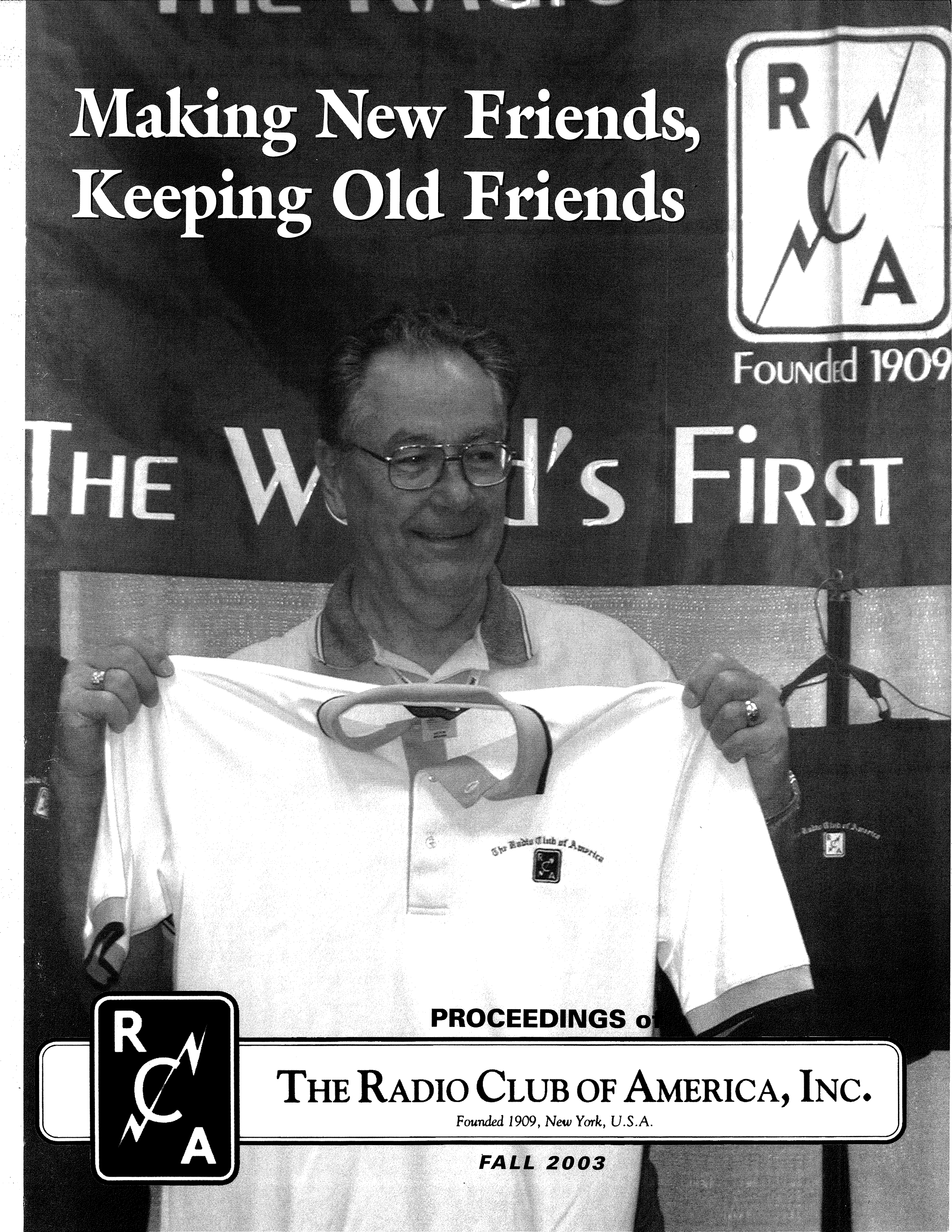
Making New Friends, Keeping Old Friends



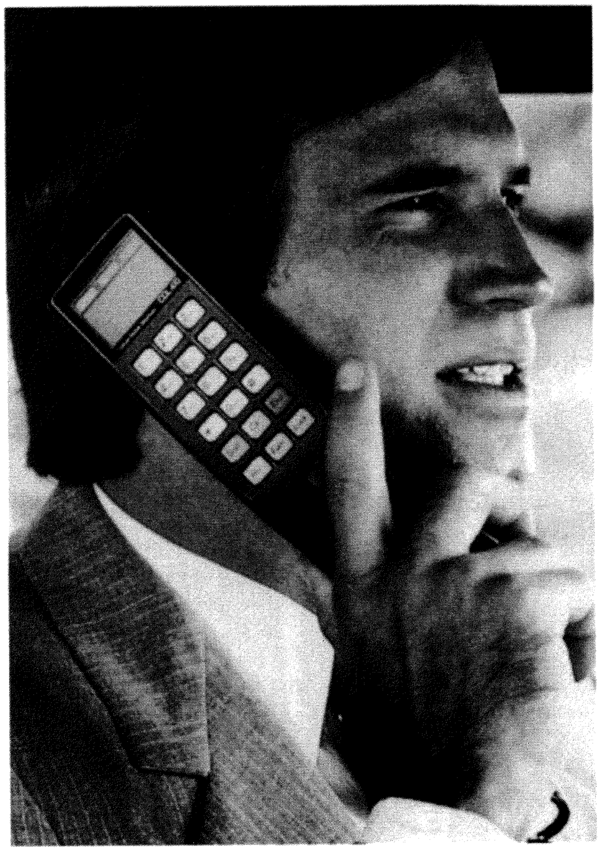
PROCEEDINGS o

THE RADIO CLUB OF AMERICA, INC.

Founded 1909, New York, U.S.A.

FALL 2003

mtol *A Company for the Future*



Experts in Design, Installation and Service of Landmobile Radio Systems

WHEN YOU THINK COMMUNICATIONS
– THINK SMART
– THINK mtol

718-767-7500
Fax: (718) 767-9858

TOM AMOSCATO
SYSTEMS CONSULTANT

AMTOL RADIO COMMUNICATIONS SYSTEMS, INC

150-47A-12th RD.
P.O. BOX 93
WHITESTONE, N.Y. 11357-0093

MANUFACTURERS' REPRESENTATIVE
SALES and SERVICE

718-767-7500
Fax: (718) 767-9858

MARTIN AMOSCATO
SYSTEMS CONSULTANT

AMTOL RADIO COMMUNICATIONS SYSTEMS, INC

150-47A-12th RD.
P.O. BOX 93
WHITESTONE, N.Y. 11357-0093

MANUFACTURERS' REPRESENTATIVE
SALES and SERVICE

mtol RADIO COMMUNICATIONS SYSTEMS, INC.
main office 150-47A 12th. road, p.o. box 93, whitestone, n.y. 11357 • 718-767-7500

355 Butler Street
Brooklyn, New York 11201
(718) 797-3770

448 Fifth Avenue
Pelham, New York 10803
(914) 738-1852

Volume 77, No. 2

FALL 2003

THE RADIO CLUB OF AMERICA, INC.

Founded 1909, New York, U.S.A.

Headquarters Office: 244 Broad Street, Red Bank NJ 07701
Tel. 732-842-5070; Fax 732-219-1938
E-mail: info@radio-club-of-america.org
Website: http//www.radio-club-of-america.org

CONTENTS

Editor: **Debra Wayne**
PBI Media, 4465 NW 97th Terrace, Sunrise, FL 33351
Tel: 954-741-4656; Fax: 954-741-4656; E-mail: beeper@mindspring.com

For Advertising Information Contact: **Karen Clark**
Tel: 303-979-0621; E-mail: kjclark33@yahoo.com

Designed by: **Shawn Warren**
Little Fish Creative, LLC

A Message From Mercy

I recently attended the 69th annual Associated Public-Safety Communications Officials International (APCO) conference and exhibition in Indianapolis. The Radio Club of America was on display in Booth 1909, and every time one of our members would come by and tell me what a miracle worker I was for having selected the booth number that corresponded with our club's birthday, I wanted to take credit. The truth? It was just a coincidence. It was no coincidence, however, that so many of the attendees at APCO noticed the correlation, because a large number of APCO members also belong to The Radio Club of America.

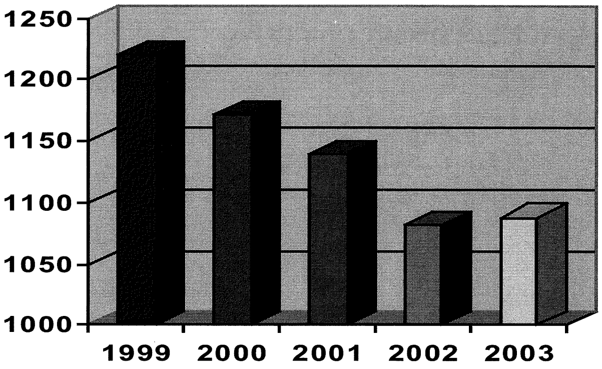
APCO and its members always have supported the Club in grand fashion, and this year was no different. More than 100 attendees were present at the Club's annual APCO breakfast. I would like to personally thank all of the members who were unable to stay for the breakfast because of a scheduling conflict, but who stopped by to see us for a few minutes. Included in this group were APCO President Vincent Stiles and Past President Joe Hanna.

The Radio Club booth was busy non-stop, but we met the challenge. We had wonderful support from members who helped us man the booth, including Jay Underdown and David Swan. President Emeritus Ray Trott and former director Don Bishop helped answer questions and recruit new members. David Byrum made it his personal goal to sign up new members. In addition, director Karen Clark and Diane Weidenbenner were on hand to promote the Club's newest venture: The Radio Club of America Store. You'll find embroidered RCA logo apparel; a black briefcase; and, of course, Club items like pins, books, etc. A special thanks to Pat Buller, a senior engineer with City of Tacoma Power, for being the store's first customer; and to Chuck Adams for placing the first online order!

The strong fraternal bond between The Radio Club of America and APCO is clear, and it's wonderful to see the two promoting each other. I, for one, am proud of my membership in both associations. Each of us should make it our personal goal to recruit qualified members from related associations. IEEE, NAB, CTIA, NENA, PCIA, ENTELEC and ARRL are a few that come to mind that are represented on the Club's membership roster. Wouldn't it be wonderful if we cultivated the same spirit of mutual respect, cooperation and industry support with those groups that we have with APCO?

I also would like to thank everyone who filled out our membership survey at the Radio Club booth; we will post the results on our Web site as soon as they have been tabulated. I can give you one statistic now: 95% of us joined The Radio Club of America for the opportunity to network, to associate with other professionals, and to have access to the expertise and experience of fellow members. I encourage you to reach out to your colleagues who have not yet joined, and to share with them the experiences you have had as a member.

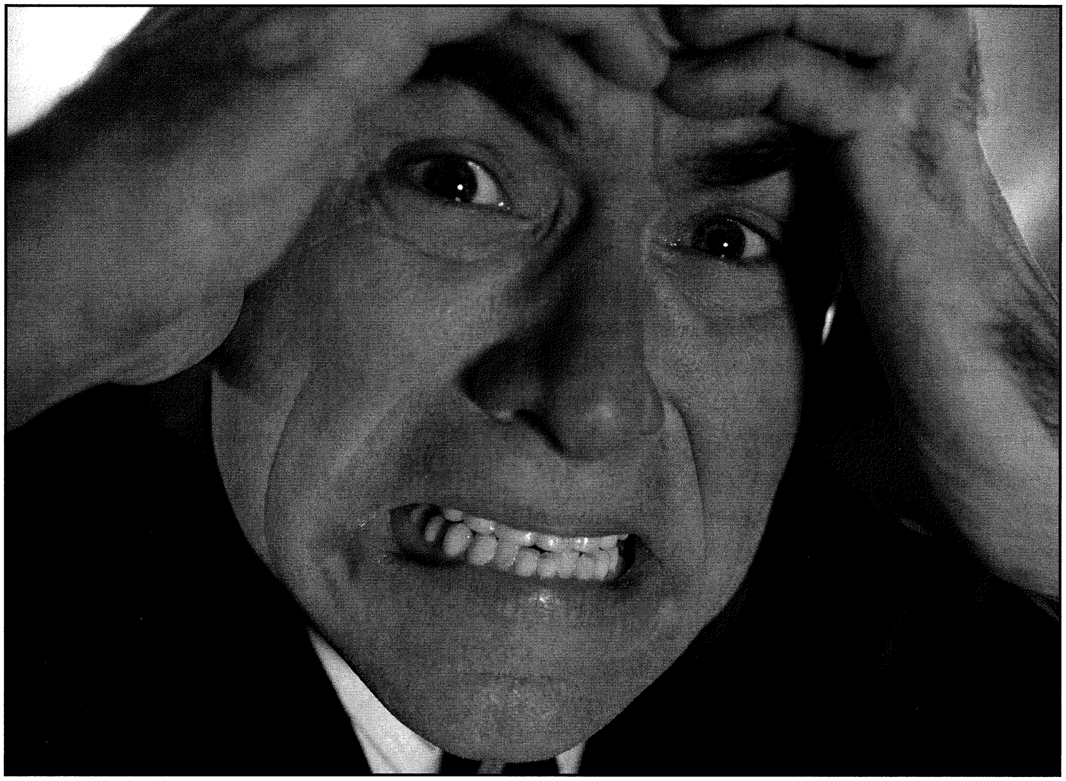
Radio Club Membership 1999–2003



As we get ready to begin a new year, I challenge all members to think about ways to promote the advantages of being a part of the Radio Club of America at every opportunity. Wear your membership pin whenever possible; it always draws attention, and it gives you an open door to talk about the Club. If you have the chance to address a high school or college group, a professional industry gathering or even in conversation with your colleagues and your vendors, talk about membership, the scholarship program and the networking opportunities. Working together, we can help ensure the future success of the Radio Club of America.

Mercy Contreras

Missing IWCE Didn't Sit Well With the Boss



Attend IWCE 2004 – the one-stop shop that you can't afford to miss.

2004 IWCE

The Wireless Marketplace

INFRASTRUCTURE • APPLICATIONS • SECURITY • SAFETY • INTELLIGENCE

Base Station Workshops: March 22-23 • Conference and Exhibits: March 24-26
Las Vegas Convention Center • Las Vegas, Nevada USA

Don't miss out on this year's exciting Keynote
Mark Bowden, author of "Black Hawk Down" speaks about communications issues during military operations

Interested in exhibiting?
Contact Renie Fuselier at 720-489-3137 or rfuselier@primediabusiness.com

Interested in attending?
Visit www.iwce-mrt.com or call us at 800-927-5007 or 203-358-3751

Managed and produced by:

PRIMEDIA
Business Exhibitions

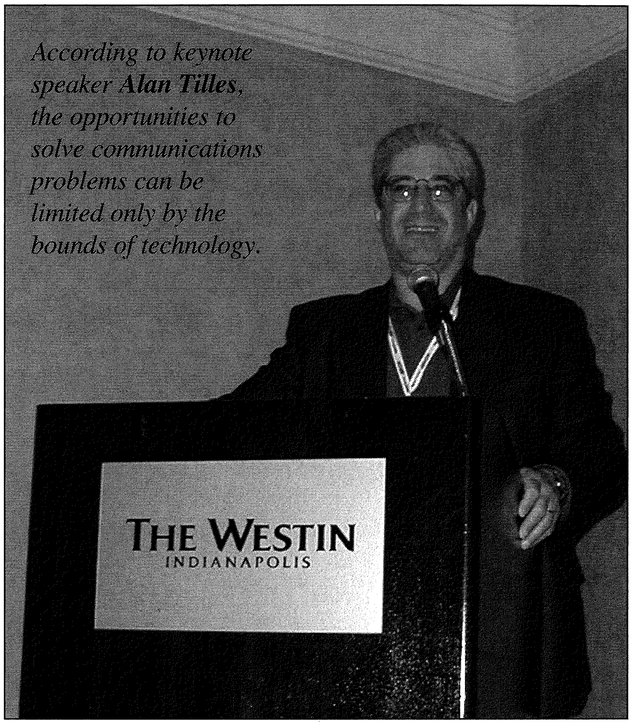
Sponsored by:

MRT
MOBILE RADIO TECHNOLOGY

North America's largest wireless communications conference and exhibition specifically geared towards:
Public Safety Professionals • Dealers • Technology End Users

Be Willing To Think Outside The Box

Speaking at the Radio Club of America Breakfast, held in conjunction with this year's meeting of the Association of Public-Safety Communications Officials International (APCO) in Indianapolis last August, attorney Alan Tilles had good news and bad news. In his breakfast address, Tilles told some 100 members and guests at the Westin Hotel to be mindful of regulatory cutbacks and a slowdown in new equipment releases, but he touted the upside of potential partnerships that carriers and users should explore in order to survive and thrive.



According to keynote speaker ***Alan Tilles****, the opportunities to solve communications problems can be limited only by the bounds of technology.*

I will start by talking a little about Nextel. Nextel has had an incredible impact on land mobile radio. Skipping the interference issues that we'll discuss later, Nextel's acquisition of many land mobile radio dealers has altered the chemistry of the industry. More importantly, Nextel has shifted a large part of the usual industry user to a different kind of service. This, in turn, has caused a significant reduction in the potential customer base for equipment manufacturers. Thus, today we have a land mobile industry that is shorter than usual on innovation. As you cruised the show floor, I doubt that you saw the kind of product advances that we've come to expect in past years, at least in the traditional land mobile product area.

Further evidence of the state of the industry is the number of FCC applications being filed. Numbers are significantly down for both public-safety and non-public-safety applications, to a third of what it used to be. The FCC's application processing division in Gettysburg, Pa., used to employ a significant number of outside contractors to help process Part 90 applications. The number of contractors has now dropped to six, and these six contractors will be eliminated from the FCC's work force at the end of September.

So be ready for application processing delays later this year. The reality of the land mobile market is coupled with government budgets that are tight for virtually every state. State and local governments no longer enjoy the surplus revenue that was flowing just a few years ago.

However, while times have changed, all is not bleak. Rather, for those who are willing to think outside of the box, there are many opportunities awaiting those who have unsatisfied communications needs.

Explore New Technologies

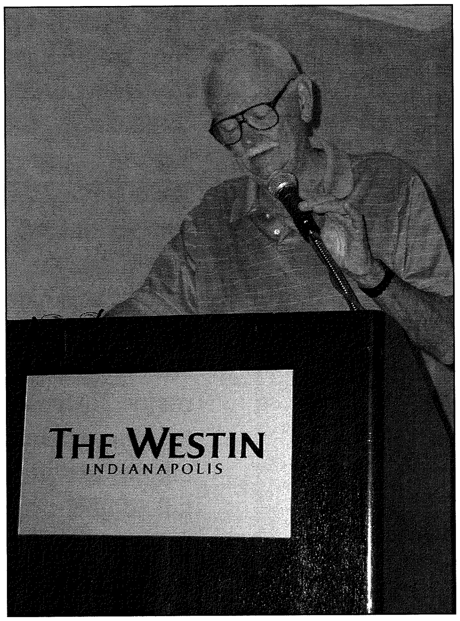
For example, wired as well as wireless advances in areas outside of land mobile are bringing opportunities to solve some of these needs. In particular, broadband technologies, from Wi-Fi to powerline communications, are exciting opportunities to resolve critical communications needs. Assuming we can solve the security problems inherent in these technologies, they serve to somewhat lessen the strain on traditional wireless capacity. In addition, Congress and the FCC are now more cognizant than ever of the need to make spectrum available for public safety agencies. Thus, what was once the largest problem facing public-safety agencies — the need for additional spectrum — may one day turn out to be public safety's biggest surplus.

So, while we might have resolved the capacity crunch, we still have a budgeting issue, and I'm not sure that will change anytime soon. It will become incumbent on public-safety agencies to seek creative means to fund their construction and operational activities as well as creating interoperability between various first responders.

For some public-safety agencies, this can mean a variety of types of partnerships between public-safety agencies and others. In the simplest example, police, fire and EMS services are combined into a single system that also is used for the municipality's utility communications needs. This system allows the construction of a larger, more feature-rich system by grouping users with similar needs onto a larger system. Many of you take advantage of this mode of operation now.

However, public-safety agencies should not stop strictly at the pure governmental model. Rather, creating the right system with the right set of features in an affordable system might require looking to more partnerships with private industry. Again, this can take a variety of forms.

I believe that most of us already are aware of partnerships between public-safety agencies and non-governmental utilities. These partnerships, like the public safety and municipal utility model, provide benefits of spreading the costs amongst more users. I believe that, ultimately, there should be more and more of this type of partnership. And, you heard the FCC say...they will continue to encourage it.



Master of Ceremonies Ray Trott tells breakfasting Radio Club members and guests in Indianapolis another in his vast repertoire of industry-related stories before introducing speaker Alan Tilles.

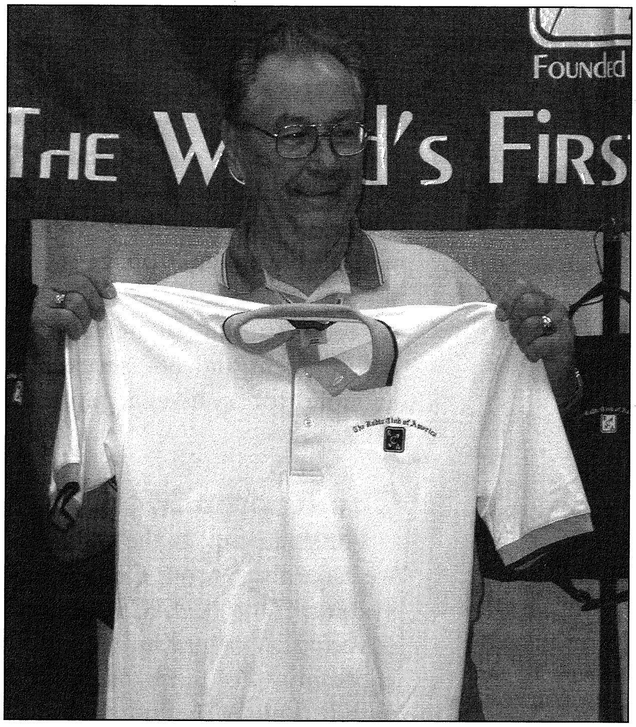
You should also be aware of the success of public-safety and commercial partnerships. Yes, I'm aware that numerous public-safety agencies have chosen to utilize Nextel or Southern Linc systems for their communications needs. However, I'm referring now to wireless systems that are tailored to the first-responder environment and not necessarily suitable for consumer applications.

The Racom Method

For example, in the Midwest, we have the Racom Corp., SMR system. This EDACS system, covering all or part of six states, is comprised of more than 10,000 mobile units. The users on the system consist primarily of traditional guns-and-hoses public-safety users and utilities — about 80 percent of the total users on the system. The Racom system represents the Holy Grail of interoperability, in that all public-safety and utility users on the system may coordinate their efforts with other agencies. Racom even has provided interoperability with a number of Motorola systems in the area.

The FCC's application-processing division used to employ a significant number of outside contractors for Part 90 applications. The number of contractors dropped to six, and then they were eliminated from the FCC's work force.

Some of the Racom users have their own radio systems; they then roam onto the Racom network when necessary. In those cases, a public-safety agency with



The Radio Club of America Store opened at the APCO show, and the first shirt was sold to Radio Club Fellow Patrick E. Buller (call sign W7RQT), a RF engineer from Washington State.

enough capacity needs to justify its own system was able to create roaming and interoperability opportunities by partnering with the commercial operator.

I don't have to tell you the operational advantages of the Racom system, but what is important to note is that the smaller communities on this system did not have the pain of floating bond issues to raise funds for the buildout and they did not have to go through the laborious bidding process.

> **Congress and the FCC are more cognizant than ever of the need to make spectrum available for public-safety agencies. Broadband can somewhat lessen the strain on traditional wireless capacity.**

For smaller public-safety entities, this also relieves the tremendous burden of dealing with the FCC and system technicians. I can't even begin to give you the numbers of public-safety agencies that have let their licenses lapse merely through the fiscal inability to have trained personnel within the agency pay attention to these mundane details.

The Racom system is not the sole example of public and nonpublic partnerships; there are many others. If you believe that iDEN technology is your future, Aeronautical Radio, which is a cooperative of the major airlines, is building out a full-featured iDEN system for airport use. It will be partnering with other entities to build out non-airport locations. The FCC has talked about the federal and non-federal communications partnership in Alaska. Recently, our office filed a waiver request for the State of South Dakota to permit the state to build a state-wide, public-safety system on common-carrier VHF frequencies — the result of cooperating with the commercial operators that had bought that spectrum at auction. Spectrum Access and others will be happy to work with you on leasing 700 MHz guard-band spectrum, directly adjacent to the 700 MHz public-safety allocation.

The FCC is cognizant of the benefits of these partnerships, and the commission is responding by creating more opportunities. For example, the commission — in the new 4.9 GHz allocation — specifically encouraged these private/public partnerships to help speed innovation and system buildouts. In its Petition for Reconsideration, the National Public Safety Telecommunications Council said that the 4.9 GHz band represents a new way of doing business for public-safety agencies. I agree. Hopefully, the FCC will release its Secondary Markets Order soon, which will look at expanding spectrum-leasing opportunities between public and private entities.

Give Something, Get Something

Of course, the problem with these partnerships is one of comfort in giving up control in operations of the system. As it is, there often are issues between police and fire departments sharing communications systems. I recognize that moving into partnerships with utilities — and particularly commercial entities — really stretches the envelope. It is, nevertheless, important that some agencies move out of their comfort zones in order to get systems built in a timely manner and without significant expense, or to create needed interoperability.

To create the perfect partnership, new attitudes are

The Racom system represents the Holy Grail of interoperability, in that all public-safety and utility users on the system may coordinate their efforts with other agencies.

required. Equally important, however, is that proper relationships between the parties must be established. Both parties must enter the relationship with their eyes wide open, discussing each entity's needs and expectations. And these needs and expectations must be memorialized in the operating agreement in order to minimize potential issues in the future.

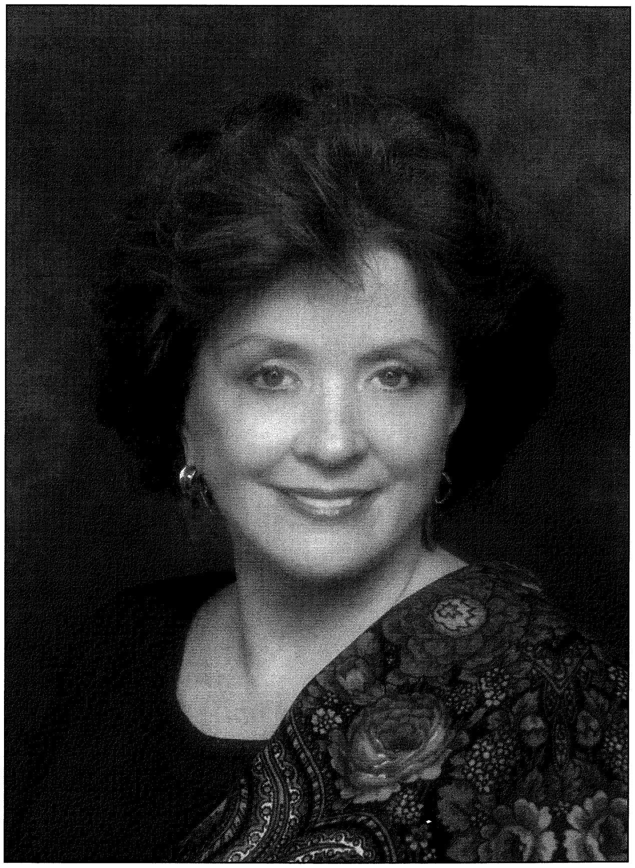
The issues that must be agreed to before entering a partnership include pricing, both now and in the future; the services to be offered; the expected system reliability; the system's coverage; the ability to have ruthless preemption; the need for system upgrades to maintain the current state-of-the art; and the terms and conditions for growth by users. Of course, this list is not exhaustive. Rather, it illustrates some of the issues that must be agreed upon.

Most often, public-safety agencies think of these partnerships as the public-safety agency being a user on a system controlled by another. This doesn't necessarily have to be the case. The Secondary Markets and 4.9 GHz orders envision partnerships in the reverse, too, where the public-safety entity is the licensee and not just the end user. So when you're thinking of what type of system might meet your needs, think of radio systems that you control, too.

I don't mean to suggest that these partnerships are for everyone. There is no "one size fits all" model for communications. In many cases, public-safety entities are large enough to warrant their own systems, built with public funds. However, for smaller entities, other options must be pursued. If there can be a meeting of the minds, the opportunities to solve communications problems can be limited only by the bounds of technology.

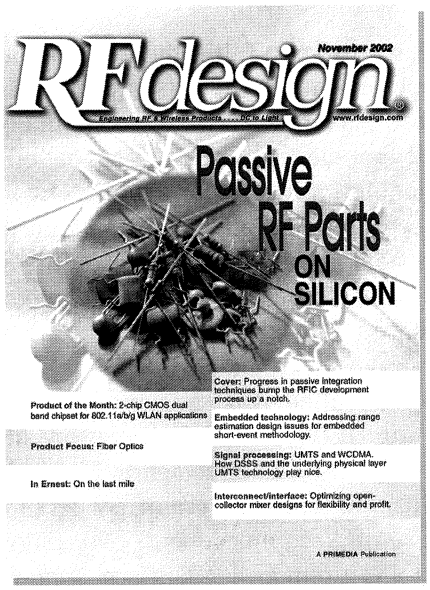
Next, we must turn our attention to the manufacturers. We must tell them what we need them to produce to serve communications needs, and we must present them with enough of a potential market to make the production of such products lucrative for the manufacturers. Thinking in the bigger picture can make this a reality.

Editor's note: Washington, D.C.-based Alan S. Tilles, an attorney with Shulman, Rogers, Gandal, Pordy & Ecker P.A., has a long and distinguished career in telecommunications law, particularly in the private-radio arena, participating in every FCC proceeding involving the private-radio industry since 1984. He has worked with such industry groups as the Personal Communications Industry Association, including its Mobile Wireless Communications Alliance and Private Systems User Alliance. Currently, his client base includes SMR operators, private-system users and radio manufacturers.



Nancy C. Smith, vice president of The Spectrum Firm Inc. in Carrollton, Texas, is the proud winner of a black Radio Club of America messenger bag, the first-ever RCA-embroidered briefcase-in-a-bag. Nancy has been a Radio Club member for three years, and she visited the club's booth at the APCO show. The briefcase is one of many items now available from "The Radio Club Store," and all net proceeds from the store go into the club's Scholarship Fund.

INFRASTRUCTURE • APPLICATIONS • SECURITY • SAFETY • INTELLIGENCE
MRT
MOBILE RADIO TECHNOLOGY
IT CAN BE FIXED
A year after the tragic radio communications debacle of Sept. 11, a McKinsey & Co. study reveals that FDNY radios would work reliably in only a fraction of New York City's more than 2,000 high-rise buildings. What must New York do?
SPECIAL ISSUE Homeland Security
WWW.MRTMAG.COM


November 2002
RF design
Engineering RF & Wireless Products . . . DC to Light
www.rfdesign.com
Passive RF Parts ON SILICON
Cover: Progress in passive integration techniques bump the RFIC development process up a notch.
Product of the Month: 2-chip CMOS dual band chipset for 802.11a/b/g WLAN applications
Embedded technology: Addressing range estimation design issues for embedded short-event methodology.
Product Focus: Fiber Optics
Signal processing: UMTS and WCDMA. How DSSS and the underlying physical layer UMTS technology play nice.
In Ernest: On the last mile
Interconnect/interface: Optimizing open-collector mixer designs for flexibility and profit.
A PRIMEDIA Publication

The FCC Faces The Wireless Challenge

The following is an abridged version of FCC Chairman Michael Powell's remarks at the APCO conference last August in Indianapolis. The chairman touched on such current topics as E911 deployment, spectrum management and customer service.

At the FCC, we strive to fulfill the unique communications policy needs of first responders. Before and since September 11th, the commission has developed policies to secure our nation's telecommunications infrastructure and network reliability. Spectrum policy and homeland security are at the forefront of my strategic plan for the commission. Central to that plan is the implementation of Enhanced 911 for wireless communications devices.

Last April, I called for a new "Era of Cooperation" on E911. That cooperation has worked, but today I issue a call to action for all the E911 stakeholders to build this era of cooperation into a "New Era of Accomplishment." My fellow commissioners and I remain vigilant and committed to ensuring that our progress continues. Government cannot be a passive observer on E911 - instead we must be an active participant. It is equally clear, however, that the FCC cannot make E911 happen. We need carriers, public safety, ILECs, equipment vendors, and state and local governments to be full partners if the "Era of Cooperation" is to yield a lasting "Era of Accomplishment."

So much has changed since the initial E911 obligations were created in 1996 and they have changed largely for the better. We now know that E911 technology works - and can save lives. We have also learned that our progress requires the use of an occasional stick. The commission has not hesitated to use its enforcement power when wireless carriers are not justified in delayed deployment. Within the past 15 months, we have taken a number of actions where carriers have failed to comply, including entering into consent decrees with multiple national carriers who did not adhere to their deployment schedules. In addition to substantial fines, each carrier is now subject to binding deployment schedules with automatic penalties if they fail to comply again.

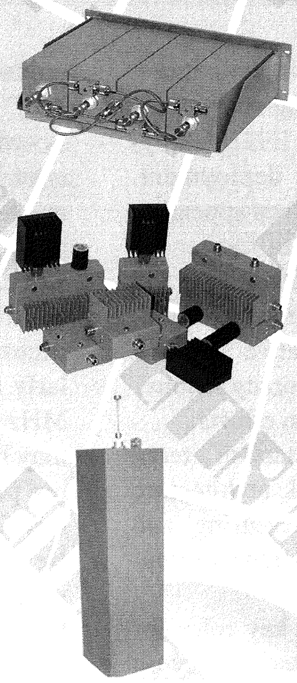
We think our efforts are starting to pay off. In partnership with all the stakeholders - including APCO, we have seen substantial progress for the American people:

- According to the Aug. 1, 2003, Reports, Phase II information is now being provided by at least one wireless carrier in approximately 480 markets to more than 1200 PSAPs, an increase of 50% compared with the prior quarter.
- For the six nationwide carriers, more than 65% of their markets deployed have come on line in the past six months.
- Every nationwide carrier using a handset-based approach is offering at least one compliant handset. Both Sprint and Verizon offer their customers at least 10, and Sprint alone has sold more than 11.6 million such phones.
- And here in Indiana, AT&T Wireless, Nextel, Sprint and Verizon Wireless have deployed Phase II in a number of areas including Indianapolis, Lake County, Bloomington and Terre Haute.

Although our progress has been impressive and sustained, we cannot rest. There is still much to be done. And here is what we are going to do:

The E911 Coordination Initiative

I am pleased to announce that the next session of the FCC's E911 Coordination Initiative will take place Oct. 29-30, 2003. At that session, we will sound the call to action to our colleagues at the state level. There — for the first time — we will convene the E911 designees of each of the states' governors and U.S. territories. These leaders will provide a key interface for E911 deployment issues in the states and important points of contact for the vital public education efforts that are essential to successful E911 deployment. We also plan to provide resources to governors' state 911 designees to help them provide leadership and



Services and products in the LMR,
Paging, Cellular, PCS, Maritime,
Aeronautical and Broadcast
industries.

Antenna Site & Filtering Equipment
Site Management
Site Consulting

Isolators
Duplexers
Cavities
Multicouplers
Combiners
Signal Boosters
Power Amplifiers

Wireless internet hardware,
engineering and installation.

EMR corp.

Web: emrcorp.com e-mail: info@emrcorp.com

&

EMRInternet.com

A full service Internet provider

Offering Internet & Web Related Services:

Web Hosting
National Dial Up
eCommerce
DSL Services
Server Collocation
Web Site & Database Programming
Wireless and Broadband Internet Access services

22402 N. 19th Avenue Phoenix, Arizona 85029 Tel: 623-581-2875 Toll: 800-796-2875 coordinate E911 deployment efforts in their states.

Central to this task will be building support for the idea that state funds set aside for E911 deployment should be used for E911 deployment. Consumers have an expectation that fees appearing on their bills for E911 will be used to further the deployment of these life-saving technologies, and we must ensure that those expectations are honored. The Second Coordination Initiative also will tackle current deployment issues, accuracy requirements and additional public education efforts.

The commission also is going to establish a technical group to focus on 911 network architecture and technical standards issues. Measuring and improving the accuracy of E911 location information will be a key priority.

As I discussed earlier, one of the key roles for government on E911 is to identify issues early on so that they can be resolved before they frustrate or undermine deployment. One area of investigation is the method by which the commission will measure carrier compliance with our accuracy rules. The Emergency Services Interconnection Forum (ESIF) has established a Working Group to examine methods for testing location accuracy. The working group's goal is to develop a set of minimum, practical requirements that will ensure that individual test methodologies provide consistent, valid, and reproducible results in a variety of environments. The Working Group plans to send its recommendations to the ESIF for review by the full body by the end of November.

Consumer Outreach

Finally the public has a central role to play in making sure that E911 is rolled out in their communities. It's my job - - and yours as well - - to make sure that when consumers are at the kiosk at the mall, they don't just ask about price and how to download the latest tune from Fifty Cent as a ringtone. They also need to ask carriers: "Do you provide E911 Phase II capability?" "How accurate is the E911 capability in this handset?" "What is your deployment schedule in my area?"

Not all carriers are created E911 equal, and consumers have a right to know. But getting this technology deployed cannot be done by the carriers alone. Consumers also need to ask whether their state and local government public safety answering points are Phase II capable. Again, if the answer is "no," we all need to ask "why not?" I urge the public-safety community to enlist consumers as allies in ensuring that E911 deployment is properly funded and tended to in the political process at all levels.

Other Concerns

First and foremost, public safety needs reliable access to its existing spectrum resources, particularly at 800 MHz. The interference issues at 800 MHz are very serious and complex. In fact, this may be one of the most challenging spectrum policy proceedings that will come before this commission. I would like to thank APCO, ITA, Nextel and other interested parties for their hard work in educating us about the interference problem and helping us build towards a workable solution for the operators in this band. I cannot tell you that we have yet resolved these issues, but I can assure you that this proceeding is an absolute priority.

The commission also is committed to speeding public safety deployment in the 700 MHz band. As you know, the band currently is encumbered by broadcasters. The delay in the initial auction of the 700 MHz commercial bands has required modification of the FCC's original voluntary band-clearing plan. Congress is exploring new options for moving this process forward. In addition, we are tackling the challenge of the digital-TV transition to hasten the clearing of the band. Whatever the ultimate mechanism, rest assured that we understand the need to make these frequencies available as soon as possible.

But increasing spectrum efficiency isn't just about technology; it's about people as well. We encourage the public safety community to develop creative solutions promoting interoperability including strategic partnerships between governmental and non-governmental users. The commission recently made an additional 50 megahertz of spectrum available at 4.9 GHz. In our decision, we encourage public safety to develop partnerships with the critical infrastructure community to provide secure communications. These types of innovative arrangements allow us to optimize the spectrum resources and to assist public-safety providers in performing their critical operations.

Team HUTTON®
...your wireless product experts

The Winning Choice

As a distributor of wireless communications products and services, Team Hutton supports you in the race to win business. We have what you need to become a winner.

Speed - bundling and kitting services with Just In Time delivery from our multiple warehouse locations

Skill - a team of wireless product experts

Products - one stop shopping on 150+ wireless product lines

Call your Team Hutton rep today for all your wireless needs. See you in the winner's circle!

Supplier Sponsors of Team Hutton

NK CABLES
RADIALL/LARSEN antenna technologies
ANDREW®
TRYLON TSF® ISO 9001 Registered
TIMES MICROWAVE SYSTEMS
EUPEN
CommScope WIRELESS
MAXRAD® STATE OF THE ART ANTENNAS
IDEAS by PANAVISE®
TAIT
DECIBEL PRODUCTS® An Allen Telecom Company
bayly
ROHN Industries, Inc.
PolyPhaser Corporation
EFJ
SINCLAIR
bp solar
PLESSEY
RADIOWAVES THE LEADER IN MICROWAVE ANTENNA INNOVATION
GAMBER JOHNSON
WiLAN™
CarrierAccess
Gabriel electronics
proxim
EVERGREEN SOLAR®
valmont COMMUNICATIONS
csi
Shell Solar
RF INDUSTRIES
KATHREIN SCALA DIVISION
SAT-PAK
SAMLEX AMERICA
CSi/SPECO
ILT
Spotwave WIRELESS
antenna specialists An Allen Telecom Company
Anritsu
ALLCOM PRODUCTS
ADTRAN
NEWMAR®
Multiplier
HUBER+SUHNER
BIRD
MAGNETEK UNCOMMON POWER
Deltec
unigy
TPL

An Overview of Wireless Networks and Security Issues For WiFi Networks

By Bo Li, Harold Lee, Narendra Kamat,
Daniel Menchaca and Prof. Ted S. Rappaport

Wireless local area networks (WLANs) provide wireless connectivity between PCs, laptops and other equipment in corporate, public and home environments. Today, tens of millions of users rely on short-range wireless connectivity between computers or automation equipment using WLAN modem gear that complies with well-known standards such as IEEE 802.11, 802.11a, 802.11b and 802.11g. The first WLAN standard IEEE 802.11, initially contemplated in the late 1980's, was finalized in 1997 (10 years later!) and provided interoperability standards for equipment makers using 11 Mbps Direct Sequence-Spread Spectrum spreading and 2 Mbps user data rates in the 900 MHz and 2.4 GHz unlicensed bands.

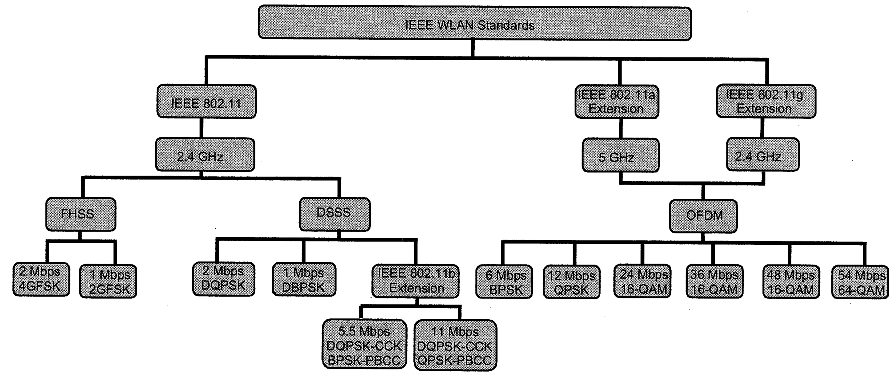
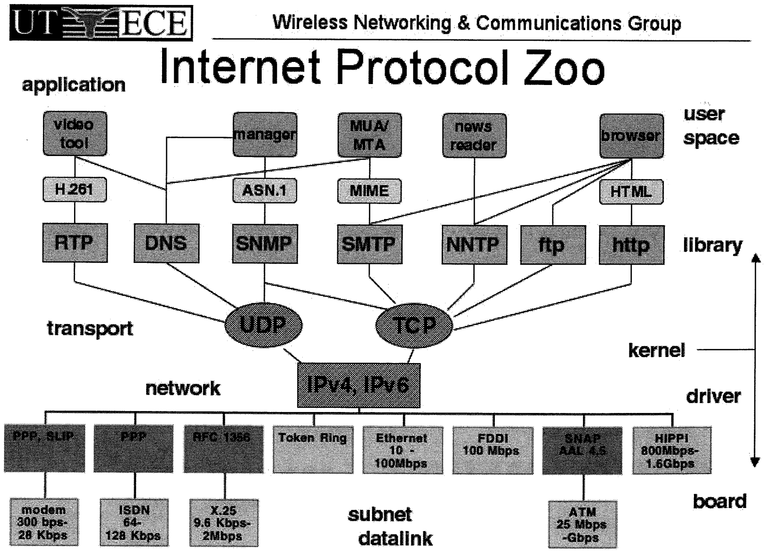


Figure 1. Evolution of WLAN standards.

In 1999, IEEE 802.11b and 802.11a standards were developed, and this created the foundation for the WiFi explosion we are witnessing today. IEEE 802.11b provided new user data rate capabilities of 11 Mbps and 5.5 Mbps in addition to the original 2 Mbps and 1 Mbps user rate of IEEE 802.11. Today, IEEE 802.11a offers high speed connectivity up to 54Mbps using OFDM in the 5 GHz frequency band, and IEEE 802.11g defines network connectivity in the 2.4 GHz band that is backward compatible with IEEE 802.11b and 802.11 standards. Figure 1 illustrates the evolution of IEEE WLAN standards. An overview of the evolution of WiFi is



MAXRAD™
An ISO-9001 Registered Company

Being there is your business. Helping you get there fast is our business.

Maxrad Land Mobile Radio Antennas

A dispatcher gets a call while you are on the road. You must get from one location to another fast. With a Maxrad high-quality antenna as a key element in your vehicle's radio communication system, you can be assured that your radio will provide the maximum range and reliability necessary to receive and respond to your calls instantly.

At Maxrad, we have one of the most extensive lines of base station, mobile and portable LMR antennas on the market. Our antennas consistently meet or exceed published specifications, and our superior quality, customer service and value pricing are recognized globally. For almost a quarter of a century, Maxrad antennas have been the best choice for public safety, healthcare, education, transportation and commercial applications worldwide.

When communication is vital you can count on Maxrad. For more information, call today or visit us online at www.maxrad.com.

MAXRAD™

4350 Chandler Drive
Hanover Park, IL 60133
(800) 323-9122 (Toll Free)
(630) 372-8077 (Fax)
http://www.maxrad.com

given in [23].

The IEEE 802.11 specifications focus on the Medium Access Control (MAC) and PHY (physical layer) for Access Point (AP) based networks and ad hoc networks. The MAC layer provides reliable data delivery from the wireless physical (PHY) layer (e.g., the channel, where bits are formed in the radio channel) to the upper layers of the Open System Interconnection (OSI) network reference model. A controlled access method called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) is used to pass data from the upper network layers to the wireless media.

Figure 2 shows different standards used for the PHY and MAC layers. The PHY layer functions as an interface to exchange data frames with the MAC layer for transmission and reception of data, and provides data modulation and demodulation. Figure 2 shows the structure of WLAN standards with reference to OSI model.

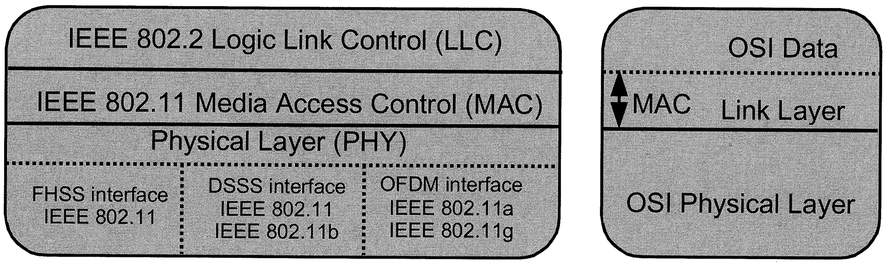


Figure 2. IEEE WLAN standards with reference to the OSI model.

IEEE WLANs operate in two modes: 1) a host-to-client mode, also known as an AP- based network where a fixed access point serves many co-channel clients, or users, and 2) in an *ad hoc* network mode where there is not a single known fixed access point, and all users are peer to one another *(also known as Independent Basic Service Set (IBSS)* or peer-to-peer mode). In the *ad hoc* mode, stations communicate directly with each other. Figure 3 depicts these two WLAN operation modes.

WiFi is exploding, and coffee shops and restaurants are deploying WiFi equipment to provide ubiquitous portable Internet access. However, the perceived lack of security has been an impeding factor in the widespread acceptance of WLANs. Unofficial studies suggest that more than 70% of wireless access points are unencrypted, and underground snoopers and sniffers, as detailed in a publication called *2600*, often publish lists of hundreds of corporate access points that can be used for instant access by strangers. Also, approximately 27% of the access points installed today use the hardware default value of the SSID (Service Set Identifier, a WLAN packet header field used in the authentication mechanism); this is akin to not changing the code on your garage door opener. Anybody with a wireless-enabled laptop can easily go near unprotected access points, sniff the traffic in the air and, at the very least, be able to see the data being transferred to and from the access point and, at the very most, become a user of the WLAN network.

Some of the popularly known security risks to WLANs include: Insertion Attacks, Interception and Traffic Monitoring, Jamming and Client to Client Attacks [2]. Insertion attacks occur when unauthorized devices are placed on the wireless network without going through a security process. Interception and monitoring of wireless traffic involve wireless sniffers, session hijackings, broadcast monitoring, and cloning access points and intercepting traffic [2]. WLANs are particularly susceptible to denial-of-service attacks, in which legitimate traffic gets jammed due to illegal traffic that overwhelms the access point. Client to client attacks are a consequence of the fact that two wireless clients can talk directly to each other, thereby bypassing the access point

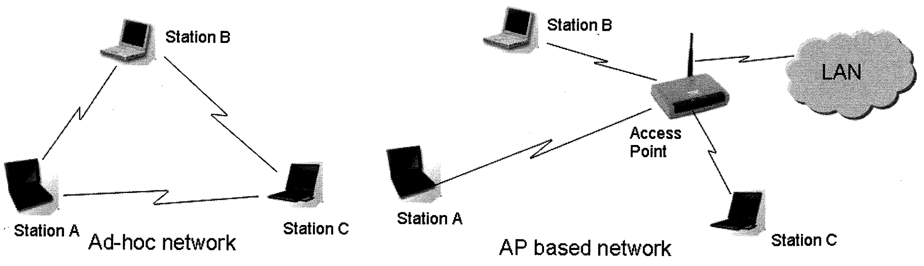
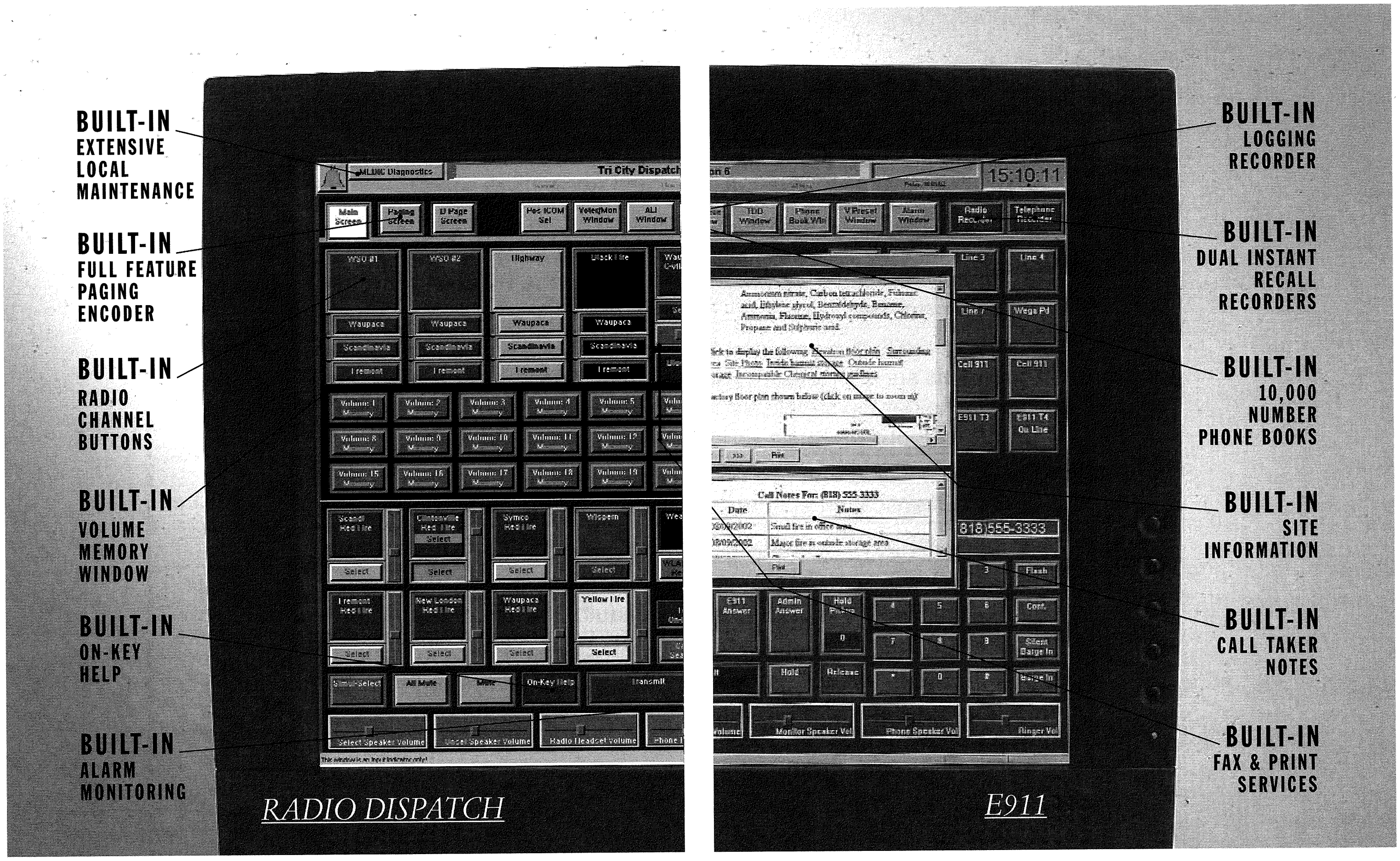
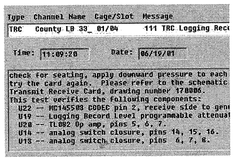


Figure 3. Two operation modes in IEEE WLAN standards.


BUILT-IN EXTENSIVE LOCAL MAINTENANCE
BUILT-IN FULL FEATURE PAGING ENCODER
BUILT-IN RADIO CHANNEL BUTTONS
BUILT-IN VOLUME MEMORY WINDOW
BUILT-IN ON-KEY HELP
BUILT-IN ALARM MONITORING
BUILT-IN LOGGING RECORDER
BUILT-IN DUAL INSTANT RECALL RECORDERS
BUILT-IN 10,000 NUMBER PHONE BOOKS
BUILT-IN SITE INFORMATION
BUILT-IN CALL TAKER NOTES
BUILT-IN FAX & PRINT SERVICES
RADIO DISPATCH
E911
Tri City Dispatch
15:10:11
Main Screen
Paging Screen
Select Speaker Volume
Unsel Speaker Volume
Radio Headset Volume
Monitor Speaker Vol
Phone Speaker Vol
Ringer Vol
E911 Answer
Admin Answer
Hold
Release
Transmit
On-Key Help
All Mute
Simul-Select
Call Notes For: (818) 555-3333
818)555-3333

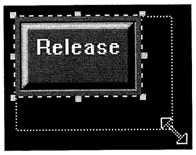
THE OPTIONS OTHER E911 AND RADIO DISPATCH SYSTEMS CHARGE YOU FOR WE BUILD-IN AT NO EXTRA CHARGE.



```
Type  Channel Name  Cage/Slot  Message
TRC   County LB 33_ 01/04      111 TRC Logging Rec
 Time: 11:09:28        Date: 06/19/01
check for seating, apply downward pressure to each
try the card again.  Please refer to the schematic
Transmit Receive Card, drawing number 170006.
This test verifies the following components:
  U22 -- MC145508 CODEC pin 2, receive side to gen
  U19 -- Logging Record Level programmable attenua
  U20 -- TL082 Op amp, pins 5, 6, 7.
  U14 -- analog switch closure, pins 14, 15, 16.
  U13 -- analog switch closure, pins  6, 7, 8.
```

The built-in MEDIC spots trouble down to the component level. It can be used remotely even by technicians back at our factory. This could mean a 50% savings in support.

Our built-in Screenmaker easily customizes any screen to meet your needs. Buttons can be easily resized, moved and changed.



The UltraCom™ E911/Radio Dispatch Console System comes complete with all its features built-in. Unlike the competition, this is not a stripped-down system with loads of expensive options to make it complete. Our built-in features and free software upgrades save you big money.

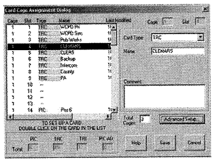
If you choose to buy the E911 or Radio component separately you also get the software for the other component at no extra cost, just add minimal hardware to save as much as 50%.

UltraCom is an all digital, 32-bit Windows, single application system. Telcordia and NENA compliant handling both E911 and ADMIN lines. Built from the ground up by us - not a collection of older systems.

Contact us today to find out just how much money you will save by eliminating all those pricey options.

Moducom holds many state & government contracts.

System programming changes can be made by the customer instead of expensive factory programmers. This makes it a snap to change levels, add cards and enable new features.



Free Demo

Demo our cost saving system software and request or download a brochure at www.moducom.com or call us at: 818-764-1333

MODUCOM

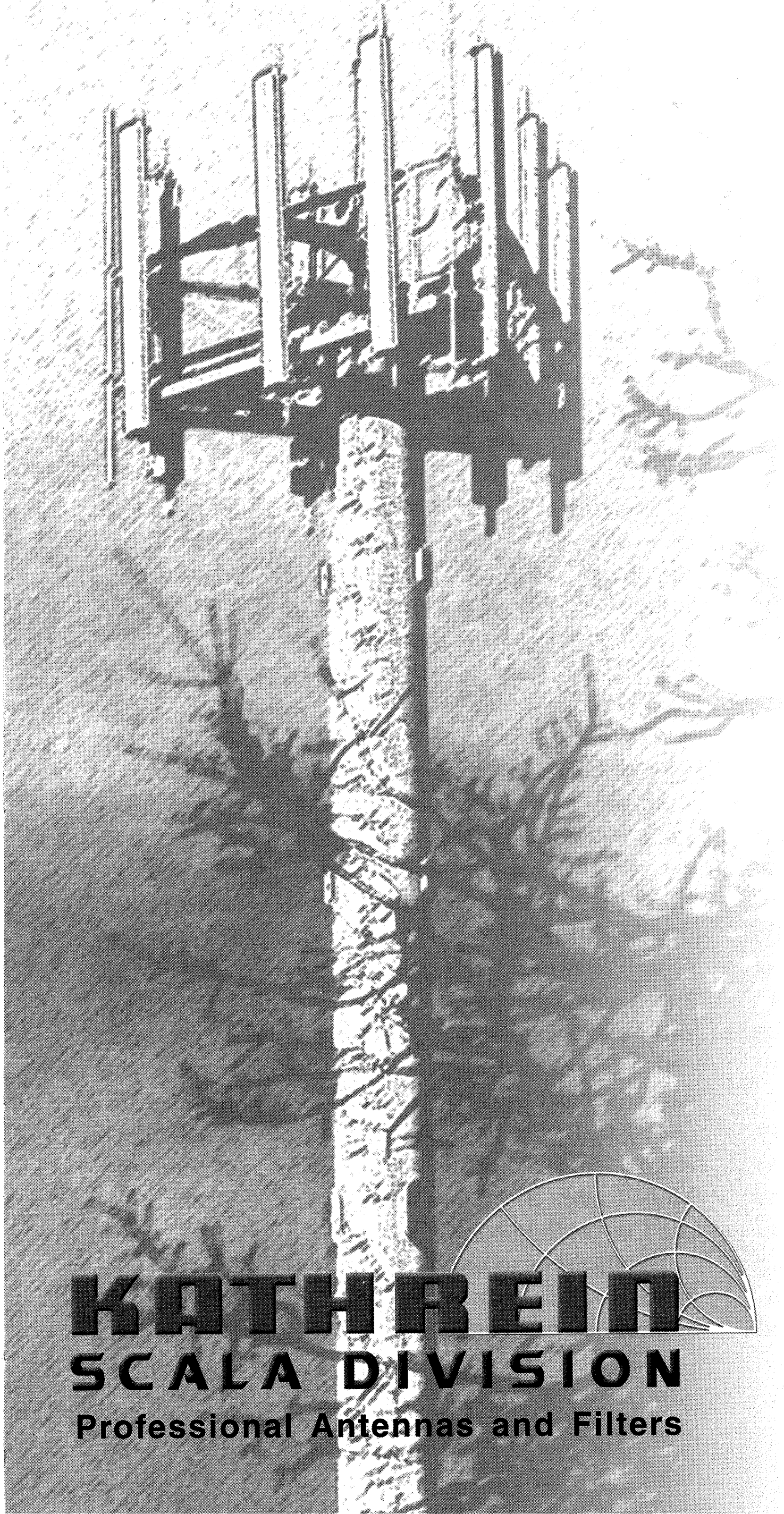
COST EFFECTIVE NOW.
MORE COST EFFECTIVE OVER TIME.

MODULAR COMMUNICATION SYSTEMS, INC. 13309 SATICOY ST. NORTH HOLLYWOOD, CA 91605. E-MAIL: moducom@1x.netcom.com

Table 1. WLAN security terminologies

Terminology	Definition
AAA Server	Authentication, Authorization and Accounting server.
AES	AES is an advanced encryption standard used by the US Government and is defined by the National Institute of Standards and Technology. It employs a symmetric encryption algorithm and the Rijndael block cipher in order to protect user data.
Authentication Server	An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator.
Authenticator	An entity at one of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.
Encapsulate	To construct a protected packet from an unprotected packet.
Encryption	Encryption is the conversion of data into a form, called a ciphertext, that can't be easily understood by unauthorized people.
Group Transient Key	A value derived from the Pseudo-Random Function using the Group Nonces. It is split up into as many as three keys (a Temporal Encryption Key and two Temporal MIC Keys) for use by the rest of the system.
Key Management Service	A service to distribute and manage cryptographic keys within a Robust Security Network.
Kerberos	Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal.
Network Access Port	A point of attachment of a system to a LAN. It can be a physical port (perhaps a single LNA MAC attached to a physical LAN segment) or a logical port (an IEEE 802.11 association between a station and an access point).
Pairwise Transient Key (PTK)	A value that is derived from the PRF using the SNonce, split up into as many as five keys (Temporal Encryption Key, two Temporal MIC Keys, EAPOL-Key Encryption Key, EAPOL-Key MIC Key) for use by the rest of the system.
RADIUS	Remote Authentication Dial In User Service, an example of software running on an authentication server.
Robust Security Network (RSN)	An IEEE 802.11 LAN relying on IEEE 802.1X for its authentication and key management service; and CCMP, WRAP, or TKIP for data protection.
Session	A session is a series of interactions between two communication end points that occur during the span of a single connection. Typically, one end point requests a connection with another specified end point and if that end point replies agreeing to the connection, the end points take turns exchanging commands and data. The session begins when the connection is established at both ends, and it terminates when the connection is ended.
Supplicant	An entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link.
VPN	A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organizations' networks.

reliable (ri lī´ə bəl), adj.
… dependable in achievement, accuracy, honesty, etc



The only reliable thing about weather is its unreliability. You just can't count on it to stay the same day after day. So, when Kathrein develops antennas and filters that live in the weather all year round, we over-engineer and over-build to handle the extremes. For instance, take our AP-Series Dual Band adjustable downtilt antennas. They can take temperature extremes from -30 to +65 degrees centigrade and still deliver consistent performance. They install easily, can be controlled remotely, and, unlike the weather, they are reliable day after day, after day.

Call us or visit our Website to find the right antenna for your application. If we don't have exactly what you need, our engineers can probably make it. Like our antennas, they're very reliable.

Kathrein Inc., Scala Division
PO Box 4580
Medford, OR 97501 USA

Phone	541-779-6500
Fax	541-779-3991
Email	mail@kathrein.com
Internet	www.kathrein-scala.com

and any security features contained therein.

The three basic security concepts concerning information on any network are ***confidentiality***, ***integrity*** and ***availability***. The requirement that information is read or copied only by authorized persons or intended recipients is known as *confidentiality*. It is a prime requirement in corporate and defense communication applications. The requirement that the message received by the recipient is identical to the message sent by the receiver is known as *integrity*. It is of primary importance in legal and financial communications. Making information or network service inaccessible to bona fide users violates the requirement of *availability*, which is most important for service-oriented businesses. Violation of this requirement is known as a denial of service.

To users of information carried by the network, the most important concepts are ***authentication***, ***authorization***, and ***non-repudiation***. *Authentication* is the process of verifying that a user is, in fact, who he or she claims to be. The proof of identity may involve something the user knows (e.g., a password), something the user has (e.g., a "smart card") or something about the user that proves a unique identity (e.g., a fingerprint). *Authorization* is the process of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. *Non-repudiation* is the requirement that if a user sends a message or performs an activity after authentication, there should be no way for him or her to deny that fact later — essentially, an electronic paper trail.

When these ideas are applied to WLANs, it must be realized that the wireless medium is unlike the wired network, in that the airwaves are shared. Wired networks afford a sense of physical security, but in WLANs, any adversary has physical access to the medium over the air. This warrants more careful deployment of security techniques at the application layer. Also, most users of WLANs are mobile, using portable computing devices (e.g., laptops). These users obtain network connectivity through access points. These access points have to run at very high speeds, switching packets to and from users at a very high data rate (several megabits per second). Therefore, introducing secure communications at the wrong point potentially can have a deleterious effect on high-speed performance, creating delays, timing jitter or outages due to synchronization problems.

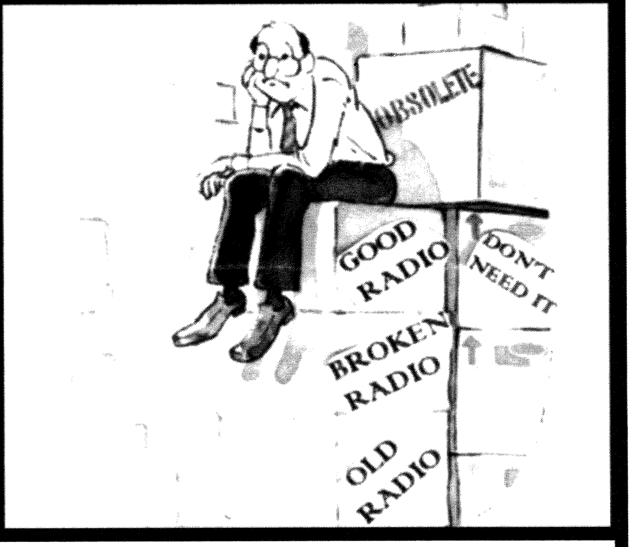
Thus, WLANS require a mechanism that allows fulfillment of security requirements without impacting data rates. For example, by letting access points manage sessions and provide packet switching, and providing a dedicated server that handles authentication/authorization, WLANs can be made to run more efficiently. Finally, strong security techniques in WLANs are inextricably linked to user awareness and co-operation. The most powerful encryption technique would be quite useless if the user has it turned off. Table 1 lists network security terminologies used by the IEEE [3, 4] and their definitions, as a requisite part of our further discussion.

A good wireless network should provide a range of different user-authentication and data-encryption options, so that users can be given the appropriate level of security for their particular applications.

Confidentiality, integrity and mutual authentication are some of the issues common to all network security discussions. When the first WLAN standard 802.11 was developed, there was an attempt to address these issues by the security mechanism known as Wired Equivalent Privacy (WEP). Although it is better than no encryption at all, WEP had some serious vulnerabilities [6, 7]. After WEP, the security standard 802.1X has been gaining popularity. However, 802.1X is not a complete security standard, but just an authentication model. The IEEE 802.1X is a standard for port-based network access control. The standard can be applied to both wired and wireless networks and provides a framework for user authentication and encryption key distribution.

However, even this new protocol is not free from some initial design flaws [8]. Currently, the industry is eagerly awaiting the security standard proposed by IEEE 802.11Task Group I, known as 802.11i. It is hoped that the experience with the previous security approaches will lead to 802.11i having properly dealt with all known vulnerabilities of WEP and 802.1X. 802.11i uses two-way authenticated 802.1X as part of its mechanism, and it is expected that encryption will be carried out using the relatively new Advanced Encryption Standard (AES) that uses two AES-based protocols: Wireless Robust Authenticated Protocol (WRAP) and Counter-Mode Cipher Block Chaining-Message Authentication and Control Protocol (CCMP).

Another way to provide security is to use an application-based login screen and a network-layer authentication technique, such as a VPN. VPNs also


OBSOLETE
GOOD RADIO
DON'T NEED IT
BROKEN RADIO
OLD RADIO

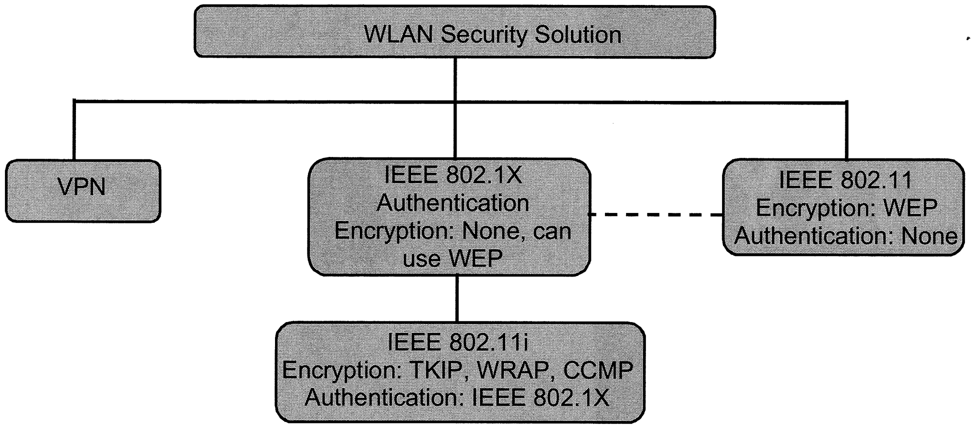


Figure 4. WLAN security solution.

are used to complement the IEEE WLAN security solutions. The structure of WLAN security solutions is illustrated in Figure 4.

• From wired network to wireless network: WEP and WEP2

To provide the basic security features of confidentiality, authentication and integrity to the stations using a WLAN, the IEEE standard 802.11 proposed a protocol known as Wired Equivalent Privacy (WEP) [9]. This section takes a look at how WEP works, the security features it provides, the vulnerabilities inherent in WEP, and suggestions to address some of these vulnerabilities.

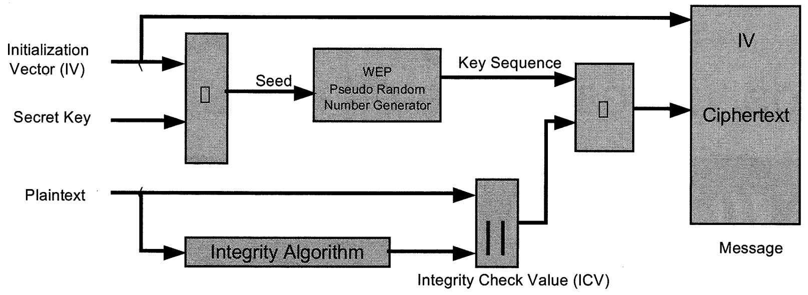

Initialization Vector (IV)
Secret Key
Seed
WEP Pseudo Random Number Generator
Key Sequence
Plaintext
Integrity Algorithm
||
Integrity Check Value (ICV)
IV
Ciphertext
Message

Figure 5. The WEP encryption engine.

• WEP architecture

As can be seen from Figure 5, WEP depends on a secret key shared between the communicating parties (client station and access point) to protect the payload of a transmitted frame in each direction. The basic encryption is carried out using the digital logic X-OR operation, where the plain-text message (with its attendant checksum) is X-ORed with a keystream. To help ensure that the keystream is not repeated, WEP uses a pseudo-random number generator using RC4. This takes as input a secret key k (one of a few possible keys, known to both parties initially) and a 24-bit Initialization Vector (*IV*).

Because, ideally, each message is X-ORed with a new keystream, the system provides an unbreakable encryption. But this *"security"* strongly depends on the fact that two keystreams should not be the same. This is somewhat hampered by the very infrequent change to the secret key, and the very small (24-bit) IV, leading to rapid reuse of the IV and, hence, the keystream. Reuse of the keystream seriously threatens the security of this encryption, although the concept of RC4 is accepted to be secure.

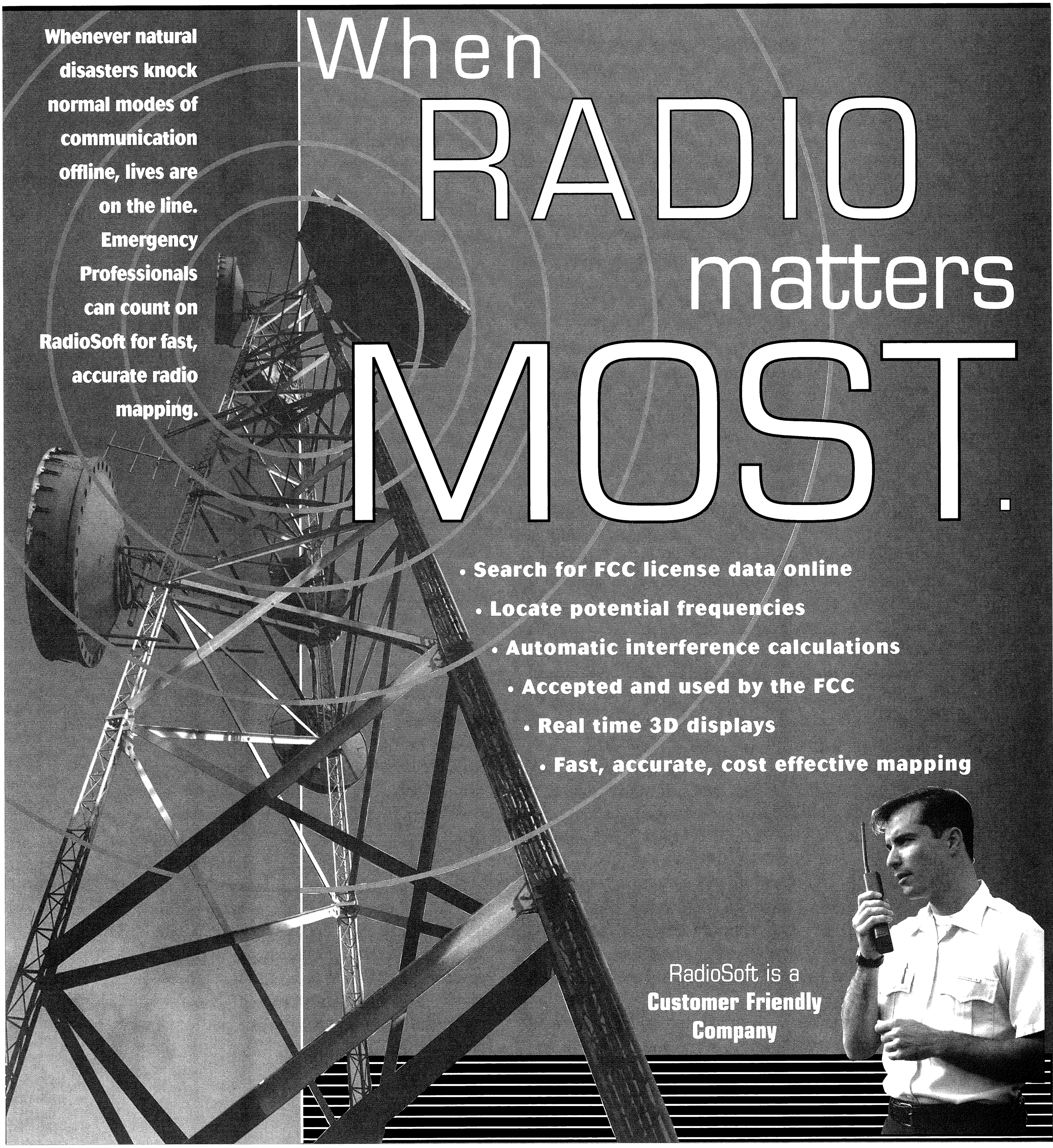
• WEP intentions

The following points discuss how WEP intended to address the security requirements for WLANs.

Integrity: WEP computes the Integrity Check Vector (ICV) by performing a 32-bit cyclical redundancy check (CRC-32) of the frame and appends the vector to the original frame, resulting in the plain text. Thus the ICV is piggybacked with the data in the encrypted frame. The inclusion of the ICV is meant to provide integrity. On receiving and decrypting the frame, the receiver recalculates the ICV using the CRC computation. The idea is that if any modification is made to a packet en-route, then the CRC checksum that is also transmitted with the packet will not match the CRC calculated at the receiver. The receiver will thus identify the packet as damaged or corrupted and discard it.

Authentication: There are two kinds of Authentication provided by WEP:

1. Open System Authentication: There is no authentication required and any station is allowed to join the Basic Service Set if the WEP



configuration has been set to Open System.

2. Shared Key Authentication: The client station requests authentication from the Access Point and indicates that it wishes to use Shared Key Authentication. The Access Point generates a random 40-bit (or 128-bit) *challenge* and sends it in the plain text to the client station. The client station encrypts the challenge using the shared key and sends it back to the Access Point. The access point decrypts the challenge and uses the CRC to verify its integrity. If the decrypted frame matches the original challenge, the station is considered authentic.

Confidentiality: The confidentiality of WEP depends on the use of a secret-key symmetric algorithm, which is used to encrypt the body of a transmitted frame of data. The message plus ICV is encrypted via the RC4 pseudo-random number generator algorithm using a long sequence key stream. Finally, it is the cipher text that is sent over the radio link. Only an intended recipient will have the secret key that is needed to generate the keystream to decrypt the frame. Because (ideally) each packet will be encrypted by a different keystream, it was thought that it will not be easy to attack the encryption unless a brute-force mechanism to obtain the key is used.

• WEP logistic issues and vulnerabilities

If the Shared Key Authentication is enabled (imposing access control), then the access points and the stations must have the secret key. The secret key is presumed to have been delivered to participating stations via a secure channel independent of the 802.11 specification. To prevent the sending of the secret key in the clear, each station has a small set of possible keys to be used, in the form of an array of secret keys. The station sends only the array index of the key it is using in its encryption algorithm.

Two stations may have a predetermined key (between the two). If the frame is to be sent to a station with which this prior arrangement has been worked out, the frame will be encrypted using a different secret key. The access point has a mapping of the secret keys of these stations to their MAC addresses, known as an Access Control List. By looking up the appropriate key, the receiver is able to decrypt the frame. This shows the system is not limited to using a single secret key for all stations.

A robust and secure key distribution mechanism is not defined in the 802.11 standard and, therefore, the implementation is left to the equipment vendors and the users. The disadvantage is that physical (safe) distribution of keys can't be carried out often; the secret key will not be changed often enough or will be easy to guess.

There are widely known fundamental security problems with WEP. In [6, 7], the authors have pointed out possible attacks on WEP, which can violate all the requirements of privacy, access control, and integrity.

• **Integrity** The CRC can be easily modified. The IC field is implemented as a CRC-32 checksum - a common error detection scheme. The problem with this scheme is that it is linear; thus, it is possible to compute the bit difference of the two CRCs based on the bit difference of the data packets. This allows the attacker to be able to determine which bits of the CRC-32 code to correct when flipping arbitrary bits in the packets so that the resulting packet seems valid.

• **Confidentiality and Authentication** There are several issues with the encryption used by WEP.

1. The WEP algorithm uses encryption provided by X-Oring, the plain text block with a keystream sequence generated by the RC4 stream-cipher pseudo-random number generator. The inputs to the RC4 algorithm are a secret key *k* (which is comparatively short) and an initialization vector. If the same keystream is used for different plain texts, then we have the following situation:

$$C1=P1\oplus RC4(IV,k)$$
$$C2=P2\oplus RC4(IV,k)$$

If $RC4(IV,k)$ gets repeated, then the eavesdropper could perform

$$C1\oplus C2=P1\oplus RC4(IV,k)\oplus P2\oplus RC4(IV,k)=P1\oplus P2$$

With some knowledge about the type of data (plain text) there is a good chance the attacker will be able to arrive at both P1 and P2, given the redundancy in real-world data. To prevent this, it is required that $RC4(IV,k)$ does not recur. This is implemented by changing the IV on a per-packet basis. Because the receiver also needs to know IV used for any packet, it also is transmitted as the unencrypted part for this packet (this makes the IV available to the attacker as well). WEP uses only 24-bit IV, so any high-volume access point, even if using totally-random IVs, will run out of IVs in about half a day and be forced to reuse an IV. This is termed an *IV collision*. An attacker can detect that an IV collision has occurred, because the IV is transmitted unencrypted in the packet. An IV collision results in the same keystream generated by

RC4, and the above attack can then be carried out. Even with a longer keylength for IV, such as that used in WPE2 (128 bits secret key), the fundamental problem is not solved.

In addition to the plain text, the successful attack also provides the attacker with the keystream corresponding to that IV. With sufficient effort, the attacker then can build a table of keystreams for each IV, which provides a direct decryption dictionary.

In addition, the secret key is one of a small set of values (four) that the two participants have. This is to help ensure the secret key need not be transmitted over the medium. Because the key is not changed frequently, the threat posed by IV collision is even more serious.

2. When an IV and its corresponding keystream are known, it can be used to construct a new message and inject it into the network. The access point will have no reason to suspect this packet as a spurious one, because it has a valid IV, and it is encrypted with the correct keystream.

3. In the challenge/response sequence while performing Shared Key Authentication, the challenge (plain text), the response (cipher text) and the IV used to encrypt the challenge are all visible to the eavesdropper. Thus, the authentication sequence provides the attacker with a keystream corresponding to that IV. If that IV is reused, (and the shared key is not changed), then the attacker has direct ability to decrypt the frame.

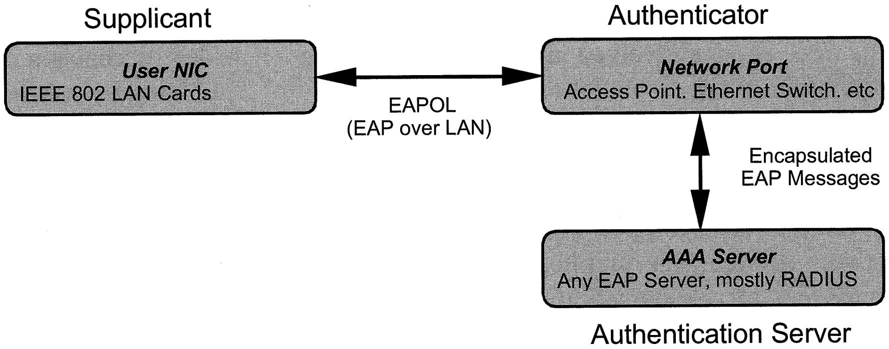


Figure 6. IEEE 802.1X architecture

The above analysis shows that only WEP cannot be relied upon as a complete security solution. While difficult to intercept by most users, the deficiencies make WEP easy to attack. The lack of transparency in the design process led to some obvious errors being overlooked. Although RC4 is in itself a secure stream cipher (without any known vulnerabilities), its application in early WLANs led to a specification that has major vulnerabilities.

• WEP2 improvements and its inherent setbacks

WEP2 was developed to acknowledge problems with the initial 802.11 security protocol WEP. It was created to be backwards compatible with WEP. Compared with WEP, WEP2 uses 128-bit secret keys. Some of the attacks on the WEP secret key can't be mounted easily if WEP2 is in use, because the attacker needs to monitor a much larger stream of traffic before being able to decode and decipher. However, because WEP2 still runs on linear scaling, it is not a significant improvement. WEP2 has the same inherent vulnerabilities that exist in WEP: static secret key, IV key reuse, and known plain text attacks [5].

• IEEE 802.1X

Solutions based on the WEP standard alone do not offer system administrators effective methods to update the keys. On larger networks, the job of renewing keys can be a huge task. As a result, companies either do not use WEP at all, or they maintain the same keys for months and even years. Both cases significantly heighten the wireless LAN's vulnerability to eavesdroppers.

The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media, and it supports multiple authentication methods, including RADIUS, Kerberos, one-time passwords, certificates and public key authentication.

• EAP essentials

EAP was designed to de-couple the mechanisms of data transfer, encryption and authentication. EAP is the Internet Engineering Task Force (IETF) standard for extensible authentication in network access. It is standardized for use within PPP (Point-to-Point Protocol, RFC 2284), wired IEEE 802 networks

(IEEE 802.1X) and VPNs (L2TP/IPsec and PIC).

Developed as a generalized framework for several different authentication methods, EAP is supposed to avoid proprietary authentication systems. It can facilitate different authentication techniques, from passwords to challenge-response tokens and public key infrastructure certificates.

With a standardized EAP, interoperability and compatibility of authentication methods becomes simpler. For example, when one dials up a remote-access server and uses EAP as part of the PPP connection, the Remote Access Server (RAS) does not need to know any of the details about the authentication system. By supporting EAP authentication, an access point gets out of the business of acting as middle man, and it just packages and repackages EAP packets to hand off to a RADIUS (or equivalent) server that will do the actual authentication.

The three entities involved in authentication using the EAP framework are as follows:

1. Supplicant: the entity that desires to use a network service. This service is offered by a port on the authenticator.

2. Authenticator (Access Point): Provides ports for a network service, (the supplicant authenticates via authenticator to authentication server). All sessions go through the access point.

3. Authentication Server: Dedicated server running any authentication protocol such as CHAP, PAP, Kerberos, etc. It receives and responds to authentication requests from clients (sent via the uncontrolled port of the access point). It directs the authenticator to provide service after successful authentication.

EAP is flexible in the sense that any authentication mechanism can be encapsulated within EAP request/response messages. It gains flexibility by operating at the network layer rather than the link layer. Because each network port is not required to make authentication decisions, this is a key performance benefit.

• IEEE 802.1X architecture

802.1X provides an architecture for authentication methods by using simple transport for EAP messages, running over all 802 LANs. 802.1X inherits the EAP (Extensible Authentication Protocol) architecture and provides port based network access control with dynamic key management. A network port is defined as an association between a client station and an access point.

In the context of an 802.11 wireless network, 802.1X is used to securely establish an authenticated association between the client and the access point. An 802.11 Robust Security Network (RSN) uses 802.1X to provide security: authentication, access control and key management. It provides mechanisms to restrict network connectivity at MAC layer to authorized entities. The network connectivity is through network port.

IEEE 802.1X authentication is a client-server architecture delivered with EAPOL (EAP over LAN). Figure 6 shows the IEEE 802.1X authentication architecture. The authentication server (mostly RADIUS) authenticates each client connected to an Access Point (Supplicant) before accessing any services offered by the WLAN. Typically, the RADIUS protocol is used for the communication between authentication server and authenticator. It encapsulates EAP messages as a RADIUS attribute. It provides mechanism for per-packet authentication and for integrity verification between access point and RADIUS server. Sometimes, an Authenticator and an Authentication Server can be co-located within the same system such as an AP, allowing it to perform the authentication function without the need for communication with an external server.

Before the authentication succeeds, the access point must allow EAP traffic. However, this traffic would originate from an (as yet) unauthenticated client. To sidestep this issue, a dual-port model is used; the access point is considered to have two logical ports. One is the uncontrolled port, on which information pertaining to those users who have not yet been authenticated can be safely sent. This port connects only to the authentication server. The other is the controlled port, which allows access to other (useful) network services. It is not possible for an unauthenticated user to use the controlled port. The job of the access point is thus simplified.

The goals of 802.1X are to provide access control and authentication, flexibility and scalability. The use of EAP fits in admirably with the latter two goals. However, as will be seen in the next subsection, the initial design of 802.1X was not free from some vulnerabilities.

• 802.1X vulnerabilities

In spite of careful design, there were some serious vulnerabilities with 802.1X as a security standard for WLANs. Here it should be noted that part of the problem was that 802.1X is not meant for the wireless environment as such, but rather it is a general specification for any 802 network. Its applicability to the wireless environment was not well thought out, initially. While some of the weaknesses reported in [6] have now been fixed by various organizations, the major vulnerabilities include:

➪ Man-in-the-middle attack (MITM): One of the main design issues with 802.1X was that it didn't specify that the authentication needed to be mutual. The authentication was only one-way. The access point could verify the identity of the client, but there was no way for the client to verify the identity of the access point. This permitted some interesting exploits, based on the adversary's placing a rogue access point in the vicinity of the client. The rogue access point would act as an access point to the client, and also as a client to the real access point (authenticator). Thus, the attacker could get all the network traffic of that particular client to pass through it.

➪ Session Hijacking: This weakness is due to a lack of coherence between the old RSN state machine and the 802.1X state machine. After a supplicant has authenticated itself, the attacker sends a 802.11 MAC disassociate management frame to the supplicant. It uses the authenticator's MAC address to do this. Upon receiving this frame, the RSN state machine of the supplicant goes into the "unassociated" state, while the 802.1X state machine stays in the "authenticated" state. In this situation, the attacker gains network access using the MAC address of the victim supplicant, because it was still in the authenticated state.

➪ Denial of Service: 802.1X enables per-user session keys. However, there is no keyed message integrity check specified in 802.1X, which allows the possibility of denial of service attack by a malicious party.

These vulnerabilities can be mitigated to a large extent by the following. Firstly, the management frames of EAP have to be authenticated and their integrity should be guarded. This should be ensured not just between the authenticator and the RADIUS server, but also between the authenticator and the supplicant. Secondly, two-way (or peer-to-peer) authentication is required to prevent the problem of rogue access points. Again, this should be enforced not just between the authenticator and the RADIUS server, but also between the authenticator and the supplicant. Most implementations of 802.1X today have dealt with these well-known problems.

It must be understood that 802.1X is just an authentication model. It is not a complete security solution because it does not provide any mechanism for encryption, which is needed for confidentiality. In other words, an attacker can passively sniff all network traffic of authenticated clients. Many vendors continue to use WEP as the encryption mechanism along with 802.1X for authentication, which causes network implementers who are most concerned about security to use a VPN for their WLAN networks (this will be detailed in the Spring 2004 *Proceedings*).

802.1X also supports dynamic key exchange. The keys are managed at the transport layer by using what is known as EAP-TLS. TLS stands for Transport Layer Security. The use of EAP-TLS is similar to the mechanism to secure web transactions on the Internet (Secure Sockets Layer protocol). The variants to this have been the use of WTLS (TLS optimized for WLANs, keeping in mind the low bandwidth, low processing power requirements of this approach) and TTLS (which requires only the authentication server to possess the digital certificate, rather than each user).

To conclude, IEEE 802.1X is an improvement over WEP with authentication, dynamic key management and MAC access control. 802.1X does not make any encryption specification; thus, vendors may keep WEP as the encryption standard. However, addition of per-packet and peer-to-peer authentication, combined with the adoption of stronger encryption algorithms, would take WLANs closer to a complete security solution.

REFERENCES:

[1]. Table for wireless standards, URL: http://medtechcorp.com/papers/WirelessStds.htm

[2]. *C. W. Klaus,* "Wireless LAN Security FAQ", URL: http://www.iss.net/wireless/WLAN_FAQ.php

[3]. IEEE Std 802.1X-2001

[4]. IEEE Std 802.11i/D3.0, November 2002

[5]. *J. Philip Craiger,* "802.11, 802.1X, and Wireless Security", URL: http://www.sans.org/rr/paper.php?id=171

[6]. *N.Borisov, I.Goldberg and D.Wagner*, "Intercepting Mobile Communications: The Insecurity of 802.11", URL: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[7]. *S.Fluhrer, I.Mantin and A.Shamir,* "Weaknesses in the Key Scheduling Algorithm of RC4", URL: http://downloads.securityfocus.com/library/rc4 ksaproc.pdf

[8]. *A.Mishra and W.Arbaugh,* "An Initial Security Analysis of the IEEE 802.1X Security Standard", URL: http://www.cs.umd.edu/ waa/1x.pdf

[9]. ANSI/IEEE Std 802.11, 1999 Edition

[10]. *D. Eaton*, "Diving into the 802.11i Spec: A Tutorial", URL:http://www.commsdesign.com/design_corner/OEG20021126S0003

[11]. *A. Wool,* "A Note on the Fragility of the 'Michael' Message Integrity Code", URL: http://www.eng.tau.ac.il/~yash/ees2003-2.ps

[12]. *J. Geier,* "WPA plugs holes in WEP", URL: http://www.nwfusion.com/research/2003/0331wpa.html

[13]. *J. D. Clercq and O. Paridaens,* " Scalability Implications of Virtual Private Networks", IEEE Communications Magazine, May 2002, pp. 151-157.

[14]. White paper, "Security in Wireless Networks", NextComm, 2002.

[15]. *M. Goldschmidt ,* G. Morrison and R. Sabhlok, "Security in 802.11", URL: http://www.informatics.ed.ac.uk/teaching/modules/cn/groupreports/securityin802.11.pdf

[16]. *E. Janzen,* "Understanding Basic WLAN Security Issues", URL: http://www.80211-planet.com/tutorials/article.php/953561

[17]. White paper, "Wireless Security and VPN", Intel, 2001

[18]. *H. Haverinen, J. Mikkonen, and T. Takamäki,* "Cellular Access Control and Charging for Mobile Operator Wireless Local Area Networks", IEEE Wireless Communications, December 2002, Pp. 52- 60.

[19]. *A. K. Salkintzis, C.Fors, and R. Pazhyannur*, "Wlan-Gprs Integration for Next-Generation Mobile Data Networks", IEEE Wireless Communications, October 2002, Pp. 112-124.

[20]. *H. Honkasalo, K. Pehkonen, M. T. Niemi, and A. T. Leino,* "WCDMA and WLAN for 3g and Beyond", IEEE Wireless Communications, April 2002, pp. 14-18.

[21]. Bluetooth SIG Security Expert Group, "Bluetooth(tm) Security White Paper", Bluetooth SIG, 2002.

[22]. *M. Träskbäck*, "Security of Bluetooth: An overview of Bluetooth Security", URL: http://www.cs.hut.fi/Opinnot/Tik-86.174/Bluetooth_Security.pdf

[23] T.S. Rappaport, Wireless Communications: Principles and Practice, 2nd Edition, c. 2002, Prentice-Hall, Chapters 2-3.

HOOKED ON WIRELESS:

Dr. Ted Rappaport Talks About The Future Of The Industry

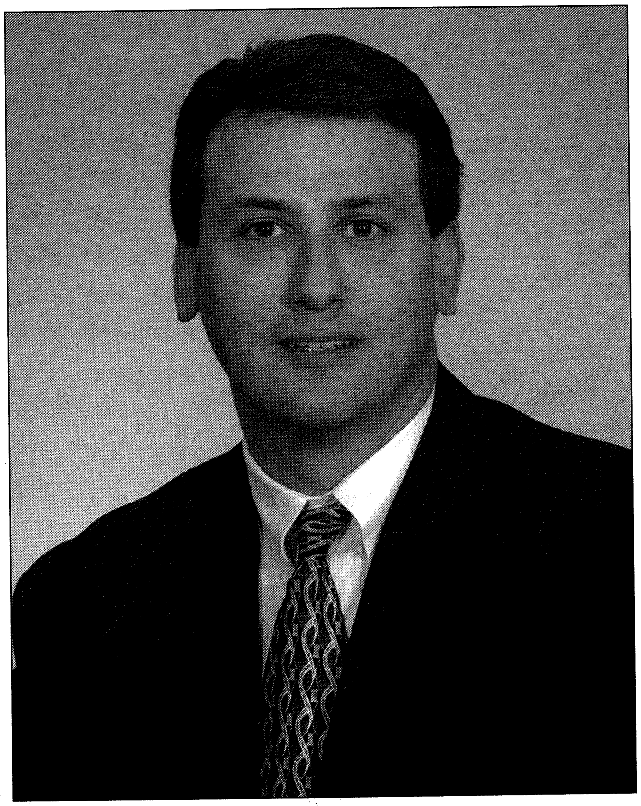
A broken leg, short-wave radios and Morse code all played a part in Ted Rappaport's wireless conversion. The teacher, researcher and entrepreneur is doing everything he can to pass that excitement on to other students.

By Debra Wayne, Proceedings editor

Dr. Ted Rappaport has a long history in the wireless industry, beginning with a non-functioning, short-wave radio he received in grade school to his present position as the William and Bettye Nowlin Chair in Engineering and the founding director of the Wireless Networking and Communications Group at the University of Texas' Austin campus. From 1988 to 2002, he was on the faculty of Virginia Tech, where he popularized a yearly wireless industry event and founded the Mobile and Portable Radio Research Group (MPRG).

Dr. Rappaport's awards and honors are many; he has written two commonly used textbooks; and he serves on a number of panels and boards, including the FCC's Technological Advisory Council. He has been appointed to a National Academy of Science panel to study the future of telecommunications research in the United States, and he is also serving as Technical Program Chairman for the IEEE Global Communications Conference, set for Dallas in late 2004. He is a fellow of the Radio Club of America as well as a past director, and he was awarded the club's Sarnoff Citation in 2000.

In a frank and freewheeling conversation with Proceedings editor Debra Wayne, Dr. Rappaport talks about his "profession of passion," this country's pressing need to excite upcoming students about the wireless industry and his recent move to the University of Texas.



Q: Right off the bat, how did you become interested in the wireless world?

A: When I was five, my grandfather showed me his short-wave radio, and I remember listening to Morse code and ship-to-shore radio, and being fascinated by signals sent from thousands of miles away actually being received. When I was 11 or 12, my grandfather got me a citizens'-band radio. It never worked. It was an old, tube-type CB radio, and I didn't realize until I was older that the reason it didn't work is because it didn't have any crystals in it. It had no channels, but I didn't know enough.

Q: How did you feed your interest throughout your junior-high and high-school years?

A: There was a fateful accident at the beginning of my freshman year of high school. I was going to be on the football team, and we were practicing before the season started in a sandlot game. My leg was broken in three places. I was laid up in a body cast at home for six months after being in the hospital a month.

For seven months of my freshman year, I could do nothing but lay on my back. My grandmother bought me a short-wave radio. I actually listened to and learned Morse code, and I became hooked on amateur radio. I studied for the test while I was laid up. As soon as I was out of my body cast, I hopped on my crutches and hobbled up to the home of a local ham radio operator, WB9NNO (Doc Woodward) who gave me the novice exam. I received my novice license when I was 14, my Extra Class N9NB when I was 16, and I was very active in amateur radio during high school.

I actually taught some Morse code classes in Richmond, Indiana, at the Whitewater Valley Amateur Radio Club during high school. My best friend Tom Poland (call sign N9NC) and I taught Morse code classes and helped others to become ham radio operators. I think that's where my love of teaching was born. Tom and I would give Saturday-morning classes to people who were three and four times our age, and we had a lot of fun. Tom, incidentally, went on to become a leading technical executive in the cellular industry.

We both went to Purdue University, and I studied electrical engineering. We were active in the Purdue Amateur Radio Club (W9YB). When I was a sophomore, I had a job in Dr. Leslie Geddes' lab, and it helped me pay my own way through school. The Radio Club of America played a big role in enabling me to stay for graduate school, because I was awarded one of its scholarships.

Q: Who piqued your interest at the college level?

A: At Purdue, there were two professors - George Cooper and Clare McGillem - who were the star communications professors, and they both liked radar and wireless. They wrote the seminal textbooks of the time, and I remember them telling us about cellular telephones, and that someday there would be a cellular-telephone industry. I was really hooked.

I went on to receive my Ph.D., and I was really lucky to be part of the first engineering research center there. The National Science Foundation had formed five engineering research centers in the United States in the mid 1980's, and these were huge centers focused on improving America's competitiveness in key manufacturing areas. Purdue's center was focused on the factory of the future. I was a communications researcher looking at the grand challenge of building better factories, so I contemplated wireless networks inside plants and developed radio channel models for wireless LANs inside buildings in 1986 and 1987, well-before the Internet and well-before IEEE 802.11. In fact, my research was partly used in the early 802.11 standards. My research anticipated where we would be in 15 years, and it was very clear to me that the WiFi explosion we are now experiencing would be a certainty.

> ***Dr. Rappaport developed radio channel models for factory-based wireless LANs in 1986-87, well-before the Internet and well-before IEEE 802.11. "In fact, my research was used in the early 802.11 standards," he says.***

Q: You got your Ph.D at a fairly young age. What kept you focused throughout all those years of school?

A: I received my Ph.D. in 1987, when I was 26, and it was very clear that wireless communications was going to be a key part of the world's infrastructure. It was a passion of mine that there needed to be an entire industry, there would need to be students and researchers, and an entire knowledge base created that didn't exist. We needed hundreds and thousands of engineers, scientists, do-ers who could bend the world and create the wireless infrastructure. And this continues to be clear to me. There's a need for students who can come out and make an impact, and that's what I tried to do at Virginia Tech with the MPRG, and what I am doing now at the University of Texas with WNCG.

Q: What was the impetus behind your move to the University of Texas, and how does this program differ from that in Virginia?

> ***The WNCG at the University of Texas is a multi-disciplinary research center that has received strong backing early on from major companies in Texas and from the National Science Foundation.***

A: The University of Texas was doing a search for someone to lead a wireless research initiative, but I didn't know about it. The leading executives in the industry in Austin called me, and then the dean, Ben Streetman, called me, asking me to come and give a lecture. I really had no intention of moving from our friends and home in Southwest Virginia, but my wife and I both liked Austin. It's a great academic opportunity, and the campus is wonderful. The summers are too hot, but winter is great.

Q: Was it a hard decision to leave Virginia Tech?

A: It was a very difficult decision - at first. I never really thought I'd leave. I'd been there 14 years, and I had a lot of history, and friends there. But I felt it was going to be hard to do any more there. I always have believed good professors spill their research out into industry, and the best professors have historically been involved in starting companies, and making an impact in industry. It was hard to attract business and investment to Southwestern Virginia, yet in my mind, this is a critical component of a very top engineering program. I was at the peak of my game as a professor, and I wondered where the next mountaintop was. There wasn't a lot of business acumen or locally created wealth there, and I felt like there was diminishing returns on what impact I could have there. We still have ties to Blacksburg, and I still work closely with Virginia Tech faculty. In fact, we have kept our season football tickets for the Virginia Tech Hokies. Yet, when I came to Austin and saw all the opportunities, the great business climate, the regional support, the terrific start-ups, and the entrepreneurial faculty, I thought I should give it a try. The University of Texas is a Top-10 school, and once I got my mind around the idea of moving and changing and starting something up again, it was pretty exciting, and it wasn't that hard to do. The Wireless Networking and Communications Group (WNCG) really is a startup research center, and in the first year, I am two years ahead of schedule.

Q: On what does the WNCG focus?

A: By coming to the University of Texas, I had a chance to really start a research center from scratch that could focus on different areas of wireless that were emerging and that only a startup could really do. The faculty at the university has a great deal of networking expertise, both in electrical and computer engineering, and in computer science. They were receptive to banding together to form a research center. So in just more than a year, we've put together 15 faculty (soon growing to 20) who are very excited about the future growth of wireless networks and systems. So the WNCG is a multi-disciplinary research center that has received strong backing early on from major companies in Texas and from the National Science Foundation.

The future of wireless communications is going to be in the network. As a researcher, the first part of my career was in radio propagation, modulation and system design. However, the future is moving to ad hoc networks, software radios, embedded security, and distributed infrastructure. There really are only a few places in the world working on that problem in a serious way. We are now one of those places.

Q: How did you go about recruiting the faculty and student who are participating in the WNCG?

A: The faculty and the students are the two most important ingredients at any university; they are the only two parameters a university can control. There were a number of senior faculty members already here who were excited to be part of this new vision, and they've been terrific. They've helped me get the program started; they're so creative, energetic and fun. I was given six new faculty positions for new recruits, and we've already filled four of those spots with some of the best young faculty in the country. My colleagues have expertise across the board in wireless, from networking and theoretical modeling of large systems to MIMO (multiple input/multiple output) communications systems, CDMA and information theory. We also have a security research component that we will be hiring into. Wireless security is going to be a big deal, and we're working on that.

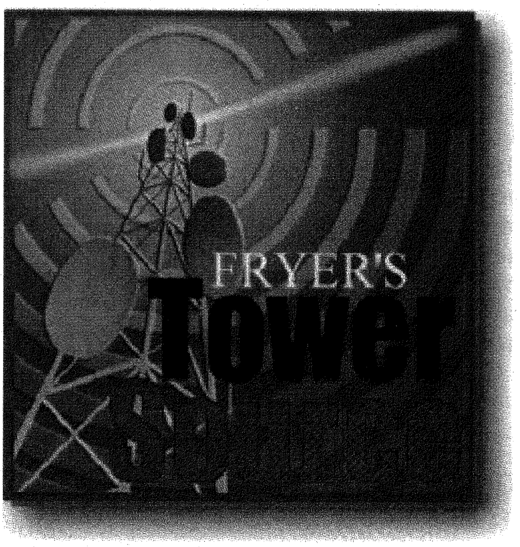
We've had a remarkable uptick in the number of students applying to the center. One thing we plan to do during the next couple of years is to become more pro-active and begin working with the top schools in the country to try to recruit students to come to WNCG. We have between 50 and 60 students right now. Motorola has donated 40 new office cubicles for the center, and we're building rapidly.

Q: What is a day in the life of one of your students like?

A: Some of my students are working closely with Schlotzsky's Restaurants; we' re helping them understand the technical issues of public wireless LAN deployment around the country. My students are measuring data in restaurants, working with Schlotzsky's IT professionals to design hot spots. Other students are working on theoretical research for a whole host of topics, such as ad hoc network or power conservation, MIMO technologies and simulators for future wireless standards.

Q: What is the most significant development coming out of the group today?

A: There are a number of significant developments. Professor Robert Heath has a Ph.D. student named David Love who has made some fundamental contributions to the field of MIMO antennas. Also, our researchers have developed new algorithms and software tools that work with National Instrument's Labview software. National Instruments is one of our industrial affiliate sponsors. Our students have developed modules that work in Labview that do complex



state-of-the-art simulation of wireless system performance.

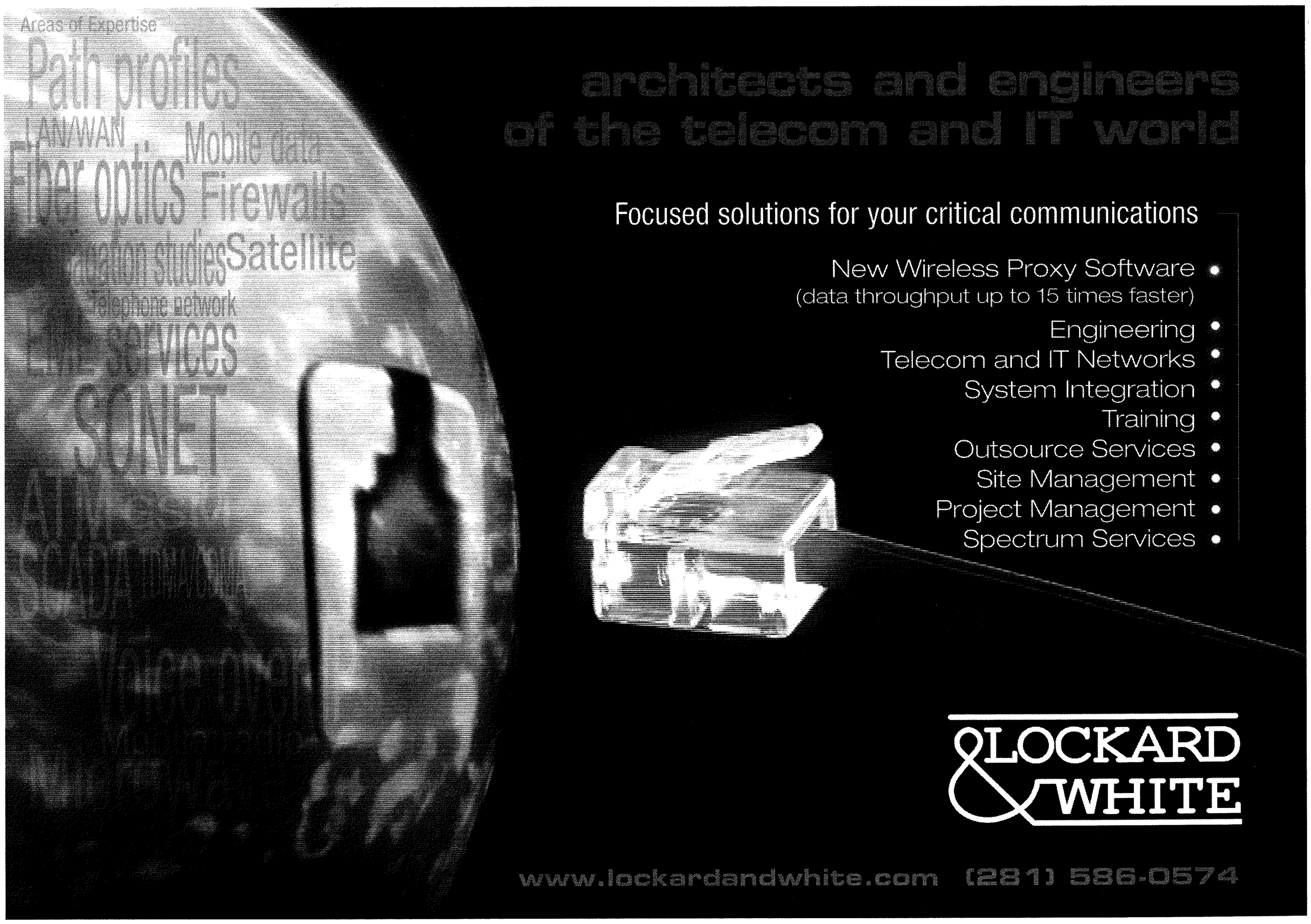
We've also built a test bed that will actually simulate and emulate large network performance on a series of parallel computers, and we're continuing that work with the National Science Foundation funding and with researchers at Virginia Tech. Professors Sanjay Shakkottai and Jeff Andrews are brand-new faculty that have made a big impact in only their first year as professors. The faculty members here are terrific, brilliant and fun to be around.

Q: When students end their education at the WNCG, do many stay with you or do they go on to teach at other universities or enter the private sector?

A: That's an interesting question. I've been in start-up mode for the last year getting our center up and going, and I made it a point to graduate all my students at Virginia Tech before I left because I wanted to make sure they all got jobs before the other shoe fell in the telecom industry. All but two of my students went into industry, and the others became professors at major universities (one in the United States and one in Brazil). Right now, I'm just now building up my own research group, and instead of doing much advising, I've had to focus on building the WNCG infrastructure and hiring staff and helping to recruit and mentor some of the younger faculty. Since our center is so new, we really don't know where our students will be going, but one thing is certain: they will possess a tremendous amount of skills and awareness of the key issues that will impact future wireless networks, and I am certain they will be the leaders of the next phase of the wireless industry.

Q: Have you seen an increase in the number of engineering students who are choosing wireless-based studies? Is wireless the new hot thing?

A: Computing networking, computer engineering and wireless communications still are very hot. At the



University of Texas, which is the largest public university in the country, communications and computing are the hottest areas by far in our Electrical and Computer Engineering department.

Q: Has there been a marked increase in the number of women getting involved?

A: Despite efforts throughout the country, unfortunately not. We need more women engineers, and we need to increase the diversity of wireless engineers. I see this as extremely critical. If you look at the workforce numbers during the next 10 to 20 years, it's vital that we get more women and minority students into undergraduate and graduate programs. I also believe it's also very important for the telecommunications industry in the United States to encourage more of our best students to pick engineering in the first place.

I only have anecdotal evidence, but it seems like U.S. students just out of high school are choosing engineering as a career path less and less. This worries me, because communications infrastructure is so vital to the economic vibrancy and security of the United States. I think the telecom bubble may have taken the luster off engineering, particularly in communications as a career path. I fear that if we don't get that shine back, it will be difficult to fulfill the workforce requirements 10-20 years from now.

Q: Besides the two universities with which you've been associated, how many colleges today are ramping up a wireless program?

A: There are a number of them. Some 15 or 20 of them have some center or research focus on wireless communications. When I say a "center," I mean a critical mass of faculty and students. However, I do know that hundreds of universities are teaching courses, usually at the graduate level but some at the undergraduate level, in wireless communications and networks. In the last five years or so, wireless communications has become a key course offering in most U.S. graduate programs and in some undergraduate engineering programs. Now, computer science as well as ECE programs are teaching wireless.

Q: Does the United States have the best programs in the world, or do other countries have a jump on us?

A: There are some terrific programs worldwide, and there are some terrific programs stateside. I think the programs in Asia and Europe have terrific faculty and student participation, and they get a good deal of help from their federal governments as well as from industry. I think there's a very symbiotic relationship between research and development with universities, companies and government in Europe and Asia. Government is more involved in Europe, because that's how the European Community had built its wireless research core; they've made it a federal mandate with hundreds of millions of dollars distributed among companies and universities.

In the United States, however, things are more individualistic. Different university models work in different ways. In this country, it's been left up to agencies with relatively small budgets - like the National Science Foundation and, in years past, DARPA — to fund this mission. There's much less government money spent on the field.

According to Dr. Rappaport, the future is going to be ad hoc networks, software radios and distributed infrastructure.

If you look at how the Internet was formed, it was based on fundamental research funded by DARPA and the National Science Foundation. Due to this focus, the United States was able to build the core competencies and talents that led to the worldwide Internet. There are dozens of companies in the telecommunications space that can attribute their success to the early government research funding at universities by DARPA and National Science Foundation. Today, however, you don't see this kind of focus in the United States, and you haven't seen it since the inception of the cellular industry. It's just the way the United States works. U.S. policy encourages the entrepreneurial, make-it-happen kind of market, whereas in Europe, there is more block funding and more government funding for economic-development priorities for the continent. Today, I worry about the few number of U.S. graduate students going into research careers. More and more, we are educating foreign students who are taking their knowledge back to their home countries. In 20 or 30 years, there will be a real level playing field for resources, talent, and innovation across the globe.

Q: Is there the fear of too much government involvement in science and academia?

A: No, I don't think that's it. In fact, I think the U.S. government needs to do much more to build the reservoir of U.S. students in engineering leadership positions and to maintain the U.S. lead in communications innovation and invention, if for no other reason than for a security/defense reason. This will require retooling how U.S. high schools and junior high schools teach math and science. U.S. government policy has traditionally not paid as much attention to the communications research infrastructure as do governments in Europe. If you look at the worldwide acceptance of GSM, you can attribute that directly to the efforts of the pan-European community and the government funding put forward to develop that standard in the 1980s. If you look at the United States, such pioneering companies as Qualcomm were able to create a standard with little, if any, government backing.

I think the United States needs to raise its awareness of the communications industry and the future of research and development in wireless communications. You can ask yourself today "where is the next Internet going to come from in the current U.S. research environment?" You have the tremendous layoffs at Bell Labs. You have telecommunications companies in the United States suffering from the terrible telecom bust, and they can't afford to pay for research anymore. Its not allowed since Wall Street does not value it (except in the Pharma sectors).

You have an installed telecommunications base in this country that is vital to our future, but where are the nuggets of ingenuity going to come from in the United States to keep the U.S. leadership that we've enjoyed with the Internet? I think that's a fair question to ask, and I think universities more and more are going to be required to develop this technology and knowledge. And furthermore, other countries in the world are developing a critical mass of knowledge and talent, and I think the United States needs to pay attention to its research future.

Q: What's on your front burner right now?

A: We have a world-class technical and business program starting in October, which will make the University of Texas a wireless melting pot for the whole industry. This wireless networking program, set for Oct. 22-24, is a new program I've launched here, and it will be an annual event. We have some of the world leaders in business and technology coming, including founders of major success stories like LCC, Aetheros, and XM Satellite Radio; Raj Singh, the founder of a number of wireless companies; and Mike Marcus, the FCC engineer who pioneered the concept of unlicensed spectrum, which is where Wi-Fi works. The program includes a large cast of dignitaries, and business and technology leaders who are willing to spend a few days in Austin this October. It also is a chance for us to get academics together with business leaders and technologists to put a finger on the pulse of the future of wireless. It will be a grand affair, and we will show case the Texas State Capitol and the Bob Bullock Texas Museum, which is an amazing place like no other.

Q: What can the Radio Club of America do to push more interest in RF communications programs?

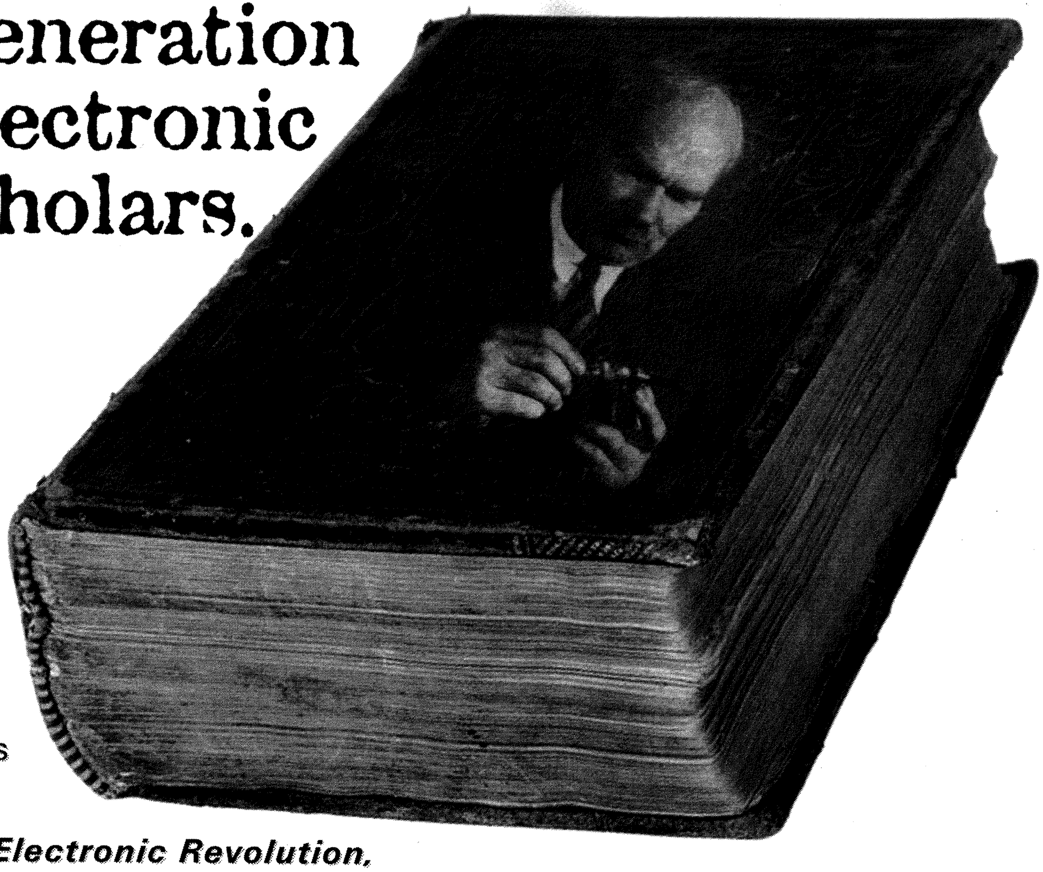
A: I think we have to get to the students in high school. I really think we have to excite them about wireless, about computers and about networks. They're users of computers and wireless, but it's almost taken for granted and it's almost made us lazy, as a country. We need to get kids to think about the critical skills needed to make the next generation of networks, and the next generation of computers and applications.

The National Science Foundation has a program geared toward trying to help K-12 teachers and teachers at community colleges to learn more about technology. While it's a tiny program within NSF, these kinds of programs are going to become more and more critical to keeping our engineering workforce in place. The Radio Club does a great job with scholarships - they changed my life when I was a student - and I would encourage the club to really grow this effort and make a national splash, perhaps teaming with NSF or GWEC, or other national wireless organizations.

Being able to make software and hardware do what you want it to in a wireless context is the future of our industry, and we need students going to college excited about learning those skills. I'm afraid our technology is becoming so much of a commodity that it is taken for granted, and we need some big, grand thinking in order to keep our talent pool coming through the universities in the United States.

Lee DeForest and his invention of the
Electronic Tube Amplifier gave birth to modern electronics.

Maurice Zouary will raise the next generation of electronic scholars.



Maurice Zouary,
Life Memberof the
Radio Club of
America, will donate
a portion of the proceeds
of his latest book,
DeForest-Father of the Electronic Revolution,
to the Radio Club to establish
a DeForest Grants-In-Aid Fund.
The book, published by 1stBooks, can be
purchased as an ebook
from **www.1stbooks.com.**

Ja, JABOS

By an unknown author, modified by C. P. (Pat) West

The June sun touched the treetops,
moved down over scarred fields, and cast
long shadows behind the farmer and his plow.
His shoulders dropped despondently inside his
Wehrmacht uniform, tiredness mirrored
in the slow plod of his aging horse.
A pale boy of four scrambled beside
them, a thin shadow lost in the furrow.
At the end of the field, they passed
a jumbled pile of masonry and steel.
Rubble lay below the chipped face of the
emplacement. Vines climbed the sides
of the pillbox, thrusting green fingers through
the gun slots, and over the cratered dome.
The farmer stared at it dully, unbelieving.
His thoughts centered on Africa, and the
Afrika Korps, and other pill boxes at El Alamain.
The boy put his hand on his father's sleeve.
"JABOS, daddy?"
The farmer nodded.
" Ja, JABOS."

How The Norden Bombsight Helped Save The 'Lost Battalion'

By C. P. (Pat) West

In the European Theater during World War II, the Germans feared our P-47 fighter-bombers, referring to them as "JABOS." The acronym stands for "Jager (fighter) bombers." Many of the highways the Germans used in France were dotted with "ACHTUNG JABOS" signs to alert vehicle drivers of a potential danger. This article tells the story of an unusual use of P-47 fighter-bombers assisted by men, communications, the SCR-584 radar and, perhaps, the Norden Bombsight, which all teamed in one effort to drop food to a lost battalion.

The SCR-584 radar (see Figure 1A) played a significant role in this event. The radar antenna pedestal is shown in Figure 1B, and the radar rectifier cabinet is shown in Figure 1C. The radar operator control position is shown in Figure 2.

This 10-centimeter radar was developed to point artillery at airborne enemy targets (see Figure 3). In England, it was successful in downing many of the German V1 missiles. A SCR-584 radar first was modified at Anzio in Italy for air surveillance and the guidance of aircraft. In France, these radars were used for guiding aircraft on close air support and bombing missions under poor weather conditions. The 6-ft.-diameter antenna could scan 360 degrees at 5 revolutions per minute. It had a search range of about 40 statute miles, and it could automatically track aircraft out to about 20 statute miles. The technical characteristics are provided in Table 1.

Many experts believe that this radar type changed the course of WWII in favor of the Allies. More than 700 SCR-584s were built during the war. With the radar's abilities in gun-laying and antiaircraft at their disposal, the Allies were unstoppable. The SCR-584 virtually stopped the V1 "Buzz Bomb" bombardment of England, with a better than 90 percent kill ratio (Ref. 6). Its accuracy made it a prime candidate for control of fighter-bombers on attack missions during overcast weather.

The Vosges Mountains campaign in Eastern France was one of the most difficult of the war. The heavily forested area presented many problems to the military forces involved in this campaign. At the time of the event, I was the Communications Officer for Control Center 2. We were operational in the vicinity of Haute Biol, France, and our primary mission was to monitor operations as backup to the main operations center: Control Center 1, located at Dole, France. I was familiar with the following incident, and at that time knew that the SCR-584 radar also was equipped with a Norden Bombsight during that particular food drop mission.

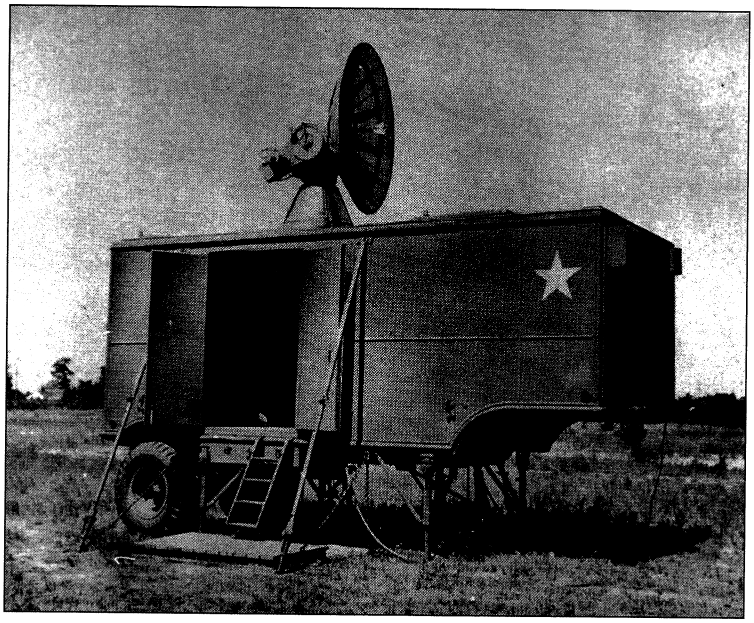


FIGURE 1A: SCR-584 RADAR. This radar type was first modified at Anzio, Italy, for air surveillance and for the guidance of aircraft. In France, it was used for close air support missions and for aircraft guidance during poor weather conditions. Note the long poles used to stabilize the trailer. For transport, the 6-ft.-diameter antenna was lowered into the trailer. Photo courtesy of Steve Bragg.

The Alamo Regiment

The 141st Infantry Regiment, which fought in the Vosges Mountains, was referred to as the "Alamo Regiment," because most of the troops had come from San Antonio, Texas. One of its battalions was referred to as "The Lost Battalion;" the 1st Battalion of the 141st Infantry Regiment of the 36th Infantry Division was trapped in the vicinity of St. Die, France. The Germans had thrown up a strong roadblock, cutting the battalion off from the rest of the regiment. For six days, the trapped foot soldiers existed on what rations they had available, probably mostly "K," "C" and "D" type rations. The K rations were packed in waterproof packages, like Cracker Jack, the C rations were cans of food, and the D rations were special chocolate-like candy bars. Due to the emergency situation, radio requests were sent for food and medical supplies (Ref. 2).

Division headquarters contacted its support artillery and had them fire chocolate bars, probably "D" rations, wrapped in propaganda leaflet shells. However, chocolate bars were not enough. The Air Corps forward controller was contacted, apprised of the situation and asked if the fighter-bombers could make a food drop in the area. On Oct. 28, 1944, P-47 fighter-bomber pilots of the 371st Fighter Group, under control of the 64th Fighter Wing, loaded their aircraft with food, medical supplies and ammunition.

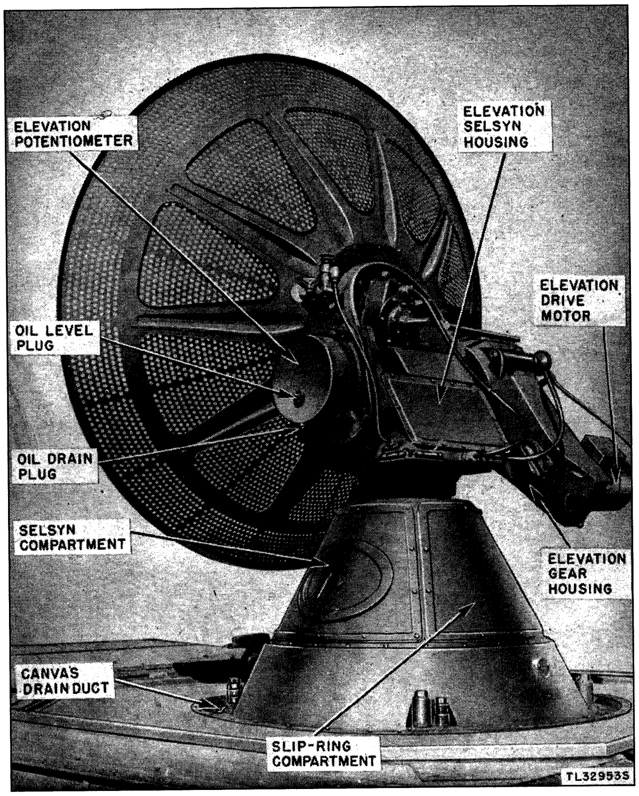


FIGURE 1B: SCR-584 RADAR ANTENNA. This huge 6-ft.-diameter antenna pointed a pencil-like beam at targets. The antenna could cover 360 degrees in search mode at five revolutions per minute. At lock-on, it could automatically track a target out to about 20 miles. Photo courtesy of Steve Bragg, taken from Preventative Maintenance Manual, March, 1946.

Technical Characteristics of the Radio Set SCR-584()

Wavelength	10 centimeters	
Frequency	Four bands around 3,000 megahertz	
Magnetron	2J32 ()	
Peak Power Output	250 kilowatts	
Pulse Width	0.8 microseconds	
Pulse Repetition Frequency	1,707 pulses per second	
Antenna Diameter	6 feet	
Beam Width To Half Power	4 degrees	
Maximum Range:	PPI Search	70,000 yards (39.7 statute miles)
	Auto-Track	32,000 yards (18.2 statute miles)
	Potentiometer Data (artillery control)	28,000 yards (15.9 statute miles)
Minimum Range	Between 500 and 1,000 yards	
Lower Elevation Limit	-175 mils (-9.8 degrees)	
Upper Elevation Limit	+1,580 mils (+88.9 degrees)	
Azimuth Coverage	360 degrees	
Azimuthal Scan Rate in Search Mode	5 revolutions per minute	
Range Error	25 yards	
Azimuth Error	1 mil (0.06 degree)	
Elevation Accuracy	1 mil (0.06 degree)	
Power Requirements	115 volts, 60 hertz, 3-phase, 10kVA maximum (without IFF)	

The SCR-584 is built into a K-78 trailer. Its gross weight is 10 tons; its overall length is 19.5 feet; its width is 8 feet; and its height is 10 feet, 4 inches.

Source: U.S. War Department technical manuals TM11-1324 and TM11-1524 (U.S. Government Printing Office, April 1946)

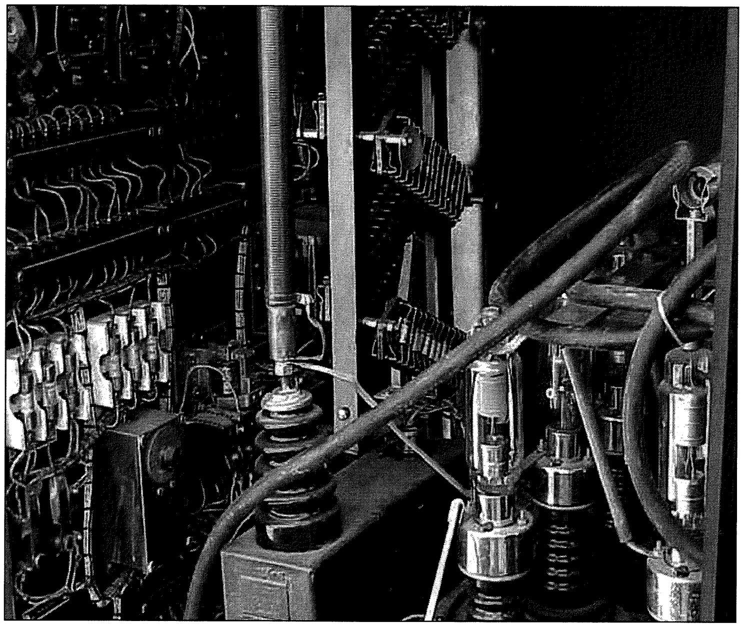


FIGURE 1C: SCR-584 RADAR RECTIFIER CABINET. This unit provided high voltage to the transmitter to produce the 250-kW, 0.8-microsecond RF pulse to the antenna. There were 1,707 pulses per second. Photo courtesy of Steve Bragg.

It was a foggy day. A ground haze and low clouds enveloped the countryside, draped a blanket of cold around the doughboys trapped near St. Die. It was a poor day for flying, especially for the type of accurate bombing required if the food and medicine were to be dropped on the correct pinpoint. The P-47s rolled down the runway, gathered speed, hurtled into the air and flew swiftly to the vicinity of Xertigny, a village northeast of Dijon. During peacetime, the villagers specialized in the manufacture of cheese, other dairy products and beer. Forward Sector Operations One (Ops 1) also was located in Xertigny, and it served as an extension of Control Center 1, located near the front lines. Beer lovers from Ops 1 found a dream situation, for the Ops 1 personnel were billeted in a brewery, where kegs stood all about. White-foamed French beer flowed generously.

These troops provided direct support to the 36th Infantry Division for the food drop. The aircraft checked in on VHF (Very High Frequency) radio with the Ops 1 controller, Capt. Lee Jordan (a typical P-47 combat flight is illustrated by Figure 4. P-47 aircraft specifications are provided in Table 2). Capt. Jordan's instructions to the aircraft were brief. Because of overcast skies, the first drop would be made by a SCR-584 radar assisted by an L-5 aircraft and SCR-575 Direction Finder (D/F} fixes from Ops 1. These D/F stations normally were referred to as "fixers." Figure 5 shows an SCR-575 DF fixer station.

Several SCR-575 D/F fixers checked into Ops 1 via wire circuits, and VHF and HF radios. At Ops 1, a table map showed the location of each station. In the days before high tech, strings, each approximately four feet long, were connected at each D/F station location on the map, and a compass rose also was at each station location. Azimuth reports from the D/F stations were provided to each string operator, who would stretch his string out at the reported azimuth bearing. The folks who communicated with the D/F stations, and handled the strings were often referred to as "String Pullers" (Ref. 3). The location, or "fix," of the aircraft would be where the strings crossed on the map. Capt. Jordan would pass this location on to the controller at the radar station.

The controller at code name Alabama, which also was the radio call sign for the SCR-584 radar, worked with the Ops and directed the aircraft on the first attempt. As Gardner Friedlander points out in his memoirs, the controllers at the radars were all experienced pilots (Ref. 4). As the fighter pilots flew on their target runs, they noticed that the visibility seemed slightly improved. The instructions from the SCR-584 radar controller came over VHF, and the flight leader

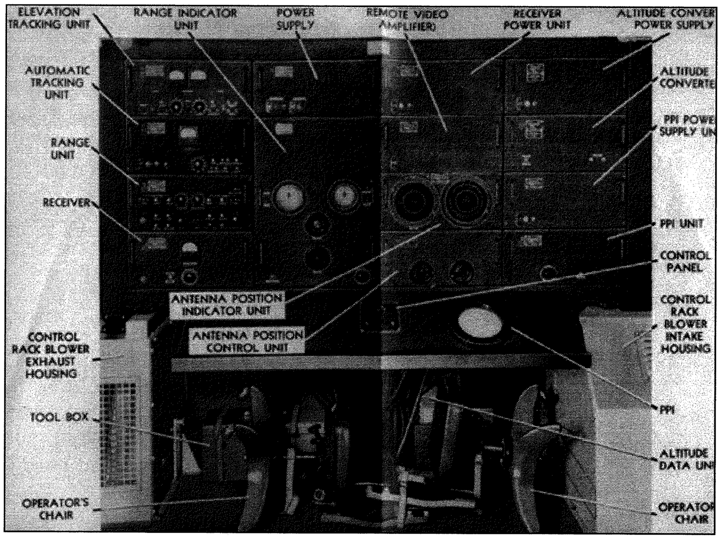


FIGURE 2: SCR-584 RADAR CONTROL POSITIONS. Note operator chairs in stowed position for transport. Note also the small Plan Position Indicator (PPI) Cathode Ray Tube (CRT). Photo courtesy of Kate Marks Persinger, director, Historical Electronics Museum, Baltimore, Md., from a radar technical manual.

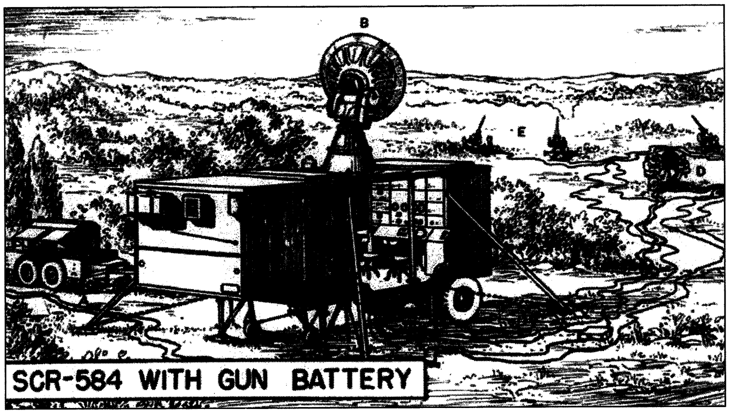


FIGURE 3: SCR-584 RADAR WITH GUN BATTERY. Items in the photo are identified as follows: A. Power Generator, M7; B. Radio Set, SCR-584; C. Gun Director, M9; D. Tracker for Director, M9; E. Anti-aircraft Artillery 90 mm battery. The radar was designed for this gun-laying application. It had a search range of about 40 statute miles, and it could automatically track aircraft out to about 20 miles. Artist sketch is from a World War II LIFE magazine.

called back corroborative descriptions of the terrain passing beneath him. At the precise moment, according to his calculations, the controller gave the signal - "bombs away." Food and medicine parachuted to the earth below. From his P-47 airplane, the flight leader called for another flight in case the first drop was not successful.

The Second Mercy Mission

A radio report came from the stranded battalion. The food and medical supplies had landed 400 yards away from the soldier. Because the enemy was watching their every move during the daytime, the U.S. troops could pick up the supplies only during the night.

A second mercy mission was dispatched. This time, visibility was very poor, and the SCR-584 radar again directed the mission with no outside assistance. A slight wind had sprung up. The controller carefully ticked off the miles as the aircraft made their run. He feverishly watched his radar scope and plotting board. Once again, he gave the signal, "bombs away." Unfortunately, the wind intervened for the enemy. The supplies were carried too far away from the surrounded battalion to be picked up under any conditions.

A third mission took off with the same flight leader who had led the first. The weather was favorable, with visibility better than before. The haze and clouds had cleared so the pilots could see the ground below and the flight leader was able to make the final drop visually. Food and medicine was parachuted to the hungry men below. A 36th Division radio unit picked up a walkie-talkie report from the trapped battalion: "Thank our pals in the Air Corps. We eat for the first time in three days."

The following day, the Japanese-American 442nd Combat Team fought its way through to the beleaguered battalion. This team was organized March 23,

P-47 Aircraft Specifications

This fighter was known affectionately as "JUG," and it was the heaviest, most destructive single-engine aircraft used during World War II. It was used primarily for aerial combat and for close ground support.

Designer	Alexander Kartveli
Manufacturer	Republic Aviation Corporation
First Flight	May 6, 1941
Total Number Built	15,683
Wing Span	40 feet, 9 inches
Length	36 feet, 2 inches
Gross Weight	More than 10 tons
Power Plant	Pratt & Whitney R2800, turbo-supercharged, 18-cylinder, air-cooled radial engine rated at more than 2,000 horsepower
Armament	8 Browning 50-caliber, wing-mounted machine guns along with more than 2,000 pounds of other types of ordnance

WWII Combat Record:	
Enemy aircraft destroyed	11,874
Enemy vehicles destroyed	160,000
Enemy trains destroyed	9,000

Source: Thunderbolt Pilots Association

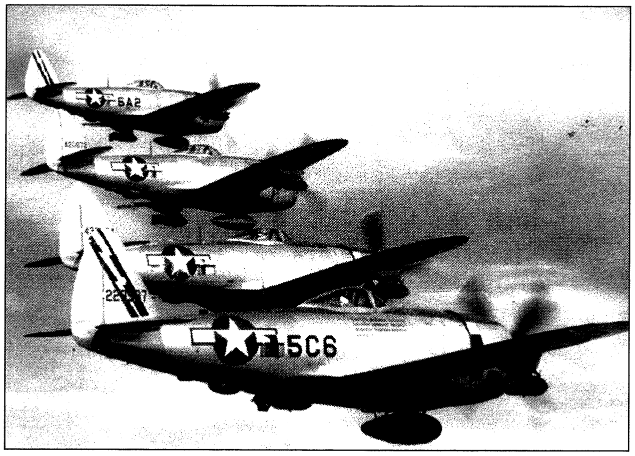


FIGURE 4: P-47 AIRCRAFT ON A TYPICAL MISSION DURING WORLD WAR II. The P-47 was named Juggernaut, and it bore the nickname "JUG" to reflect the durability and strength of the aircraft, which was said to be capable of out-diving anything in the skies. In addition to bombs, air-droppable fuel tanks were carried. If modified, they could be used to drop ammunition, radios, batteries, water and rations to friendly ground forces. Photo courtesy of U. S. Air Force Air Combat Multimedia Gallery.

1943, and more than 12,000 Japanese-American volunteers responded to the call. They trained at Camp Shelby in Mississippi (the same place the author trained in 1941), and their first assignment was with Gen. Mark Clark's Fifth Army in June, 1944, where they engaged the Germans south of the Arno River in Italy. They used the battle cry "Go For Broke," and they earned the honor and distinction of being the most decorated unit of its size and length of service in battle in U.S. military history (Ref. 5).

A barrage of machine gun fire and mortars from the Germans on the hilltop rained hot metal and splinters down on the 442nd, taking them out in droves. The incident at St. Die finally was over, but the 442nd suffered more than 800 casualties, including 100 killed in the process of rescuing approximately 200 marooned Texans (Ref. 5).

Memoirs prepared by Gardner Friedlander, who commanded a signal-corps company that operated several SCR-584 radars, pointed out that these radars had been equipped with the Norden Bombsight (Ref. 4) (see Figure 6). The mission report contained in the 64th Fighter Wing History does not mention use of the bombsight, because it was considered a part of the radar station. Capt. Jordan probably used the Norden Bombsight's wind and drift calculator as an aid in guiding the mission aircraft. It also appears that it took both a visual sighting and the SCR-584 radar to put the food close enough so the troops on the ground could recover it.

The Eggbasket

Later on, the Norden Bombsight was used extensively during the campaign in France. A procedure known as the "eggbasket" was developed, made possible by the SCR-584 radars. Laid out on a plotting board at the radar would be two or three tentative "eggbaskets," towns with strong points in them like marshaling yards, railroad stations and ammunition or supply dumps. Usually an eggbasket was handled by a SCR-584 controller. If fighter-bombers discovered they could not see the target they were trying to bomb or if the weather was so closed in they could not see the ground at all, they called the Corps Forward Control or Forward Sector Operations to ask for an eggbasket. The controller would give the flight leader of the fighter-bombers a vector to get him in the vicinity of the eggbasket.

Once the fighter-bombers were in position, the controller functioned as their bombardier. He used the standard instruments a bombardier would use on a heavy or medium bomber aircraft, including the Norden Bombsight's wind and drift calculator. He always knew the exact location of the aircraft on an eggbasket mission, and trained operators followed the flight on the SCR-584 scope.

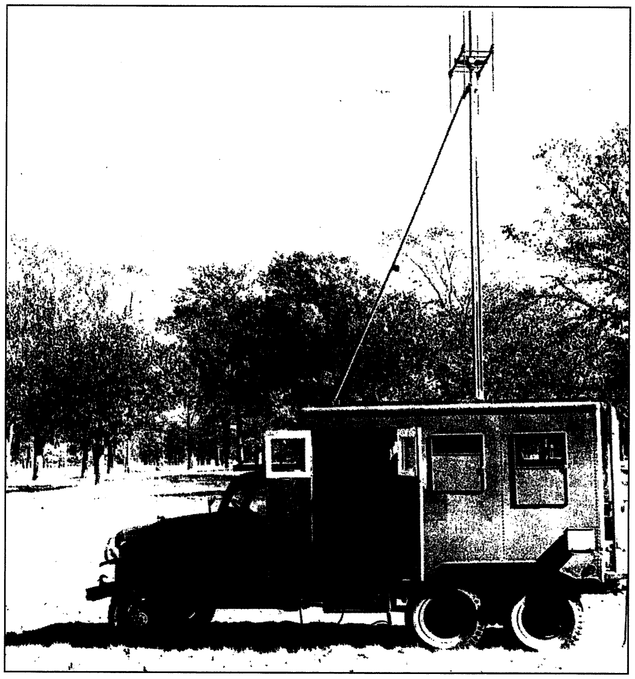


FIGURE 5: SCR-575 DIRECTION FINDING SET. These radio-receiving sets were located at high elevations. Reports from two or more sets were used to locate airborne aircraft by triangulation. Plotters, who used strings at a control center to locate aircraft on a map, were identified as "string pullers." Photo from the SCR-575 technical manual.

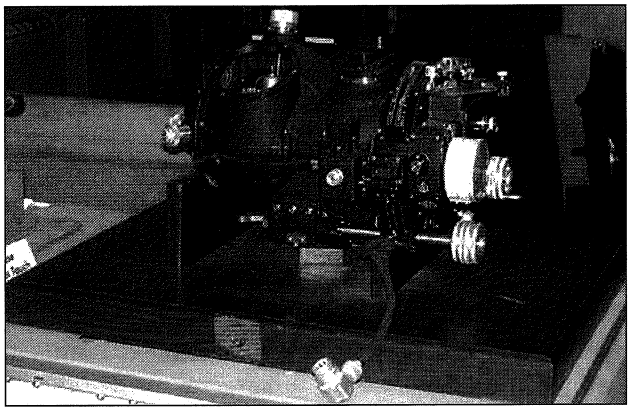


FIGURE 6: NORDEN BOMBSIGHT. Although this equipment normally was used in heavy bombers during World War II, a use was found for these units in France, installed in SCR-584 radar sets on the ground. A controller used information provided by the radar and the bombsight to guide fighter-bombers to targets during foul weather. Photo courtesy of Ed Thelen and The Computer History Museum, Mountain View, Calif.

Because the controller had laid out the target run beforehand, he had only to direct the fighter-bombers by giving them a series of vectors to the spot where the bombing run would begin. Then, through a stopwatch check, he followed them on the run, giving a call as they passed through each two-mile marker on a course laid out on his plotting board. If there was wind, he calculated the drift and allowed for it in the run. As the echoes on the radar scope indicated the planes were over the target, the controller gave the voice radio command, "bombs away," and another eggbasket was completed.

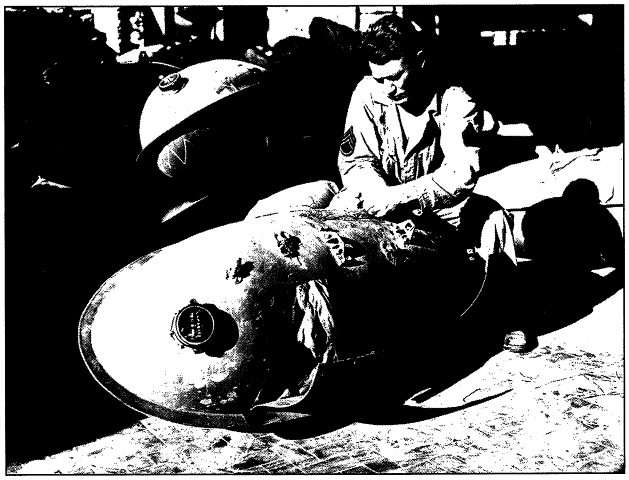


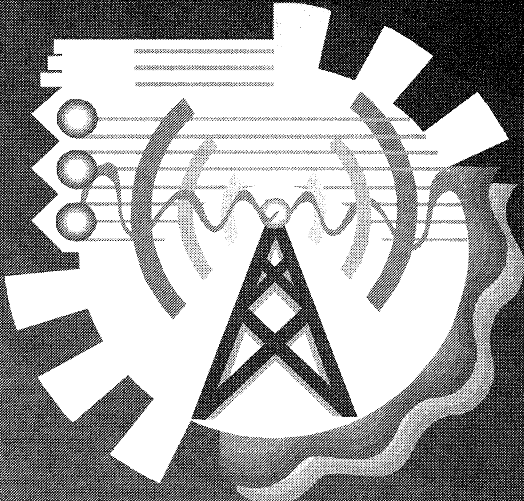
FIGURE 7: MODIFIED DETACHABLE FUEL TANKS. A detachable fuel tank is shown, modified to drop supplies to friendly troops. Records reveal that parachutes were used to drop rations to the lost battalion. The author was unable to obtain details on how this was accomplished. Photo courtesy of Quartermaster Corps Museum, Fort Lee, Va.

Another element not covered was how material was dropped from the P-47 aircraft. I suspect that special bomb- like containers were used, fastened to release mechanisms on the aircraft's wings or fuselage belly. Figure 7 shows a detachable fuel tank that has been modified to drop supplies to friendly troops. Two full cases of K rations or five cases of D rations wrapped in a piece of salvage blanket and bound with wire straps could be loaded in a single tank. The wired blanket combination then was enclosed with a section of canvas, which again was wired. These packages were then placed in a tank and insulated against shock with waste material pushed into the blank spaces. The tank then was sealed with duct-tape-like material to prevent cracking by air pressure during flight. The best height from which to drop a belly tank was about 50 feet (Ref. 7). The 64th Fighter Wing History says parachutes were used on the drop to the lost battalion. [Editor's note: The author was unable to obtain details on how this was accomplished. The quantity of aircraft used for each mission was also not disclosed.]

About Our Author: *C. P. (Pat) West is a Fellow of the Radio Club of America, an IEEE Senior Member and a retired Boeing engineer. He was involved in nine campaigns, including five beachhead invasions, during three years of service during World War II in the African/European Theater. He served as a radar station commander in Africa and Sicily; as a communications officer in Italy and France; and as a signal officer of the Air Corps 64th Fighter Wing, Control Center 2 in France. The majority of the data for this story was obtained from the 64th Fighter Wing History (Ref. 1) and the writer's personal knowledge of the food-drop incident. He left the service with the rank of captain in 1946.*

References:

1. "History of the 64th Fighter Wing," Lt. Col. Edward C. Danford, editor. Printed in Tubingen, Germany, July, 1945.
2. The 141st Infantry Regiment, 36th Infantry Division, "Forging the Vosges," (http://www.kwanah.com/txmilmus/).
3. "The String Pullers," by C. P. West, Radio Club of America Fall Proceedings, 1999.
4. "The Early Days of RADAR: Secrets and My Recollections of World War II," by Gardner L. Friedlander (http://freepages.military.rootsweb.com/~memoirs).
5. "442nd Regimental Combat Team," by GO FOR BROKE Educational Foundation (http://santacruzpl.org/ history/ww2/goforbroke.shtml).
6. "The SCR-584 Radar Tribute Page," by Steve Bragg, KA9MVA, (http://hamhud.net/darts/scr584.html).
7. "Aerial Delivery of Supplies," by Maj. Raymond C. Altermatt, QMC, The Quartermaster Review, September-October, 1945.



INDUSTRIAL COMMUNICATIONS COMPANY

Charles F. Adams, President
Authorized Dealer - Sales & Service

121 N. Sitgreaves Street
Easton, PA 18042-3697
Phone: (610) 253-1214
Fax: (610) 253-4504
Email: *cadams1214@aol.com*

IC

TWO-WAY RADIO SALES & SERVICE
LTR and Conventional UHF Service Provider

INFORMATICA

Donald Christiansen, P.E., F.I.E.E.E., President and Principal

434 West Main Street
Huntington, N.Y. 11743
Tel: (631) 423-3143
Fax: (631) 385-4940
Email: *donchristiansen@ieee.org*

■■ INFORMATICA ■■

CONSULTING IN THE COMMUNICATION ARTS

DETTRA COMMUNICATIONS, INC.

John E. Dettra, Jr., President

7906 Foxhound Road
McLean, VA 22102-2403
Phone: (703) 790-1427
Fax: (703) 790-0497

CONSULTING ENGINEERS

SCOREBOARD

John Arpee, CTO, Founder
13595 Dulles Technology Drive, Suite 200
Herndon, VA 20171-3424
Phone: (703) 713-3022
Cell: (703) 623-9040
Fax: (703) 713-9766
Email: *jarpee@scoreboardinc.com*
Web Site: www.scoreboardinc.com

ScoreBoard

PEAK PERFORMANCE FOR THE MOBILE INDUSTRY

DALEY & ASSOCIATES, INC.

William J. Daley, President
23480 Park Sorrento, Suite 2008
Calabasas, CA 91302
Phone: 818-716-7777
Fax: 818-225-1509
Email: *wdaley@ix.netcom.com*

DALEY & ASSOCIATES, INC.
EMERGENCY COMMUNICATIONS SPECIALISTS

EMERGENCY COMMUNICATIONS SPECIALISTS

DORR ENGINEERING SERVICES, INC.

DESI

Barry L. Dorr, P.E., Consulting Engineer
120 North Pacific Street, Suite K-9
San Marcos, CA 92069
Phone: 760-510-1835
Fax: 760-510-1809
Email: *bdorr@dorrengineering.com*
Website: www.dorrengineering.com

COMMUNICATION SYSTEM DESIGN, RF MODEM DESIGN, DIGITAL SIGNAL PROCESSING, AND AUDIO

BIX TECH LLC

J. M. "Bix" Bixby
457 West Middle Road
Lykens, PA 17048
Phone: 717-365-4081
Fax: 717-365-4083
Email: *bix@bixtech.com*

Bix Tech LLC

AM ANTENNA SYSTEM - DESIGN, CONSTRUCTION AND MEASUREMENTS

DANIELS ELECTRONICS LTD.

Terry Daniels, President
43 Erie Street
Victoria, B.C. V8V 1P8
Canada
Phone: (250) 382-8268 Ext. 222
Fax: (250) 382-6139
Toll Free: 1-800-664-4066
Email: *Sales@danele.com*
Web Site: www.danelec.com

DANIELS ELECTRONICS LTD.

RADIO COMMUNICATION MANUFACTURER

TELCO COMMUNICATIONS INC.

David A. Ehehalt, President
P. O. Box 468
Mt. Freedom, NJ 07970-0468
Phone: 973-895-5500, 800-345-5538
Fax: 973-361-on request

TELCO COMMUNICATIONS INC.
A TOTAL COMMUNICATIONS ORGANIZATION

CELLULAR MOBILE TELEPHONES, RADIO PAGING SYSTEMS, TWO WAY RADIO SYSTEMS, COMMUNICATIONS REPEATERS, COMMUNICATIONS CONSULTING, TELEPHONE SYSTEMS & EQUIPMENT

WIRELESS MARCOM LLC

Maxine Carter-Lome & Bob Chapin
P.O. Box 388
S. Egremont, MA 01258
Phone: 413-528-0813
Fax 413-528-1348
Email: *Maxine@wirelessmarcom.com*
Website: www.wirelessmarcom.com

MARKET RESEARCH & MARKETING COMMUNICATIONS

MAXRAD, INC.

Steven L. Deppe, Chief Executive Officer
4350 Chandler Dr.
Hanover Park IL 60103-6763
Orders: (800) 323-9122
Phone: (630) 372-6800
Fax: (630) 213-7508
Email: *steve.deppe@maxrad.com*
Website: www.maxrad.com

MAXRAD®
STATE OF THE ART ANTENNAS

STATE OF THE ART ANTENNAS

DIGITAL AND ANALOG WIRELESS FACILITIES

Gary Eisenberg
Phone: 831-373-7742 **Direct Office,**
831-384-3375 **Direct Shop,**
Cell CA: 831-601-9790
Cell NY: 917-847-6500
Fax: 831-646-0595
Email: *rfsites@aol.com*

Digital and Analog Wireless Facilities

COMMUNICATIONS PLANNING

PMC ASSOCIATES

Phil Casciano
9 Westlake Court
Somerset, NJ 08873
Phone: (732) 563-0366
Pager: (732) 603-1900
Email: *philc@pmcreps.com*

P•M•C
ASSOCIATES

MANUFACTURERS' REPRESENTATIVES SERVICING THE COMMUNICATIONS INDUSTRY

AC VIDEO SERVICES

Andy Conte
113 Mapes Ave. • Nutley, NJ 07110
Toll free: 800-710-8804
Phone: 973-661-1976
Fax: 973-667-3458
Email: a2dj@aol.com
Website: www.takeonenetwork.com/acvideo

AC VIDEO SERVICES

VIDEO DUPLICATION, FORMAT CONVERSIONS, DVD & CD ROM, VIDEO PRODUCTION INTERNAITONAL CONVERSIONS, TAPE REPAIR LEGAL VIDEO, EDITING, MOVIE SLIDE TRANSFERS

CTA COMMUNICATIONS

Nicholas W. Diamond, Vice President
20715 Timberlake Road, Suite 106
P. O. Box 4579
Lynchburg, VA 24502
Phone: 434-239-9200
Fax: 434-239-9221
Email: *ndiamond@ctacommunications.com*
Website: www.ctacommunications.com

CTA COMMUNICATIONS

ACRE ENGINEERING SERVICES, LLC

Robert I. Elms, P.E., President

72 Smithtown Road
Budd Lake, NJ 07828
Phone: 973-347-9300
Fax: 973-347-4474

ACRE
ENGINEERING SERVICES, LLC

RF SYSTEM DESIGN & SITE SAFETY ANALYSIS

TELE-MEASUREMENTS INC.

William E. Endres, President
145 Main Avenue
Clifton, N.J. 07014
Voice: (973) 473-8822 • (800) 223-0052
Fax: (973) 473-0521
Email: *tmcorp@aol.com*
Web Site: www.tele-measurements.com
Teleconferencing: (973) 773-1102

TELE-MEASUREMENTS INC.
Communications Systems Equipment & Service

VIDEO-VOICE DATA SYSTEMS, PRESENTATION–DISTANCE LEARNING–VIDEOCONFERENCING

ANDREW CORPORATION

Robert "Scott" Harvey, Senior Account Executive
1320 Central Park Blvd., Suite 238
Fredericksburg, VA 22401
Phone: (540) 786-6009
Fax: (540) 786-6679
Cell: (540) 379-0802
Email: scott.harvey@andrew.com

ANDREW®

WIRELESS INFRASTRUCTURE SYSTEMS

KAHN COMMUNICATIONS INC.

Leonard R. Kahn, President

Production and R&D

501 Fifth Avenue, Suite 2002
New York, NY 10017
Phone: (212) 983-6765
338 Westbury Avenue
Carle Place, NY 11514
Phone: (516) 222-2221

CHRIS FAGAS CONSULTING, LLC

Chris Fagas
57 Kennedy Road
Foster, RI 02825
Phone:
Fax: 401-392-1324
Email: *chris.fagas@ieee.org*

CELLULAR AND PCS RF ENGINEERING

FORCENINE CONSULTING

Michael E. Hofe, Partner
2000 M Street, NW, Suite 345
Washington, DC 20036
Phone: 301-667-0001
Office: 202-887-0118
Fax: 303-318-7646
Email: *mhofe@forcenine.net*
Website: www.forcenine.net

ForceNine
Telecommunications Consultants

TELECOMMUNICATIONS CONSULTANTS

TGA TECHNOLOGIES, INC.

Barry Kane, President
100 Pinnacle Way, Suite 140
Norcross, GA 30071-3633
Phone: 800-998-8421
Fax: 800-842-3908
Email: *barry@tga.com*
Website: www.tga.com

TGA

RADIO PAGING TERMINALS

INDUSTRIAL COMMUNICATIONS

David J. Fenton Jr., President
40 Lone Street
Marshfield, MA 02050
Phone: 781-319-1008
Fax: 781-837-4000
Cell: 617-799-9999
Service:800-323-7212
Email: *djfentonjr@aol.com*
Website: www.industrialcommunications.com

Industrial Communications.

BROADBAND NETWORK DEVELOPMENT

Jim Innes
4217 Ridge Ave, Unit 2
Philadelphia, PA 19129
Phone: 267-481-1461
Fax: 215-483-1220
Email: *james.e.innes.cgs80@alumni.vpenn.edu*

WIRELESS SITE CONSULTING SERVICES

COMTRAN ASSOCIATES, INC.

Leonard R. Knigin, President
1961 Utica Avenue
Brooklyn, NY 11234
Phone: (718) 531-7676
Fax: (718) 968-1679
Email: *lrknigin@comtran-radio.com*
Web Site: comtran-radio.com

COMTRAN
ASSOCIATES INC

WIRELESS COMMUNICATIONS
TODAY FOR TOMORROW

FOX RIDGE COMMUNICATIONS, INC.

Ralph A. Haller, President
122 Baltimore St
Gettysburg, PA 17325
Phone: 717-334-7991
Fax: 717-334-5656
Email: *rhaller@frci.com*

TELECOMMUNICATIONS CONSULTANTS

GEORGE JACOBS & ASSOCIATES, INC.

George Jacobs, P.E., President

8701 Georgia Avenue, Suite 711
Silver Spring, MD 20910
Phone: (301) 587-8800
Fax: (301) 587-8801
Email: *gja@gjainc.com*
Web Site: www.gjainc.com

CONSULTATING BROADCAST ENGINEERS

FAIRLEIGH DICKINSON UNIVERSITY

Carl J. Kraus, Director
Division of Telecommunications
Teaneck-Hackensack Campus
1000 River Road, T-WFDU
Teaneck, NJ 07666-1914
Phone: 201-692-2806 Voice
Fax: 201-692-2807
Email: *ckraus@fdu.edu*
Website: www.fdu.edu

FAIRLEIGH DICKINSON UNIVERSITY

THE LEADER IN GLOBAL EDUCATION

HARTECH, INC.

James W. Hart, P.E., President
6882 S. Prince Circle
Littleton, CO 80120
Phone: 303-795-2813
Fax: 303-347-2652
Email: *jhart@du.edu*
Website: www.hartechinc.com

HarTech, inc.
Telecommunications Consulting Engineering

COMMUNICATIONS CONSULTING ENGINEERING

DH MARKETING

Carroll Hollingsworth
P. O. Box 5680
7301A Bar-K Ranch Road
Lago Vista, TX 78645
Phone: 800-966-3357
Fax: 512-267-7760
Cell: 512-751-5472
Email: carroll@dhmarketing.biz
Website: www.dhmarketing.biz

DH MARKETING
MANUFACTURERS REPRESENTATIVES

MANUFACTURERS REPRESENTATIVES
WIRELESS CONNUMICATION INDUSTRY

Business & Professional Directory

AMERICAN MUSEUM OF RADIO

John Jenkins,
Curator, Chairman of the Board
1312 Bay Street
Bellingham, WA 98225
Phone: 360-738-3886
Fax: 360-738-3472
www.americanradiomuseum.org

AMERICAN MUSEUM OF RADIO

WHERE DISCOVERY SPARKS IMAGINATION

POWER SALES COMPANY

Carl Mathis, President

POWER SALES COMPANY

PO Box 99356
Raleigh, NC 27624-9356
Phone: (919) 676-0602
Toll Free: (888) 262-8447 or (888) 2MATHIS
Fax: (919) 847-4742
Email: *carlm@power-sales.biz*
Web Site: www.power-sales.biz

DECIBEL PRODUCTS

Louis J. Meyer, *Vice President, International OEM Relations and Sales*
8635 Stemmons Freeway
Dallas, TX 75247-3701
Phone: (214) 634-8502, (214) 819-4226
Fax: (214) 631-4706
Email: *lmeyer@decibelproducts.com*
Web Site: www.decibelproducts.com

DECIBEL PRODUCTS®

AURORA MARKETING COMPANY

Stan Reubenstein, *WA6RNU*
2018 S Pontiac Way
Denver, CO 80224-2412
Phone: (303) 758-3051
Toll Free: (800) 525-3580
Fax: (303) 758-6630
Email: *stan@auroramkt.com*
Web Site: www.auroramkt.com

Aurora Marketing

MANUFACTURER'S REPRESENTATIVE

ATLANTIC COAST COMMUNICATIONS

Michael W. Schmidt, *President*

P. O. Box 340
Telegraph Hill, Holmdel, NJ 07733
Phone: 732-264-8766
Fax: 732-264-7738
Email: *mike@atl-coast.com*

ATLANTIC COAST COMMUNICATIONS

NEMAL CABLE & CONNECTORS

Benjamin L. Nemser, *President*

NEMAL Cable & Connectors for the Electronics Industry

12240 NE 14th Avenue
North Miami, FL 33161
Phone: 305-899-0900, 800-522-2253
Fax: 305-895-8178
Brasil 011-5535-2368
Email: *bnemser@nemal.com*
Website: www.nemal.com

RICHTER GROUP

Henry L. Richter, *Ph. D., PE , W6VZA*
2755 Alondra Way
Palm Springs, CA 92264-8754
Phone: 760-322-9122
Fax: 760-325-7364
Cell: 818-400-5043
Email: *hrichter@alumni-caltech.edu*

RICHTER GROUP
Communications Consultants

COMMUNICATIONS CONSULTANTS

RADIOMATE

Carolyn M. Servidio, *President*

RadioMate®

4030-A Pike Lane
Concord, CA 94520
Phone: (925) 676 -3376 • (800) 346-6442
Fax: (925) 676-3387
Email: *servidio@radiomate.com*
Web Site: www.radiomate.com

PARKINSON ELECTRONICS COMPANY

M.E. (Gene) Parkinson, *President, CEO*

1515 Houston St.
Levelland, TX 79336
Phone: (806) 894-1576
Email: *gpark@nts-online.net*

CELL-X®

MOBILE COMMUNICATIONS

RADIO OP

Lloyd B. Roach, *Director*
1025 Meeting House Road
West Chester, PA 19382
Phone: (610) 793-2552
Cell: (610) 420-3023
Fax: (610) 793-1298
Email: *W3QT@aol.com*

Radio Op

RADIO BROADCASTING CONSULTANT

TYCO ELECTRONICS

Stephen J. Shaver, *Major Accounts Manager*
Wireless Systems

tyco

3901 Derry Street
Harrisburg, PA 17111
Phone: (717) 565-1221
Fax: (717) 565-1210
Mobile: (717) 579-8097
Email: *shavers@tycoelectronics.com*
Web Site: www.macom-wireless.com

M/A-COM

THE CAMBRIDGE GROUP, INC.

David Patton, *Vice President & General Manager*
15851 Dallas Parkway, Suite 190
Addison, TX 75001
Phone: 972-481-7877
Fax: 972-481-7887
Cell: 214-727-1337
Email: *davidp@cgwireless.com*
Website: cgwireless.com

THE CAMBRIDGE GROUP
Wireless System Solutions

MANUFACTUERES REPRESENTATIVE

ANTHONY J. RUSSO & ASSOCIATES

Anthony "Tony" Russo
P. O. Box 325
Franklin Lakes, NJ 07417
Phone: 201-337-7665
Fax: 201-337-7665
Email: *tkrusso@bellatlantic.net*

WIRELESS BUSINESS DEVELOPMENT CONSULTANTS
SALES, MARKETING, DISTRIBUTION,
BUSINESS & STRATEGIC PLANNING

RADIOWAVES, INC.

Andy Singer, *Executive V.P.*

RADIOWAVES

495 R Billerica Ave.
N. Billerica, MA 01862
Phone: 978-459-8800 ext. 12
Fax: 978-459-8814
Cell: 978-270-2590
Email: *andy_singer@radiowavesinc.com*
Website: radiowavesinc.com

RJR WIRELESS

Richard "Rich" J. Reichler, *President*
23501 Park Sorrento, Suite 218
Calabasas, CA 91302-1381
Phone: (818) 222-SITE (7483)
Fax: (818) 222-7487
Cell: (818) 903-5189
Email: *RJRWireles@aol.com*

CONSULTING AND SPECIAL PROJECTS
FOR ANTENNA SITE MANAGERS,
OWNERS, AND USERS.

Business & Professional Directory

REGIONAL COMMUNICATIONS, INC.

Tony Sabino
E64 Midland Ave, Box 144
Paramus, NJ 07653-0144
Phone: (201) 261-6600
Fax: (201) 261-6304
Email: *tsabino@regionalcom.com*
Web Site: www.regionalcom.com

SALES, SERVICE, INSTALLATION OF WIRELESS PRODUCTS & SYSTEMS

E. R. SMAR & ASSOCIATES

***Eugene E. Smar**, PE, MBA, Principal*

16900 Governors Way
Rockville, MD 20853
Phone: 301-379-3805
Email: *ersmar@ieee.org*

E. R. Smar & Associates
Wireless & Telecommunications Consulting

WIRELESS & TELECOMMUNICATONS CONSULTING

SOIFER CONSULTING, LLC

***Raphael "Ray" Soifer**, Chairman*

38 East Ridgewood Avenue, #295
Ridgewood, NJ 07450
Phone: (201) 444-3111
Fax: (201) 447-5472
Email: *ray@soiferconsulting.com*
Web Site: soiferconsulting.com

CAPELLA WIRELESS COMMUNICATIONS CONSULTANTS

J.C. (Jim) Stratt, (E.C. Tserestopoulos)
Senior Consultant

139 Devins Drive
Aurora, ONT L4G 2Z5
Phone: (905) 841-1424
Fax: (905) 841-3562
Email: *capella.wireless@sympatico.ca*

CAPELLA

SWS SECURITY

***Stephen E. Uhrig**, President*
1300 Boyd Road
Street, MD 21154-1836
Phone: 410-879-4035
Fax: 410-836-1190
Email: *steve@swssec.com*
Website: www.swssec.com

SWS Security

MANIFCATURERS OF ELECTRONIC SURVELLIANCE, INTELLIGENCE GATHERINE AND COMMUNICATIONS SYSTEMS SINCE 1972

MIDIAN ELECTRONICS INC.

***Chuck Soulliard**, President, K7JTJ*

2302 E. 22nd St
Tucson, AZ 85713-2024
Orders: 800-MIDIANS
Service: 520-884-7981
Fax: 520-884-0422
Email: *chuck@midians.com*
Website: www.midians.com

MIDIAN
MIDIAN ELECTRONICS, INC.

BROOKLINE BROADCAST DEVELOPMENT, LLC

***W. Thomas Thornton**, President*

11471 Twin Lakes Lane
San Angelo, TX 76904
Phone: 915-947-3436
Fax: 915-947-7160
Email: *Brooklinewest@aol.com*

BROOKLINE BROADCAST DEVELOPMENT, LLC

DH MARKETING

Carroll Hollingsworth

P. O. Box 5680
7301A Bar-K Ranch Road
Lago Vista, TX 78645
Phone: 800-966-3357 • **Fax:** 512-267-7760
Cell: 512-751-5472 • **Email:** carroll@dhmarketing.biz
Website: www.dhmarketing.biz

Multiplier
RECHARGEABLE BATTERIES

MANUFACTURERS REPRESENTATIVES
WIRELESS COMMUNICATION INDUSTRY

WALLACE & WALLACE

***Donald G. Werner**, President*
2600 S. California Ave., Suite F
Monrovia, CA 91016
Phone: 626-305-8800
Fax: 626-305-8801
Email: *don.werner@prodigy.net*
Res: 626-914-7216

WALLACE & WALLACE
A CORPORATION
ELECTRONIC MANUFACTURERS' REPRESENTATIVE

ELECTRONIC MANUFACTURERS' REPRESENTATIVE

ITT INDUSTRIES
ITT Aerospace/Communications

***Eric D. Stoll, Ph.D., P.E.**, Sr. Staff Engineer*

100 Kingsland Road
Clifton, NJ 07014-1993
Phone: (973) 284-4887
Fax: (973) 284-3394
Email: *eric.stoll@itt.com*

ITT Industries

TROTT COMMUNICATIONS GROUP

***Raymond C. Trott, P.E.**, Chairman*

1425 Greenway Dr, Suite 350
Irving, TX 75038
Phone: (972) 580-1911
Fax: (972) 580-0641
Email: *ray.trott@trottgroup.com*
Web Site: www.trottgroup.com

TROTT

RF ENGINEERING CONSULTANTS

TV

***Larry H. Will, PE**, Professional Engineer*

1055 Powderhorn Drive
Glen Mills, PA 19342-9504
Phone: (610) 399-1826
Fax: (610) 399-0995
Email: *lwill@voicenet.com*

TV

ENGINEERING CONSULTANT

Ad Index

The Radio Club of America, Inc.
Awards Committee

Fellow Nomination Form

The Club annually elevates worthy Club members to the grade of Fellow in recognition of outstanding achievement, and to provide inspiration for many people, both currently and in the future. As a member of the Club, your help in nominating and sponsoring candidates is appreciated. This form is provided to assist you in this process. In order to complete the elevation process in time for the annual Awards Banquet in November, the Awards Committee prefers to receive nominations prior to April of the year of the proposed elevation.

Article I of the Club's By-Laws states the following:

Section 6: Elevation or transfer to the grade of Fellow shall be by a majority vote of the Board of Directors.

Section 7: A Fellow shall have been a member of the Club for at least five (5) years and/or a Senior Member for at least two (2) years and one whose contributions have been outstanding with extraordinary qualifications in the art and science of radio and electronics. The five and two years referenced above may be waived by a majority vote of the Board of Directors.

Section 8: Elevation to the status of Fellow is by invitation only. If such person is not a Senior Member, his/her sponsor must submit a Senior Member form to the Executive Committee for recommendation to the Board of Directors

To nominate an RCA member, please **legibly provide the information below** to the Club's Awards Committee in care of the Club's Executive Secretary in any of the following ways:

Fax:	(732) 219-1938
E-mail:	ExSec@Radio-Club-of-America.org
U.S.P.S. mail:	244 Broad St., Red Bank, NJ 07701-2003

A. Full name of candidate:______________________________

B. Proposed citation (between 5 and 25 words), based on why it is felt that this candidate should be considered: (to be announced at the presentation of the award)

____

____

____

C. Attach supporting material such as an expanded explanation, a biography, a resume, and any significant published articles: (please list your attachments below)

____

____

<u>Sponsor submitting this nomination</u>:

Full name:____________________ **Phone number:**____________________

E-mail address:____________________ **Fax number:**____________________

U.S.P.S. mailing address:______________________________

Date submitted:____________________

Vertex Standard
BASE
Vertex Standard
DESKTOP REPEATER
VXR-7000
RESCUE
LTR WIDE
LTR WIDE
RESCUE
POLICE-1
vertex
vertex
vertex
vertex

RadioMate