Summer 2003

ACUTA Journal of Telecommunications in Higher Education

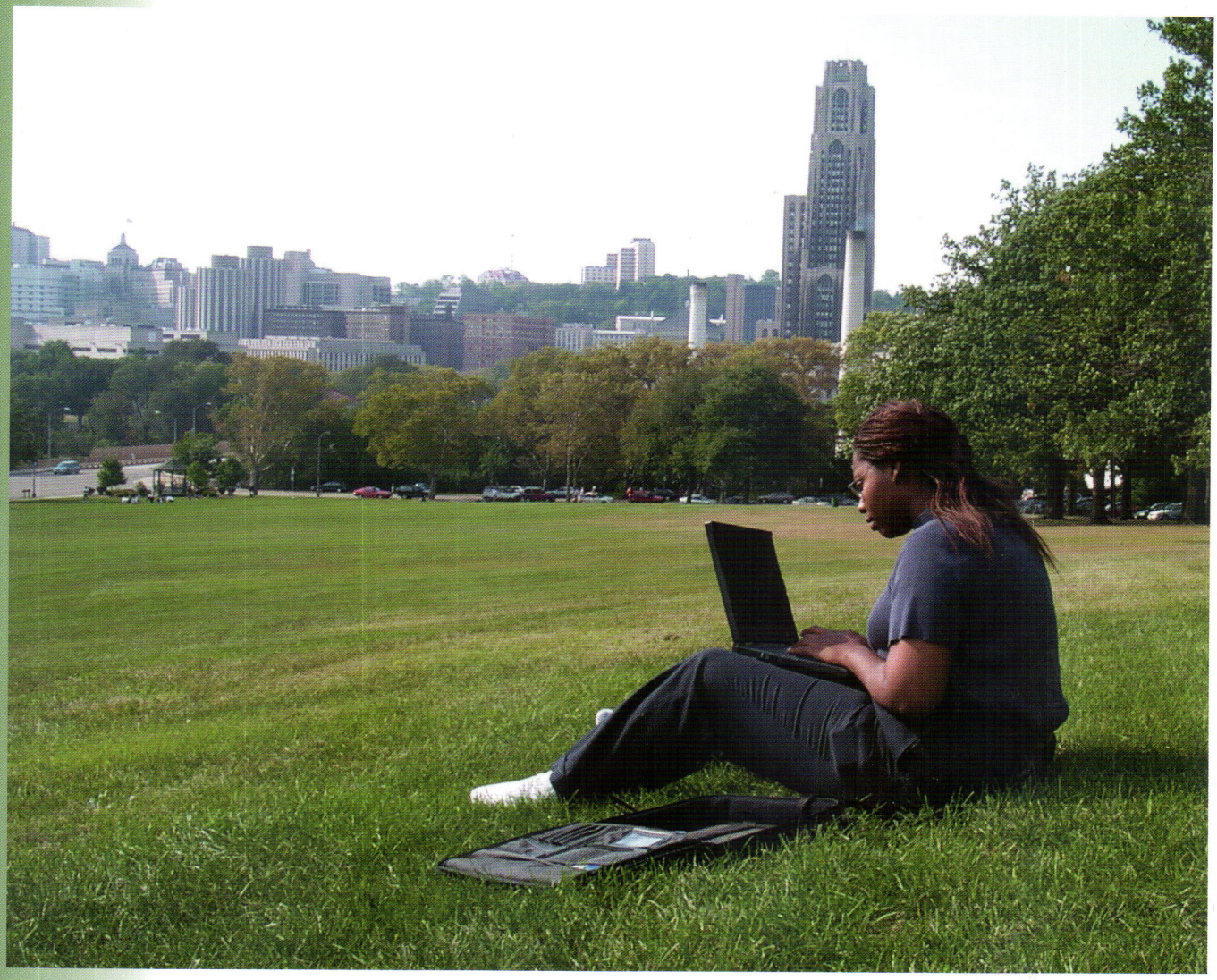
Summer, 2003
Vol.7, No.2

acuta

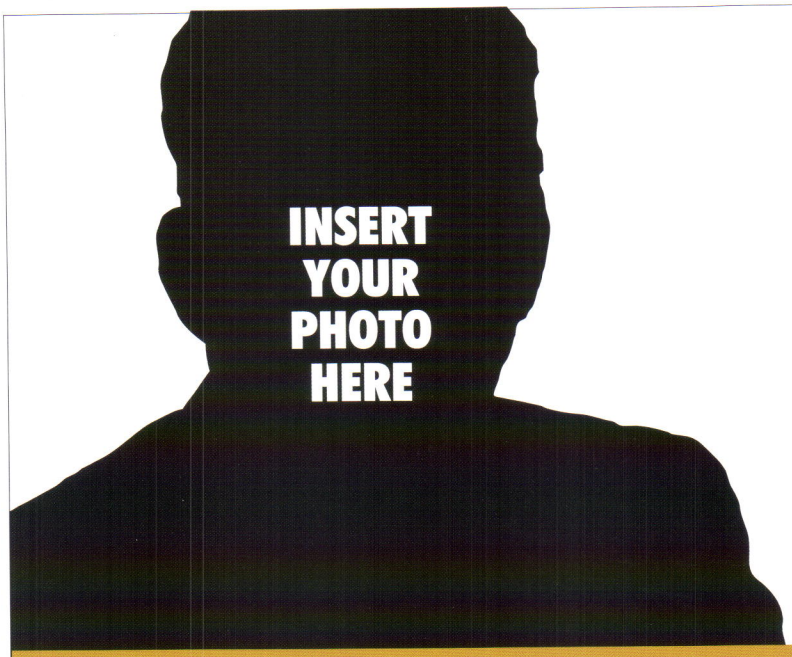
Journal

of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education



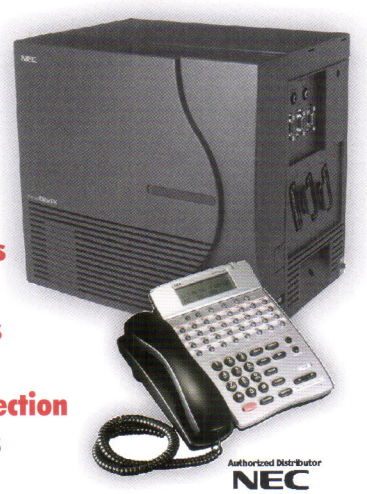
This Issue: Wireless Technologies



The new Dean of Communication.

NEC
Nortel
Avaya
And most other major manufacturers

Plantronics Headsets
Minuteman UPS
ITW Linx Power Protection
Scitec Analog Phones
Adtran CSU/DSU



Authorized Distributor
NEC
NEC America, Inc.
Business Systems Sales Division

Technical Support
Advance Replacement
Repair
New and Refurbished Equipment

When you choose OPTUS

as your telecom partner, you'll quickly earn the reputation as the leading communications authority on campus! We make it easy for you to "set the curve" among administrators and department heads.

OPTUS is your single-source solution for on-campus telephony challenges from single line phones to large, multi-site networks...TDM to VoIP, or any number of add-ons.

OPTUS is the right choice for your institution from the laboratory to the dormitory!

Call OPTUS for a free professional consultation.

OPTUS
TELEQUIP

800.628.7491
870.974.7700
www.optustelequip.com

Quality System Registered
ISO 9002
Certificate QSR-689

Events Calendar

Event	Date	Place
Annual Conference	July 27–31, 2003	The Westin Diplomat Resort and Spa Hollywood, Florida
Fall Seminars	October 19–22, 2003	Hilton San Diego Resort San Diego, California
Winter Seminars	January 11–14, 2004	Sheraton New Orleans New Orleans, Louisiana
Spring Seminars	April 18–21, 2004	Wyndham Miami Beach Resort Miami Beach, Florida

ACUTA's Core Purpose is to: Support higher education institutions in achieving optimal use of communications technologies.

ACUTA's Core Values are to:

- Share information, resources and insight,
- Respect the expression of individual opinions and solutions,
- Maintain our commitment to professional development and growth,
- Advance the unique values and needs of higher education communications technologies, and
- Encourage volunteerism and individual contribution of members in support of organizational goals.

"Wi-Fi's real security risks and rumored performance lags seem to be small obstacles to its acceptance among institutions of higher education. With increasing frequency, extending the campus LAN means going wireless.

—David Geer
page 30

THE **ACUTA** JOURNAL OF TELECOMMUNICATIONS IN HIGHER EDUCATION

Published Quarterly by
ACUTA: The Association for Communications Technology Professionals in Higher Education
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

PHONE 859/278-3338
FAX 859/278-3268
E-MAIL pscott@acuta.org

Publisher
Jeri A. Semer, CAE, Executive Director

Editor-in-Chief
Pat Scott, Communications Manager

Contributing Editor
Curt Harler

Advertising Sales
KCS International, LLC
717/397-7100 or www.kcsinternational.com

Submissions Policy
The ACUTA Journal welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-chief. Author's guidelines are available upon request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

The ACUTA Journal is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by telecommunications managers and staff.

ISSN 1097-8658

POSTMASTER, send all address changes to:

ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486
Postage paid at Louisville, Kentucky.

Visit the ACUTA site on the World Wide Web:
http://www.acuta.org

Membership and Subscriptions
Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for $80 per year or $20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 222, or e-mail, kbowman@acuta.org.

Contents

Summer 2003 • Volume 7, Number 2
Wireless Technologies

Cover photo: Carnegie Mellon University; Yerin Kay, photographer

FEATURES

INTERVIEW

COLUMNS

ADVERTISERS' INDEX

PRESIDENT'S MESSAGE

It's a Brave New *Wireless* World ...

Jeanne Jansenius
University of the South
ACUTA President
2002–2003

Interesting, isn't it, how a new device can change even our most basic behavior patterns? Without a doubt, wireless technology is changing the way I live—from where I go to what I take with me to how I accomplish what I need to do, even on a daily basis. And the changes are universal in the industrialized world.

As digital images are transmitted across a wireless network, the TV commercial that asks "Can you hear me now?" could go a step further: "Can you *see* me now?" With instant transmission of images via wireless we share photos with just about anyone anywhere. As this has become even more commonplace, traditional film and print are becoming obsolete. Technology continually changes the way we live. For many of us, myself included, it means freedom from the constraints and clutter of wires that have bound us since they were invented.

Think about this. The mechanical clock was invented in the early 14th century, and shortly afterward watches appeared in pockets and on wrists. For hundreds of years, we have relied on these devices for telling time. But today I do not wear a wristwatch. Nor do I carry an appointment book or take a travel alarm when I am away from home, as I always have done in the past. Because of the advancements in wireless technology, I find that now I can even leave my laptop computer behind. My constant companion is my cellular phone—which is also a PDA that allows me to read and respond to my e-mail and takes digital images I can transmit while talking on my wireless phone. Yes, wireless is more difficult to manage and less stable, but I, like the rest of society, am putting up with it for the convenience and ease of staying connected.

What's next? Will wireless devices be used for identification? In Singapore, you can buy a soft drink from a vending machine by simply pressing a button on your cell phone and having the cost of the drink charged to your phone number. Need a discount coupon? Just download a coupon to your cell phone and show the screen on your cell phone at the counter. Now 3-D technology is beginning to make its way into the wireless arena as developers are busy planning exciting new games for all wireless handhelds.

As in most environments where performance is a priority, there are some disadvantages to wireless technology. Wireless developments saw a slowdown during the post-9/11 period because of security concerns. Security is regularly cited as the No. 1 obstacle.

For a variety of reasons, campuses must still provide a wired infrastructure in addition to wireless. We must also provide justification for two networks as we demonstrate a positive return on investment. One of the major challenges you'll face as you implement this new technology on your campus is to select WLAN infra-

structure that provides some level of investment protection and does not become obsolete as new standards emerge.

In 1997, Jim Cross, now the vice provost of information technology at Michigan Tech, was president of ACUTA. He wrote in his May *ACUTA News* column, "We are moving into an age of global connectivity and turbocharged economic and technological growth. This exciting new stage of societal development in which humanity continues to extend its reach into the dimensions of time, space, quantity, quality, size, and scope is being fueled in part by a new generation of satellite communication systems." Jim's vision of the future is now reality.

The WLAN market has taken a supermarket approach. On the shelf you will find 802.11b, 802.11a, and 802.11g; and now Intel has introduced the 802.16 standard that is supposed to be good for a 30-mile range.

Change happens so quickly that one of the major challenges continues to be return on investment. How long will this product be viable? Which standard will be the winner? I am reminded of something said by inventor Thomas Alva Edison, who lived from 1847 to 1931: "I have not failed. I've just found 10,000 ways that won't work."

The wireless market is here to stay, but what it will look like in a few years we can only imagine. As you read the articles in this issue of the *ACUTA Journal*, I hope you will feel more confident that you can make good decisions for your campus about wireless technology.

What's Driving Wireless on Campus?

by Patrick Rafter

In November 2001, Gartner analyst Ron Yanosky began an interesting brief entitled "Unwiring Higher Education" with a story about President James Garfield's reflections on his student days at Williams College. Garfield once commented, "[T]he ideal college is Mark Hopkins [Williams's president] at one end of a log and a student at the other."

Garfield might be surprised to see that in 2003, a present-day Williams student might interact with a faculty member in Garfield's ideal way but would also be able to wirelessly connect to the entire world via the World Wide Web. From small, private colleges like Williams to community colleges, and from large state to private universities, 802.11 (Wi-Fi) wireless local area networks (WLANs) are being installed in dorms, common areas, and academic buildings in greater numbers and at a faster pace than wired networks.

Research from In-Stat/MDR suggests that despite a general economic downturn, the market for shipments of WLAN equipment into universities continues to be very strong. In 2001, the education sector accounted for 35 percent of WLAN product shipments—more than twice the market share of the next two highest vertical markets adopting wireless, healthcare and financial.

The use of wireless technology and PDAs in higher education was the focus of "No Strings Attached," a national virtual conference that took place at Case Western Reserve University in Cleveland, Ohio, in May 2002. The conference brought together hundreds of university IT managers with technology solutions providers including Apple, Bluesocket, Cisco, Microsoft, and Palm for two days of real-world sessions on current and future wireless deployments.

What's Driving Wireless?

These and other university IT managers have identified the following five principal factors driving wireless adoption on their campuses:

1. Student demand

Students are influential and vocal about what they want. In the same way that students' increased use of cellular phones and pagers changed telephone use in dormitories, student passion for wireless devices like laptops and PDAs is forcing university IT staff to support wireless access.

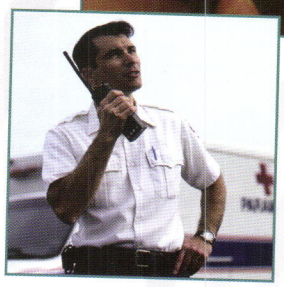
2. Simplicity

Wireless networks are easier to install and maintain than Ethernet cables. Wireless access points can provide access in hard-to-wire locations on campus such as outdoor campus commons, stadiums, cafeterias,

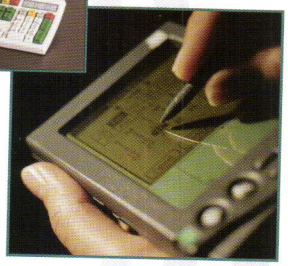
▶

Cut your costs.
Streamline your communications.
Bring it all together with one system.

Amcom
Comprehensive Call Processing Solutions



- Speech recognition
- PC attendant console
- Web-enabled information and services via PC and wireless devices
- Event notification and response



Never has unified communications been more important to your faculty, administrators and students. Never has it offered greater productivity gains and cost reductions. And never has it been easier to implement and use.

Amcom CTI solutions. Designed with innovation in mind. Built to last using industry-standard hardware, software and protocols.

SERVICES
- Professional system planning and project management
- Turn-key installation and end user training
- 7 x 24 x 365 support

PLATFORMS
Oracle database
Nuance • Intel/Dialogic
Windows NT • Linux

AmCom

1-800-852-8935
www.amcomsoft.com

libraries, and historic buildings. The average school building is 45 years old, making dropping cables undesirable and difficult, if not impossible.

3. Cost

WLANs can reduce the cost to deploy and operate a network. California State University installed wireless classrooms when it estimated the cost to wire a 60-person classroom on its Monterey campus at $60,000—four to five times the cost it paid to provide unwired access.

In addition to the affordability of wireless access points (as low as $50), Wi-Fi access is increasingly built into the new laptops students are bringing to school. Thus, by working wirelessly, students don't incur the additional costs or complications inherent in the wired world.

Universities may find that wireless can save or even make them money. When Harvard Medical School converted its curriculum to a digital e-curriculum called "MyCourses," the university saved $150,000 it would have spent in paper costs as students now track their schedules, appointments, classroom locations, courseware, and lecture notes online.

4. Quality of life and productivity

Perhaps the most significant way in which wireless is changing university life is the transformation of how and where students and faculty interact. Deborah Gelch of Lasell College in Massachusetts says, "[W]ireless is tearing down the walls of the classroom, bringing students and professors together as never before—improving interaction and collaboration. Wireless lets them correspond with each other, connect to the Web for research materials from wherever they choose—the student center, the library, even on the grass outside academic buildings."

5. Mobility

Whereas many workers in the corporate world stay put in their offices/cubes for much of their workday, college students and faculty are extraordinarily mobile. Their need to stay connected and in touch as they move between classrooms, or from a laboratory to a dormitory, is a strong driver for working untethered. The latest technologies even enable wireless users to remain securely connected as they move across subnets from one wireless coverage area to another.

Achilles' Heel: Wireless Insecurity

This brings to mind the Achilles' heel of wireless networks: security. Consider the dichotomy: The *best* thing about wireless networks is that they are so open and easy to access, and the *worst* thing about WLANs is that they are so open and easy to access.

IT departments at higher-education institutions are faced with the challenge of enabling collaboration among students, faculty, and administrative staff via wireless technology. Educators want to provide the student body with the freedom to roam and work on Internet-connected computers throughout the campus; however, they want to ensure that proper safeguards are in place.

Within the past year alone, countless articles have appeared in the trade press about the lack of security in 802.11 wireless networks and how *war drivers* can easily break into those networks with shareware and an antenna crudely fashioned from a Pringles potato chip can.

Maintaining airlink privacy and network integrity and controlling user authentication and authorization are particularly crucial issues to university IT managers. In a presentation delivered at EDUCAUSE 2002 on "Creative Solutions for Wired and Wireless Network Authentication," Jay Graham of the University of Pittsburgh outlined how Pitt's wireless network service meets the university's strategic infrastructure design standards for security, scalability, and central authentication support.

Given that students are often up to what Lasell College's Gelch calls "tomfoolery," IT managers on university campuses are especially keen to prevent students from accessing network resources to which they aren't authorized (e.g., the servers that contain grade information, exam materials, or financial aid).

Role-Based Access Control

To address this issue, universities such as those above, as well as the University of Georgia, the London School of Economics, Rutgers University, and the University of Arizona, are integrating appliances that provide role-based access control for wireless networks.

These appliances, called wireless gateways, work like a bouncer at a nightclub—stopping people as they try to get in, checking their ID, and deciding who should go where and what they can do when they get in. On many of these campuses the wireless gateway connects to central authentication servers (e.g., RADIUS, LDAP) containing users' information. Once authenticated, wireless users can access those resources to which they have been authorized. Setting up and maintaining service classes based on roles is easy (because wireless access is browser based and doesn't require the installation of client software on the users' wireless devices).

Role-based access control is flexible (can be modified remotely by IT staff) and scalable—as the number of roles is infinite. Accordingly a role called *sophomore/liberal*

arts allows one level of access; roles for *grad student,dean,* or *guest* (for visiting professors, parents of prospective students, alumni, and campus vendors and suppliers) would allow different levels of appropriate access and bandwidth shaping, limiting, for example, the network storage space allowed undergrads who are prone to download storage-intensive MP3 and MPEG files.

"We needed to stop unauthorized users gaining access to the Internet through our wireless network and, also in case of misuse, we need to be able to track network access back to an individual user," said Jeremy Skelton, network specialist, London School of Economics. "With a wireless gateway, we are able to manage both requirements with the added benefit that it is interoperable with our existing wireless access points."

Conclusion

Wireless networks are changing the nature of life and learning in today's universities. Ensuring that these networks are as secure and reliable as they are simple and easy to use will be crucial to their success. Even though Wi-Fi networks have been available only since 1999, university administrators are already finding that providing wireless access will be a competitive differentiator in attracting the best and brightest students, faculty, research grants, and donations. An October 2001 Gartner report, *Wireless Higher Education: A Strategic Choice,* concludes, "By 2005, institutions not offering wireless access will be at a recruiting disadvantage."

College administrators and admissions officers—take heed!

Patrick Rafter is chief communications officer at Bluesocket Inc. Contact him at prafter@bluesocket.com.

Additional Resources

Graham, Joseph. Senior technology specialist, Univ. of Pittsburgh. "Creative Solutions for Wired and Wireless Network Authentication." Paper presented at EDUCAUSE 2002, Oct. 2, 2002. http://technology.pitt.edu (*presentations* at *EDUCAUSE, ACM, SIGUCCS*)

"Managing Wireless Access on Campus," Bluesocket BluePaper. http://www.bluesocket.com/solutions/Wireless-Access-On-Campus-BluePaper.pdf

"No Strings Attached." Conference. Case Western Reserve Univ., May 2002. http://www.cwru.edu/is/no_strings/defaultpage.htm

Yanowsky, Ron. Gartner, Inc. "Unwiring Higher Educatio.n" by Ron Yanosky, Gartner, Inc. (Nov. 6, 2001) http://www4.gartner.com/pages/story.php.id.2449.s.8.jsp

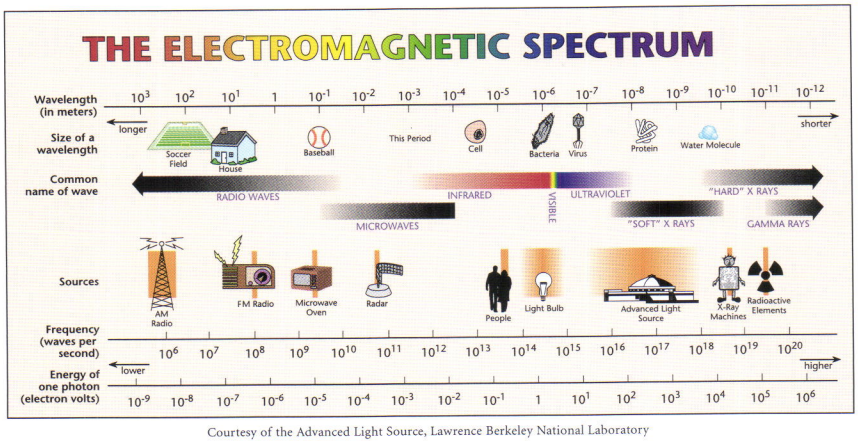
Understanding Wireless: Medium- and Long-Range Technologies

by Joseph Kershenbaum

Back when Guglielmo Marconi began experimenting with "Hertzian waves" in 1894, wireless meant "wireless telegraphy," and Marconi called his system the "cable telegraph." Hertzian waves later became known as radio waves, and the cable telegraph became better known, at least in North America, as the radio.

Even the meaning of wireless itself has changed. Originally, wireless described telecommunications in which radio waves (rather than some form of wire conductor) carried a signal over all or part of a communications path. The definition of wireless today has broadened to incorporate other parts of the electromagnetic spectrum in which information is transmitted without wires. These include not only radio frequency (RF) transmission but also communications via infrared, laser, visible light, and acoustic energy. (See Figure 1.)

Figure 1: The electromagnetic spectrum. Frequencies below 100 KHz (10^5), such as low frequencies (LF), very low frequencies (VLF), extremely low frequencies (ELF) and voice frequencies (VF), are not shown.



Courtesy of the Advanced Light Source, Lawrence Berkeley National Laboratory

Wireless communications has blossomed. In a mere 20 years, wireless services have accumulated more than a billion users and combined service revenues of nearly US $400 billion a year. As wireless use has developed, it has engendered a great multitude of technical terms, jargon, trade names, and legal definitions. This terminology is seldom readily understandable and, at best, is often confusing. Nonetheless, wireless technologies are expected to continue to grow dramatically in the next decade and play an increasingly greater role in our lives.

For those who need to start at the beginning for a better understanding of wireless technology and its language, let's consider (1) some of the terminology that is frequently used today, (2) some of the categories by which wireless systems have been classified, (3) the standard technologies underlying wireless cellular networks, and (4) the stages in the growth and development of wireless telecommunications networks and services.

Wireless Categories

Wireless systems can be categorized in various ways, including, for example, classifications based on network architecture or mobility factors. These

differing taxonomies are one reason wireless can be so confusing. One wireless taxonomy bases its nomenclature on the area of spectrum utilized. Examples of this type of organization include the following:

- *IR wireless*: Communication with devices that utilize infrared radiation (IR). Devices that use IR include home-entertainment remote-control boxes, wireless local area networks, links between notebook computers and desktop computers, cordless modems, intrusion detectors, motion detectors, and fire sensors.
- *Acoustic wireless*: Communication by operating devices that employ acoustic waves. These include military (e.g., surveillance, underwater reconnaissance), government (e.g., earthquake and tsunami warning systems), and commercial applications (e.g., pipeline monitoring, ship traffic control).

An alternative categorization classifies wireless technologies by range. In this arrangement, the apportioning factor is the geographical region covered by the network. Examples include the wide area network (WAN), which covers a broad geographical area, such as a state or country; a metropolitan area network (MAN), which interconnects users in a city or similar-sized region; a local area network (LAN), sometimes referred to as a campus network; and a personal area network (PAN), a small wireless LAN, often connecting a single user's devices.

Yet another common method divides wireless systems into categories according to the type of device involved in the communication. These categories, which sometimes overlap, include the following:

- *Fixed wireless*: Communication using devices at fixed locations such as homes or offices. Standard utility mains typically power fixed wireless systems. Frequencies allotted for fixed wireless systems range from 900 megahertz (MHz) to 40 gigahertz (GHz).

Many types of fixed wireless systems exist and have been developed based upon the frequency of the spectrum utilized. These systems include private licensed microwave links; private unlicensed links; 38 GHz carrier service; local multipoint distribution service/system (LMDS); multichannel/microwave multipoint distribution service/system) (MMDS); optical wireless (laser); and unlicensed national information infrastructure band (UNII). Even satellite service and high-altitude aircraft systems proposed to offer round-the-clock wireless service are sometimes considered fixed wireless systems because their ground stations are at fixed locations.

The technical limitations of fixed wireless systems limit them to metropolitan area geographies. Therefore, they are considered MAN technologies.

- *Mobile wireless*: Communication via the operation of devices aboard motorized vehicles via battery power, such as personal communication services (PCS) units and automotive cell phones.
- *Portable wireless*: Communication by means of autonomous, battery-powered devices outside the home, office, or vehicle, such as PCS units and handheld cell phones.

Mobile and portable wireless systems are both WAN technologies.

Broadband Wireless

Like wireless, broadband also can be defined a number of ways. In its simplest description, broadband is a method of delivering voice, data, and video using a wide range of frequencies at high speed over a given period of time. Broadband wireless is the wireless transmission of such information. Although spectrum ▶

licenses can be expensive, setting up a wireless transmission system is often more economical, more convenient, and faster to deploy than laying cable to the user.

When defined by the RF section of the electromagnetic spectrum that is employed, broadband wireless includes LMDS, MMDS, and PCS. Broadband wireless also includes the transmission of information employing optical wireless technologies.

- *LMDS*: LMDS is a broadband microwave fixed wireless system that offers one-way and two-way communication. It was designed to provide voice, data, and video (wireless cable television) service.

LMDS is a point-to-multipoint service, which means that in an LMDS system, a local antenna transmits to receivers at homes and businesses. It provides connections of up to 5 miles, depending on the terrain and weather conditions. LMDS requires a clear line of sight between the transmitter and the receiver. This means that if a hill, trees, walls, or similar obstructions are in the way, its signal can distort or fade. Rain also can scatter and distort the signal.

Some LMDS providers offer two-way wireless transmission. This is called downstream and upstream, or *symmetrical,* service. Other providers offer only downstream, or *asymmetrical,* service, and a wire connection is required for upstream service. (Standard telephone lines supply the wire connection.) LMDS offers a bandwidth of up to 1.5 Gbps downstream to users, although a more common transmission rate is 38 Mbps downstream. It offers 200 Mbps upstream from the user.

LMDS operates in the 27.5–31.3 GHz frequency band in North America and from 24 to 40 GHz overseas. In Canada, it is known as local multipoint communications systems (LMCS).

- *MMDS*: MMDS is a broadband microwave fixed wireless system quite similar to LMDS. The primary differences are that MMDS can operate over greater distances but has less bandwidth than LMDS offers.

Initially, MMDS began as a one-way service to broadcast wireless cable television. However, it could not compete with wireline and satellite cable offerings because quality was problematic and satellite television, in particular, offered a greater number of channels. While MMDS still provides up to 33 analog and more than 100 digital television channels in some locations, it now is available as a two-way transmission service, supplying voice and data communication applications, such as Internet service. In some cases, the upstream path employs a wire connection.

In an MMDS system, an antenna located at or near the highest tower, tall building, or mountain in a geographical area transmits to small microwave dishes. It has a range of up to 35 miles, depending on the terrain. Like LMDS, MMDS requires a clear line of sight between the transmitter and the receiver. When used for two-way service, MMDS, which operates on licensed and unlicensed channels, can transfer information at rates up to 30 Mbps over unlicensed channels or 1 Gbps over licensed channels. Two-way service reduces the effective range of MMDS to about 6 miles (10 km).

MMDS operates in the 2.1–2.7 GHz frequency band in the United States and Canada and at 3.5 GHz in international markets.

- *PCS*: PCS is a two-way digital wireless voice and data service similar to cellular telephone service. In both PCS and cell systems, antennas blanket an area of coverage. As a user moves around, the nearest antenna acquires the user's signal and transmits it to a base station connected to the wired telephone network. PCS and cell systems use separate networks of antennas.

PCS differs from cell service in several ways. PCS is digital while cell systems may be both analog and digital. PCS was meant to offer greater geographic coverage and, thus, more personal mobility than cell service, which was designed for use in cars with transmitters located around roads. PCS has fewer blind spots (areas in which access is not available) than cell service. PCS has smaller cells and thus requires more antennas than cell systems. Further, PCS transmitters are generally closer together.

In North America, PCS operates in the 1,850–1,990 MHz frequency band while cellular systems operate at frequencies between 824–894 MHz.

- *Optical wireless*: Optical wireless, also known as atmospheric laser transmission, free space optics (FSO), or free space photonics (FSP), is a broadband fixed wireless system that offers two-way voice, data, and video communication. In an optical wireless system, laser beams transmit information through the air, typically linking buildings and campuses together at distances of up to 6 kilometers.

Optical wireless can transfer information at up to 1 Gbps. It operates in the infrared portion of the electromagnetic spectrum, typically at wavelengths ranging from 750 to 1,550 nanometers (nm).

Wireless Cellular Network Technologies

Several standard technologies provide the means by which PCS and cellular telephone networks may operate. While there are quite a number of variations, there are three basic themes: FDMA, TDMA, and CDMA. Each differs in the technique—time, space, or frequency—used for sharing the RF spectrum. In

other words, these three major wireless standards offer different ways of multiplexing.

Multiplexing means combining and transmitting two or more signals or streams of information simultaneously as a single complex signal. Demultiplexing refers to recovering the individual signals at the receiving end. Because they multiplex in different ways, the three standards are incompatible.

- *Frequency division multiple access (FDMA)*: FDMA works by dividing the RF spectrum into a range of frequencies. Each user is assigned to a different 30 KHz-wide channel. (See Figure 2.) It is used by analog mobile phone systems and is still in use today, primarily in rural areas. It is not efficient for digital communications because it requires a lot of bandwidth. In an FDMA system, multiple frequency channels are required for each call (one for the uplink and one for the downlink).
- *Time division multiple access (TDMA)*: Like FDMA communication systems, TDMA systems also divide the RF spectrum into 30 KHz channels. However, in a TDMA system, the 30 KHz channel is further divided into tiny time slots that are 6.7 milliseconds (ms) long. Each user takes turns communicating in rotation over the channel by having access to one time slot at regular intervals. (See Figure 3.) Thus, TDMA tripled the capacity of the original FDMA-based analog systems. In a TDMA system, multiple calls may be made on a single frequency.

TDMA is used in communications networks such as the Global System for Mobile Communications (GSM), Integrated Digital Enhanced Network (iDEN, a technology that combines a mobile phone with a two-way dispatch business radio), and Personal Digital Cellular (PDC), a system used in Japan.

▶

Figure 2: Frequency division multiple access (FDMA)

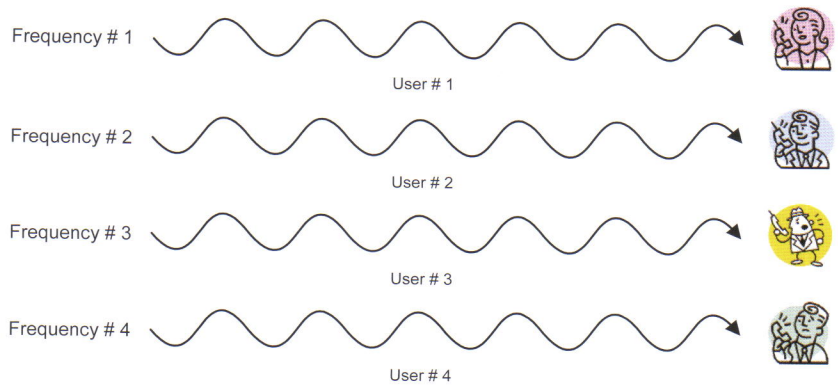


Figure 3: Time division multiple access (TDMA)

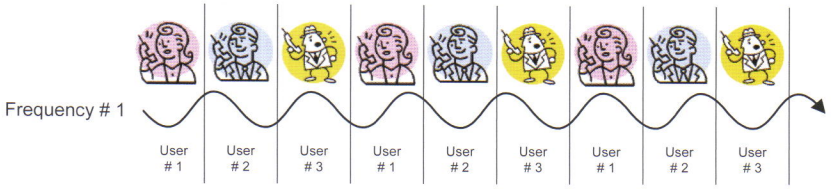


Figure 4: Code division multiple access (CDMA)

- *Global System for Mobile Communications:* Originally called Groupe Spécial Mobile, GSM is the world's most widely used mobile communications system. It presently provides seamless, same-number communication in more than 170 countries.

GSM operates on a 25 MHz wide frequency band by combining FDMA and TDMA access schemes. First, using FDMA, it divides the 25 MHz band into 124 200 KHz channels. Then, using TDMA, it divides each 200 KHz channel into eight separate time slots, each .577 ms long. Users communicate in turn by having access to one time slot at regular intervals. This is known as narrowband TDMA technology.

- *Code division multiple access (CDMA):* CDMA is a digital technology that divides the RF spectrum into 1.25 MHz wide channels, much larger than those in FDMA or TDMA systems. With CDMA, a unique code, known as a pseudo-random code sequence, is assigned to each user's signal in order to differentiate users. The signal is then transmitted simultaneously with all other users' signals on the same channel. At the receiving end, the user's unique code is deciphered and used to extract and reassemble the user's specific information from all other information being broadcast. CDMA is known as "spread spectrum" technology because the signal is spread across a bandwidth much wider than the original signal. (See Figure 4.)

The difference between TDMA and CDMA has been compared to conversations involving different languages. In a TDMA system, each person takes turns speaking in his own language. However, in a CDMA system, the listener listens for the one person speaking his language in a place where everyone speaks simultaneously in a different language.

CDMA has many advantages over FDMA and TDMA. First, there are about 4.4 trillion possible frequency-sequencing codes, allowing for much greater use of frequency bands and, thus, greater capacity. CDMA systems offer 8 to 20 times the capacity of FDMA systems and three times the capacity of TDMA systems. The trillions of combinations also provide enhanced privacy and security. Second, it is a low-power system that increases battery life in mobile units. Third, its unique coding allows for improved transmission quality, with no crosstalk or interference. Fourth, its spread spectrum technology allows networks to be built with fewer cell sites, improving coverage while lowering system costs and planning. Finally, because it is a packet-switched technology (discussed below under GPRS), it offers bandwidth on demand.

Wireless Generations

1G, 2G, 2.5G, 3G, and 4G describe stages in the growth and development of wireless networks and services. "G" means generation.

- *1G:* The first generation of wireless service provided voice communication via analog mobile phones, but no data transmission. Analog mobile wireless service began in the late 1970s and early 1980s and operated using FDMA.

Several different systems existed. In North and South America and 35 other countries, the system deployed was the Advanced Mobile Phone Service (AMPS). It began operating in the United States in the early 1980s in the 800 MHz band. Another system, Nordic Mobile Telephone, was deployed in more than 40 European countries. It operated in the 450 and 900 MHz frequency bands. Another European system, the Total Access Communication System (TACS), operated at frequencies in the 800–900 MHz range.

Analog systems offered limited capacity; as traffic increased, bandwidth constraints reduced service. Further, handoff between cells was unreliable.

- *2G:* In the early 1990s, service providers introduced second generation wireless cellular systems. These systems were digital; they are referred to as digital cellular and PCS systems. They have been used primarily for voice communication but offer enhanced features, such as caller ID. In North America, they operate using GSM, TDMA, CDMA, and iDEN to communicate.

2G systems, like 1G ones, are based on circuit-switched technology. In such a system, each call requires its own cell channel, which makes data transmission very slow. Thus, 2G systems are oriented to simple, low-speed data services, such as short message service (SMS), a point-to-point text-message service offered on GSM systems that allows a user to send messages of up to 160 characters simply by entering the recipient's phone number. SMS is similar to paging, except that a cell phone can receive a message even if a voice or data transmission is in progress.

Digital systems offer a number of advantages over analog ones. They require lower power and provide better voice quality and greater security and transmission capacity (from 9.6 to 14.4 Kbps). In North America, 2G cellular systems operate at frequencies between 824 and 894 MHz, and PCS operates in the 1,850–1,990 MHz frequency band.

- *2.5G:* The present state of wireless infrastructure, 2.5G or 2G+, is a phase between second and third generation technology. 2.5G appeared as a cost-effective migration to 3G because upgrading directly from 2G to 3G networks is quite expensive. Essentially, it extended 2G systems to increase data transmission rates, so that additional features

such as enhanced e-mail and Internet access may be offered.

2.5G systems introduce technologies such as the following:

1. General packet radio services (GPRS) and high-speed circuit-switched data (HSCSD) for GSM networks, which offer increased data transmission capabilities;

2. Enhanced data GSM environment (EDGE), a faster version of GSM service that increases data rates for GSM and TDMA networks; and

3. Interim standard 95B (IS-95B) and high data rate (HDR), which improve data transmission capacity for CDMA networks.

GPRS and EDGE are packet-switched technologies. In such a system, information is broken up into discrete packets of data and transmitted over the network to its destination. Network resources are used only when packets are transmitted. This is more efficient than circuit switching, used in traditional phone systems and 2G networks, in which a single circuit must be dedicated to the users for the duration of the connection. Packet-switched phones seem to be always connected to the network compared with circuit-switched connections in which a user must dial into a network, requiring a setup time of up to 30 seconds to connect to the network.

- *3G*: The third generation of mobile wireless communications will be packet switched and based on CDMA technology. It will provide an enormous leap in the speed and capacity of wireless networks, offering high-quality voice, data, and full-motion video transmission capabilities. 3G's design contemplates that a user will be able to go anywhere in Europe, Japan, and North America and be connected seamlessly to any other user through fixed, mobile, or portable wireless systems on or over the earth's surface. Cell phone, e-mail, fax, paging, videoconferencing, and the Web will be accessible over 3G systems. 3G systems will operate in the 2 Ghz frequency band.

- *4G*: Fourth generation wireless is the stage of communications that will follow the still-developing 3G. The boundaries between 3G and 4G systems are not clear, although as with earlier generations, 4G services will offer vastly increased data transmission rates. Anticipated 4G features include worldwide roaming capability, which means that the system will connect the entire globe and be accessible from any location on or above the earth, and wireless video conferencing in 3-D, an enhancement not even available in wireline today.

Conclusion

While the global economic slowdown has delayed the introduction of 3G systems, Guglielmo Marconi might well be amazed at the extent to which wireless telecommunications technologies have permeated our lives. Similarly, it is hard for us to conceive of which standards will dominate and what applications will appeal to us in years to come. What we can expect is that wireless technologies will continue to play a significant role in communications infrastructures and, thus, will have a substantial effect on expanding our ability to convey information.

Joseph Kershenbaum, BA, MBA, JD, is a technology executive/attorney who has advised manufacturers and service providers in the telecommunications industry. The author thanks Edward Kershenbaum, chief technology officer of Grand Virtual, Inc., for his assistance with this article. Reach Joseph at joseph@kershenbaum.com.

Wireless Security: How Do You Lock the Doors?

by Curt Harler

It's great to untether your network as long as everything else associated with it does not come undone. Wireless networking is one of the few bright and growing areas in today's telecom slump. Security, however, remains a challenge.

Organizations are rapidly adopting intrusion-detection solutions, confirms Jeff Wilson, executive director of Infonetics Research (www.infonetics.com, San Jose, California).

In 2002, 48 percent of medium-sized organizations had adopted intrusion-detection systems. That figure will jump to 83 percent by 2007, Wilson predicts. At smaller organizations the growth will be from 38 percent in 2002 to 62 percent by 2007. The figures are based on 4,300 telephone interviews in North America and more than 4,000 interviews in Europe, where the trend is similar. In France, for example, the five-year growth is projected to rise from 27 percent to 60 percent, and in Germany from 20 percent to 54 percent.

This growth in demand for intrusion detection parallels the growth in demand for WLANs (wireless local area networks). In larger organizations, Infonetics projects adoption will almost double, from 38 percent to 66 percent; and in small organizations it will more than double, from 19 percent in 2002 to 42 percent by 2007.

Easy Setup

Wireless LANs are quickly expanding to "hot spots." These are areas—typically in libraries, dining halls, or other places where people congregate—that give access to the Internet. Hot spots are found lots of places other than colleges: Airports, hotels, railroad terminals, and convention centers are becoming speckled with hot spots. In fact, they are big anywhere people with PCs are likely to congregate.

Migrating a campus to wireless entails the hassles of placing multiple wireless access points and dealing with the cards in the users' computers. But that's not all.

"The chief concern in migrating to WLAN access is security," says Joe Ryan, vice president of sales at Funk Software (www.funk.com, Cambridge, Massachusetts).

"Physical wires turn out to be one of the primary obstacles to attackers looking to hack their way onto a LAN," he continues. "On a WLAN, of course, this obstacle disappears. Instead, user credentials and data are broadcast from both the client and the wireless access point in a radius which may reach 300 feet or more." Still, the benefits and ease of going wireless demand that network managers wrestle with security.

"The ease with which most wireless access points install is astounding. No wonder wireless networking has become so hot so quick," say security experts Chey and Stephen Cobb. "There's only one problem: By default, most wireless installations offer no security. None. Nil. Zilch. This means that your next-door neighbor or the business in the next office can surf for free off your connection and can probably access some of your hard drives as well."

According to the Cobbs, "The good news is that this can be fixed. The bad news is that you'll definitely need the user manual as not all wireless access points are the same." Chey Cobb, author of *Network Security for Dummies*, is an independent consultant

(www.cheycobb.com) and a former senior technical security advisor to the National Reconnaissance Office. Her e-mail address, chey@patriot.net, is heavily spam filtered. Stephen Cobb, the author of *Privacy for Business: Web Sites and E-mail,* is senior vice president of research and education for ePrivacy Group (www.eprivacy group.com). He can be reached at scobb@cobb.com.

The Situation

According to Ryan, most password-based protocols today rely on a hash of the password with a random challenge. The server issues a challenge and the client hashes the challenge with the password and forwards a response to the server, which validates it. Most common authentications—CHAP, MS-CHAP, MS-CHAP2, EAP/MD5-Challenge, and EAP/One-time Password—run this way. However, an eavesdropper who captures both challenge and response can mount a dictionary attack. This is testing random passwords against a known challenge. Eventually one works.

This brings up an interesting point. If the system used offers its own proprietary security, then the system is likely to be more secure than one relying on a public method of some sort. In most cases, the bad guys would have to have a radio from the same manufacturer in order to butt in on the wireless transmissions.

"Proprietary systems offer a whole new level of security," says Edward Milbury, management consultant with NavCom Technology (www.navcomtech.com, Newport Beach, California). "Without our radio, you're not going to get on the network. Even if you get your hands on a company radio, each unit has its own ID. So there is a lot of hardware-level security."

If the security used is a common, off-the-shelf variety of software, however, the intruder is more likely to be familiar with the system.

The most popular encryption is WEP (wired equivalent privacy). WEP is known to be broken. AT&T, for example, did a good job of cracking WEP and published its results in 2001. The problem with WEP is that both the client and the access point have the same 40-bit encryption key. When the client attempts to authenticate this "shared secret," the access point sends out a random challenge that the client returns, encrypted with the key and 24-bit initialization vector (IV) intended to randomize part of the key, using the RC4PRNG encryption algorithm. If the challenges match, the client is authenticated.

"The chief vulnerability of WEP results from the constant encryption ▶

key, the small IV, and the high speed of the connection," Kelly says. At maximum transmission speeds of 11 MBps, the system has to reuse an IV within five hours. Because few networks run flat out, the practical reuse time is 24 hours.

Early attacks against WEP developed by the University of California at Berkeley and the University of Maryland took between eight hours and several days. AT&T, using a different approach, did the job in about 15 minutes.

There is hope. TKIP (temporal key integrity protocol) is becoming available about the time this issue hits readers' in-boxes. It fixes the rotating key problem. Down the road, perhaps as soon as mid-2004, another solution called AES (advanced encryption standard) should be available. This, however, will require new hardware at the access ports. Both AES and TKIP are in the 802.11 standard.

Proprietary solutions do an end run around the problem. Funk has a system, developed with Certicom, called EAP-TTLS (enhanced authentication protocol—tunneled transport layer security). It is strong on the wireless link but still easy to set up. It is an extension of EAP-TLS (transport layer security), which is the security method used in 802.1X for Windows XP. EAP-TLS is strong but requires that each WLAN user be running a client certificate.

Cisco (www.cisco.com, San Jose, California) has an authentication called LEAP (lightweight extensible authentication protocol). It is used in the Aironet series. LEAP encrypts data transmission using dynamically generated WEP keys and supports mutual authentication.

Any proprietary solution, however, begs the point of "openness" and forward migration. As with all proprietary solutions, it means putting a lot of faith in a single vendor. With good vendors, it's a sterling solution. Otherwise, it is medicine that can be worse than the work involved to secure the network properly.

Bluesocket (www.bluesocket.com, Burlington, Massachusetts) offers technology called Secure Mobility, which gives users of laptops, PDAs, or other mobile devices wireless access to networks while moving around a campus. The system allows users to roam seamlessly across subnets, even those using IPSec tunneling, without the need to re-authenticate.

"Unlike traditional firewalls and VPNs [virtual private networks], our approach goes beyond merely preventing intruders from breaking into the LAN," says Patrick Rafter, director of corporate communications. [Read more from Patrick on page 6.] Their wireless gateway uses role-based access control to provide differing levels of access for every user on the wireless LAN.

Citrix Systems (www.citrix.com, Fort Lauderdale, Florida) markets a MetaFrame solution, which lets organizations give workers wireless access to the same applications without rewriting code. It works with Windows, Web, UNIX, and Java applications.

The company says its solution is inherently secure because it is based on a centralized model. However, Citrix does recommend adding secure gateway and VPN software to provide multilayer, end-to-end wireless security with encryption and authentication.

Funk sells its Steel-Belted Radius product, which manages VPN/tunnel access. It has support for Microsoft's RAS and PPTP connections. Tunnel authorization is based on either the username format or on DNIS (dialed number identification service).

Making It Secure

A number of companies provide spread-spectrum technology. Most claim it is inherently more secure than other wireless applications. There is truth to this. However, most wireless hot spots are not going to be spread-spectrum based.

The first thing the Cobbs recommend a college do to secure a wireless network is turn off the SSID "broadcasts." The SSID is the service set identifier, otherwise known as the name of the network. By default this name is continually shouted over the airwaves, and anyone with a wireless card in his or her laptop can walk by your office and pick up this broadcast. The default names of the SSIDs are also generally known, so this makes it easier for people to hop on your network.

If you think the Cobbs are joking, visit www.pasadena.net/apmap/ for maps of southern California showing more than 1,500 available wireless networks.

The next thing you need to do is change the default SSID name. For example, the default SSID for Linksys wireless access points is "linksys." Is it, the Cobbs ask, as if all the company's imagination was expended on product design, before the time came to choose a name? The new name should be meaningful to you but not to potential hackers, who will frequently try to guess names of

networks. Frequently used names are "accounting," the business name, or the street address.

"Remember that you're only obscuring your network from casual viewers right now. You haven't actually done anything to prevent them from finding you and hopping on," the Cobbs say.

The next task is to change the default password for maintenance and changes to the wireless access point. Again, the default passwords are widely known in the hacking community, and many wireless users forget this simple change. It's of no use to make other security enhancements to your wireless network if someone else can simply use an unchanged default password to put everything back the way it was.

After you've changed the password to something strong and unguessable, you'll want to turn off "remote management" if your system allows it. Frequently the wireless access points will have a Web interface that allows you to log on to the access point from outside your network. This is set by default for ease of maintenance and is a big security vulnerability, but turning off remote management will mean you can make changes to the access point only from inside your own network.

The most difficult task is really not all that difficult: enabling WEP (wired equivalent privacy). This is a weak encryption scheme that scrambles the data passing over the network. It's not perfect by any means, but as long as you're aware that it is not perfect, it's much better than nothing. You'll definitely need your user's manual for this change. The vendors all have different methods of enabling WEP, and you'll want to make sure you're doing it correctly. Either you will need to enter a pass phrase that will generate a shared key, or the keys will be already coded for you. Remember the pass phrase because you may need it later.

"You'll also want to make WEP 'required' for all connections, too," the Cobbs advise. "Just because you've enabled it doesn't mean that everyone will need to use it yet. After you've made WEP required, you'll have to go around to all the machines using the wireless connection to

▶

make sure that they are WEP enabled."

For colleges running Windows XP, the job is made simpler by using the Wireless Connection Manager.

Authentication

Part of the problem with wireless security is that the authentication required to get onto the network is very weak. There are a couple of ways to strengthen this weakness.

By filtering on the media access control (MAC) addresses of the college's computers, you can restrict access to only the MAC addresses you've listed. The MAC address is a unique number associated with the network card, and, if you have a small network, it's an easy way to keep outsiders out. Simply enter all the MAC addresses of the computers on your school's network into the appropriate area of your wireless access point.

Be sure to keep the list up-to-date when you change or add computers. "MAC addresses can be spoofed, so this measure isn't foolproof, but it is effective against casual hacks," the Cobbs say.

In large networks, keeping track of MAC addresses might be judged too cumbersome. In that case, upgrade your wireless access points and cards to use EAP, or enhanced authentication protocol. Enabling this will require more work and sophistication on your part because you'll have to have a strong authentication scheme to go along with it. You'll need a server that can handle digital certificates and/or security tokens for authentication. In addition, all wireless cards must be upgraded to make sure they can handle EAP.

EAP is one protocol that is not backwards compatible, and older wireless network cards may not work. All of this represents an outlay of some capital to implement, so you should have a serious commitment to it before you begin.

What Are You Protecting?

While most network administrators would like to make everything airtight and secure, remember that keeping the crown jewels secure is the main objective.

Brian Montgomery with Amdocs, Champaign-Urbana, Illinois, points out the value of encrypting the channel between the wireless and the back channel. "Even if they are able to hijack the bandwidth, they can't get into the back office," he points out.

Kelly offers six points for consideration on any wireless security:

1. Does it provide adequate credential security?
2. Does it permit mutual authentication of the client and the network?
3. Does it require dynamic encryption keys?
4. Does it support rekeying or generation of new keys during a WLAN client session?
5. Is it easy for you, the manager, to manage?
6. Related to 5, can you implement it easily on the network?

Conclusion

Wireless technology opens the door to many conveniences, and students as well as faculty and administrators will undoubtedly demand more and more wireless access to campus resources. As you provide that access, be careful to lock the doors securely behind you.

Curt Harler is a contributing editor of the ACUTA Journal, a freelance writer who specializes in technology topics, and a frequent speaker at technology events. Reach Curt at curtharler@adelphia.net.

802.11: Are You Sure You're Secure?

by Gary Audin

Attacking computer networks is a challenge for some, a business for others, and a hobby for many. Why break into a network at all? Motivations may be political, social, religious, economic, a result of boredom, or simply satisfying a need to feel superior. Whatever the motivation, time, money, and staff must be devoted to increasing network security. While wired networks and their computers are the usual targets for security attacks, wireless networks have the same problems, but also add new dimensions to the security factor. As pointed out in war-driving events, most enterprises do not adequately configure and activate the security features that are already available to them.

War Driving

War driving is an effort by individuals with wireless devices, usually laptops, to drive around in their cars and trucks attempting to connect themselves, as authorized users, to wireless networks. The First Worldwide War Drive was held from August 31 to September 7, 2002. The Second Worldwide War Drive followed quickly, during the week of October 26 to November 2, 2002. The war drive is an effort, supported by security professionals and hobbyists, to create awareness for users, encouraging them to secure their access points (APs). The war drive (www.worldwidewardrive.org/) collected and analyzed statistics relating to the ease of access to wireless networks. The November drive located 24,958 access points at risk for security breaches. The results of this war drive are summarized in Table 1. The study concluded that:

- users do not use the security features that they already own;
- those who do use the available security features adopt the default settings for the service set identifier(SSID), like everyone else, making the SSID a useless identifier;
- very few users are expending any effort to discover whether their networks are secure.

Table 1: Worldwide War Drive (November 2002).

Category	Total APs	Percentage
WEP Enabled	6,970	27.92
No WEP Enabled	17,988	72.07
Default SSID	8,802	35.27
Default SSID and No WEP Enabled	7,847	31.44
Most Common SSID Used	5,310	21.28
2nd Most Common SSID Used	2,048	8.21

What's Next? 802.11i

Improving WLAN security is an ongoing debate. The IEEE is close to completing the 802.11i standard. This standard, known as the robust security network (RSN) feature, is one that many in the industry want to adopt. RSN works, however, only when the WLAN has completely transitioned to the standard.

Wireless Dictionary

802.11 (Wi-Fi) — The IEEE Wireless LAN (WLAN) standard defined for different frequencies and speeds, with 802.11b on the market first, followed by 802.11a and continuing through 802.11g.

AES (advanced encryption standard) — A 128-bit block data encryption technique.

AP (access point) — The WLAN antenna and transmitter/receiver for multiple users.

BSS (basic service set) — A group of wireless stations.

DHCP (dynamic host configuration protocol) — Dynamically assigns IP addresses to devices.

EAP (extensible authentication protocol) — A newer protocol for authorizing users.

ESS (extended service set) — An arrangement of two or more BSSs that form a single network.

RADIUS — A protocol used for remote authentication.

RC4 — A file encryption technique.

RSN (robust security network) — The security recommendations defined in the 802.11i standard.

SSID (service set identifier) — A 32-character, unique identifier attached to each data packet. May also be called by the network name. It is not normally secured.

TKIP (temporal key integrity protocol) — An encryption protocol designed to fill the gaps of WEP.

TSN (transition security network) — Part of the 802.11i standard.

WEP (wired equivalent privacy) — An encrypted security protocol for wireless LANs.

WPA (Wi-Fi Protected Access) — Security certification for 802.11i.

(See www.webopedia.com for more information on these terms.)

RSN defines two security networks: The legacy method is hardware based on RC4 (see Wireless Dictionary at left for acronyms). The newer hardware method is based on the advanced encryption standard (AES). The AES standard has an open format that will allow new methodologies to be incorporated as they are developed. RSN uses the IEEE 802.1x LAN port authentication standard to authenticate wireless devices and to provide dynamic keys for encryption.

The migration effort to RSN includes the concept of a transition security network (TSN). The standard states that a TSN is insecure, because the pre-RSN equipment can compromise the larger network. Access points broadcast and multicast packets using the weakest configured security methods: WEP (wired equivalent privacy), or TKEP (RSN + RC4), or CCMP (RSN + AES). Critics point out that the IEEE 802.11i standard provides only legacy approaches to authentication, key distribution, and data confidentiality.

Cisco-Compatible vs. Wi-Fi Certified

If the lack of standards implementation and emerging standards were not enough, consider Cisco's announcements in February 2003. Cisco is offering to license, free of charge, its WLAN security suite to chip vendors and WLAN network interface card manufacturers. This is good... and bad. Cisco has seen the weaknesses of WEP and has been a leader in plugging the gaps. Because Cisco has more than 30 percent of the WLAN market, many users will take advantage of its security improvements. Many may have already done so. These security strengths have helped keep the WLAN market going. The WLAN market could benefit by using the Cisco technologies at no cost.

The other side of the argument sees Cisco as trying to circumvent the 802.11i standard. The standard, as supported by the Wi-Fi Alliance, will be defined as Wi-Fi protected access (WPA). This circumventing of the standard would allow products supporting WPA to be stamped "Wi-Fi Certified." We can expect subsequent levels of certification, such as WPA2, WPA3, and so on, to be introduced. Symbol and Proxim have already announced WPA compliance.

This leaves the WLAN industry with two competing and incompatible approaches: Cisco compatible vs. WPA

compatible. The Cisco version uses a proprietary authentication protocol called LEAP. LEAP is Cisco's version of extensible authentication protocol (EAP). LEAP has already been licensed to Apple, Interlink, LXE, and Funk Networks. The question then arises: Is this a generous gesture or an effort to dominate the WLAN market through security features? We need to watch this competition as well as the reaction of WPA-compliant vendors.

What Can You Do to Improve WLAN Security?

First, understand that WLAN security is a moving target. The tools, techniques, and methodologies that exist have weaknesses. However, if the security tools are *not* used, there is no security. The user organization that says "We have not had a security breach" should finish the sentence with "that we know of." Undetected breaches will be hard to quantify and even harder to prevent. Security is like insurance; you don't want to collect on the policy, but you also don't know if you have enough coverage until it is too late.

Much has been published on the subject of network security. There are many products, standards, methodologies, and techniques that cover the network itself. WLAN security is really dealing with the data-link (OSI Layer 2) and physical (Layer 1) aspects of network security. In wired networks, there is some semblance of security because of the physical nature of the cabling. The user authentication and authorization can be related to a fixed physical cable, port, and connection. The wired devices are immobile. The protocol support at Layer 2 (data link) is very similar, if not the same, for both wired and wireless networks. You must de-encrypt Layer 2, or else you must have all devices use the same encryption key when initially accessing the network. I recommend that you not encrypt the Ethernet protocol. If you do, then everyone has to have the same key—which compromises the security of the network.

Anything that increases the time it takes to break into a network improves security—maybe a little, maybe a lot—and is worth implementing. My recommendations include the following:

- *Service set identifier.* Make it more difficult to access the network by picking an unusual network name or SSID, and do not distribute it widely. *Do not* use the defaults. Turn off the SSID broadcast. Doing this may at least slow down initial intrusion attempts.
- *802.11x .* Buy the additional hardware and software to implement this standard.
- *WEP.* If you do not, or cannot, implement 802.11x, at least effect WEP. As stated earlier, WEP is not perfect, but it will make it harder to breach the network. Unfortunately, free WEP-cracking tools, such as WEPCrack and AirSnort, are readily available on the Internet. Try these against your own network to see how secure it is against attacks from these sources. Changing keys frequently will help make it more difficult to continuously hack into a network. *Never* distribute new key information over the network. Find a secure method to distribute key information manually.

- *RADIUS.* Implement this authentication protocol. A RADIUS server can be used for both wired and wireless networks.
- *Windows 2000.* Use the Internet Access Service (IAS) server option that comes from Microsoft. It has to be installed and configured before use; it is not part of the initial setup.
- *Windows XP.* This is an operating system that supports 802.1x and provides a native client that can take advantage of IAS for wired and wireless LAN security service.
- *Extensible authentication protocol .* Supported by IAS, versions include EAP-TLS (EAP with transport layer security), PEAP (protected EAP), and PEAP with EAP-MS-CHAP. All of these improve upon and make up for the deficiencies of EAP.
- *Firewalls.* Provide a boundary that, when placed between the WLAN and the wired LAN, will prevent most attacks from penetrating the wired resources.
- *IP address.* Make each of the wireless device's IP address static and turn off the dynamic host configuration protocol (DHCP) on the access point.
- *MAC address.* Require a legal address for access. This will make it more difficult to even begin an illegal authentication.
- *VPN tunneling.* This is a technique in which users' packets are wrapped in protected network packets commonly using IPsec.
- *Diversifying antenna locations.* This technique allows a single radio to use two or more antennas. The best antenna location will be automatically chosen for access. This can help prevent a denial-of-service attack.
- *Distance is not enough.* Assuming the signal will be too weak from hundreds of feet away is not a valid supposition. By rotating the antennas, the location of users and their distance from the AP can be extended. A recent vendor announcement described a phased array antenna, an electronically (not mechanical) rotatable antenna that can focus signals and increase the distance for 802.11 devices to 900 feet.
- *Disabling the stolen device.* This is a newer idea wherein a central authority downloads an internal code that triggers a disabling function and renders the stolen device useless.
- *Identifying rogue access points.* An unauthorized AP does not usually conform to the security policies that have been established. Sniffing tools such as AirMagnet or NetStumber can be used to detect security breaches of this type. AirWave can provide centralized monitoring.

Planning and Policing Security

Defense in depth, a common term in the security industry, is a multilayered security architecture that combines security tools with good management. In addition to the recommendations above, some nontechnical measures must also be implemented. Consider the following three important components of a well-managed nontechnical approach to security:

First, establish a security team of at least two people, never just one person, in order to have a system of checks and balances. You may even want to establish a chief security officer for all network and computer security.

Next, create, publish, and distribute policies that are well written, that define acceptable resource usage, and that will ensure that users understand what the potential threats may produce.

Finally, train, train, train the users and especially the first responders to a security breach.

The goals of a well-organized security team are prevention, detection, and reaction. *Prevention* requires strong user authentication, authorization and access control, good software patch management, configuration management, and recurring verifications that the security tools are working properly.

Detection of breaches or attempts on your system means you are successfully identifying threats with firewalls, intrusion-detection systems, and activity logging.

Reaction should be swift and sure. The security response team must always be ready to react immediately to isolate the problem and limit the liabilities. They must also have the tools necessary to produce evidence of the intrusion.

Typically, those who manage networks do not have a security background. Since September 11, 2001, the necessity for increased security in just about every aspect of our lives has been obvious to us all. Planet3 Wireless (www.cwne.com) is one company that offers training and certification for network professionals. Their Certified Wireless Security Professional (CWSP™) program will be available by mid-2003. The training covers WLAN intrusion, security policy, and security solutions.

In an article that appeared in the February 2003 issue of *Security Insight*, Pete Lindstrom expressed the following five DON'Ts of network security:

1. Don't say "No" to new technology.
2. Don't assume a high-security, low-risk posture; balance benefits and risk.
3. Don't react without thinking.
4. Don't neglect valuation of information assets.
5. Don't focus on the trees and ignore the forest.

When you build a WLAN you can generally close the closet door. You need only inspect it occasionally. Building a *secure* WLAN requires that you go into the closet every day. How can you know what has changed since yesterday unless you look?

Gary Audin is president of Delphi, Inc., a consulting firm based in Arlington, Virginia. A familiar face to ACUTA, he has spoken at numerous ACUTA events. Reach Gary at delphi-inc@att.net or 973/492-5655.

Campus Wireless: What to Consider

by Howie Frisch

Discussion on the ACUTA listserv recently focused on a question that went, in essence, much like this: We are considering going 100 percent wireless for our whole campus. We'll be the first in the country, if not in the world, to do this. Is this a great idea or what?

Before jumping into the technical details—which is always very comfortable for most of us and can initiate many interesting conversations—let's briefly mention some of the other issues that must be considered when looking at a wireless system implementation.

First on the list, as with any technology deployment, is to understand what services you intend to provide and who will take responsibility for providing them. Only then is it reasonable to move on to the technical details of how to best deliver those services.

From there, you should consider all the alternatives, including running your own system, contracting with a public service provider, or just "letting things happen," meaning that individual users will make their own arrangements for different services. If you decide that operating your own wireless system is a good choice, you need to move on to technical and economic considerations including spectrum, capital equipment, aesthetics, security, and likely user acceptance.

Considering these things will help you arrive at a good long-term solution that meets the needs of most constituents and makes life pleasant for the telecommunications professional who ends up responsible for handling most user problems.

Strategic decisions aside, we are free to delve into the more technical aspects of implementing wireless voice, data, and video service.

Voice Service

Most people view access to basic voice telephone service in the United States as a *right,* or at least as a *utility,* in a class with access to clean drinking water and electricity. This service has traditionally been provided on campus via a PBX or Centrex system. The package of local phone service generally includes flat rate (often called "free") local calling and incoming calling as well as some form of access to long distance.

In the early days of deregulation, the long-distance access provided a tremendous opportunity to traffic aggregators, including those serving student housing. This opportunity resulted from the fact that the aggregator could get a much lower rate per minute for long-distance service than could an individual. By charging "market" prices for long distance while paying deeply discounted rates, many institutions could fund entire communications systems for both voice and data.

In more recent times, *anyone* can get a low per-minute rate for long distance, so the opportunity to fund

Access to basic voice telephone service in the United States is viewed by most people as a *right,* or at least as a *utility,* in a class with access to clean drinking water and electricity.

major projects from this margin has evaporated. The result of this is that many institutions are considering abandoning voice services completely and suggesting that students simply use their cell phones all the time. As "they are doing this anyway," or so we hear, going wireless in this manner does seem to make sense.

In considering moving to an "all cellular" model for service, it is important to look at what service the end user really wants. Users want to be able to make outgoing calls to wherever they like, receive incoming calls from wherever they originate, do this whenever they like, and do all this at the lowest cost possible. There are many attractive cellular plans that seem to offer this option, but taking a closer look at some of the plans and the supporting technologies puts that into question. Some of the questions revolve around *when* calls can be made, while others revolve around *where*.

While a cellular provider, interested in installing equipment on campus, will show some very attractive calling rates, it is important to understand how the cellular carrier expects to get its money back and what impact that has on the institution. One easy place to start is with the concept of *average revenue per user* (ARPU) for the carrier and compare that to the offer it is making. ARPU is a common industry measure carriers use to determine profitability. The ARPU for U.S. wireless carriers ranges from about $42 to almost $70 per month per user (plus taxes and fees).

Carriers all tell the financial community that one of their objectives is to increase their ARPU to provide good returns. Of course, the other side of the story is that adding taxes and assorted fees to ARPU results in what most people know as their *phone bill.* If the "deal" offered to students is far lower than the carrier's ARPU, it may be worth a look at some of the "catches" that are likely to be included in the package to get more than the minimum from most people.

Voice Expectations vs. Limitations

Looking at a campus deployment, while an offer of thousands of free *off-peak* minutes looks attractive, there is no guarantee that anyone on campus will actually be able to use those minutes. The carrier is not likely to spend a great deal of money to carry these so-called free calls but instead may install only enough infrastructure to serve peak traffic while letting the free calls contend for the available capacity at off-peak times. This applies to both incoming and outgoing calls—even outgoing emergency calls. Depending on a 100 percent wireless solution in this environment is likely to cause dissatisfaction when callers wait just until the rates drop to place their calls, creating a major blocking condition. Should a caller need to place an emergency call to 911 during peak traffic times, this could become a substantial problem if no channels are available, raising some serious safety and liability concerns.

It is important to understand the traffic capacity that a carrier proposes to install before going to this type of all wireless solution. Additional considerations here include actual coverage inside buildings and in shadows of buildings, though these are less likely to cause dissatisfaction as the coverage holes quickly become well known and understood.

Before giving up the traditional wired phones for a full wireless service, be sure you understand the limitations of coverage as well as what you as an operator of your own system or your public cellular provider will do to address any concerns of your constituents. In the case of the outside provider, also understand what you will do should the provider choose to do nothing to address concerns.

As an alternative, the institution may want to consider operating a *local area wireless voice* or *extended range cordless* system using unlicensed PCS spectrum around 1,920 MHz. Operating a small, local system has several advantages for the campus community:

1. It gives subscribers (students and staff) a local phone number, including local-area mobility, rather than a number that would be considered long distance if dialed from campus.

2. It offers an assured price that compares to that of traditional wired phone service.

3. It provides connection to the existing campus voicemail system and access to long distance through the existing campus wired network, including prepaid and authorization-code-based long-distance access.

4. Coverage, based on microcells connected and powered using existing (Category 3) wiring, would include all buildings—even basements, tunnels, and other obscure spaces, plus outdoor areas.

Clearly, this type of system, while partially wireless, still uses some distribution wiring on campus. Traffic-handling capacity, based on the number of microcells, could easily be adjusted to meet requirements, without extensive negotiations with a wireless carrier headquartered in some remote place. Few households are ready to rely solely on their cellular phone yet. Pairing a fixed-rate campuswide cordless service, served from the local PBX or Centrex, with a second fully mobile phone with an attractive rate package would likely result in savings for most users. The plan with fewer minutes costs less, and with limited usage, users are able to stay within their allotted minutes.

This system would also allow the telecom group to offer a new, valued service to the community. Equipment to provide this service has historically been very proprietary to specific vendors as well as very expensive. However, with the likely adoption of new rules being proposed by the FCC allowing the use of high-volume, standard wireless PBX phones and infrastructure from Asia in the United States, U.S. prices should be expected to drop, resulting in high adoption rates as seen in places with competitive pricing.

Delivering Data

Campus users have come to expect virtually unlimited bandwidth at what looks like zero cost. Few are concerned with how this bandwidth is delivered. Most recent attention to wireless has been with respect to the wireless LAN access based on the 802.11 Wi-Fi standards. While Wi-Fi continues to prove its value as a very convenient access technology, it is not well suited to serving as the *only* data access for a campus based on its cost and capacity characteristics.

Of the different versions of 802.11 available, the most common are 802.11b at 2.4 GHz and 802.11a at 5 GHz. 802.11b runs at a maximum of 11 Mbps while 802.11a runs at a maximum of 54 Mbps. These data rates seem to make the technology an attractive alternative to wired service. However, before going for a full wireless solution, it is very important to understand the bandwidth demands on the system and how it will be used, keeping in mind that the quoted data rates are ideal (your mileage may vary) and that they are also shared.

Having wireless access available as a convenience would be appreciated by most in the community. Contending for this limited bandwidth from home would likely be unacceptable, especially when compared with a dedicated 100BaseT wired connection.

One technical consideration in 802.11 deployment is the impact of interference from other *uncontrolled* devices. 802.11b, at 2.4 GHz, is the most commonly deployed system based on the low cost of components and favorable radio frequency (RF) characteristics of the 2.4 GHz ISM band. The low cost of units in this band can become an issue as more devices become available in that band, particularly very low cost cordless phones. When an 802.11b LAN encounters a 2.4 GHz cordless phone, the phone interferes with the operation of the LAN. This is observed as degradation of data throughput as well as reduction in range. The Wi-Fi LAN does not stop working; it just does not work as well while the cordless phone is in use.

Moving to 802.11a, at a somewhat higher cost, has the temporary advantage of using radio frequencies that are not heavily used, so ranges could actually be better even though the RF characteristics are less robust at the higher frequencies.

Considering that standard data service expectations on campus have come to mean higher data rates than even a dedicated 802.11a connection, it seems that traditional wire may still be the best choice for primary data service. 802.11 LAN connectivity is a great added convenience and can work in places where adding wire may be difficult, but it should not be considered as the primary access technology for the campus.

A campuswide 802.11 deployment can also provide a few users with portable voice connectivity on campus. While the bandwidth available in this application would not be a good solution for general voice service, it could provide a small number of users with on-campus mobile voice access, assuming that the campus was already *wired* for 802.11 data.

As another data access convenience option, a campus that has deployed an extended range unlicensed PCS cordless system can add data capability to that system at minimal expense. While the system would function more like a dial-up network, it would provide a clear 64Kbps (ISDN equivalent) data connection in places that may be difficult to reach. It would also allow

use of phone-based short message services and could provide other "3G" features while on campus. Analogous to running voice over an 802.11 LAN, using this type of system for data is best suited to low-data-traffic applications where the primary use of the system is to carry voice traffic. Like wireless voice systems, wireless data systems do not eliminate wire; they simply make additional use of existing wiring to connect wireless access points.

Video Issues

Video subscribers have come to expect high-quality connections complete with more than 50 different programming options. Most people are at least a little bit familiar with wireless video delivery, originally known as *broadcast television* but now extended to include satellite TV and a few other alternatives. Wireless technologies are not well suited to deliver the large channel selection that viewers expect. Instead, more traditional fiber or coax systems should be used. Alternately, it is very practical to use existing and upcoming DSL technologies, running at up to 12 Mbps to provide video services on campus using existing building wiring. This type of service, based on *fiber-to-the-building* architectures, can be well suited to campus building applications using twisted-pair wire for access to rooms.

Conclusion

A few clichés can be used to sum up the state of wireless technology as a replacement for *all* communications access on campus. They are as follows:

- Wireless really means "less wire," not "no wire."
- Any new technology that looks too good to be true is probably not true.
- A lot of media attention does not make any specific technology the best solution to all problems.
- Always understand what your customers want and what things are worth to them.
- Appropriate use of different technologies will usually lead to the most efficient solution to any particular problem.
- There's no such thing as a free lunch.

Howie Frisch is sales director for UTStarcom, Inc., and a frequent contributor to ACUTA's listserv. Reach Howie at hfrisch@utstar.com.

802.11 Topologies Excel in Higher Ed

by David Geer

Wi-Fi's real security risks and rumored performance lags seem to be small obstacles to its acceptance among institutions of higher education. With increasing frequency, extending the campus LAN means going wireless. The topologies are often similar from campus to campus, applying one and sometimes two of the IEEE's 802.11x wireless protocols. Most often, 802.11b is the standard selected, either as a precursor to the coming 802.11g (with which it is backward compatible) or because it is so broadly available, having been first on the market. But some campuses have also chosen 802.11a.

Referred to as WLAN, Wi-Fi, and 802.11x, these wireless topologies find few roadblocks to implementation among colleges and universities. In this environment, return on investment (ROI) is calculated in terms of savings, value, services, and the investment made in students themselves by enhancing the learning environment.

Wi-Fi installations also present few physical challenges. Usually, campus IT departments perform the installations quickly—sometimes in just a few weeks. Once an institution has invested in vendor selection and gathered vendor input, there is little further delay before the proposed WLAN is up and running. Wireless access points (APs) deliver freedom of movement and untethered access at about 6 Mbps (adjusting from the advertised 11 Mbps for about 5 Mbps of overhead traffic, which routes and delivers the payload). Campus constituents seem to be satisfied with this speed—at least for now.

The following is a brief overview of seven campuses who agreed to share their wireless stories.

Practical Considerations at Clarion University

The Clarion University library is currently served by a wireless LAN of 30 APs, optimally placed throughout the building. "The library was recently renovated," says Michael A. Phillips, network and communications manager at the university (mphillips@clarion. edu), "so, as part of that renovation, we wired it with CAT5e cabling, but we also planned for a wireless network."

The five-story structure has adequate wireless coverage throughout as well as some outdoor access. The WLAN is interconnected through a dedicated VLAN, set up exclusively for the wireless network. The infrastructure includes Cisco wireless access points, a Bluesocket wireless firewall, and Marconi Ethernet equipment.

Clarion chose the 802.11b standard in part based on price and availability. Clarion is strongly considering 802.11g for upgrades, as many campuses are. The 802.11g protocol is not only backward compatible with 802.11b but is also expected to deliver on the promise of 54 Mbps, almost five times the speed of 802.11b. (802.11a delivers 54 Mbps but is not compatible with 802.11b or g). The 802.11g standard is expected to be finalized this year—perhaps as early as this

summer—with some producers like Linksys already rolling out 802.11g products.

What about Clarion's wireless hardware?

"We're not using the standard, 'off-the-shelf' APs from Cisco with the integrated antennas," says Phillips. Rather, Clarion is using a model from the Cisco 350 Series that adds the option of an external antenna. The Clarion library's drop-ceiling tiles were retrofitted with integrated antennas from Armstrong as part of the networking. "We wanted uniform coverage cosmetically consistent with the rest of the building," says Phillips.

Wireless ceiling tiles allow Clarion more control over where the radio signal travels. In dense areas such as Clarion's library, this helps keep any one AP from bearing the load for the whole network. The wireless ceiling tiles keep the service seamlessly invisible to its users.

Accommodating Students at RIT

Rochester Institute of Technology (RIT) prepared for the possibility of an upgrade in 802.11 protocols and APs while deploying 802.11b. By installing two Ethernet jacks at every AP location during the 802.11b installation, RIT made ready to carry two standards to ease migration. Should 802.11a or g look inviting, RIT can test the additional protocol and APs while maintaining 802.11b coverage.

For RIT, Wi-Fi is an extension of a flat, single network on a single subnet. "We expect that as wireless usage grows, we are going to run into the typical problems that are present on a flat, single network. That will dictate the need to change the topology," says Patrick Saeva, program manager for the IT department at RIT (pjsits@rit.edu). For now, this simple flat topology guarantees seamless roaming for campus constituents.

RIT plans eventually to consider additional wireless services beyond surfing and basic Internet use. As traditional return on investment concerns (and financing) are not obstacles, only a strong demand for expanded services will determine implementation.

Calculating ROI is a difficult process. RIT's decision to invest in wireless services was based on whether it would help the students. A similar philosophy guides the decision-making process at other educational institutions.

Flexibility at Syracuse University

"We bought APs that will accommodate either 802.11a or g," says Lee Badman, network engineer at Syracuse University (lhbadman@syr.edu). With a solid 802.11b base, Syracuse would lean toward advancing to 802.11g when the need for greater speed arises. The 802.11g standard provides the same speeds as 802.11a but within the 2.4 GHz ISM band. (Residing in the 2.4 band is the commonality between 802.11g and b that makes g backward compatible with b.)

The wireless topology is a neutral, demilitarized-zone network that sits outside the university's main network. It exists on one subnet across the campus. A gateway/firewall provides protected access. "It's considered untrusted, and the gateway/firewall separates the users from the rest of the campus," says Badman.

Syracuse's wireless LAN has presented no problems in the areas of speed, performance, and reliability. Security risks are mitigated by the value of having wireless LAN service and by the separation from other campus networks. Badman expects that there will always be some security risks.

Dual-Mode Solution at UNC

The University of Northern Colorado uses Vernier Networks' IS 6000 (an integrated control server and access manager) to authenticate students on its 802.11a and b networks. The wireless network is separate from the campus's wired network. Following a site survey (performed by NetCom International) Vernier was selected along with Cisco for the APs and the wireless virtual private network (VPN).

Asked why UNC uses both 802.11a *and* b, Jeanette Van Galder, director of administrative information technology (jeanette.vangalderl@unco.edu), said, "While the 802.11b network interface cards [NICs] are more prevalent in the consumer market, we wanted a dual-mode solution for individuals requiring higher speeds and additional capacity."

Segmentation from the primary network is accomplished with VLANs. UNC uses Cisco's VPN for faculty and staff for data encryption and for drive mappings to the current active directory, says Van Galder.

UNC installed in-house based on NetCom's findings for the optimal placement of APs. It also installed its own wireless security using not only VPN but also LDAP. Van Galder says that although they use the network only for WLAN, VoIP could be considered among added services.

▶

The 802.11 standard and the FCC

The FCC doesn't require licenses for any of the 802.11 protocols and so these are freely used.

"Since the FCC does not require licenses for use of the 2.4 GHz or the 5.15–5.35 and 5.725–5.875 GHz spectrum bands, companies may develop products and services according to business plans that they think will best suit users—subscription, free or whatever," says Anita Wallgren, attorney at Sidley, Austin, Brown, and Wood, LLP (awallgren@sidley.com).

Wallgren notes that the FCC does, however, stipulate that companies obtain Part 15 certification for the APs and receivers. This is in order to meet power and performance specifications. The unlicensed spectrum model for 802.11 will likely continue due in large part to its level of success.

Productivity and efficiency improvements are a big part of UNC's ROI. Because students are sharing files directly between laptops, server loads are decreasing. Students are spending more time on the network and are more productive.

Meeting Many Needs at OIT

"Basic service set [BSS] is the current layout for Oregon Institute of Technology [OIT] wireless networking. Each AP is connected to a wired Ethernet jack," says Agnes Box, telecommunications coordinator, information technology systems, OIT (boxa@oit.edu). As with other 802.11 topologies, there is some overlap of coverage by APs in order to ensure sufficient coverage everywhere.

OIT used products from vendors Cisco and Avaya (formerly Lucent), already familiar from their use at other Oregon University campuses. Specifically, these are the Avaya Wireless Access Point-3 APs with power-injected Ethernet, silver and gold wireless cards, and antennas from Avaya, which were once the WaveLAN products.

Criteria used for evaluating 802.11b solutions included the number of users connected at any one time, the ease of migration, and scalability. OIT will likely migrate to 802.11g to meet eventual demands for greater speed. Campus topology will probably evolve to extended service set (ESS) when this happens. With ESS, overlapping broadcast rings will provide roaming from building to building. As a natural enhancement to the network, the corrugated metal buildings at OIT act as antennas, sending a strong Wi-Fi signal throughout the buildings.

An Integrated System at Collegis/Salt Lake Community College

Larry Maughan's team at Collegis/Salt Lake Community College went to Proactive Network Management Corporation "for engineering, coordination, and support in integrating [wireless] into the existing network," says Maughan, director of netcomm (larry.maughan@slcc.edu). Collegis/Salt Lake is now implementing VLANs as a solution to conflicts between APs. Future services will expand to include PDAs (in trial mode now) and soft phones.

As it has for other institutions, 802.11b has been very reliable for Collegis/Salt Lake. The Cisco LEAP security product manages security, and all users are required to log on via an account on the active directory. The only problem seems to arise from weeding out bad APs. The process will be greatly unburdened by the adoption of the Cisco Wireless LAN Solutions Engine (WLSE), which will allow remote identification, location, troubleshooting, and configuration of APs. Until this solution, Collegis/Salt Lake has been searching for bad APs manually by touring the suspect coverage area with wireless laptops upon notification of the problem to technical support.

John Dunn and Proactive Network Management Corporation helped Maughan and his group with their wireless deployment. Together they set up 802.11b coverage for 13 sites including four major campuses—every room in every building. "We used Cisco ACS products for the authentication, and then it was tied back into its closest switch where it also receives its power," says John Dunn, president of Proactive Network Management (john@pnmc.com). Maughan and his team did most of the design, and the two organizations worked together on the site survey and implementations.

Seeking Security at Bridgewater State

Using Enterasys R2 APs and Cisco switches, director of telecommunications Patrick Cronin (pcronin@bridgew.edu) and the Bridgewater State College team set up 802.11a. As the

topology evolves from a simple routed network, Cronin plans for "some sort of solution to segment the collision domains without requiring an additional login as you roam." Bridgewater is considering Bluesocket, Vernier, and other solutions.

As far as security goes, "Right now we don't allow access to our administrative systems from the wireless network," says Cronin. However, as Bridgewater comes to rely more and more on the wireless network, more critical data will be transferred over it, and security will become more of an issue.

Just as many other institutions today, Bridgewater is conservative about plans for services in addition to WLAN. It has taken a glance at 802.11b phones.

Enterasys helped Cronin set up Bridgewater's 802.11a network. When asked about the topology, John-Paul Gorsky, director, wireless product line, at Enterasys (gorsky@enterasys.com), said, "The typical topology you will see is buildings, or floors in buildings, connecting back to the intermediate distribution frame on the particular floor." The wireless topology depends a lot on what the wired topology is—whether the wired networks on each floor are individual subnets, for example. Roaming works best on the same subnet.

Conclusion

There are a variety of ways to approach implementation of 802.11 protocols, and a selection of hardware solutions is available. Flexibility, keeping your options open for the future, seems to be the secret of success.

David Geer, Geer Communications, is a freelance writer who specializes in technology. He can be reached at d@geercom.com.

Shelby F. Thames is the eighth President of the University of Southern Mississippi in Hattiesburg, Mississippi. He took office on May 1, 2002, continuing an illustrious career of 38 years at Southern Miss. His previous administrative positions at Southern Miss were Chair of the Department of Polymer Science, Dean of the College of Science and Technology, Vice President for Administration and Regional Campuses, and Executive Vice President. In 1970 he was the founder of the Department of Polymer Science and in 1973 cofounder of the Waterborne and High-Solids Coatings Symposium.

At the time of his selection as president of Southern Miss, Dr. Thames had a research team of 50 people and supervised five graduate students. Most recently this team is known for the new paint based on agricultural products, which is completely environmentally safe. One of the initial uses of the paint named "American Pride" will be in the construction and repair of the Pentagon in Washington, D.C.

Dr. Thames earned his B.S. and M..S. degrees from the University of Southern Mississippi in chemistry and organic chemistry and his Ph.D. degree from the University of Tennessee in organic chemistry.

William A. Brichta has served as an ACUTA director-at-large and as board advocate for ACUTA's Publications Committee. Bill has conducted a number of our presidential interviews for the *Journal*.

Interview

Shelby F. Thames, Ph.D.

President, University of Southern Mississippi

ACUTA: For the benefit of our readers, briefly profile the University of Southern Mississippi in terms of enrollment, academic programs, research, service area, and relationship to the other public universities in the State of Mississippi system.

Thames: Southern Miss is an institution of about 15,300 students. It's a public, state university. Our principle functions are teaching, research, service, and economic development. We offer 90 Bachelor's degree programs, 80 grad programs, and our Polymer Science program was ranked among the top 10 programs in the country.

Our psychology program is one of the few worldwide accredited programs in clinical, school, and counseling psychology.

According to the Association of Education and Journalism in Mass Communications, our School of Communications ranks among the top 10 programs in the nation.

Our Special Education program is one of the largest in the U. S. Along with Harvard, Stanford, Arizona, and Colgate, we are a charter member of the Calculus Consortium.

Our Medical Technology Department is the largest in the state, and in 1998 it ranked in the top ten nationally in terms of a passing rate on the national certification exam.

The College of the Arts is one of only 20 programs in the whole nation to hold accreditation in four areas: art, dance, theater, and music.

Southern Miss has been ranked among the top doctoral institutions nationally in the International Studies program.

The Chemical and Engineering News ranked Southern Miss Chemical Sciences program among the top 50 in the nation.

Our Center of Marine Sciences offers students opportunities in marine-related sciences that are unparalleled in the Gulf Coast region.

And our University Center for Writers has received national recognition for fiction and poetry.

In terms of how good an institution we are, we are a Carnegie 1 research-extensive university. We are one of 150 institutions with that ranking out of a total of 1,500 universities in America. That puts us in the top 10 percent of universities in this country. We're also ranked number one as an SREB university. We're a Division 1 NCAA Athletic school. We're in Conference USA, and right now doing quite well with our baseball season. We're ranked in the top 25 and above, depending on which forecast you look at.

So, we are a vibrant institution. We were very strong in research this past year. Well, in 1995 we had $20 million in external funds from outside sources coming into the

campus. In the year 2002 we had $62 million. Our goal for 2005 is $100 million. And our goal in enrollment for 2007 is 20,000 students. So we have a lot of work ahead of us. We have a tremendously good group of faculty members, and we think that we will be successful.

So you can see from that little backdrop, we came from being a teacher's college—our first name was Mississippi Normal College—where we taught teachers to teach. We are the only dual campus in the state of Mississippi, and by that I mean we have a main campus in Hattiesburg where the majority of the enrollment is currently located, and then we have educational operations along the Mississippi Gulf Coast starting with Stennis Space Center on the west side moving over to Long Beach at our Gulf Park Campus, then going to Keesler Air Force Base. We have an operation at the Jackson County Junior College System, and finally over in Ocean Springs our Gulf Coast Research Laboratory has a very fine program. So we pervade south Mississippi as far as the university is concerned. We are the only university in south Mississippi. There are seven other universities in our state that are in mid to north Mississippi. The demographics are in our favor—the majority of people who live in Mississippi live in south Mississippi. That's a little bit of a backdrop.

ACUTA: In planning and engineering a campus wireless LAN, most experts indicate that the three most important steps for success are designing the network, managing the network, and security. What was the experience at USM in implementing "Eagle Air"? Briefly profile Eagle Air at USM from conception to the production system today.

Thames: In 1997 when we began looking in earnest at this process, we identified more than 100 campus buildings that needed network connectivity. When you think about the expense that would be involved in going non-wireless to those 100 campus buildings, it's somewhat astronomical. This innovative technology allowed us to provide network connectivity at about one tenth of the time and the cost for a

▶

comparable hardwired system. We partnered with AVAYA to utilize their Orinoco technology that provides Radius authentication for increased security.

Today we have more than 500 access points in more than 70 buildings at the core of the Hattiesburg campus. Several outlying areas of campus are still awaiting wireless implementation; the largest of these is our married-student housing complex where we are currently in the process of installing 85 access points. When this project is complete, all major sections of the Hattiesburg campus will have wireless connectivity.

We've had great success and have been able to do this at an insignificant cost compared to what hardwiring would have cost in terms of dollars, and as a result we are the first wireless campus in the state of Mississippi, and we're kind of proud of that. We like leading the pack.

ACUTA: One of the key challenges of wireless technologies is designing a grid of access points to maximize coverage and minimize costs in providing coverage to the service area. What have been the unexpected benefits and disappointments of the access grid designed at USM? What criteria are used to add or delete access points? What have been the important lessons learned from the initiative?

Thames: I hope you can appreciate the analogy I'm going to use. If you've ever tried to install a sprinkler system in your yard, then you can understand some of the challenges my colleagues have had with this system. You might think that in a particular area of the campus you'd get excellent coverage and in another you might not get coverage, and in some cases that has been true. We've had to experiment with that and move those sprinkler heads from one place to another so we can maximize coverage and get overlap that we need; but in the main, that has not been what we would consider a major impediment to the use of this technology. It's just something we've had to experiment with and learn, and I'm not sure anybody would have been able to select the perfect sites the first time. I think we've done a good job of that.

One of the benefits we've seen is that we've been able to use wireless for special events and functions. For example, Athletics has been using wireless for student entrance to athletic events.

The most beneficial opportunity has been the ability to use the wireless network during student registration and for previewing functions for new students who come on campus. We're able to set up wireless laptops over in the Student Union for students to register for their classes. We have reorganized the university from nine colleges to five colleges. I'm looking forward to setting up registration areas in those five colleges. One of the reasons for going to five colleges was so that we could provide more of the support that a student needed in that one area rather than running them all over campus from building to building to building. Wireless gives us the ability to provide more of the resources that a student needs in a particular locality. There might be four or five of those localities scattered over the campus. We're excited about that. This is what I would consider student-friendly technology, and we're going to use it to its fullest extent.

ACUTA: Students are carrying more and more electronic gadgets these days, such as PDAs, PDSs, phones, laptops, pagers, MP3 players, etc. Do you envision these being integrated at the University and will the University ever fulfill the role of being an ISP or common carrier for these "local" devices? What is your vision of the future broadband wireless network at USM? What are the killer apps that will spur growth? What are the major impediments to widespread deployment in the Hattiesburg area?

Thames: In terms of the local devices, those suckers are coming out at such a fast pace right now that I can't keep up with them. There's a tremendous amount of technology coming out all the time, as you well know. And what we have to do is sit back, look at our basic technology, and evaluate the technology that we think is going to have some utility for our campus. Whenever we find one of those technologies that we feel will be useful and not just faddish, then, if it is cost-effective, we're going to implement it.

I don't anticipate us being a common carrier for these local devices. That may change. No one knows what the future will hold. But at this point, I don't know that that's in the cards.

What is the future for broadband wireless? As we move forward with planned upgrades to our infrastruc-

ture, we anticipate continuous performance increases and security enhancements for our wireless network. Eventually we'll reach a point where our current 11 Mb implementation is no longer sufficient to meet the expectations of our wireless users. That seems to happen. And with that in mind we will continue to explore possible strategies for implementing next-generation wireless technologies as they become available because we are sold on wireless.

You asked what are the killer applications that will spur our growth. Well, it will typically arise from what my colleagues have told me is the convergence of voice and data networks. As VoIP and videoconferencing technologies continue to mature, the demand for fast and reliable wireless network resources will continue to increase—and at a dramatic rate.

What do we think are the major impediments to widespread deployment in Hattiesburg? Well, there is little demand for mobile computing outside the university environment. We're sort of a small town—Hattiesburg is not like New Orleans or larger cities, and there are several local businesses that are providing wireless network access to their customers, but we think this low demand for this type of connectivity will make it economically unfeasible to establish a widespread wireless network at this time. You can always do it, but we don't see that right now.

ACUTA: Although great strides are being made to resolve the security issues with wireless technologies, this area continues to be the main problem holding back widespread deployment for many applications. What are the key security features of Eagle Air? What major problems have been encountered, and how have they been solved?

Thames: Much of our concern about our security issues related to wireless

▶

networking arises from the weak authentication and encryption provided by WEP [wireless equivalent privacy]. There is a misconception that it should be possible to fully secure a wireless network using WEP. In actuality, WEP was designed to provide the same protection against casual eavesdropping that we have come to expect from switched hardwired networks. In order to ensure security, it is necessary to implement additional layers of encryption and authentication in either hardwired or wireless environments.

Access to the Eagle Air network is limited to registered users via the use of MAC address-based authentication using RADIUS. This authentication requirement was implemented with the expectation that it would prevent unauthorized users from gaining access to the wireless network while not requiring any additional action of the part of legitimate users. There are now tools available in the hacking community that allow the masking of wireless card MAC addresses, so this authentication method is no longer entirely sufficient, and we are exploring several possibilities for adding additional authentication requirements to access Eagle Air.

As mentioned earlier, a second perceived shortcoming of the WEP is its weak encryption. We strongly discourage our Eagle Air users from relying on WEP for encryption. Any network traffic that is of such a nature as to require encryption should be transferred using appropriate encryption (SSL, SSH, PGP, etc.).

ACUTA: The critical issue for colleges and universities is not whether new and innovative wireless technologies will change business processes and practices, but what aspect will change and how quickly. What key business processes and practices have changed at USM since Eagle Air was introduced? How have these changes been perceived by various constituents? Were these changes anticipated in the business case and value proposition developed in planning the project?

Thames: Our student registration has been the most beneficial business process that has changed. Student registration is a bear. It's something you want to be efficient—you don't want students standing in a line. You want to make sure they get registered appropriately, they pay the right amount of fees, not too many and not too few. That's very important. And this wireless has provided a more convenient, more efficient avenue of providing registration services to university students in different localities.

The universal connectivity provided to the campus for major events that require some type of network connectivity has been substantial allowing for dynamic reallocation of networking sources. We'll see more and more of this in our student life center that we're building—about $40 million when it's complete. And we're renovating our stadium, and, of course, all our athletic events will use the technology.

How have these changes been perceived by the various constituents? We did not anticipate all of these business process changes, but they were benefits inherent to the implementation of wireless. The original plan was to duplicate the functionality of hard-wire at a reduced cost. We weren't aware at the time of just how valuable it would be to move a computer from one side of the campus to the other by just simply walking across campus. The ease of mobility is a tremendous benefit, and it's a resource. It's a cost-saving resource that's allowed us to take advantage of our network in more ways than we had originally anticipated.

ACUTA: So you've got some added benefits that you hadn't even bargained for and that's been nice.

Thames: I guess if we had sat down and thought about it in the most simplistic terms, we would have. But you know, we were too concerned about the technologies and the depth of technology to realize just how nice it's going to be to just walk to the other side of the campus and turn your computer on, or just don't even turn it off. Walk from one side of the campus to the other with it still on.

ACUTA: P2P (peer-to-peer) technologies, in their evolution, have become harder and harder to detect. A new generation of file-sharing technologies such as Filetopia and Kazaa has upped the ante for those seeking to enforce the Digital Millennium Copyright Act by hiding the user's identity and encrypting information about the types of files (e-mail, general Internet and rich media traffic) to avoid detection. Checking any of the general download sites on the Internet consistently shows P2P client programs rank as the 1st and 2nd most downloaded files. What advice do you offer to campus leaders struggling with the challenges and dilemmas of vulnerability assessment and being a good citizen?

Thames: I would encourage campus leaders to discourage the use of P2P file sharing. An education program should be initiated to make the constituents aware of the harm that's being caused to their network traffic through these P2P channels. The Internet is an evolving technology and thus must be constantly monitored for security threats. A valid security policy must be in place and enforced by not only the security administrator but by all the leaders of the university. There must be a top-down implementation for a successful program.

ACUTA: The higher-education community and society have witnessed significant gains in leveraging the information technologies over the last 30 years. How has your campus crafted strategy to create and expand value for institutional success? What other new and innovative endeavors has USM implemented that you are especially proud of?

Thames: We've been able to obtain seed money from the Department of Education's Title IIIA. That's a strengthening-institutions grant from the Office of Technology Resources. It's a PDA initiative which has been provided to faculty members across campus to maximize the utility of the university's wireless technology and makes the promise of mobility a reality for student and faculty. As a matter of fact, just about a year ago we were out here in the administration building giving computers away to faculty members who had competed for them, and I believe they were the recipients of some of the Title III dollars.

A lady by the name of Thelma Roberson has a project where a set of PDAs was purchased and used in the Master's program in Educational Administration. That's Title III dollars. And students in the national cohort are allowed to check these out and are using them in their administrative internships. In particular, these future principals are using the PDAs and software for classroom observations, for teaching supervision, for planning, and for time management. When the students return to the Southern Miss campus this summer, they will use the data they collected and will further use their PDAs to present that data in a Power Point format.

Then we've got Dr. Steve Yuen's project. The purpose of this project is to integrate the PDA technology to foster active and collaborative learning experiences in the classroom. Students will access and interact with IT 645 "Computers in Education," a course required for the Master of Science program in Instructional Technology, on their PDA to synchronization with a desktop computer or wireless through their device infrared port and 802.11b connection to the classroom. Students will be able to check class schedules, study instructor-prepared materials, and download the weekly lecture notes, assignments, and other instructional materials to their PDA while they are in class. In addition, they will have immediate communication with their instructors, turn in electronic assignments, and share other information with their classmates and the instructor. By regularly synchronizing their PDAs they receive up-to-date class information and instruction materials or they may learn that a test has been postponed or a class schedule changed. This particular PDA-integrated course will be offered in the fall of 2003.

And then Dr. Jim Siders has a project. It's a Palm initiative which is intended to recruit and orient a cadre of faculty to infuse PDA applications into the learning activities. Ultimately, as project administrator, Dr. Siders envisions PDA media will provide the most flexible, cost-effective method of technology infusion into the general lay community as well as the university classroom. Palm devices will enhance learning through problem-solving, learning by (1) promoting data sharing or beaming files; (2) anywhere-anytime operation—in other words, portability takes the university classroom out of the classroom; (3) with encouraging through displays of data and presentation projection. Learners will better engage with the introduction of Palm devices and a shift in instruction will be realized by moving traditional direct instruction to constructionist, flexible concept development.

We think wireless is pretty neat. We appreciate what it's done for us, and we appreciate the opportunity to talk with you about what's going on at Southern Miss.

ACUTA thanks Dr. Thames for taking time to speak with us and give us this overview of the place of wireless technology on the campus of Southern Mississippi.

INSTITUTIONAL EXCELLENCE IN TELECOMMUNICATIONS AWARD 2002

Harvard University

Network and Advanced Applications Support for the Northern Crossroads

by Leo Donnelly
Nancy Kinchla

Harvard University was recognized at ACUTA's 31st Annual Conference for its operational support of the Northern Crossroads (www.nox.org), an affiliation of academic, corporate, and commercial carrier (ISP) partners with a common interest in facilitating advanced networking in New England. The Northern Crossroads meets several times each year to consider issues at hand and to hear from and talk with advanced network advocates, manufacturers, and service providers about their efforts, products, and services, as well as their commitment to advanced networking initiatives generally and Internet2 (I2) specifically. Participants include institutions of higher learning and other organizations that support research, education, and economic development. The Northern Crossroads is one of the 22 large regional advanced networks in the United States. (www.thequilt.net).

A project of the Northern Crossroads, the NoX-AP (aggregation point), was established in October 1999 under a collocation arrangement with Qwest Communications at their point-of-presence (PoP) in Boston at 230 Congress Street. Harvard University serves as the NoX-AP (Internet2 gigaPOP) network operations center. GigaPOP participants connect to the AP in various ways, including dark fiber, metro area Ethernets (802.1q), and local and regional commodity ATM services. Membership in the Northern Crossroads is not limited to those connecting to the gigaPOP. Additional members in the Boston area and throughout New England participate in the monthly meetings.

Harvard University as an institution is committed to providing the support for the network operations of the Northern Crossroads gigaPOP and promoting the use of advanced data and voice applications across its infrastructure.

Description of Endeavor, Product, or Service

Since 1999, Harvard University has worked closely with the Northern Crossroads members to provide operational support for the New England Internet2 gigaPOP as well as significant network design and planning. This effort included working with each member to develop the best plan to connect their institution to the regional network as well as jointly executing the plan with the institution and providing continued advocacy for Internet2 among current and potential members. The gigaPOP also provides private peering (exchanging routes) with commercial Internet service providers and commercial Internet access. The gigaPOP achieved operational status with nine primary members and is

quickly approaching 25 primary members, including direct connections to New England state networks, K-12, corporate, and government participants. The basic support functions we provide are the day-to-day management and operation of the gigaPOP. Yet our role, and those of all members, goes much further.

A list of the key NOC goals, objectives, and services follows:

- establish a high-performance regional exchange point for participants and commodity network service providers
- share human, material, and intellectual resources to foster the development and delivery of advanced network services and applications to our respective communities
- monitor and troubleshoot networks with four-hour response time to failures
- provide primary DNS services for both IPv4 and IPv6
- provide network element data including up-to-the minute and historical reports on bandwidth usage
- consult and coordinate with vendors on a member's behalf
- configure and install network elements
- provide support for advanced networking protocols including multicast routing (MBGP, MSDP, PIM-Sparse) and Internet Protocol version 6 (IPv6) native routing
- plan for future network services and infrastructure
- communicate with members in an effective and timely manner
- provide superior customer service to the membership

Additionally, the NOC works with participants to establish mutually agreed-upon performance objectives and operational procedures to enable each participant a practicable quality of service over the gigaPOP. Scheduled maintenance procedures provide for notification to a participant of all scheduled maintenance that could cause end-to-end connectivity loss for any user. A participant may ask the NOC to act as its agent in coordinating with vendors, or Internet2 related agencies, including the Abilene NOC. The NOC works with individual members with a wide variety of experience and skill sets.

Additional Network Operations Servers & Services

Network Element Proxy: NoX members can execute commands on the NoX network elements for trouble-shooting and informational purposes.

Intermapper Server: NoX members have remote access to bandwidth statistics and network map of the Northern Crossroads.

MRTG Server: Web-based package allowing access to up to the minute and historical bandwidth data.

Shell Accounts: Members can request shell accounts on servers hosted at the NOC that reside in NoX-AP address space.

Streaming Servers: The NoX has two Apple Quicktime streaming servers for use by the membership.

K-12 Support: Support for K-12 networking initiatives in cooperation with the participant sponsor

Vendor Related Services

The NOC negotiates with vendors on the participants' behalf for services, including equipment maintenance, fiber connectivity, and circuit pricing. The NOC provides rack and circuit location information to vendors for interconnectivity and works with regional and national providers to seek advantages to interconnection between the Northern Crossroads and a vendor's network. Harvard's Leo Donnelly, the senior technical analyst responsible for the NOC operations of the gigaPOP, meets on a continuing basis with Internet service providers and dark fiber providers and is active in local government pole and conduit commissions in the Boston metro Area.

Community Outreach

The endeavor impacts all of the participating university communities. Students and faculty have access to high speed connections via the Northern Crossroads to other regional and national participating institutions. Outreach efforts to K-12 students provide access to videoconferencing and enrichment programs. As an example, a K-12 science teacher and his/her class is able to remotely control telescopes at sites around the world via a program at the Harvard Smithsonian Center for AstroPhysics.

Applications once used across campus are now being used across the country and internationally. Harvard

▶

currently has VoIP extensions (Harvard five-digit numbers) deployed in Japan, California, and Europe. There is a close working relationship between the Department of Applied Sciences and University Information Systems providing graduate students access to the gigaPOP operations, and staff network engineers now are invited to sit in on graduate student presentations. The knowledge sharing is beneficial to both.

When connecting a primary university member, in essence we are also connecting that member's affiliates, and *Communities of Interest* are formed across the gigaPOP. With the Northern Crossroads, five primary communities have formed with high-speed connectivity joining them. All of the major hospitals in New England are affiliated with one or more of the University members. In Maine and Rhode Island, K-12 is connected with the university infrastructure and, by extension, to each other via the Northern Crossroads and nationally via the Internet2 network Abilene.

Along with the hospitals and schools, which were expected, the marine sciences discipline has formed a large community in New England via the Northern Crossroads. This not only includes the marine sciences departments at the universities, but regional aquariums, data-collecting sites on the coast, and the WoodsHole area research institutions. The physics departments of the New England institutions are collaborating in the Hadron Collider project (a tier-two data-collecting site will be located in New England), and much of the bandwidth required within the region for this collaboration is already in place via the Northern Crossroads.

Libraries are the fifth group, including one corporate participant, EBSCO, which provides services to university libraries.

Planning, Leadership, and Management Support Institution's Vision

The Northern Crossroads is a continuing project and has the support of the Harvard community. This is an ongoing commitment by the university, both financially and with dedicated personnel resources. Harvard University, within the Office of the assistant provost for Information Technology, has designated senior technical analyst Leo Donnelly to coordinate the effort. Leo is also the Internet2 technical coordinator for the university and the chief architect of the Northern Crossroads gigaPOP. Planning for this project is lead by senior management in the office of the assistant provost for Information Technology, along with the support and review by the University Technical Architecture Group, The Network Advisory Group, and the Harvard Academic Advisory Committee as well as other technical advisory committees within the university. At the operational level, Internet2 efforts are supported within the University Information Systems networking group. The Internet2 effort, including the NOC operations for the Northern Crossroads and emerging technology projects such as VoIP, represents the combined efforts of University Information Systems Telecommunications and Networking teams. All connectivity is now viewed as a potential link for multi-service operations.

Telecommunications plays a major role in all the external fiber planning for the university and with emerging technologies that cross the telecom/data boundary such as VoIP. The Northern Crossroads is viewed by the university not only as a regional cornerstone for research, but also as the foundation of connectivity to the commercial Internet, Internet2, and private peering with corporate, and government institutions.

Future Planning

This is an ongoing endeavor, and the next generation of the gigaPOP is already in the planning stages. This may include metro and possibly New England regional fiber rings, prompting discussions about defining how the region and the members look at cost-sharing and application collaboration. The regional gigaPOP is viewed as an infrastructure foundation and is the cornerstone of high-performance networking in New England. A distributed gigaPOP that may span states is in the planning stages. We are also expanding to additional carrier hotels in the Boston and Cambridge Massachusetts area to accommodate new connections and provide additional connectivity options to the members.

Business Planning

Business Planning for the Northern Crossroads NOC is done by the gigaPOP executive committee, which meets six times per year. The NOC does charge a fee for operational support as a cost-recovery mechanism only. New services are being considered, and the focus is on shared services of benefit to all of the members. These services range from: NTP (network time protocol), metro VLANs, MPLS VPNs, to shared VoIP PBXs, IP

SANs for storage, video conferencing, and video streaming. Members also share circuits to commercial carriers via Ethernet 802.1q links. Security is also an area where services are strongly being considered.

Human Resource Planning

Harvard's University Information Systems, in taking on the role of the NOC for the Northern Crossroads, has launched a continuing effort to aggressively train its network engineers on advanced networking protocols and applications. This effort far exceeds the standard two-week training period, and involves as much as four weeks of training and participation in outreach efforts, conferences, and standards bodies.

In supporting the gigaPOP, Harvard has been required to implement services for members in advance of needing those services ourselves. We need to anticipate the needs of the membership for new services and work closely with the membership to facilitate the exchange of knowledge and best practice.

Promotion of Technology and Maturity of Effort

The Northern Crossroads achieved operational status in November 1999 and has been growing on a consistent basis since that time. The National Science Foundation has just completed the second round of awards for High Performance Connections grants which has spurred a new group of New England institutions into seeking connections to the Northern Crossroads with many of their connections scheduled for spring and summer of this year. The National Science Foundation is also beginning the third round of the program and is seeking applications. It is no longer a question of growth or making it beyond the critical mass phase of the project, but how we manage the growth, the addition of new services, and plan for the next generation of the Northern Crossroads.

Many of the primary contacts at our respective institutions are involved in local, state, and regional networking initiatives. This includes fiber-to-the-curb (FTTC) and fiber-to-the-home (FTTH) committees at the city and town level. K-12 involvement is a key and strategic goal. Discussions on the future of advancing networking with our respective state governments are ongoing. Discussions are moving in a regional direction along these lines as well.

V²D (Voice, Video, and Data) Applications

A number of trials require very low latency links back to the participant's respective institution. This includes video and VoIP. This forms a major component of the model. The commercial peering connections provide high-speed access from the commercial carrier's network back to the participants' institutions. We have a number of employees now with VoIP extensions at home in pilots. A number of video conferencing projects involving MPEG2 video have been conducted across the gigaPOP infrastructure with excellent results. The advanced applications are many and cover a broad range of disciplines. For more examples of applications see www.internet2.harvard.edu or www.internet2.edu .

Quality, Performance, and Productivity Measurements

The NOC on a daily basis is responsible for monitoring 19 circuits ranging from DS-3s to 1GB Ethernet connections. The Northern Crossroads is technology agnostic,

and these circuits may be POS (packet over SONET), ATM, or Gigabit Ethernet connections. Not only is typical up/down status monitored, but we also monitor session status for the unicast and multicast routing protocols including BGP, MBGP, and MSDP.

The NOC defines the routing policy and handles routing prefix updates for the members. This includes coordinating with the Abilene NOC. Network management systems monitor the quality and performance of the circuits, and members have direct feedback via remote access to these systems.

The NOC also provides a unique monitoring and training tool via e-mail. Whenever a change is made to a gigaPOP network element, a "diff" is done with the old configuration, and the change is e-mailed to the gigaPOP members with the preceding 10 lines of code and the trailing 10 lines of code. This allows all the members to see every change. Even if a member is not running multicast or IPv6, he can learn from the configurations done by those that are. Template configurations for multicast, ATM, and IPv6 are available to all members. Within network operations, quality, performance, and productivity are measured continuously on a 7 x 24 basis with the gigaPOP members having access to the same systems the NOC uses.

Cost, Benefit, and Risk Analysis

Direct and Indirect Cost

The Northern Crossroads uses a weighted divide-by-N model for allocating the Abilene connection costs and Internet2 fees associated with the gigaPOP. Participants connecting at 1Gb (1000 MBps) pay more for their annual fee than a participant with a DS3 (45 MBps) connection. The Northern Crossroads currently has an OC48 (2.4 GBps) connection to the Abilene Network and is planning an upgrade to OC192 (10 Gbps) when required. In theory, the participants with the larger connections could use all or more of the bandwidth at any given point in time, while a participant with a DS3 (45 MBps) or OC-3 (155 MBps) is limited by the speed of his respective local loop; thus his yearly operational costs for the gigaPOP are less.

Commercial Internet bandwidth can range from $125/MBps to $200 plus/MBps. The cost of bandwidth at the Northern Crossroads is now at $7 dollars/MBps. Even though traffic today is limited to Internet2 members and international research and academic peers, a significant reduction in cost to the members could result when combined with the private, non-transit peering with the commercial ISPs.

Every bit sent via the Northern Crossroads gigaPOP is an inexpensive bit. For example, if Harvard is sending 100 Mbps of traffic to the gigaPOP, that is 100 Mb of traffic not being sent out its commercial Internet connection at the much higher rate per bit. The members share the operational costs on a divide-by-N model as well. However, there are no weights in this portion of the model. The operational expenses include the equipment maintenance, carrier hotel space, power and equipment upgrade and additional port fees. These fees include the network operations cost provided by Harvard University.

Benefits

A key strategic goal of the Northern Crossroads has been the deepening of the relationships among the New England academic institutions. The advantages of the collaborative nature of the Northern Crossroads are many and varied. We share information, best practices, technical expertise, and, most importantly, a sense of being in this together. This translates into cost savings for all of us, and we tend to think regionally, even when acting locally. Of course the original, but not the sole reason for collaboration, was to share the costs of the connection to Abilene. This has evolved into a much broader context to the benefit of all the participants.

Risk Analysis

The current economic conditions in the telecommunications marketplace highlight the reasons for collaboration, and in fact have driven home the advantages of cooperation within our community. The participants in the Northern Crossroads are in a position to take advantage of multiple Internet service provider connections, including arrangements with service providers for insurance bandwidth to the commercial Internet at low cost. This is possible because of the aggregation of circuits by the Northern Crossroads' participants and the facilities-based access to commercial Internet service providers. The time to turn up a new circuit is also considerably quicker because of collocation with those vendors.

The biggest risk is managing the growth and the resulting increase in cost of the Northern Crossroads, as we plan the next generation of the network. Since the model is a divide-by-N model weighted by speed of connection, each new customer, particularly ones

connecting at a higher speed, will reallocate the costs across all the members and, to a degree, insulate the smaller participants.

Long-term planning is required to anticipate technology upgrades at roughly three-year intervals. This planning is underway, and the current condition of the telecommunications market has many of us viewing owning our own local loops and metro assets as a way of controlling costs in the future and allowing us to switch carriers if required within short time frames. Time frames may be measured in days and weeks as opposed to months by many carriers.

This material was updated from the material submitted by Leo Donnelly (leo_donnelly@harvard.edu) and Nancy Kinchla (nkinchla@camail.harvard.edu) for the 2001-2002 Institutional Excellence Award. ACUTA thanks Harvard for sharing this information with our membership.

Advertisers' Index

★ Indicates ACUTA Corporate Affiliate

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to telecommunications in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal.

security requirements. The community generally opposes such requirements.

The HEIT Alliance also agreed to advocate for increased funding of cybersecurity R&D and to support the development of training opportunities for cyber-security professionals and campus IT personnel.

Nancy Wong of the Office of Homeland Security described that new department's efforts to create an integrated structure for homeland security, including science and technology. One of her comments was perhaps the most profound of the entire forum: Increased concern for security is not a temporary matter—it is likely to be a necessity in the United States for the rest of our lives. The role of her office will be to develop an implementation plan for the National Strategy to Secure Cyberspace, which was released in 2002. She discussed several important roles for the academic community:

1. Protection of cyberassets
2. Research and development
3. Training of cybersecurity professionals
4. Integration of security training into all areas of the curriculum, not just computer science and information technology

Cyberinfrastructure: The National Science Foundation (NSF) is being urged by a blue-ribbon committee of scientific and engineering experts to establish a large-scale cyberinfrastructure to enable university scientists and engineers to work in new ways on advanced research projects. The NSF has requested $20 million to begin the initiative, but it will be a major multi-year program that could require an investment of up to a billion dollars a year. The HEIT Alliance endorsed the findings of the blue-ribbon panel and will support legislation to further the goals of the report.

Intellectual Property: As intellectual property issues on college and university campuses continue to draw interest in the press and on Capitol Hill, this was a major issue at the forum. The group agreed that the Digital Millennium Copyright Act (DMCA) may have tipped the scales too far in favor of owners of copyrighted material, hindering *fair use* for legitimate educational purposes. Legislation (H.R. 107) has been introduced to correct perceived deficiencies in the law. Several higher-education and library associations are supporting the legislation.

In the area of peer-to-peer (P2P) file trading, there is a joint committee of higher education and the entertainment community working on solutions. However, Congress seems to be growing impatient, and the recording industry is not waiting for cooperative solutions to be crafted (hence, the lawsuits filed against students by the Recording Industry Association of America in early April). The HEIT Alliance urged institutions to seek ways to reduce or eliminate the illegitimate use of P2P file sharing, without interfering with legitimate activities and the academic culture of collaboration among students and scholars. They also encouraged the development of best practice models in the higher-education community.

Privacy: The 108th Congress is expected to be very active on privacy issues. The HEIT Alliance will monitor legislation to ensure that higher education and library interests are represented.

Spectrum Management and Wireless Internet Access: The FCC and Congress are both looking at available spectrum and spectrum management policy. It is possible that ITFS spectrum could once again be on the table as an option for new wireless technologies. The HEIT Alliance urged its members to respond to FCC public inquiries and to monitor ITFS spectrum and usage issues.

The HEIT Alliance also looked at a number of funding priorities. A full report of the Alliance's policy program and funding recommendations for 2003 will be available soon, and we will ensure that it is linked to the ACUTA Legislative/Regulatory Web page.

ACUTA is fortunate to have the opportunity to participate in and contribute to the HEIT Alliance forum. We will continue to share relevant information about federal policy issues as they arise and to provide useful background information on the Legislative/Regulatory Web page and in our publications and educational programs.

Jeri A. Semer, CAE
ACUTA Executive Director

From the Executive Director

Higher Education Technology Forum Examines High-Priority Issues

Once a year, ACUTA is invited to participate in a forum of higher-education associations that meets to examine high-priority federal technology-policy issues. The Higher Education Alliance for Information Technology (the HEIT Alliance) sponsors the forum. This year's meeting took place in a highly charged environment in Washington, D.C., two days prior to the start of the armed conflict in Iraq. Everyone at the meeting, including presenters from federal government agencies and attendees from the higher-education community, was cognizant of the fact that war could begin at any time. Both physical security and cybersecurity were at the forefront of everyone's concerns, followed by uncertainties of the cost of the coming war and its impact on the federal budget and the U.S. economy.

The result of the forum will be a set of positions on various issues to be considered by the federal government, including both Congress and the executive branch, during the coming year. I would like to share just a few of the issues that I think will be of interest to ACUTA members.

Broadband: The HEIT Alliance will become more active in making the case in Congress and with the administration that higher-education institutions play a significant role in developing new broadband services and driving demand for those already in use. The Alliance will seek additional federal resources for R&D for advanced broadband technology. The important role of broadband in workforce development and the support for municipalities and other public agencies by higher-education institutions will be emphasized.

Computer and Network Security: The HEIT Alliance members will continue efforts to raise awareness at institutions of the importance of improving the security of college and university computers and networks. On February 28, the president of the American Council on Education sent a letter to college and university presidents urging them to set a tone of awareness and establish responsibility for campuswide cybersecurity at the cabinet level.

The EDUCAUSE/Internet2 Task Force on Computer and Network Security has commissioned a legal memorandum on "IT Security for Higher Education: A Legal Perspective," available at www.educause. edu/ir/library/pdf/csd2746.pdf. The memo presents a good summary of the applicable laws and is worth reading.

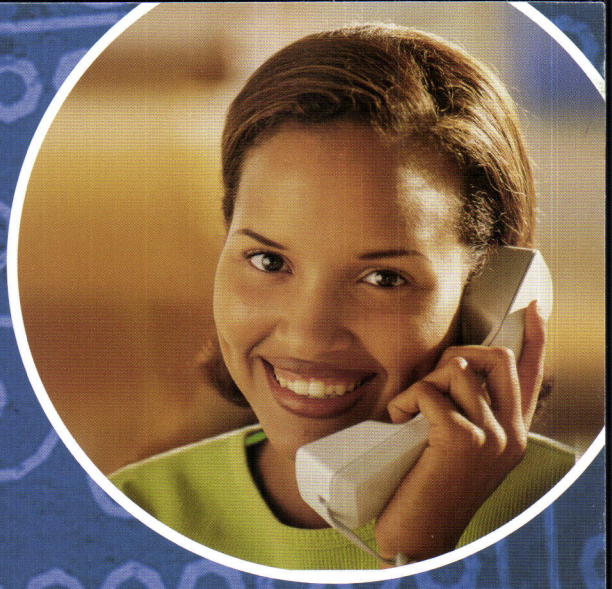
The group will also closely monitor legislative developments in areas such as identity theft and the use of Social Security numbers for identification. Other areas of interest that will be monitored are federal research grants and contracts, with particular concern for any proposals that tie the receipt of federal research funds to specific IT

continued on page 47

Making your University a

Communications Profit Center

Interaction Center for Higher Education



Course loads in college can be grueling.
Campus communications don't need to be too.

Students, professors and administrators all present diverse communications needs, especially with their laptops and wireless devices. Yet the outdated proprietary systems pieced together on most campuses can't give users and institutions of higher learning what they need.

The *Interaction Center for Higher Education* software does.

Once it puts every school, administrative office and library on a **single non-proprietary communications platform,** IC for Higher Education takes anytime communications & unwired access campus-wide and beyond.

It can even make bursars smile.

Generate Revenues via Subscriber Services
Unified messaging • Voice mail • Student / faculty locator services • Find-me/Forward message routing • Conferencing • Status & calendar management • Info on demand • PDA access to contact directories & personal settings

Reduce Total Cost of Ownership
Integrate University call centers, hospitals and other operations • Manage campus directories & message stores from a common interface • Make in-house adds, moves & changes in one directory

Protect Existing Investments
Migrate to **SIP-enabled IP telephony** (VoIP) with no forklift upgrades • Scale to hundreds of thousands of users • Deploy functionality as needed for mobile users, IVR, and "in demand" interaction applications

Maximize Time Management & Productivity
Access messages via phone, PC, cell phone, PDA & the Web • Schedule appointments & reminders from a database • Fax from the desktop • Check the status of users & workgroups in real-time

Interactive Intelligence. Lowering the expense of higher ed.

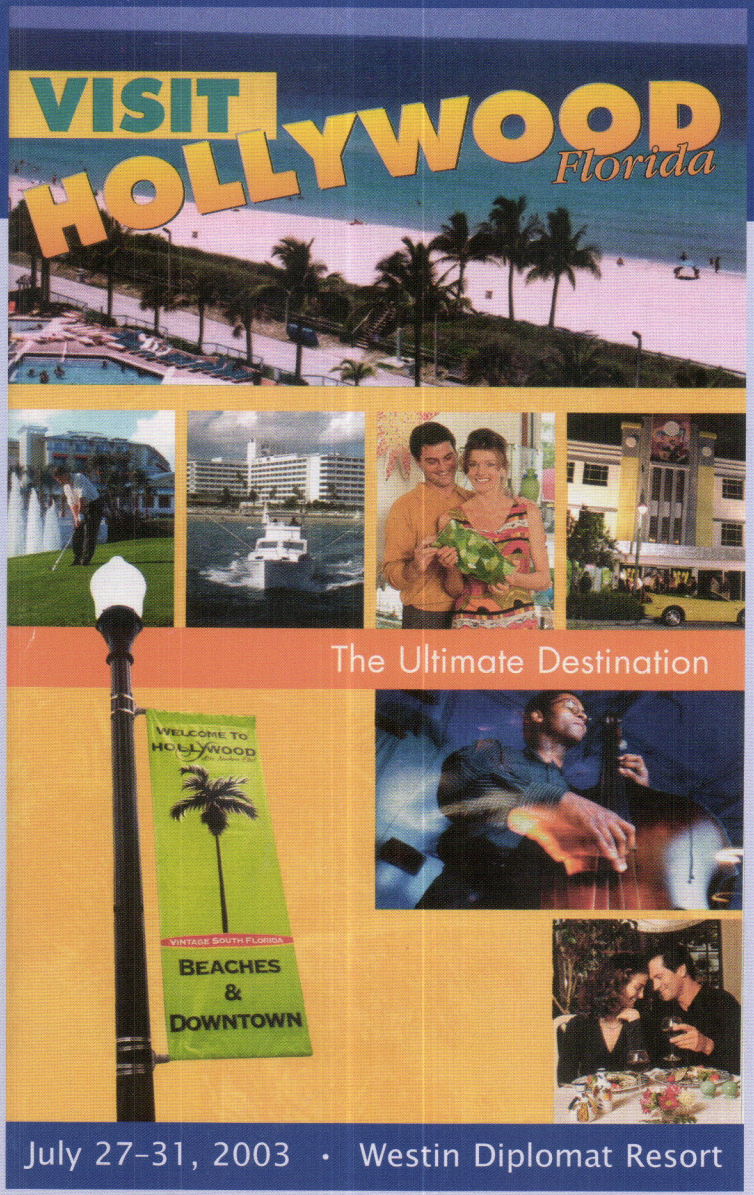
INTERACTIVE INTELLIGENCE®

WORLD HEADQUARTERS
7601 Interactive Way
Indianapolis, IN 46278 USA
317.872.3000 voice and fax

www.ININ.com

ACUTA

32nd Annual Conference & Exhibition



July 27–31, 2003 · Westin Diplomat Resort

For More Details or to Register Online,
Visit Our Website at

www.acuta.org

or call 859/278-3338

In Addition to the BEST in **Professional Networking,** Here's What You'll Find at the ACUTA conference:

Keynote Speaker

- Bruce Jenner

General Sessions

- Technology Strategist Larry Irving
- Attorney Jeff Linder
- Humorist Tom Ryan

53 Breakout Sessions

- Network Security
- Is VoIP Cost Effective?
- Negotiating Contracts
- Lesson in Leadership
- IT Reorganization

...and more

Exhibit Hall

- Carriers
- Equipment Vendors
- Networking Companies
- Consultants

...and more

Riding the Wave of Change

ACUTA

Benefits of Membership Just Keep on Growing

Matrix Covers Legislative/Regulatory Issues at a Glance

Sometimes you want to know—briefly—what's going on in Washington that might have an impact on your campus. ACUTA is proud to present the new Legislative/Regulatory Issues Matrix, a document that provides a brief description of the major issues, the status of each, ACUTA's position or action taken, the date of the last update, a link to ACUTA's Legislative-Regulatory Newsletter, and whom within ACUTA to contact for more information.

The URL is http://www.acuta.org/Relation/downloadFile.cfm?DocNum=767. This document will be updated quarterly, and we plan to include a link in the Leg/Reg Update electronic newsletter each time it is updated.

ACUTA Resource Library Allows Online Uploading of Documents

A new feature has been added to the "MY ACUTA" portion of the ACUTA Portal/Web Page which will allow online uploading of documents being contributed to the ACUTA Resource Library. This feature is accessible to anyone who has registered their login and password for the portal and can be accessed by clicking on "My ACUTA" in the upper right corner of the Web page.

If you are not sure you have a Web preferences account, use the URL: http://www.acuta.org/myacuta

Now when someone on the listserv asks for a document and several other people say they'd like it as well, you have the option of posting it to the Resource Library and referring everyone to it there. Submitted documents will be reviewed by ACUTA staff for appropriate content and then posted, generally within 24 hours.

The Resource Library contains more than 100 useful documents including RFPs, position descriptions, campus directory samples, and documents of general interest. They can be listed by these categories or searched by keyword. All have been contributed by ACUTA members. Access the library and the document upload feature by going to the URL: http://www.acuta.org/Dynamic/Library/index.cfm

Database of University Telephone Numbers Reduces Unauthorized Charges

The ACUTA Telephone Numbers Database provides subscribers access to a list of telephone numbers belonging to participating colleges and universities. Since those numbers are ineligible for billing of services not ordered by the institution, local and long-distance telecommunications carriers and billing companies who subscribe to this service may flag the numbers in their systems. The service is designed to greatly reduce or even eliminate costly and time-consuming incidents of cramming, slamming and other unauthorized charges.

Unauthorized charges can include calling plans, calling cards, and other products and services that are being billed to colleges and universities without proper authorization from the institution.

The annual subscription fee of $1,000 for companies is calculated to cover the cost of developing and maintaining this service. There is no charge for institutions to list their numbers. The database will allow unlimited access to the information at a cost far less than the potential expense of responding to even one complaint to the FCC for slamming or cramming.

Schools can enter their numbers into the database at http://www.acuta.org/relation/downloadfile.cfm?docnum=718.

Companies that wish to subscribe to the database can do so at: http://www.acuta.org/relation/downloadfile.cfm?DocNum=723.

The ACUTA Store

If you haven't visited the ACUTA website lately, you may not know that a number of items may be purchased from ACUTA, including ACUTA logo merchandise such as an organizer padfolio, a portfolio clock calculator with a pen, a sports bag, and a mug.

In addition, audio tapes of past Web seminars, audio seminars, and other events are also available, at a very reasonable cost. Listed below are just some of the titles from these presentations. These tapes provide valuable information on a variety of subjects tailored specifically to the ACUTA audience. You will find them especially useful for training new staff or those who were unable to attend the events.

You are encouraged to visit "The ACUTA Store" on the Web at www.acuta.org. Click on "Member Services" on the menu bar, then "The ACUTA Store."

Web Seminar Audio Tapes
Wireless Hot Topics (June 24, 2003--planned)
Wireless LAN Security Issues (August 27, 2002)

2003 Audio Seminar Tape
The Current State of the Telecom Industry (May 6, 2003)
Network Security Issues (March 19, 2003)
Wireless Business and Regulatory Trends (March 4, 2003)
Design & Service Impact of Putting Voice Traffic on a Converged Network (Feb 11, 2003)

2002 Audio Seminar Tape
Economic Conditions in the Telecommunications Industry (August 8, 2002)
Division 25 Construction Specifications for Telecommunications (June 20, 2002)
A Model to Train IT Support Staff (April 2, 2002)
Implications of Counter-Terrorism Law for Higher Ed Telecommunications and IT Operations (February 5, 2002)

2002 Winter Seminar Handouts and Audio Tapes
Handouts and audio tapes are available for purchase.
Topics include Track 1: Supporting Telecom and IT Customers
Track 2: New Technologies

2001 Fall Seminar Handouts and Audio Tapes
Handouts and audio tapes are available for purchase.
Topics include: Track 1: Maintaining or Improving the Bottom Line
Track 2: Management of Data Networks

CD-ROM: Intro to Data Networking for Voice Managers
Instructional CD-ROM; Custom designed for ACUTA members with a background in telephony who need to understand data networking. Presenter is Gary Audin.

ACUTA

ACUTA's core purpose is to support higher education institutions in achieving optimal use of communications technologies.

Be a good neighbor: Invite a colleague to be a part of the ACUTA network!

Conference Registration Form

32nd Annual ACUTA Conference & Exhibition • July 27–31, 2003

REGISTER BY JUNE 20 and SAVE!

REGISTER ON THE WEB: WWW.ACUTA.ORG

Name

Title — First name as it should appear on name badge

Institution/Company

Address

City, State/Province, Zip Code

Phone # — Fax # — E-mail Address

Emergency Contact — Daytime Phone — Evening Phone

❒ School Reps Only: Check here if this is your first ACUTA event.

❒ Check here if you have special needs (accommodations, restricted diet, etc.) during the conference, or call Lisa Cheshire, ACUTA Meetings Manager, 859/278-3338.

For travel discount information, call Commonwealth Travel 800/274-7135 859/277-7135

Send this form plus full payment of registration fee or valid purchase order to:
ACUTA, 152 W. Zandale, Ste. 200
Lexington, KY 40503-2486
Fax: 859/278-3268
Make check payable to ACUTA.

• Charge $_____ to my:

❒ AmEx ❒ VISA ❒ MC Exp _____

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Verification code _____

Print Name on card

Signature required

Early registrations cannot be processed unless accompanied by check, purchase order, or credit card payment.

• Federal ID #61-1185913

• **Confirmation materials** will be sent within 2 weeks of receipt of payment or purchase order. If you have not received confirmation within a few weeks, please check with your Accounts Payable office to confirm processing, then call ACUTA. **Direct inquiries to Kellie Bowman 859/278-3338 or e-mail: kbowman@acuta.org**

PRECONFERENCE SEMINARS Half-day seminars, Sunday, July 27, 2003

$ _____	❒	8:30-11:45 am	Planning Issues for Mobile Computing
$ _____	❒	8:30-11:45 am	Everything You Want to Know About Security
$ _____	❒	1:15-4:30 pm	Strategic Business Technology Planning
$ _____	❒	1:15-4:30 pm	IT Policy, Procedures, and Services

Cost: $129 each. Includes course materials & coffee break. Space is limited; register early.

CONFERENCE For Early Registration discount, response must be postmarked or received no later than 6/20/03

		by 6/20/03	after 6/20/03
$ _____	ACUTA Member/NASTD Member	$595	$645
$ _____	Nonmember	$725	$775
$ _____	Emeritus Member	$395	$395
$ _____	Student	$350	$350

SPECIAL OFFER TO NONMEMBERS If you attend the ACUTA Conference then purchase a membership within 90 days, the difference between member & nonmember registration fees will be applied to your initial membership dues.

Conference Registration Includes:

- All educational sessions
- Course materials
- Access to Exhibits
- Sunday evening reception
- Monday evening event
- Wednesday banquet
- Breakfast 4 days, lunch 3 days
- Coffee breaks
- Hospitality Suite

ONE-DAY REGISTRATION

Cost: $295 Includes sessions, materials, meals, breaks, and evening events if scheduled for that day.

$ _____ ❒ Mon ❒ Tues ❒ Wed (Check one box only.)

ACUTA FORUM FOR STRATEGIC LEADERSHIP IN COMMUNICATIONS TECHNOLOGY

This event has a targeted audience. Please check the Web site or call for details.

$ _____ **Leadership Forum**
Members: $595/ $645 after 6/20/03 • Nonmembers: $725/$775 after 6/20/03

$ _____ **TOTAL DUE** (Add all items in shaded area)

COMPANION FEES FOR EVENING EVENTS

Anyone **other than** registered attendees & exhibitors who have paid a social registration fee must pay to attend the Sunday evening reception ($25), Monday evening event ($55), and Wednesday banquet ($60). Please enclose payment (remit to address shown above) or indicate that payment will be made at registration. (Sorry, children under age 16 may not attend.)

Name _____

City, State/Province _____

$ _____	❒ Sunday Opening Reception in Exhibit Hall	$25
$ _____	❒ Monday Evening Dinner Event	$55
$ _____	❒ Wednesday Night Banquet	$60
$ _____	**TOTAL COMPANION FEES**	

❒ PAYMENT ENCLOSED ❒ WILL PAY COMPANION FEES AT REGISTRATION ❒ CHARGE (Info top right)

Cancellation/Refund Policy

• **Cancellations received by July 11, 2003:** Full refund if notice of cancellation is received in the ACUTA office by July 11.

• **Cancellations received July 12–25, 2003:** Registration fee must be paid. Credit memo will be issued for any cancellation received July 12–25. Credit must be applied to registration for another ACUTA event in 2003 or 2004.

• **Cancellations received after July 25, 2003,** are not eligible for refund or credit.

• **Cancellations may be mailed, faxed, or e-mailed to Kellie Bowman 152 W. Zandale Dr., Ste. 200, Lexington, KY 40503; fax 859/278-3268; or e-mail kbowman @acuta.org.**

FOR HOTEL INFORMATION/RESERVATIONS, CONTACT: Westin Diplomat Resort & Spa,3555 S. Ocean Dr., Hollywood, FL 33019. Phone 888/627-9057 or 954/602-6000. Ask for ACUTA rate: $130 single/double. Cutoff date is June 20.

Program Selection

Please indicate which concurrent sessions you plan to attend. This is not a commitment, but will help us plan rooms, handout quantities, etc. CORP indicates corporate presentation.

Selected sessions will be video streamed over the ACUTA website after the conference.

SUN

2:30–4:00 p.m.

___ User Group: InteCom
___ User Group: Siemens

MON

10:45–11:45 a.m.

___ FISH, Part 1
___ Convergence Readiness Assessment
___ Network Security
___ Creating a Community Network
___ CORP: Managing Telecom Spend

1:15–2:15 p.m.

___ FISH, Part 2
___ Broadband Issues
___ Technology Infrastructure Trends & Directions
___ Successfully Deploying VoIP
___ CORP: Speech Recognition

3:45–5:15 p.m.

___ University Survivors
___ What Technologies Students Want
___ Mobile User Challenges
___ Is VoIP Cost Effective?
___ CORP: Next Generation Call Center
___ User Group: Compco
___ User Group: Pinnacle
___ User Group: Telesoft

TUES

10:30–Noon

___ Managing Communications Infrastructure Projects
___ Computer & Network Security Advice
___ Structured Cabling Challenge: Cat 5e vs Cat 6
___ The Beacon Project
___ CORP: ASP Resale & Chargeback Call-Accounting Service
___ User Group: Cisco

1:15–2:15 p.m.

___ Negotiating Telecom & Network Contracts
___ Wireless at NC State
___ Security for Major Campus Events
___ Role of the Contact Center
___ CORP: Assuring High-Speed Cabling Capabilities

3:45–5:15 p.m.

___ How to Hire a Technology Consultant
___ Making the Case for IT Funding
___ Making Hard Choices re VoIP
___ Law & Technology for Accessible Telecommunications
___ CORP: Harvard Medical School Wireless Campus Project
___ User Group: Avaya
___ User Group: NEC

WED

9:45–10:45 a.m.

___ Cost Analysis
___ Hot Topics in Legislation & Regulation
___ California Video over IP System
___ Music File Sharing and the RIAA
___ CORP: Using Voice Automation During a Disaster

11:15 a.m.–12:15 p.m.

___ Pinpoint E911 Implementation
___ How Will You Migrate to VoIP?
___ Privacy Issues
___ The Latest Technology in High-Speed Cabling
___ CORP: Event Management—Are You Prepared?

1:30–2:30 p.m.

___ People Make a Program—A Lesson in Leadership
___ Copyright Issues
___ Managing Wireless vs. Wireline Trends
___ IP-Based Videoconferencing Successes
___ CORP: Applications for Directories & Speech Recognition

3:00–4:00 p.m.

___ Directory Database Services
___ Disaster Management for Public Safety Communications
___ DC Power Preventive Maintenance
___ IT Infrastructure Quality & Savings through Commissioning
___ CORP: Utilizing Power over the Ethernet
___ User Group: AT&T (ACUS)
___ User Group: Centrex

THUR

9:45–10:45 a.m.

___ Executing a Successful IT Reorganization
___ Universal Service
___ Unified Messaging Benefits & Applications at Michigan
___ Broadband Services to the Off-Campus Community

Birds of a Feather

Topic Suggestions (See details on page 16.)

_____

_____

_____

Please return both conference registration pages to ACUTA.
FAX: 859/278-3268

Questions about registration?
Contact Kellie Bowman · 859/278-3338 ext. 222 · kbowman@acuta.org