during recent security assessments and security design efforts. Although we are assisting a federal government client that will provide public access to their Web-based services over wireless phones in the future, the primary adoption of wireless technology we've seen lies in the arena of IEEE 802.11b wireless LANs. Our lessons learned from reviewing the security of these wireless implementations are described below.

Wireless LAN technology has several features that may help meet the requirements of a constantly evolving government IT infrastructure:

- Data rates up to 11Mbps
- Flexible and convenient local area infrastructure
- Long-range (radio line-of-sight) bridging for connectivity between sites
- Encryption and access control features
- A variety of products and vendors to choose from

Unfortunately, wireless LANs also have some inherent security risks that should not be ignored when planning and deploying such a network:

- Security features are not turned on by default—vendors want their products to work out of the box, and security is not necessarily a convenient feature.
- Radio Frequency (RF) is a broadcast medium, susceptible to interception. 802.11 wireless LANs operate in the 2.4 GHz frequency range using spread spectrum technologies. The spread spectrum implementation reduces interference, but since everyone knows the spreading sequence, little security is gained and interception is trivial.
- Unlike wired networks, it is difficult to limit availability of the wireless network to a defined area; the range of the network accessibility may extend beyond your perimeter of control. Without encryption and authentication, any nearby wireless network card can join a wireless network, either accidentally or intentionally.
- The Wired Equivalent Protocol (WEP), which can be used to encrypt communications between the access point (AP) and the client, suffers from some security flaws that can lead to a number of practical attacks. (See http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf)

Blackbird Technologies: Lessons Learned in Wireless Technology and Security

This does not mean that wireless LANs should not be used. However, security features should be enabled, and organizations should deploy wireless with a clear understanding of the risks. A recent security assessment Blackbird conducted for a government organization illustrates some of these risks.

This government organization had a fairly complex network connecting over 120 sites, utilizing a wide array of network technologies and supporting a diverse range of activities and services. Although the organization was mostly wired, we encountered a small portion of the network that was connected using IEEE 802.11b wireless LAN technology as part of a beta. With a quickly growing IT infrastructure, wireless LANs and bridging provided the organization easy connectivity without the cost of wired infrastructure, particularly for temporary sites and buildings in close proximity. Unfortunately, the system had been deployed without considering the security of the organization's network.

The organization did not enable WEP or access control features. Consequently, many nearby public areas provided access to their internal network to anyone with a laptop and a standard IEEE 802.11b wireless network card. As a result, network traffic—including passwords and other sensitive data—could be sniffed from the sessions of other wireless users. We demonstrated this with a wireless card and laptop from several public areas.

Security devices did not separate the wireless connectivity from more sensitive areas of the wired network, including areas they considered critical resources. This increased the risks associated with not enabling WEP.

In addition, none of the access points had an administrative password set—the configuration could be modified by anyone on the wired or wireless portions of the network. Like most out of the box installations, unnecessary services were running on the access points to support remote management, including http, telnet, and login.

Once the technology is understood, the organization's vulnerabilities seem apparent. The government organization wasn't aware of the risks they were accepting with the convenience of this technology, and they were preparing to deploy the same wireless configuration in other parts of their network. Because personal privacy of citizens was one of the most critical concerns to this organization, their IT staff immediately made the recommended modifications and planned to move ahead with manageable risks.

There are several things that can be done to help minimize the risk of IEEE 802.11b deployments. The following five recommendations should be considered when designing and deploying such a network.

1. ***Utilize access control***. Access points that implement WEP can also implement access control that requires all packets to be encrypted using a shared secret. If the AP discards all packets that are not encrypted, a casual eavesdropper would not be able to actively join the wireless network.
2. ***Utilize encryption.*** Many vendors provide 40-bit (the WEP standard) and 128-bit encryption (an extended version with 104-bit keys) for the RF links. Although there are flaws in WEP, it certainly takes a more resourceful attacker to compromise your network if the traffic is encrypted.
3. ***Harden the access points***. Standard principles of hardening network devices apply to the AP's—set strong administrative passwords, disable unnecessary services, and maintain the most recent firmware and software versions.
4. ***Separate the wireless access points from critical resources on the wired network using packet filtering or firewalls***. This follows the security principle of "security in depth"—a failure in security of the wireless LAN should not necessarily compromise the critical resources located on the wired network. This also enforces the security principle of "least privilege," which states that the wireless users and computers should have access only to the resources they require.

Blackbird Technologies: Lessons Learned in Wireless Technology and Security

5. ***Select the appropriate antenna and antenna location.*** The selection of the antenna and its placement help define the boundary of the wireless network (as does the power output). For wireless bridging between sites, typically highly directional antennas are used to narrow the RF transmission/reception path while extending the range. For wireless clients to access the network via access points, the coverage area should be defined and appropriate antennas and mounting locations selected to provide the necessary coverage, whether a building, campus, or city. Antennas should be installed in an appropriately secure location to help ensure availability. An understanding of RF and antenna installations is helpful when surveying for a wireless LAN deployment.

It is important for an organization to weigh the security risks versus its business requirements. Like most decisions regarding security, it is important to understand the technical and business risks of a solution in order to determine what security is appropriate and what risk level is acceptable. As IEEE 802.11b wireless networks have grown in popularity, we have been quite surprised by the vulnerabilities clients have introduced into their networks using wireless LANs, because the risks are poorly understood and security poorly implemented.

However, organizations that have considered and understand the risks of this emerging technology are finding wireless networks an important part of their network infrastructure.

For more information, contact Roger Edmiston, Senior Consultant, Blackbird Technologies, Inc., by e-mail at redmiston@blackbirdtech.com

DasNet Corporation Shares Wireless Technology Experiences

DasNet Corporation Shares Wireless Technology Experiences

By David Salley,
President & CEO
DasNet Corporation

Background

DasNet Corporation is a Network Systems Integration firm specializing in providing communication technology solutions and services to the federal sector, foreign governments and commercial local exchange carriers. Wireless solutions, consisting of satellite, microwave and wireless WAN/LAN platforms, are at the forefront of our service offerings for our international clients, particularly in the Middle East. This case study will provide insight into the market and government customers served, architectures and applications developed and instituted, and lessons and experiences obtained from the Middle Eastern market for U.S. and foreign governments only.

Government Clients

A listing of DasNet's international government clients consists of the following: Royal Saudi Air Force, Saudi Arabia; Royal Family of Saudi Arabia (Monarch Society); U.S. Military Training Mission to Saudi Arabia; U. S. Air Force, Coalition Forces Saudi Arabia; U.S. Air Force, ESC–ITSP Saudi Arabia; Defense Contracting Management Agency, Saudi Arabia; Foreign Military Sales (FMS) Contractors, Saudi Arabia; Saudi Telecom Company (State Monopolized Telecom), Saudi Arabia.

Wireless Topologies

Satellite

Establishing private communications between offices in different cities or on separate continents may appear unrealistic and cost prohibitive for most entities, which prefer to rely upon traditional commercial local exchange carriers (CLECs) venues. However, when CLEC services are commercially unobtainable, financially impracticable or security issues are relevant, private satellite systems have been found to satisfy our government clients' requirements. The systems we have installed within the region provide secure, private international services between the United States and Saudi Arabia. These systems form secure conduits for integrating voice, video, dedicated data, LANs, and video teleconferencing sub-networks across single platforms between end points.

Benefits

- Secure Platform
- Client Ownership
- Homogeneous Backbone
- Robust Architecture
- Reliable Transport Media(>/=10-7)
- Manageable Costs

DasNet Corporation Shares Wireless Technology Experiences

Problems

- Licensing Requirements
- Landing Rights
- Bandwidth Availability and Footprint Coverage
- Equipment Provisioning
- Facility Engineering
- Cost of Implementation, Lease and Maintenance

Microwave

As a microwave value added reseller (VAR), DasNet represents some of the industries most reliable microwave and wireless manufacturers. Selection as an original equipment manufacturer (OEM) VAR provides us with the opportunity to select from a variety of proven quality products and systems to suit the connectivity needs of our government clients or respond precisely to customer technical support issues.

Our government clients in Saudi Arabia have very few options to choose from given the limited services provided by STC, the only state-run telecom provider. Line-of-sight microwave systems, once implemented, provide a one time cost for equipment and installation, operate with a constant reliability of 99.995 percent and require very little maintenance. Conditions within the interior of the Kingdom of Saudi Arabia are excellent for microwave networks and serve as the core for many government and commercial architectures.

DasNet offers products and services to satisfy solutions requiring licensed or unlicensed microwave connectivity. Microwave systems requiring licensing by the Federal Communications Commission (FCC) consist of those fixed services operating within a specific frequency band, i.e. 15, 18, or 23 GHZ range. These systems are capable of extending LAN solutions (10, 20, 30, or 100MBS Ethernet) or providing facility interconnections (Single or Multiple T1/E1/STM1). The primary advantages of utilizing a licensed system over an unlicensed system revolve around minimized frequency interference with adjacent facilities, greater bandwidth or longer distances as outlined by path profile requirements.

Systems not requiring approval to operate by the FCC fall within the lower bandwidth region of 900MHZ, 2.4 or 5.8 GHZ. An assortment of technologies such as spread spectrum or frequency hopping are utilized to minimize interference and have been found to be very effective in saturated inner-city markets. These systems are normally utilized for short distances between 100 ft and 16 km and typically support standard Ethernet bandwidths between 1 and 11 MBS with an actual constant throughput of approximately 8 MBS.

Wireless WAN/LAN (WLAN)

DasNet Corporation supports a variety of new wireless products for the rapidly growing government and commercial wireless local area network (WLAN) market. Given the low cost, ease of installation and limited maintenance required, many network administrators have begun integrating WLAN cells with their wired infrastructures. Project managers have found WLANs to be an effective solution for interconnecting remote offices across town and multiple non-connected building LANs. They also serve as low cost exceptional solutions for local loop issues without the cost of expensive PSTN circuits or the installation charges for dedicated wired connections.

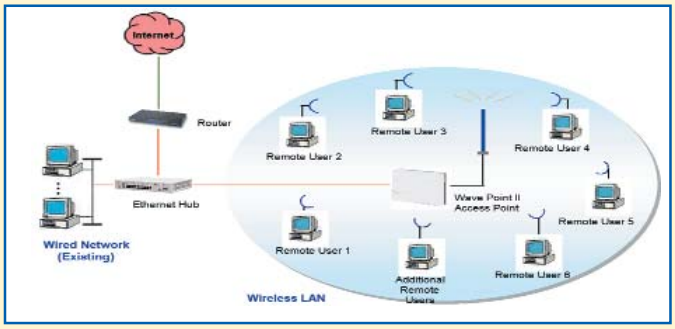
A wireless network can be as simple as connecting two PCs together to allow file and printer sharing using a peer-to-peer configuration or as elaborate as a multiple cell, multi-point wireless mesh integrated into one or more disparate WAN, MAN, LAN or Internet infrastructures. Obstacles encountered are normally created by line-of-sight obstructions or excessive distance requirements.

A wireless LAN solution makes it possible to interconnect a single remote wireless workstation or an entire local area network (wired or wireless), located a maximum distance of 16 kilometers away, to the nearest available access point. The primary stipulation is the necessity of line-of-sight between those two points. WLAN solutions provide network management administration and monitoring, Ethernet data transmissions up to 11MB, multi-cell configuration and domain separation, and unauthorized protection through

DasNet Corporation Shares Wireless Technology Experiences

Direct Sequence Spread Spectrum, Network Access Coding, and Optional Data Encryption.

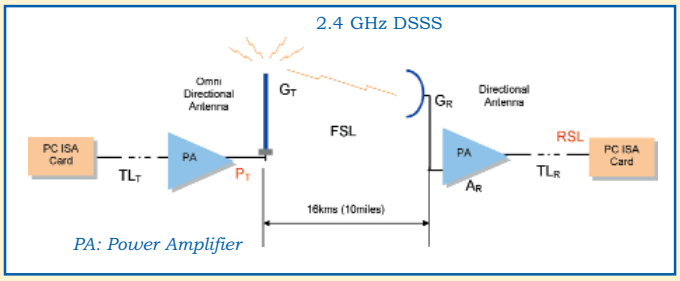
Most WLAN configurations are quite simple. However, to ensure that our clients are able to optimize each link for the greatest throughput possible, we perform an in-depth site survey and engineering analysis for all of the specified access and remote points.

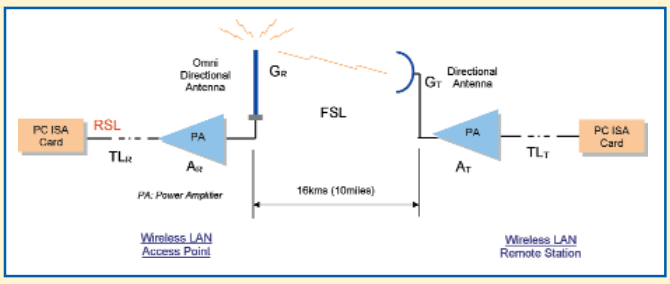


Sample network configurations have been provided for:

a: Point-to-Point WLAN and **b: Point-to-Multi-Point**

Wireless Access Point to Remote Station (Multi-Point)





Remote Station to Wireless Access Point

Abbreviations:

TL_T	= Transmitter Transmission Line Loss, dB
A_T	= Transmit Amplifier Gain, dB
P_T	= Transmitter Power Level, dBm
G_T	= Transmit Antenna Gain, dB
FSL	= Free-Space Loss, dB
G_R	= Receive Antenna Gain, dB
A_R	= Receive Ampifier Gain, dB
TL_R	= Receive Transmission Line Loss, dB
RSL	= Receive Signal Level, dBm
R_{THRESH}	= Receiver Sensitivity, dBm
FM	= Fade Margin, dB

Using our product specification sheet, the RSL may be calculated as follows:

RSL(dBm) = PT(dBm) +GT(dB) – FSL(dB) + GR(dB) + AR(dB) – TLR(dB)

where:
FSL(dB) = 20log f(MHz) + 20log D(mi) + 36.58
FSL(dB) = 20log (2400) + 20log(10) + 36.58
FSL(dB) = 124.18

RSL(dBm) = 30.00dBm +15.00dB – 124.18 + 19.00dB + 20.00dB – 6.00dB
RSL(dBm) = -46.18

The receiver sensitivity of the PC-ISA Card is –90.00dBm for maximum data rate. Fade margin (FM) is the allowable signal degradation in dB before a radio link system starts to experience service interruption. A fade margin of 30.00dB (99.999 percent one-way reliability) has been widely accepted. Fade margin is calculated as:

FM(dB) = RSL(dBm) – RTHRESH(dBm)
FM(dB) = -46.18dBm – (-90.00dBm)
FM(dB) = 43.82

A fade margin of 43.82 results in a one-way reliability of 99.9999 percent.

For more information, contact Fred Miltenberger, Director of Business Development, by e-mail at fred.miltenberger@dasnetcorp.com or David Salley, President & CEO of DasNet Corporation, by e-mail at dave.salley@dasnetcorp.com.

Military Sealift Command Uses Wireless Technology

Military Sealift Command Uses Wireless Technology

By Sybase, Inc.

Business Challenge

Create a fast, flexible, easy-to-learn, portable application to replace Military Sealift Command's (MSC's) traditional paper-based system, allowing MSC to improve its readiness to support and re-supply Navy ships at sea around the world.

Solution

A Palm-based solution created by Sybase Professional Services and powered by Sybase SQL Anywhere® Studio that enhanced an existing MSC application called Snapshot®, which was developed by Seaworthy Systems.

Results

- The Sybase developed and powered Palm-based Snapshot application is expected to reduce the man-hours required for inspections by as much as 50 percent, collect more data, enable the synchronization of data between ships and the MSC operations center and reduce data latency from as much as one year to 48 hours.
- Snapshot has met or exceeded all of MSC's initial criteria for functionality, flexibility, reliability and ease-of-use, enabling it to manage its inspections more effectively.
- Sybase Professional Services' mobile computing expertise kept application development time to a mere four months.

Long before "supply chain" became a hot technology topic, it was old news to the military. For thousands of years, military leaders have known that if you can't get the right supplies to the right people at the right time, you're not going to accomplish your mission.

In today's complex geopolitical world, this is truer than ever. The mission of Military Sealift Command is to provide ocean transportation of equipment, fuel, supplies and ammunition to sustain U.S. forces worldwide during peacetime and war. MSC deploys about 120 ships that are operated within the Department of the Navy by civilian mariners. The ships include tankers, ammo carriers, hospital ships and equipment movers ready to support military and humanitarian support missions around the world.

To ensure the readiness of these ships, MSC conducts regular inspections. Traditionally, these inspections have involved MSC inspectors walking, climbing and crawling around the ships, through engine spaces and other tight quarters, documenting the safety and maintenance needs of the ships on numerous checklists. The checklists were contained in multiple large binders they had to carry with them. Then they had to manually re-enter their findings into laptop systems they also had to carry onboard with them.

Military Sealift Command Uses Wireless Technology

MSC kissed its paper process goodbye, thanks to a SQL Anywhere-powered handheld application called Snapshot. MSC inspectors no longer carry large binders around the ship and have eliminated the time-consuming, error-prone process of manually entering their findings into MSC's computer systems.

"Our goals for this project," explains Mark Andress, Project Manager for the Snapshot application, "were to migrate from a paper-based inspection system to a PDA-based system and to improve the efficiency and consistency of inspection data collection. We also wanted to make inspection results readily available to interested parties in an electronic format and reduce costs by eliminating the need to issue notebook computers to all inspectors."

"My clients are on ships that have intermittent connectivity. I needed a hands-off solution that would allow for remote operations and would support multiple platforms including handhelds. SQL Anywhere Studio, with its Ultralite deployment option met these requirements " said Bill Merkle, Shipboard Systems Engineer, Military Sealift Command.

For more information, visit Sybase, Inc., at http://www.sybase.com

Mobile Workforce: Data and Messaging Unlimited

Mobile Workforce: Data and Messaging Unlimited

By Kristin Watt

Product Marketing Manager

Government Services

TeleCommunication Systems

Problem
Government consists of many agencies deploying mobile personnel to conduct inspections and collect information. While away from the office, productivity can be dramatically increased with the ability to remotely retrieve and update information contained in databases or documents at the "home office." Further, system or human activated message alerts and two-way text messaging using Short Message Service (SMS) can provide real-time triggers to initiate a more in-depth information exchange.

At best, these mobile workers are tethered to a laptop computer dependent upon a telephone line or data port to exchange information needed in the course of their duties. Worst case, they are forced to gather information on paper, then transfer it into a computer system when they return to the office. Efficiency could be greatly increased with wireless access to information using a laptop, handheld PDA (Personal Digital Assistant) or other such device.

Solution
Equip the mobile work force with the device that makes sense for the objective of their particular job. Provide wireless remote access to mission critical enterprise data, and initiate immediate message alerts to cell phones or pagers advising key personnel to retrieve or update information or complete required tasking.

Cases in point
In discussions with the U.S. Customs Service, the U.S. State Department and the Defense Information Systems Agency (DISA), TeleCommunication Systems, Inc. (NASDAQ: TSYS) found an overwhelming acceptance that access to enterprise data using wireless devices can greatly increase the productivity of field agents. We also found that while government procurement strategies take advantage of commercial-off-the-shelf (COTS) solutions where possible, disparate operations run by the various government agencies dictate that a wireless solution must be tailored at some level to meet the unique requirements of each agency.

There are several reasons for this, a few of which revolve around the nature of a wireless application. Any application residing on a PDA such as a Palm™, HP Jornada™ or Compaq iPaq™ consists of very lean programming code due to the limited storage available on the devices. By the same token, any data retrieved from a database or sent back to a database must be concise. Invariably, different divisions within an agency or different grades of field agents have different datasets for which they are responsible for retrieval and population, as suggested by the U.S. Customs Service. While it would be ideal if all data was available, again, due to the limited memory available, this may not be possible and slightly different variations of the application must be developed. This is not difficult, but it must be managed properly.

Another compelling reason for a less-than-COTS solution is due to the various levels of security required of an application. For some agencies, a Secure Sockets Layer is adequate, while others are concerned about the possibility of data leakage via the IR port on the

Mobile Workforce: Data and Messaging Unlimited

devices. For each application, the level of security must be evaluated and implemented as requested. Personal privacy issues as well as classification issues must be considered when choosing a security strategy, as well as the form of wireless transmission being deployed. For instance, when using CDPD access (through wireless carrier towers), 128-bit Elliptical Curve Cryptography is used. A Virtual Private Network is a very strong method for secure transmission in that it not only encrypts the data outbound, but also encrypts the network addresses associated with the system. In our experience, each client has demonstrated a different need for security and therefore has requested a slightly different solution.

Applications

1. In discussions with U.S. Customs field agents, we discovered they are currently testing several different PDAs to meet their wireless needs. They anticipate using PDAs to reach back to criminal information databases for suspect descriptions, photos and other information used to identify known criminals. They envision using the device to display a photo, receive up-to-date location information (for example, a plane carrying a suspect has a last minute gate change) and file reports about encounters and arrests. Immediate SMS message notification of newly available information is critical to mission success. An area of concern for the group was the reliability of wireless coverage in an airport or in areas in which they are several feet below ground. Solutions include implementation of a wireless Local Area Network (WLAN) within that particular location.
2. Meetings with DISA focused on the use of PDAs for retrieving and filing task orders and trouble reports. A mobile technician would receive an SMS message notification of a new trouble ticket from a help desk and would be dispatched from one location to another without need for a phone call or return trip to headquarters. Parts required to complete the task are compared to on-board inventory for distribution prior to arrival at the location. Ordering parts from on-site is an additional way of improving the speed of repair. By wirelessly connecting to the field service or manufacturing control system database, information shared in both directions insures instantaneous service order and parts status and eliminates the need for duplicate data entry when the technician returns.
3. Finally, Telecommunications Systems has developed a product to assist government healthcare facilities and health plans dramatically reduce annual drug costs while improving physician, nurse and pharmacist workflow. The TCS Medication Order Management System‰ provides a robust drug information database for reference. Most importantly, at the time the physician prepares an inpatient medication order, the order is compared to the approved hospital formulary, and potential patient drug interactions are displayed as alerts. With a wireless transfer to the hospital information system, the patient record is updated, and the pharmacy receives a legible, accurate order for medications that takes advantage of the best-cost alternative. Nurses no longer have to re-enter hand written medication orders into a desktop system and are freed for much needed patient bedside care. An outpatient variation of the system compares health plan formulary and delivers a wireless prescription directly to the retail pharmacy. In both cases, SMS messaging to the physician is triggered for exceptions or questions on patient medication.

In conclusion, it has been the experience of TeleCommunication Systems that the government has much to gain from the use of wireless technology. The costs of implementation are clearly offset by the improvement in productivity of workers and the ability to get the right information in the hands of the right people at any time. While there are some significant security concerns, the multitude of security solutions ensures that most requirements can be met effectively.

For more information, contact Kristin Watt, Marketing Coordinator, TeleCommunication Systems, by e-mail at WattK@telecomsys.com.

What's Driving the Future of Wireless Technologies in Government?

What's Driving the Future of Wireless Technologies in Government?

By Enterasys Networks™

In recent years, the popularity of wireless networking products has grown rapidly, not only in commercial enterprise environments, but also in education and federal, state and local government organizations. In fact, regardless of the industry, wireless provides on-the-fly connectivity to an organization's computing resources or the Internet—in temporary offices, conference rooms, classrooms, historic buildings and more—without sacrificing performance. Wireless is becoming an innovative and affordable way to supplement rather than replace wired networks. And this connectivity can be achieved without complicated wiring, while still maintaining total security.

Governments and their constituencies are becoming increasingly reliant on data systems, as officials, employees and citizens demand efficient and effective delivery of information. Key to ensuring efficiency and effectiveness are three critical elements of information delivery: security, availability and mobility—all of which have been recognized as vital components of both wired and wireless networking. In addition, the pace of transactions is on the rise, and the geographical reach of governments' services will expand as the constituency grows—across the Nation and around the globe for some agencies.

Increasing Productivity, Improving Efficiency

A recent study by the Wireless LAN Association (WLANA) revealed that wireless networks are consistently delivering better productivity and efficiency.[1] So what does this mean for the future of this technology and its functionality? One thing's for sure; it won't be a boring ride. Here are some factors to consider along the way:

- ***Higher Bandwidth.*** As the analog modem and the RJ45 Ethernet port have already proven, once a medium becomes popular, higher-speed versions of that medium will remain in demand. Wireless will be a particularly interesting test of this theory because the wireless interface is actually a complex radio system. And when it comes to higher bandwidth, there are multiple options and standards to choose from. To date, the Institute of Electrical and Electronics Engineers (IEEE) standards have proven most successful because they have quickly delivered affordable products to the market and have won over many influential supporters. At the same time, consortiums such as Bluetooth, with its proposed high-rate standard, and other competing standards like HyperLan2 are certain to have a significant impact as well.

  Unfortunately, unlike the RJ45 port, these radios can't just jump to a different frequency band or data rate. Vendors will be challenged in continuing the momentum of the technology despite the potential obsolescence of today's current products. Innovation and creativity will be required to protect customer investments.

What's Driving the Future of Wireless Technologies in Government?

- ***Scalability***. As customers looking for reduced cost of ownership become increasingly resistant to the planned obsolescence of any solution they choose, the ability to scale to higher bandwidths will become vital. True scalability in any wireless LAN solution will allow it to meet the needs of a specific network environment, then quickly be redeployed or easily upgraded to accommodate new users and applications, including emerging technologies such as voice-over-IP, video-to-desktop and distance learning. Wireless technology, after all, is used in organizations because of its flexibility. It must offer total mobility and availability.

  New IEEE 802.11a devices, for example, can provide performance of 54 Mbps. Wireless devices that are both IEEE 802.11a and 802.11b compliant devices can scale from 11 Mbps to 54 Mbps in the same platform, further protecting an organization's investment in equipment.

- ***Advanced Networking Services.*** Wireless LANs should be able to bring users the same features and functionality found in wired deployments. As a result, advanced networking services for wireless are on the way too. In fact, the IEEE 802.11 committee currently has study groups working on topics like Quality of Service (QoS). QoS will be especially crucial as more bandwidth-intensive and time-sensitive applications, such as video streaming, IP telephony and video teleconferencing begin to travel across more wireless networks. Soon e-mail over wireless will be old news, and video-enabled meetings over a network of flat touch-screens and hand-held PDAs will be the norm.

- ***Security***. In wired and wireless networks alike, meeting security requirements is a key challenge and calls for continuous technical development. Wireless security is particularly a challenge because the signal is so inherently available. It's in the air that surrounds us. The dilemma is that there is no such thing as an impenetrable lock or an "end-all, be-all" security technology, so we must scale (or layer) security to meet our needs. For example, at home a padlock secures a shed behind a house. In the shed, a lawn mower, bicycle, tools, etc. are stored. The owner is well aware that a simple hacksaw could cut the lock and breech the security of the shed. Despite the risk, the owner has decided that the value of the contents doesn't warrant an armed guard.

  Likewise, security technologies for networks must be appropriately layered to match the potential loss, and the strength of those layers must be maintained through active management. Network users must be authenticated. Information must be safeguarded with encryption. Intrusions must be detected and neutralized. Technologies such as RADIUS-based authentication, which verifies users before allowing them access to a network, Virtual Private Networking (VPN) technologies, which encapsulate and encrypt traffic, and intrusion detection software (IDS) for the network are an important start.

- ***User Personalized Networking.*** Today, the vast majority of networking equipment serves simply to switch and route data packets. Much of the equipment on the market generally has no ability to "know" (or care about) who is accessing the network or what activities are taking place on and across the network. New technologies and standards, such as the 802.1x/Extensible Authentication Protocol (for which Microsoft has recently announced support), user directories and policy services will enable a new generation of user-personalized network services.

  User-personalized networks will be a dramatic departure from the traditional paradigm of grouping users by workgroups or even virtual LANs. But the geographically dynamic nature of wireless LANs begs for the shift to user, or people-focused, networking. The specified services must follow the user,

What's Driving the Future of Wireless Technologies in Government?

whether they be QoS, bandwidth provisioning, access restrictions, a specific encryption requirement or whatever else the organization deems necessary to meet business goals and objectives. Ultimately, this people-focused approach to availability of services, combined with the mobility of wireless, will enable the vision of the mobile office of the future. Anytime. Anywhere.

So, How Is it Working?

In a recent Dataquest survey, 21 percent of respondents indicated that they have deployed wireless LANs in their network infrastructure. Of that 21 percent, two-thirds reported deploying wireless networks based on the IEEE 802.11b (commonly called Wi-Fi™) standard. Among those 802.11b networks, the level of deployment varied significantly, with fewer than 15 percent having deployed wireless at all of their locations and many deploying wireless at point locations in their networks.[2]

These numbers are impressive considering that wireless LANs have only recently benefited from the spotlight of the media and strong attention from enterprise-focused vendors. As network managers become more comfortable with the technology, new ideas for wireless applications continue to emerge.

Wireless Solutions Connect Government to the People

The Town of Enfield, Connecticut, deploys a wireless solution to connect several buildings to the town network—saving money, sharing resources and preserving a historic landmark. The local government uses the town network to deliver a wide range of services, including education, public safety and public works, tax assessment, planning and development, social services, attendance, payroll, insurance and Internet access.

Charlene S. Bond, Enfield's Director of Information Technology, was looking to connect a school wing, a branch library and an activity center to the town network—maximizing resource sharing while preserving building structure and appearance. It was important to Bond to keep upgrade costs down and data speed up. The new setup needed to offer data protection, fully support current demand and be scalable to keep up with new technology.

Bond was impressed by the cost savings, speed, convenience, security and flexibility of a wireless-to-LAN solution. Thanks to 11 Mbps bandwidth, Enfield users can access all their important applications, including e-mail and the .

Enfield's Pearl Street branch library is located in a "Carnegie Building" that was nominated for listing on the National Register of Historic Places in September 1999. After the library received a grant to become wired for Internet access and share computer resources, Bond decided to use wireless to connect to the LAN within the library. This preserved the building's historic design without the need to knock down walls, drill access holes or run unsightly wires.

In addition, wireless was used to connect the activity center to the town hall. "This latest enhancement increased the bandwidth from 56K Frame Relay with a committed information rate of 28.8K up to 11 Mbps and saved us approximately $3,000 per year in recurring costs," said Bond.

Wireless Ensures Efficient Disaster Recovery

In Salt Lake City, where preparation is underway for the 2002 Winter Olympics, a utility company crew working downtown in the early morning hours severed a fiber optic line. The accident left a third of the city's campus without access to its network, e-mail or the Internet. Complicating the issue was the fact that the disconnected area of the network included a high-volume print center that is not only responsible for the vast majority of the city's printing, but also prints employee paychecks, which were due in a matter of days.

The utility company estimated that the line could be fixed within ten days, but being without network access for this length of time would have severely impacted a number of city operations. Keith Barlow, the city's network administrator, got to work on an interim solution. He had been

What's Driving the Future of Wireless Technologies in Government?

researching wireless technology just prior to the accident, ironically because he wanted to be prepared in case of an emergency. Barlow thought wireless would the best option for quick and reliable connectivity.

Barlow knew that to restore communications in "down" locations using a wireless LAN, all he needed was line-of-sight access to another city building that had a working network. By late morning, access points had been delivered, and by early afternoon—just six hours after the accident—network operations in all sites were up and running again. A wireless LAN had enabled the city to meet disaster-recovery requirements without compromising security.

Pleased with the results, Barlow noted, "The wireless LAN proved to be an outstanding, cost-effective way to get data signals between line-of-sight buildings. It completely eliminated the expense of installing dedicated ISDN or T1 lines. In fact, we liked its performance so much that we're expanding this solution to more nodes and additional sites."

Building a High-Performance Wireless Network

The Public Buildings Service (PBS) of the U.S. General Services Administration is the largest real estate organization in the United States, maintaining more than 339 million square feet of workspace for more than a million federal employees in over 1,600 communities. In the Great Lakes Region, PBS offers workspace for federal employees in Minnesota, Wisconsin, Michigan, Illinois, Indiana and Ohio. The PBS Network Team provides IT support for all Public Buildings Service employees—nearly 1,200—in the region, who depend on the network for important day-to-day operations and national applications, in addition to communications such as e-mail and the Internet.

It was clear to Charles Pierce, Network Team Leader in GSA's Great Lakes Region, that providing a high-performance network infrastructure was critical to the success of the enterprise. At the same time, Pierce and his team were faced with the challenge of ensuring connectivity between buildings on each field office campus. In most cases, installing cable wasn't an option, so using leased lines, a costly alternative, was the only choice. That is, until Pierce had an opportunity to test a wireless solution.

"I admit to being very skeptical," Pierce says. "I mean, how could a wireless network, that depended on antennas and access points to provide connectivity, operate continuously in our windy midwestern weather? Yet, the end result has exceeded all my expectations."

The Public Buildings Service deployed their first wireless network to connect two of the three buildings that make up the Detroit field office. "Implementation was simple, literally plug-and-play." comments Pierce. "And since we've eliminated the monthly cost associated with two 56K leased lines, the network will literally pay for itself in no time."

Setting New Standards in Education Wireless Technology on Campus

Part of the University System of Georgia, Valdosta State University (VSU) strives to provide an educational environment that fosters special concern for individual student needs, while providing the best instruction at both the undergraduate and graduate levels. Valdosta's diverse and comprehensive curriculum includes the humanities, education, nursing, sciences, business and the arts. VSU's student body of more than 8,700 represents 48 states and 50 countries; 1,800 of these students live in on-campus residence halls. Small classes at all levels are taught by 500 highly qualified faculty members, and unique cultural, business and industry educational opportunities are available through performances, workshops, institutes and continuing education programs.

In order to be competitive with other colleges and universities—and with other student housing alternatives—Valdosta wanted to provide port-per-pillow, 24/ 7 connectivity that would enable students to access Internet resources outside the traditional hours of the university lab setting.

What's Driving the Future of Wireless Technologies in Government?

To meet this demand, Valdosta initially considered wiring the residence halls, but VSU decided against the disruption and time involved with wiring each residence hall room. The more than half million-dollar price tag that went with this type of installation was another deciding factor. In the end, VSU looked to wireless. "We didn't immediately jump on the wireless bandwagon," emphasizes Paul Worth, VSU's network coordinator. "We did look at other options because, frankly, we were skeptical that wireless would fit the bill. We knew we needed a solution that would interoperate seamlessly. It also needed to be convenient to install and efficient to operate.

"Of course, cost was a major driver," Worth continues. "A wireless network is actually a more cost-effective solution than a wired network since it brings connectivity only to those rooms in which students have a computer, currently about one third of the on-campus population. The cost of installing our wireless infrastructure was less than $50,000, compared to a much higher cost for the hard-wired alternative."

The response to the new wireless network at VSU has been so positive that plans are underway to expand wireless to cover public meeting areas like the library, cafeteria and building lobbies. In the long term, Worth envisions the wireless network expanding to classrooms and laboratories. "Our wired network extends to many of these areas already," Worth says, "but we see a real advantage in offering students the freedom to move around a classroom with a laptop, particularly in a lab setting."

Importantly, the University's new wireless network is an investment in the future, helping students succeed at the university and preparing them for life after VSU.

The Future of Wireless Networking

An interesting trend from the private sector is a new breed of service-oriented wireless companies that has emerged for the travel market, specifically focused on delivering wireless networking to business and leisure travelers. Skynet Global is outfitting airports and hotels throughout Australia and Eastern Asia with wireless LANs for travelers who subscribe to their services. They have also partnered with a similar provider in North America and have announced plans to expand globally in the future.

Dataquest believes that these new types of wireless applications will drive growth through the coming years, leading to a market penetration rate of 50 percent by the end of 2002.[3] A recent *London Sunday Times* article by Paul Durman suggests that these growth trends and the superior functionality of wireless LANs might even threaten the future of the much anticipated "3G," or third-generation, cellular networks.[4] Ironically, many telecommunications companies have already spent hundreds of millions of dollars to procure frequency licenses for 3G technology.

Regardless of the future availability of new technologies, however, it is evident that the wireless LAN—with its secure, scalable and seamless interoperability, high-performance operation, cost-effective ownership and complete availability and mobility—is here to stay. Simply put, wireless LANs have established themselves as a viable supplement, and sometimes an alternative, to wired networks.

For more information, contact Michaela Mezo, Business Development Specialist, State & Local Government, Enterasys, Inc., by e-mail at mmezo@enterasys.com.

Notes:

1. WLANA (Wireless LAN Association), "Wireless LAN ROI," www.wlana.org/learn/roi.htm
2. Joseph Byrne and Stan Bruederle, "End-User Analysis: Half of All Businesses to Deploy Wireless LANs by 2002," *Gartner Dataquest Report*, January 8, 2001, page 3.
3. Joseph Byrne and Stan Bruederle, "End-User Analysis: Half of All Businesses to Deploy Wireless LANs by 2002," *Gartner Dataquest Report*, January 8, 2001, page 4.
4. Paul Durman, "Nomura Says Technology 'Will Destroy Nokia,'" *The Sunday Times (London),* March 18, 2001.

Winning the Wireless Applications Race

Winning the Wireless Applications Race

By Michael Corcoran, Larry Reagan and Rebecca Umberger

Information Builders

The Message is Clear

Wireless communication has advanced rapidly in a short time as worldwide interest in the technology fuels rapid innovation. Increasingly, personal digital assistants (PDAs) and wireless handsets can connect to back-office, agency-wide and even corporate information systems. The power and finesse of these devices is making them look more and more like mini PCs. Many industry experts believe these mobile communicators represent not only the next generation of mobile phones, but also the next generation of the Internet.

The Yankee Group speculates that by the end of 2001, 25 million data subscribers on Internet-enabled wireless devices in the United States will generate $3 billion a year in subscription revenue to content providers. And that's just the start. Market research firm Ovum predicts that in 2005, about 484 million people worldwide will make wireless connections. Penetration is highest in Japan and many parts of Europe. There is a seemingly insatiable demand for new mobile Internet services in Scandinavia where most people over the age of 15 carry wireless phones. The wireless wave is sweeping over Japan like a tsunami, with more than 20,000 people signing up for Internet access through their phones each day.

Government users are no different. The U.S. Navy, for example, is using mobile devices onboard ships to reduce weight and keep their sailors connected. Several of the civilian agencies, such as the U.S. Department of Agriculture and the U.S. Department of the Treasury, are using, or considering using, wireless devices to perform remote inspection functions. Additionally, state and local governments have embraced the technology to provide remote connectivity to electrical and water systems.

The message is clear. Wireless communication is growing at a very rapid pace. The race to use these applications is just beginning. Governments and commercial users alike need to understand the impact of this technology and use it to their advantage.

Hesitation at the Starting Blocks

Of course, wireless communication isn't new. Since the first half of the 20th century, radio and television have delivered content into homes, tying populations and cultures together in new and exciting ways. As short wave and ham radios gained popularity, wireless communication became two-way, though mostly for hobbyists. It wasn't until the debut of cellular telephone networks in the 1980s and 1990s that personal wireless communication began to explode.

The military was one of the first users of personal wireless devices. As radio communications developed into mobile phones, often called “Bricks,” many of the military users were connected with a personalized phone number. Still, the communications networks were

Winning the Wireless Applications Race

not robust enough to provide users the support they needed.

As Local Area Networks and Wide Area Networks have grown and communications networks have matured, these technologies have converged into one system—both wired and wireless. Business users are the early adopters as it becomes more and more valuable to be able to send and receive e-mail, check inventory or communicate with corporate information systems from remote locations.

Despite all the enthusiasm about mobile networking, though, there remains a dearth of working applications. This gap between potential and reality is partly due to confusion about what is possible and also to conflicting standards for wireless information delivery. Particularly in the United States, there is a lack of standardization among device types, like phones and PDAs, as well as among the wireless networks and transmission services available from service providers. Confusion and the lack of standards have caused hesitation in this industry.

Running with the Message

Information Builders has pioneered technologies that insulate users from conflicting devices, standards and delivery networks, thereby reducing the confusion. Whether an organization has Palm Pilots, RIM devices, Pocket PCs or any combination of devices, the technology now exists to allow users to build cohesive mobile applications. Users can access current applications anywhere in the enterprise. Additionally, because users don't need to worry about standardization, they can concentrate on building applications that make sense.

A government agency was one of the first to step forward in using this cutting-edge technology. The City of Richmond in British Columbia, Canada, is using handheld devices to monitor its water and sewage systems. For the city of 180,000 people on an island, it's a critical application.

The City of Richmond is using wireless technologies to monitor and analyze field operations. Information Builders' technology summarizes and integrates the data across the city's database systems, putting real-time intelligence in the hands of anyone in the city, including users of wireless devices. By using WebFOCUS with AvantGo EnterpriseTM, customers such as the City of Richmond are able to download information from their government computer systems directly to their PDA devices for viewing and analysis away from the office. They also enjoy centralized administration and automatic reformatting of customized reports for delivery.

[For more information on the City of Richmond application, see the case study entitled Wireless Technology Keeps the City of Richmond, British Columbia, Above Water.]

The Next Race: Two-Way E-mail Reporting

Information Builders integrated typical e-mail protocols with its enterprise reporting system. This unique software technology, called WebFOCUS Two-Way E-mail, enables communication between people and information systems, automatically exchanging messages among dissimilar devices and networks. Based on any standard e-mail system, organizations can now provide cost-effective, reliable and secure access to existing information sources through any handheld device without having to build custom interfaces. Government agencies will not only "push" critical information to managers, employees, partners, customers, constituents and lawmakers. Now they can "pull" information from enterprise systems via e-mail using preformatted requests that respect all security systems.

For example, a scheduled message might be sent to military commanders each morning that sums up the previous day's activities. This message would be sent using the commander's e-mail system and could include additional reports or actions to be started at the commander's request. If the daily message showed one area within the commander's authority that was performing below expectations, the commander could request additional reports that show trends. Additionally, the commander could request that a report be sent to another person

Winning the Wireless Applications Race

in the organization, such as a budget analyst, for further analysis.

As another example, item managers could be sent an alert when a particular inventory item is out of stock or at a critical threshold level. The alert could be triggered by a pre-defined database event, such as when a certain threshold is reached in the inventory system. This alert could be sent to the item manager via his/her e-mail system and offer several alternative actions. The item manager could respond by asking the system to redirect inventory from another warehouse, redirecting inventory enroute or starting the purchase order process to replace the inventory.

Race Hurdles: Content and Volume

Rich content is what makes wireless data services valuable, and much of the same material that makes the Web popular is already available to mobile communicators. In a growing number of locations, doctors can get immediate access to patients' lab results on their cell phones—days earlier than they did before. And many leading brokerage firms are giving their customers the ability to make stock trades online from wireless devices.

To casual users, this type of mobility is enviable. But to people who follow the wireless industry, it's just the start. Many industry watchers believe wireless data transmission will mushroom in the next three to four years as mobile networks migrate to third-generation (3G) communication standards capable of moving wireless data at broadband speeds. When the 3G mobile Internet devices do make the scene, they may not even be perceived as phones but as mobile communicators or mobile terminals. Voice conversations will be just one of their many capabilities. Eventually they may replace cell phones altogether, allowing users to access a movable feast of personal services—anytime, anywhere.

Relay Handoffs: Getting in Sync

In many cases, the solution involves regular synchronization with a PC or server. For example, field personnel who want to update the agency database with new information gathered while at a remote site can set up simple procedures that exchange the data automatically when they return to the office, rather than sending wireless updates after each call. Each time they connect mobile devices to the network, they will upload pertinent data from the field and also automatically gather information about new tasks that have come in during an absence.

Information Builders has extended these synchronization capabilities to specific databases and reports to make them even more useful. RIM wireless devices, for example, allow synchronization to occur whenever field personnel are within the range of a wireless signal, so they do not have to come into the office at all. For many government workers in rural areas, this capability is significant if they are to use wireless applications.

Synchronization works because not every communication has to be immediate. For example, individuals performing field inspections could collect data on a handheld device and upload it into their applications every hour or at the end of their shift. In a more detailed inspection environment, they might compile site information while in their office, and then later gather detailed information on their PDA while visiting the specific site. Once back in the office, inspectors can then synchronize the data collected on the PDA with the data already compiled. This gives inspectors a complete up-to-the-minute status of the specific location. Synchronization technologies make this possible.

The lesson mobile users can learn is simple: Save the actual wireless transmissions for times when users really need data exchange in the field. Rely on synchronization with a PC or network server for bulk downloads or to gather additional information.

Running and Winning with Open Sources

Whatever wireless devices and architectures are chosen, government customers have plenty of options for quickly and cost effectively rolling out wireless applications.

Winning the Wireless Applications Race

Information Builders' wireless business intelligence technology is independent of devices or back-office systems and offers a comprehensive set of interfaces so users can tailor solutions to a wide range of people and needs. Whether they need data at the office or in the field, Information Builders maintains a high level of consistency in how users gather, aggregate and deliver information throughout the extended enterprise.

For more information, contact Larry Reagan, Director, Federal Systems Group, Information Builders at (703) 276-9006 ext. 2249 or by e-mail at Larry_Reagan@ibi.com or Rebecca Umberger, Federal Marketing Communications Manager, Information Builders at (703) 276-9006 ext. 2212 or by e-mail at Rebecca_Umberger@ibi.com.

Wireless Technology in Government: Business Objects Shares Lessons Learnt

Wireless Technology in Government: Business Objects Shares Lessons Learnt

By Business Objects

Lessons Learned From the Wireless Sector

Technology in the wireless sector changes rapidly. To be competitive in this field, wireless solutions providers need to be able to adapt quickly to this change. For example, until recently many organizations were focused on providing wireless information via mobile phones. It would now seem that technologies such as wireless application protocol (WAP) have not been able to meet market expectations.

Today, organizations are making a shift towards enterprise wide deployments of personal digital assistants (PDAs), such as those using the Palm, Pocket PC, or RIM operating systems, to get information to their mobile staff members. As PDA devices are able to access information in both an online mode (with a wireless telecommunications connection) or by synchronizing and downloading reports for offline viewing, they fully utilize both the mobile and wireless technologies. The computing power in the PDA devices also enables much greater functionality in terms of analysis and graphics.

With InfoView Mobile, Business Objects has implemented a solution that meets the requirements of all wireless standards. This experience suggests that wireless applications should be built with a substantial degree of flexibility to ensure that users are not locked into outdated technology. Business Objects has been able to move quickly in response to these changes by working with the best of breed partners in the wireless sector (AvantGo, Neomar, Nokia, Microsoft, IBM, etc.) and by keeping its underlying technology flexible.

Case Study: U.S. Army CECOM

The electronic commerce/paperless contracting office of the U.S. Army Communications-Electronics Command (CECOM) in Fort. Monmouth, New Jersey, uses the Business Objects' platform to produce executive reports and then makes these reports available to senior leadership via their Palm VIIx PDAs. These reports contain monthly summaries from the division's monitoring and analysis group. Prior to using Business Objects' InfoView Mobile, the leaders had to use hard copies of the reports. The new wireless capability has enabled senior leadership to obtain more timely access to these reports.

According to Matthew Meinert, IT manager with U.S. Army CECOM, Managers are able to access reports, and therefore answer questions 'live' during meetings and briefings. They can also look up information as discussions steer away from the material they had prepared for the particular meeting. "During a recent meeting on delinquency," says Meinert, " a question arose about cycle time. Our director had not brought his cycle time statistics, but luckily had his PDA with a cycle time report by division. He was able to answer the questions while other directors could not provide the information until they got back to their offices. So our leadership gets real time information. This has greatly improved the decision process time lines. We no longer have to

Wireless Technology in Government: Business Objects Shares Lessons Learnt

wait for mid-level managers to get data."

Meinert goes on, “Providing our leadership with timely, concise information is a core function of the U.S. Army CECOM Acquisition Electronic Initiatives Group. We have been rolling out PDAs to a pilot group to facilitate information sharing. We saw the opportunity to expand the PDA pilot and incorporate InfoView Mobile 4.0 into the mix. Leadership now has the ability to use PDAs with Business Objects’ executive reports and have instant access to the information. We hope to soon enable leadership to refresh reports while on travel or in a meeting and provide instant, real-time answers to critical business questions."

The Business Case for a Wireless Strategy

The widespread growth in enterprise PDA deployments, as mentioned earlier, has only recently come about due to the increase in the number of companies offering wireless business applications. Consumers have been using wireless devices for some time in order to access news, stock information, weather forecasts, etc. However, for organizations, true business applications have been limited.

With either a PDA or Internet enabled mobile phone, mobile workers can already access some of their standard business applications. E-mail, contact lists and calendar management are already well established as wireless applications, but these functions alone have not been sufficient to represent a business case for a wireless strategy. Now with applications such as InfoView Mobile, a strong case is emerging for wireless as organizations seek to make their employees more efficient, even when they are away from the office. It is common for organizations to purchase PDA devices for their employees., and it is also in their interest to make the most of these purchases. Business applications that leverage existing technologies and extend these to the mobile workforce are now in real demand, because they offer a clear return on investment.

It is hard for any organization to predict the future of wireless technology, so it is important to choose a vendor who has shown a strong commitment to wireless development. In this way, the investment in wireless applications will be assured, regardless of technology changes.

Off-the-Shelf or Customized Solutions

While InfoView Mobile can be applied immediately to extend the value of an organization’s Business Objects reports, Business Objects also recognizes the importance of working with strategic integrators and partners. Many organizations will choose to engage a consultant in order to devise the most valuable and far-reaching wireless strategy.

For more information, contact Business Objects at (408) 953-6000 or visit their website at http://www.businessobjects.com.

Wireless Glossary

3G An industry term used to describe the next generation of public wireless voice and data networks. To qualify as 3G, a network must meet certain requirements for speed, availability, reliability and other criteria set forth by the International Telecommunications Union. There are many 3G network technologies being developed, and they are generally packet-based, "always on" networks.

802.11 A family of wireless Local Area Network specifications. The 802.11b standard in particular is seeing widespread acceptance and deployment in corporate campuses, as well as at commercial facilities such as airports and coffee shops that want to offer wireless networking to their patrons.

Bandwidth The size of the network "pipe" or channel for communications in wired networks. In wireless networks, bandwidth is determined in part by the range of frequencies that can carry a signal, as well as the efficiency of the wireless network for supporting multiple "conversations" on any given frequency. Bandwidth is measured in Kbps or Mbps.

Bluetooth A short-range wireless specification that allows radio connections between devices within a ten meter range of each other. Bluetooth is designed as a Personal Area Network technology with a wide variety of theoretical uses though few products have been released that incorporate the technology.

Broadband Descriptive term for evolving digital technology that provides consumers a single switch facility offering integrated access to voice, high-speed data service, video demand services, and interactive delivery services.

CDMA Code Division Multiple Access. US carriers such as Sprint PCS and Verizon use CDMA technology to power their wireless networks. CDMA allows for multiple transmissions to be carried simultaneously on a single wireless channel. CDMA is a 2G wireless technology that is an alternative to GSM the standard in Europe and Asia.

CDPD Cellular Digital Packet Data. Allows telecommunications companies to transfer data over existing cellular networks to users. CDPD is currently a common choice for wireless data in the United States..

Cellular General name for analog and digital networks that divide large areas into smaller coverage areas called cells. As a user moves from cell to cell, his/her connection is theoretically handed off without interruption.

Circuit Switched A classification for networks where the device connects to the network only when placing or receiving a call, such as with a traditional phone line. Next generation wireless networks will use packet-based networks, which are "always on."

GPRS General Packet Radio Service. A 2.5G technology being implemented in GSM networks. It is a packet-based, "always on" technology with data transfer speeds of up to 114Kbps.

GSM Global Systems for Mobile Communications. A digital cellular or PCS standard for how data is coded and transferred through the wireless spectrum. It is the 2G wireless standard throughout the world—except in the United States. GSM is an alternative to CDMA.

Wireless Glossary

LMR A Land Mobile Radio system is typically characterized by one or more base stations, each providing coverage for several square miles, and numerous mobile radios that provide two-way voice and data connectivity. LMR systems operate in several frequency bands and use a wide range of technologies, some of them proprietary.

Packet A way of organizing data for transmission that breaks larger data streams up into smaller bundles that are then pieced back together by the recipient, based on header, text and trailer information in each packet. Packet based networks are typically "always on" and do not require the user to initiate a dial-in to connect to the server.

PCS Personal Communication Services. A general category for two-way digital networks with integrated voice, data and messaging capabilities.

PDA Personal Digital Assistant. A small computing device based on the Microsoft Pocket PC standard or Palm OS. Generally PDA means the same as "handheld," a term that is more frequently used as the devices have taken on a growing role in corporate computing. Typically available with embedded e-mail, calendaring, address book, tasks and memo applications. Third party and custom developed software can extend the functionality of the device.

SMS Short Messaging Service. A service through which users can send text based messages from one device to another. The message is limited to 160 characters. This is typically the delivery mechanism for “e-mail” to digital phones today. The e-mail is converted to an SMS message, truncated to 160 characters and delivered to the users handset.

WAP Wireless Application Protocol. A set of protocols that provide optimized access on digital wireless devices such as mobile phones. WAP is designed to work over existing wireless networks, including CDMA and GSM, and typically involves a WAP microbrowser on the device and a WAP gateway server at the carrier facility to connect to the Internet.

Wireless Spectrum A band of frequencies where wireless signals travel carrying voice and data information. Wireless spectrum is typically auctioned or assigned to carriers by each national government.

.