Spring 2001

ACUTA Journal of Telecommunications in Higher Education

Follow this and additional works at: http://digitalcommons.unl.edu/acutajournal

http://digitalcommons.unl.edu/acutajournal/22

This Article is brought to you for free and open access by the ACUTA: Association for College and University Technology Advancement at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in ACUTA Journal by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
If the cost of automating your call center is hard to swallow, try smaller bites.

Any way you slice it, STARTEL's call center technology is a cut above the rest.

Our PC-based system offers comprehensive communication capabilities to efficiently process calls, messages and information requests. Centralized Attendant, Security Monitoring, Desk, Information Exchange, Operatorless Paging are just a taste of what this powerful system can do. So if you're looking for call center technology at a price that's not too hard to swallow, we have the answer. Call 1-800-STARTEL today.

STARTEL, a Converse Company

17661 Cowan Avenue
Irvine, CA 92614
www.startelcorp.com
ACUTA is a member-driven organization dedicated to the enhancement of teaching, learning, research, and public (community) service by providing leadership in the application of telecommunications technology for higher education.

Spring Seminars
April 8–11, 2001
Newport Beach Marriott
Newport Beach, California

30th Annual Conference
July 29–August 2, 2001
Disney's Contemporary Resort
Lake Buena Vista, Florida

Fall Seminars
October 21–24, 2001
Hyatt Regency
Albuquerque, New Mexico

Winter Seminars
January 13–16, 2002
Wyndham Resort & Spa
Ft. Lauderdale, Florida

For details about ACUTA events or to register, visit our Web site at www.acuta.org
Cyberthreats can be categorized into three groups: unstructured threats from insiders and hackers; structured threats from "hacktivists," economic espionage, and organized crime; and national security threats from terrorists and foreign intelligence agencies.

—Evan Corcoran, Attorney
Wiley, Rein & Fielding page 13

The ACUTA Journal
of Telecommunications in Higher Education

Published Quarterly by
The Association for Telecommunications Professionals in Higher Education
152 W. Zandale Dr., Suite 200, Lexington, KY 40503-2486
Phone: 859/278-3338
Fax: 859/278-3268
E-mail: scott@acuta.org

Publisher: Jeri Semer, CAE, ACUTA Executive Director
Editor-in-Chief: Pat Scott, ACUTA Communications Manager
Contributing Editor, Curt Harler
Advertising Sales, KCS Int'l., LLC, phone 717/397-7100, www.kcsinternational.com

ACUTA BOARD OF DIRECTORS 2000–2001
President Anthony Tanzi, RCDD, Brown University
President-Elect Maureen Trimm, Stanford University
Secretary/Treasurer Dave Lewis, University of Rochester
Immediate Past President Tony Mordosky, Rowan University
Directors-at-Large
William A. Brichta, DeSales University
Steve Harward, University of North Carolina, Chapel Hill
Jeanne Jansenius, University of the South
Patricia Todus, Northwestern University

PUBLICATIONS COMMITTEE
Chair: James S. Cross, PhD, Michigan Technological University
Ron Kovac, PhD, Ball State University
Walt Magnusson, Texas A & M University
Barb Renner, University of Cincinnati
Jan Weller, Washington University in St.Louis
Ex Officio: Anthony Tanzi, RCDD, Brown University
Jeri Semer, ACUTA Executive Director
Board Advocate: Dave Barta, University of Oregon
Staff Liaison: Pat Scott, ACUTA Communications Manager

EDITORIAL REVIEW BOARD
Diane Blake, University of California, Los Angeles
James S. Cross, PhD, Michigan Technological University
Jay Gillette, PhD, Ball State University
Ray Horak, The Context Corporation
Angela Imming, Southern Illinois University, Edwardsville
Mick McKellar, Michigan Technological University
Dave Metz, Compass Consulting International Inc.
Ruth Michalecki, University of Nebraska, Lincoln
Marj Minnigh, Tufts University
Larry Wakefield, Tennessee State University

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 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. Subscriptions: Provided as a benefit of membership; $80/year, $20/issue for nonmembers. Contents of The ACUTA Journal are copyrighted © 2001 by ACUTA.

ISSN 1097-8658

POSTMASTER send all address changes to
ACUTA, 152 W. Zandale Dr., Ste. 200, Lexington, KY 40503-2486. Postage paid at Louisville, KY.

ACUTA WORLD WIDE WEB SITE: http://www.acuta.org

FOR INFORMATION ABOUT SUBSCRIPTIONS OR ACUTA MEMBERSHIP
contact Kellie Bowman, Membership Development Manager
Phone 859/278-3338 ext. 22, or e-mail kbowman@acuta.org.
FEATURES

6
Security: It's More than a Warm Blanket
Curt Harler
This overview of security problems and solutions exposes and addresses some of the pitfalls that plague campus network security.

13
Security in Cyberspace: Legal Perspectives
Based on a presentation by Evan Corcoran, Attorney at Law
Evan Corcoran's presentation in New Orleans provided useful information and valuable insights into the legal aspects of cybersecurity.

18
Bluetooth: An Evolving De Facto Standard
James S. Cross, PhD
Bluetooth is a short-range wireless communication system that allows computers and telecommunications devices to be connected without cables. This article describes the potential impact it could have on campus.

28
Middleware: Core Network Services
John Roman, PhD
As it provides the critical layer of the enterprise IT infrastructure between the network and application levels, middleware is improving efficiencies and facilitating provision of network services.

36
Old Cables Out—New Cables In: Improved Fire Safety Ahead
Frank Peri
Students, staff, property, and sensitive and expensive electronic equipment must be protected from the ravages of fire. Read about proposed changes to standards and how they are designed to improve security in the face of fire.

40
IP Telephony at Michigan Tech
Kevin Johnson
Michigan Technological University faced an explosion in demand for network services. The challenge was to find an architecture that was both flexible and scalable enough to enable growth and to support new network applications.

44
Institutional Excellence Awards: Binghamton and FSU
As winners of Honorable Mention in the 2000 Institutional Excellence Award competition, Binghamton University and Florida State University describe how telecommunications has recently made notable contributions to their campuses.

COLUMNS

4
President's Message
Anthony Tanzi, RCDD, Brown University

INTERVIEW

22
Patrick H. Wood, III
Patrick H. Wood, Chair of the Texas Public Utility Commission, shares insights he has gained into security, USF, and the regulatory environment in this interview with Walt Magnussen of Texas A & M University.
President's Message
Planning for Cybersecurity

How do we balance what seems to be a continuing explosive growth in the number of users connecting to the Internet with concerns for privacy and security?

Keeping unauthorized people from accessing information and keeping our networks safe from internal and external attacks requires sound planning. Planning must incorporate ideas as diverse as the selection of the applications we intend to use, the infrastructure that will carry and deliver the requests for information from those applications, and the management systems needed to ensure that everything works and is protected.

The general guideline that the more complex the service you offer in an online environment the more critical security is to the success of the service demands that we understand the different components of security.

Several questions come to mind when thinking about security. Do we use traditional security services like virus scanners, access control devices, firewalls, virtual private networks or encryption?

Do we use them in a stand-alone mode or as part of an integrated solution?

Do we and others in our organizations have a complete understanding of what each component brings to the proposed security solution, or do we find ourselves in the situation of having implemented “first line” security measures and having others think that our implementation is the “cure all” solution?

Have we integrated our security requirements into our business plans and presented a strategy for sustained support and upgrades during a security system's life cycle?

Do we have staff with the skills required to keep our systems operational, and have we considered questions as commonplace as What protects sensitive university data when that data is downloaded to the desktops of people working from home?

The questions seem endless and often result in solutions that appear overwhelming from fiscal and operational perspectives. Yet, we cannot ignore what has been called the most significant barrier to the success of an enterprise’s e-commerce growth—a lack of security.

We need to recognize that no one solution fits all needs, and a successful implementation of security measures is a result of a comprehensive plan involving input from many parts of the institution’s community.

Lest we think that we are immune from concern, ask the Microsoft™ people how they feel about the theft of their source code. If a security breach can happen to Microsoft, it surely can happen to us.

The timely and thoughtful articles in this issue of the Journal should provide a framework for us to build on as we assess our needs and design our plans.

Anthony R. Tanzi, RCDD
Brown University
ACUTA President
2000–2001

The theme of this ACUTA Journal, Security in Cyberspace, is particularly relevant to higher education. The “anytime, anywhere” principle of connectivity brings with it the challenge of security and privacy when conducting such university business as retrieving grades, registering for courses, using e-mail, providing financial information, etc.

Traditional applications such as wired Ethernet and new technologies similar to Bluetooth and the wireless Web each present significant and specific issues and opportunities for us to consider and implement.

Yet, in an October 26, 2000, article in the Toronto Sun, Jim Wolf from the Reuters News Agency reported, “Almost two thirds of the U.S. Internet users and three-quarters of non-users say they fear that going on-line endangers their privacy.”

The Center for Communication Policy at the University of California at Los Angeles found that fears about the possible misuse of personal data created big barriers to the growth of electronic commerce.
Think about it. One of the biggest problems you face is communication, or rather the lack of good, efficient communication, among all the members of your educational community. FirstClass Unified Communications from Centrinity solves the problem.

FirstClass enables and promotes easy one-to-one and collaborative communication among community members. Seamless group communications are enhanced through shared calendars and workspaces, distance learning, online conferences, secure discussion areas, Internet publishing and database integration. And FirstClass Unified Communications brings it all together. Voicemail, email, faxes and real-time chat are all unified on one platform and can be accessed from anywhere, anytime using a computer, web browser, telephone or hand-held device.

Learn how easy it is to put FirstClass Unified Communications to work for your academic community. Call 1-888-808-0388 for a free CD-ROM that will show you that there really is a better way to communicate.
Security is a strange animal. We feel secure going through a green traffic signal, believing that the person with the red light will stop. For some of us, security is a fluffy down comforter on a cold night. For others it is knowing that an eight-hour workday will bring a slip of green paper from an employer. For increasing numbers of us, it’s knowing that information sent over the Internet is private and secure.

Anyone can see the flaws in each of these scenarios. In most cases, the user is placing a large degree of faith and trust in someone or something else. Careless drivers run red lights. The down comforter may feel warm and secure as it protects us from the cold, but it wouldn’t be much help in the face of danger. Checks bounce. And even the most secure of government and banking systems on the Internet have been breached.

So what’s a college to do? It may be tempting to pull the comforter up around our ears and snuggle in. However, with the expansion of the Internet and its increasing presence in our lives, it is impossible to predict who may be poised to yank that cover off.

Who’s Out There?

In fact, both the beauty and the bane of the Internet is its very openness. Yet despite this openness and because of its ubiquity, many colleges are using the Internet for more than simple communications. One wonderfully potent tool is the implementation in October of e-
attacks created at all. The ever-changing technology worldwide, always be an interesting challenge.

Two Common Systems

There are two common kinds of document or communication security: secure sockets layer (SSL) and the public key pair, variously termed public key infrastructure (PKI) or public key encryption (PKE).

SSL was developed by Netscape Communications to allow encrypted, authenticated messages to be sent across the Internet with a relative degree of security. Typically, SSL transmissions carry the "https" designation in the URL line. In the SSL connection, each side of the connection presents a certification to the other which shows it is using security. SSL is found in many transmissions which run between a Web browser and a Web server.

The SSL protocol is designed to provide privacy, authentication, and message integrity. To accomplish this, each end of the conversation must have a security certificate which it exchanges with the computer at the other end. Each end then encrypts what it is sending, using information from both its own certificate and from the target computer's certificate.

The result is that, under normal...
Migrating your call center to a 21st Century multimedia contact center is easier and more affordable than you would think.

Let us show you how.
conditions, only the intended recipient can decrypt the message. When the message arrives, there is a level of security since SSL offers assurances that the data really came from the place which purports to have sent the information and that the message has not been changed or tampered with on its journey through cyberspace.

PKI is an algorithm used in devices like smart cards. Each is based on a key pair, one private and one public. Data encrypted with one key can be decrypted with the other key. It provides pretty good, if not bomb-proof, security for most colleges’ everyday applications. With PKI, the public key is, obviously, public. The private key is kept confidential to the user.

Robert Monsour, a member of the Internet Engineering Task Force’s IP Payload Compression Protocol (IPPCP) Working Group, offers a tip. “Pillage first, then burn,” he told the RSA Data Security Conference a year ago in San Francisco. By that he meant to compress data first, then encrypt it. Compression works by finding repetitive patterns in data and replacing them with shorter tokens. Encryption works by hiding any discernible patterns in data. For this reason, he emphasizes, compression must precede encryption.

**Security Providers**

The Bear Stearns report found that additional network traffic—a given as we look to the future—will not be the only strain on security; analysts believe that technological advances that offer “always on” connectivity will also intensify Internet security demands.

“As 24-hour online service increases, the demand for security will also increase,” says Bob Lam. Analysts predict that spending for Internet security could climb to $15 billion or more by 2004. “Internet security companies have reached their sweet spot. They are benefiting from the growing need for updated security, and with the right blend of technology, they stand to have extremely successful futures.”

One such firm is E-Lock Technologies of Fairfax, Virginia, which launched the first of many e-sign-compliant security management solutions, Assured Office 4.0, in a demonstration on Capitol Hill in front of the House Commerce Committee. Assured Office enables schools, their partners, and students to securely sign and approve documents electronically. It integrates within existing business processes and programs like MS Word, MS Excel, and Adobe Exchange to efficiently manage signing needs through automated features and wizards. A fully functional preview edition of the program is available for download at http://www.elock.com. Through the application of PKI-based digital signatures, Assured Office allows today’s new economy businesses to operate virtually by providing an electronic means to sign documents securely.

“The Internet is considered by many to be an equalizer. I believe digital signature technology and its recent legitimization with the e-sign legislation is the ultimate equalizer,” says Dr. Prakash Ambegaonkar, chairman and CEO of E-Lock Technologies. “We can now go beyond just the addition of signatures to content as organizations can integrate the benefits of digital signature technology into their business processes.”

Key features of such software include tailoring the application of digital signatures within an organization’s business process. It must provide the ability to create and administer signing policies, the ability for multiple people to view and/or sign a document through an approval management process, and the ability to restrict access to high-value documents.

Assured Office also provides for the electronic representation of handwritten signatures, batch approvals, the insertion of a time stamp, real-time online validation of digital certificates, and the ability to create user profiles, which assist in expediting the usage of these features in the signing process.

“The mere application of digital signatures to documents does not duplicate paper-based physical signatures,” notes Dr. Nimish Shah, vice president of market development at E-Lock. “The real significance of digital signatures lies in how these signatures are used within the business process and in their inherent application and management.”
Citibank of New York (www.citiedu.citibank.com) has a series of e-business and financial solutions aimed at the higher education market. It provides streamlined processes, improved infrastructure and communications, and specially priced financial products and services.

Working with other Citigroup businesses, the education solutions group targets paperless, electronic bill presentment and payment over the Internet. Billing data is translated from its legacy system and routed electronically to the school’s Web site. Instead of a paper bill, customers get billed and can schedule payment over the Internet. The customer’s account is automatically debited and the college’s account credited. Files go to the accounts receivables system for posting, all but eliminating exception postings.

Both software and hardware companies are developing good security solutions.

Marconi (www.marconi.com), of Pittsburgh, Pennsylvania, has a line of SA-400 security appliances which are invisible to would-be hackers from outside the campus or to unauthorized users from inside. With these firewall-protected interfaces, unwanted users simply cannot see what is blocking their access.

The SA-400 line is targeted at operations such as colleges and medical institutions which require resilient, secure, high-speed networks. Based on standard architecture, it includes an IP/ATM firewall card with options of ATM OC-12c and ATM OC-3e ports, standard dual AC power supplies, and built-in Ethernet and serial management ports. (IT lists at $15,000 for the OC-3e option, $25,000 for the OC-12c option.)

DICA Technologies of Portsmouth, Rhode Island (www.dica tech.com), offers its new ScryptGuard Mail Encryptor, a powerful, easy-to-install e-mail encryption device. It is based on the company’s Secure Mail technology, ensuring automatic key generation, certification, and PKI

which is transparent to users but allows only authorized persons access to confidential data. It provides authentication and digital signatures, enhances privacy and user accountability, and protects data integrity to ensure no one has tampered with or changed data without authority.

Need to link several systems behind a single firewall? Stonesoft (http://www.stonesoft.com) of Helsinki, Finland, is one of many firms offering firewall technology. Its StoneBeat FullCluster is a software solution that allows building of continuously available firewall systems using Check Point Software Technology’s software. StoneBeat interconnects multiple FireWall-1 systems to form a scalable firewall cluster.

Digital Certificates

Digital certificates vouch for the owner’s association with a particular organization and endorse his or her authority to participate in specific transactions. However, these certificates may be cancelled or revoked, for instance, in case of a change in job status or termination of employment.

Certificate validation can be performed online, and the validation result should be stored within the document itself. This provides a high level of non-repudiation and attests the validity of a certificate with regard to a particular point in time. For instance, a document signed earlier by an authorized person may later show as invalid due to the revoked status of his signature. However, storing the validation response will indicate that the signature was indeed valid at the time of verification and that the transaction was authorized.
Just about anybody can sell you a phone system. Yawn.

At Optus, we’re in a class by ourselves. From our renowned refurbishing skills to our expansive inventory to our free technical support, we deliver on Price, Product Availability and Peace of Mind.

If you need support (upgrades, components, peripherals or add-ons) on an existing system, we’re your choice—we support all major systems and product lines. Plus, we offer top dollar for your old system through our Asset Management buy-back program.

We’re Optus. Savings Without Compromise!™
Want to Know More?

No matter which security products are on your short list for buying, there always is a bit of uncertainty about how well they will perform.

TruSecure Corporation (www.trusecure.com) of Reston, Virginia, is a good source for security information. Formerly known as the National Computer Security Association (NCSA), it still maintains NCSA's testing labs in Carlisle, Pennsylvania, where they attempt to develop unbiased, evolving criteria to define good security products. For years, NCSA tested and certified antivirus and firewall products. Its certification program is not competitive analysis or product review. Rather, it offers a simple pass/fail grading of a firewall system based on whether the product provides protection from known attacks and, at the same time, provides real operational functionality.

TruSecure also offers a series of buyers' guides and white papers on topics ranging from creating an access policy to firewall products.

In addition, remember that ACUTA is an excellent source of information. Other articles in this issue of the ACUTA Journal will address security concerns, and the listserve is a reliable quick-response medium. When it comes time to buy, hop on the listserv e and post questions about applications and specific products. Remember to share your experiences with others as well.

Having done all this, when you nestle under that warm down comforter, you'll know the feeling of real security: a network security system that should let you sleep well at night.

Curt Harler is a freelance writer and contributing editor to the ACUTA Journal. He is well respected for his understanding of telecommunications issues and is a popular speaker at technology conferences.
Track 1 at ACUTA’s Winter Seminars in New Orleans in January dealt with cybersecurity. Based on feedback from those who attended, one presenter who was particularly well received was M. Evan Corcoran, attorney with Wiley, Rein & Fielding, who looked at cybersecurity from a legal and policy perspective. The following material is based on his presentation plus comments made in a follow-up interview.

“ACUTA members, as nonlawyers, should not be hesitant to wade in and participate with lawyers when dealing with computer security issues,” said Evan Corcoran as he identified one of the primary goals of his presentation in January. “It is useful for nonlawyers in the information security field to understand the general legal framework so that they are prepared to minimize liability in the wake of a security breach. It’s also helpful to understand the benchmarks when they talk with their legal counsel. Having a plan in place as a part of a strategy to deal with computer attacks and other computer-related incidents can provide a level of comfort between lawyers and nonlawyers so that whatever the problem is, it can be solved.”

How serious is the threat to security in cyberspace? Corcoran cited some telling statistics (see Figure 1) which indicate that the problem is growing exponentially. As the number of people online increases—240 million users worldwide last year—Lloyd’s of London suggests that the potential costs are tremendous as e-commerce will emerge as the single biggest insurance risk of the 21st century.

Figure 1. Increases in the incidence and costs of cybersecurity are a major concern.
“There is no question that ACUTA members will want to assist law enforcement in stopping cybercriminals, but it should be done in consultation with counsel, so the institution makes sure it has the proper authorization—whether subpoena or court order—to provide the information.”

It’s the Law

Cyberthreats can be categorized into three groups: unstructured threats from insiders and hackers; structured threats from “hacktivists,” economic espionage, and organized crime; and national security threats from terrorists and foreign intelligence agencies.

A number of laws already on the books help to combat some cybercrime. The Computer Fraud and Abuse Act (CFAA) prohibits hacking into a system to steal or destroy data or damage hardware by transmitting commands. It covers denial-of-service attacks and extortion based on a threat to crash the system or steal and destroy data.

The Electronic Communications Privacy Act of 1986 (ECPA) updated the federal telephone wiretap laws to extend protection to e-mail and other nonvoice communications. It covers both communications content and subscriber records, and it created civil and criminal penalties for privacy violations. According to the law, it is generally illegal for a third party to “intercept” an electronic communication or to access a stored electronic communication without authorization. Exceptions to that prohibition include the interception of publicly available communications, interceptions where consent was given, interceptions made to protect system operators’ rights or property, and government access under law (that is, with a subpoena or court order).

There are certain privileges extended specifically to the system operator. A provider may monitor private real-time communications to protect its rights or property, such as logging every keystroke typed by a suspected intruder, and a provider may access stored e-mail of its customers. However, a public provider (an ISP) may not freely disclose to others the content of that e-mail. Also, a system operator may independently disclose the contents of a communication in certain cases, such as to an intended recipient of the communication or his or her agent; to a person who is employed or authorized to forward such communications to its destination; or to a law enforcement agency where the contents were inadvertently obtained and the contents appear to pertain to the commission of a crime.

Government Access

“There is no question that ACUTA members will want to assist law enforcement in stopping cybercriminals,” Corcoran explained, “but it should be done in consultation with counsel so the institution makes sure it has the proper authorization—whether subpoena or court order—to provide the information.”

Under certain circumstances a government agency may be able to obtain access to electronic communications and records. With a search warrant, the government may access unopened e-mail. With a court order or subpoena, government agents may obtain and read opened e-mail. A court order will also give the government access to transactional records and subscriber information.

For real-time interception of electronic communications, the government must obtain a wiretap order from a court. A search warrant will allow them access to unopened e-mail stored on a provider’s system less than 180 days. For opened e-mail or other stored files, the government must send the provider a subpoena or a court order.
There are two categories of noncontent information: subscriber information, such as name, address, account number, and local and long distance telephone toll records; and transactional records, such as credit card number, Web sites visited, log-in date/time records, and names of senders or recipients of e-mail.

**Emerging Issues**

A number of issues are emerging as activity increases in cyberspace. As in any industry where vast numbers of the public are involved, liability is of growing concern as a potential legal abyss. Privacy concerns have been in the news recently. An example was the outcry that accompanied disclosure of FBI use of the Carnivore system.

Additional wiretapping and security legislation has been introduced in the new Congress, as lawmakers struggle with balancing personal privacy and the need to combat the threat of cybercrime.

Professional liability is another issue. While professionals must exercise the skill and competence of their profession, most courts have rejected the notion that individuals in the computer business should be subject to an elevated standard of care. Nonetheless, information security professionals may be liable on a negligence theory if a third party suffers some loss and the professional has not lived up to the standard of care.

Keeping up with the standard of care may involve keeping abreast of publicly available security fixes, such as those published by the SANS Institute at www.sans.org.

With the number of users increasing, the number of instances of abuse that end up in court has no place to go but up.

**Make a Plan**

More and more campuses are seeing the necessity of planning ahead for breaches to their security in cyberspace. Some have established a response team composed of technical experts, legal counsel, administrative officials, and public relations experts. The team is directed to identify the vulnerabilities specific to their campus presence in cyberspace. They identify portals to the Internet and to the physical world and how they are used. They establish user rules and practices. They investigate protective software, and they conduct periodic security reviews.

In the event of a security breach, the team has in place legal and public-relations responses, as well as a technical response. From a technical perspective, the first order is to stop the attack. In addition, the campus needs to communicate with other parties, identify the attack source, save and analyze evidence, and identify the costs of the attack.

From a legal and public-relations perspective, the team must reassure users and customers that they are in control. They must inform downstream victims as well as the public at large. Importantly,
they should consult with the university and outside counsel.

It is also critical to determine whether to report a security breach to federal or local law enforcement. If you have developed an efficient channel of communications with your local officials, it should not be difficult to balance user privacy with legitimate law enforcement needs.

Many excellent reasons exist that support informing law enforcemen-
tment of instances of cybercrime, not the least of which is that they probably have better resources for investigating the crime and for confidentially alerting other victims or potential victims. In addition, they have law enforcement experience and should know how to effectively pursue criminals. Besides apprehending the criminals more expeditiously, your campus may avoid some costly liability issues by enlisting law enforcement specialists.

Prevention Is the Best Approach

If you have not been "bugged" by a virus or had your network brought to its knees by a clever hacker, consider yourself lucky and thank whoever has been protecting your systems. The potential for damage is very real. You can and should take steps to minimize the risks of cyberattack.

The law firm of Wiley, Rein & Fielding specializes in telecommu-
nications law. Contact Euan Corcoran at ecorcora@wrf.com.

ACUTA 30th Annual
Conference & Exposition
July 29-August 2
Lake Buena Vista, Florida
Disney's Contemporary Resort

- Preconference Seminars
- Keynote Speaker
- General Session Speakers
- 50+ Breakout Sessions
- Peer Networking
- 100+ Exhibits
- User Groups

Register online at www.acuta.org
**PAETEC** offers our Higher Education customers the most comprehensive communications solution in the business. The merger of PaeTec with Pinnacle and Campuslink further strengthens our commitment to Higher Education and provides a powerful, integrated offering including:

- Advanced voice services including local and long distance, enhanced high-speed data, video and Internet network services;
- Broadband services tailored specifically for colleges and universities;
- Revenue-sharing programs;
- Unparalleled customer service and support.

**PINNACLE Communications Management Solution**

**Pinnacle** now features Campuslink Student Billing and Management Services and a new ASP offering all centered on the world-class Pinnacle software. The Pinnacle software solution provides:

- Comprehensive Billing & Facilities Management;
- Converged voice, data and video support;
- Web Access.

For more information, visit [www.paetec.com](http://www.paetec.com) or contact us toll free at **877.472.3832**
Bluetooth:
An Evolving De Facto Standard

by James S. Cross, PhD
Michigan Technological University

"There will be more Web-connected handsets than PCs in the world as early as 2002."
—Nokia press release

As we embark upon a new century, the proliferation of wireless technologies will continue to transform the landscape of the campus community and the way we live, work, and play. Little happens on a campus that is not impacted by the wireless revolution—from the simplest phone call to mobile computing, instruction delivery, biotech research, admission and class registration, electronic commerce, energy management, and the most complicated digital operation.

The critical issue for colleges and universities is not whether new and innovative technologies such as Bluetooth will change business processes, but what aspects they will change and how quickly they will change them. Andy Seybold, a wireless industry analyst states, "Bluetooth changes everything by connecting a myriad of gadgets that previously couldn't speak the same language."1 Allied Business Intelligence projects the aggregated annual shipment of Bluetooth-enabled devices will reach 1.4 billion units in 2005 as indicated in Figure 1 (on page 20)—a sharp increase from the 56 million devices in 2000.2

The Bluetooth Concept

Bluetooth is a short-range wireless communication system that allows computers and telecommunications devices to be connected without cables. The system, conceived by a consortium of mobile phone manufacturers and silicon chip makers as a way of making wireless headsets for cell phones, has been rapidly adopted across the electronics industry. The concept behind Bluetooth is simple: Using radio frequencies in the 2.4–2.5 GHz industrial-scientific-medical (ISM) band, the technology enables devices within 30 feet (10 meters) of each other to exchange data, audio, graphics, or video at rates of 30 Kbps to one Mbps. This is
approximately six times faster than serial ports and three times faster than parallel ports.

The 2.4–2.5 GHz ISM radio frequency is designed for data transmission and exchanging digital data between a laptop and cell phone, pager, PDA, game console, digital camera, or other digital appliance. To avoid interference with other devices, the technology uses a frequency-hopping spread-spectrum (FHSS) modulation scheme to transmit data packets in a pseudo-random pattern in the 2.4–2.5 GHz band at approximately 1,600 hops per second.

In addition to eliminating the need for cables, the technology makes it easy to set up wireless networks in homes, offices, and public spaces by enabling devices to swap information with each other whenever they come within range. Phil Hester, chief technology officer for IBM’s Personal Systems Group, states, “It’s a convenience factor. Today, cell phones and pagers don’t communicate with each other. If someone pages you, you have to read the screen, then punch in the numbers on a cell phone. With Bluetooth, simply pointing the devices at each other and clicking an icon will transmit the phone number, which can be dialed automatically.” (Staff, eWeek, 2000) The result is a wireless personal area network (PAN).

For years, Bluetooth advocates have been promising simple wireless networking that will revolutionize business and leisure. The technology envisions a wireless PAN on a single chip, aimed at creating cordless connectivity cheaply enough to be built into all mobile phones, PCs, PDAs, digital cameras, and other devices. The current specifications support up to seven devices linked to a master device using a Bluetooth chip to form a piconet. Multiple piconets can be linked to form a scatternet to allow communications between varying configurations. The Bluetooth specifications are divided into two sections: (1) the core section which specifies required components such as radio, baseband, link manager, protocol control, transport layer, and interoperability; and (2) the profile section which specifies the different protocols and procedures required to support various types of applications.


**Bluetooth Consortium**

Bluetooth, named after Harald Bluetooth, the Danish king who united Denmark with Norway, was developed by an international consortium of companies and supports both point-to-point and point-to-multipoint communications. The short-range (up to 10 meters) wireless technology, which ensures protection and security through software control and identity coding built into each radio chip, is rapidly evolving into a de facto industry standard. Backers predict the technology will turn cell phones into electronic wallets and individuals into PANs—with music players, digital cameras, pagers, headphones, and electronic organizers all swapping information. The nine consortium backers (Ericsson, Nokia, IBM, Intel, Toshiba, Microsoft, Lucent, Motorola, and 3Com) plus approximately 1,900 other companies worldwide that have signed up for royalty-free rights to the emerging standards, provide an impressive platform for future growth and application development.

The Japanese hope Bluetooth will make them a global technology leader again as gadget makers set ambitious plans to launch Bluetooth-equipped devices. In 2001, Nippon Telegraph & Telephone will begin rolling out speedy next-generation Internet services over third-generation (3G) mobile phones that download data from the Web and beam it with Bluetooth to other devices. Ericsson plans to introduce a wireless headset for use with Bluetooth-enabled cell phones, Palm plans to market a Bluetooth add-on to its PDAs, and Intel and Microsoft have announced they will jointly develop a Windows operating system that supports the Bluetooth wireless standard.

**WAP**

Although wireless Web Internet access has been the subject of much self-parodying hype, and has been hobbled by incompatible standards, awkward interfaces, expensive service charges, and slow data transmission speeds, it is slowly weaving itself into everyday life with the roll-out of wireless application protocol (WAP) designed for low-bandwidth cellular networks. WAP is a set of technical standards specifying how cell phones connect and communicate across the Internet.

WAP is not intended as a substitute for Web browsing with a PC, but is targeted at delivering unique content—streamlined and optimized for a cell phone and other wireless devices. For example, a user with a WAP-enabled cell phone may send an Internet
request to a WAP gateway that handles the translation between wireless markup language (WML) used by cell phones and hypertext markup language (HTML) used by the Internet. The WAP gateway retrieves the requested Web page, converts the page to WML, handles the translation between markup languages, and then transmits the converted page to the cell phone. Because HTML-to-WML conversion frequently makes Web pages unreadable and limits the amount of accessible information, some sites are being expressly tailored for WAP-enabled devices—for example, MapQuest and Go2Online.


Growth Potential

Although less than 5 percent of companies are using mobile applications today, Meta Group Inc., predicts that number will grow quickly as application server vendors like Mobile Media, Bluestone, Lutris, and others roll out a new breed of software that extends existing applications to mobile devices and supports new wireless applications (Holland, eWeek, 2000).

In the United States, some 90 million people use mobile phones, which represents a tremendous market, even if only a small portion of these customers subscribe to a data service. Although many of the wireless data networks are limited to major metropolitan areas and are restrained by slow speeds, the implementation of 3G wireless networks may change all that. To spur growth, telecommunications companies such as Nextel, Sprint, Verizon, AT&T, and SBC are developing 3G networks which embrace technologies capable of handling huge amounts of data. These 3G wireless-access technologies increase data handling rates of mobile devices to the 2-Mbps range by spreading each wireless signal over a wide band of frequencies. Visit the International Telecommunications Union (ITU) Web site at http://www.itu.org for more details on the IMT-2000 3G wireless technology standard ratified by the ITU.

Cell phone, game, and entertainment companies are experimenting with several designs for handheld gadgets that will communicate with enhanced 3G wireless networks. For example, Lernout & Hauspie, a Belgian software company, is prototyping a handheld gadget that allows users to issue voice commands and dictate e-mail. Nokia, Motorola, and Ericsson are developing concept 3G super cell phones that incorporate Bluetooth technology to link the phone, earpiece, and microphone so that users can speak, listen, see, and manipulate the display. The 3G super phones will be capable of playing MP3 music files and displaying high-resolution graphics, video, and Web pages. Finally, Nintendo and Sony are expected to incorporate the technology into portable music players and their Gameboy and Playstation consoles.

Benefits Potential

The potential benefits that 3G networks make possible are motivating colleges and universities to modify their business processes and operations to embrace economies of scale, added value, and efficiencies. The analysis of potential benefits to the campus must be based on these factors:

- Infrastructure-related savings
- Staff productivity gains
- Strategic partner and vendor-related savings
- Value-added features and functionality
- Regulatory compliance
- Publicity and goodwill

This business case must embrace the creation of an integrated strategy for wireless technologies...
that addresses scalability, availability, security, manageability, and extensibility in differentiating campus products and services from competitors. Jack Trout and Steve Rivkin in Differentiate or Die (John Wiley & Sons, 2000) assert that far too many organizations still don’t understand how vital it is that they differentiate their products and services from those of their competition. In the face of stiff competition, successful organizations have to give the customers a reason to choose their product or service.

The Business Model

The business model for embracing the Bluetooth technologies is based on these premises: (1) that the campus will migrate to wireless Web-based applications for delivery of services; (2) that an integrated campus wireless technology strategy can provide competitive advantage and dramatically reduce transaction costs; and (3) that campus business processes are being transformed as an evolving set of wireless technologies and are being adapted for Web-enabled applications supporting the following:

- Collaboration
- Admissions
- Financial aid
- Procurement
- Digital signatures
- Digital certificates
- Encryption
- Financial control
- Grade reporting
- Course management/delivery
- Textbook delivery
- Content distribution
- Building access
- Fundraising
- Merchandising and retailing
- Learning portals
- Identification and authentication
- Process control and monitoring
- Data mining

**The Challenge and Value Proposition**

The challenge is in selecting and synchronizing a wireless technology vision consistent with the culture of the organization. The value proposition is built upon these factors:

- Anywhere, anytime, anyplace access
- Faster and smarter mobile professionals
- Satisfied customers
- Relationship management
- Learning organizations
- Leveraging of core competencies
- Brand recognition
- Alliances and partnerships
- Technology enablers
- Value-added functionality
- Security requirements
- Infrastructures for change and agility
- Regulatory compliance

Although many of our faculty, staff, and students can intuitively imagine the value of an integrated wireless technology strategy, the complexities of making the transition from the environment to which we have all grown accustomed will be disconcerting to many. Leadership and the ability to crystallize a vision lie at the heart of a campus’s ability to realize the potential and the opportunities wireless technologies make possible.

New and innovative products continue to dramatically change the way colleges and universities operate, communicate, collaborate, and interact with constituents.

Gary Hamel in Leading the Revolution (Harvard University Press, 2000) asserts that the 21st century challenge is not to compete for the future, but to create it. Success means unleashing revolutionary offerings that delight customers and shock the competition and long-entrenched industry leaders.

Jim Cross is vice provost of information technology at Michigan Technological University. An active member and former president of ACUTA, he is a frequent contributor to the ACUTA Journal.

**Notes**


**Additional References**


Staff. “Bluetooth PAN Moves to Front Burner,” eWeek, (June 26, 2000), 81.


Since 1995, Patrick Henry Wood III has served as chairman of the Public Utility Commission of Texas.

Wood strongly believes that competition can do better than regulation in delivering customer benefits and service innovations. Throughout his career, he has worked to advance a pro-customer, market-oriented vision of utility regulation.

For this issue of the Journal, ACUTA Publications Committee member Walt Magnussen of Texas A & M University interviewed Mr. Wood for his views on a variety of issues of importance to higher education telecommunications.

The following is the text of that interview.

ACUTA: What are your views on the fairness and appropriateness of the universal service fund (USF), e-rates, and subsidies for technology in K-12 and higher education for telecommunication infrastructure enhancements?

Wood: USF has been a big issue here in Texas. Although I'm also one of the state commissioners on the FCC's state-federal board on USF, I wasn't on that board when they set up the e-rate, so I can't take the credit or blame for that. But we do have a similar program here in Texas that put an obligation on incumbent providers to build up infrastructure to schools. That same bill also set up a Texas infrastructure fund to do inside wiring, equipment installation, and training. So the federal e-rate really is the consolidation of the two independent programs here on the state level.

My first question as a states-rights-oriented guy is, do you really need a federal program to do what your state programs are already doing? But given that we've got one, I certainly think it's important to keep incentives matched to what is being used by the educational world. I think everybody felt it was important to get out there and take advantage of the discounts.

The most important question I've never seen an answer to is how much of the infrastructure that was built out over the last five years to the schools, libraries, and hospitals is actually being used to its full potential. I don't know the answer to that. I hope that the money that has been spent in the explicit subsidy program has
been put to good use, but I think it's always a wise thing, and certainly at the five-year anniversary, to look back and see if this money really was spent on what the legislature and Congress intended it be spent on.

That leads me to my second main concern, and that is that the subsidies be competitively and technologically neutral. First of all, competitive neutrality: That’s one of the mistakes we made in Texas back in 1995. We didn’t have much competition anywhere then. We do now, and so you’ve got the incumbent provider with an obligation to build out infrastructure, whereas competitive providers don’t have that same obligation. It ought to be on everybody or nobody, and once it’s done it ought to be subsidized through a competitively neutral fund, like a USF or an e-rate. The structure of the e-rate is fine. It’s available to everyone and every provider can qualify for the fund.

And then, technological neutrality: With the increasing use of different wireless and satellite technologies, we need to make sure if we deploy things for schools—particularly out in the rural areas where there’s not a whole lot of infrastructure in the first place—that the subsidies are indifferent to the technology. We don’t want to favor one over the other, but rather to go with the best, most efficient technology.

So if the USF is accomplishing the purpose it was supposed to accomplish and is technologically neutral and competitively neutral, then to me those are public dollars well spent. As one who’s been on the public side of the fence for a decade now, I do tend to have a skeptical view about publicly administered funds. We must always be cognizant that this is someone else’s money that we’re spending.

ACUTA: With some projects, seed funding is provided for two years, then it becomes incumbent upon the recipients to deal with it. With the e-rate you typically get funding every year. What’s your gut feel about the role of these public funds? In other words, is the money best spent by providing initial seed money, then let the grant recipients deal with the sustainability issues on their own, or would this lead to situations where initial investments go to waste after the grant period?

Wood: That’s a good question. I think it’s hard to go cold turkey, but on the other hand, having to keep going back to get that annual subsidy requires a lot of bureaucratic infrastructure to fill out those grant forms. So there’s a real advantage to going with an up-front, seed-money concept.

On the other hand, if we’re talking about a T1 here, market costs for those things can be higher than schools are able to afford, particularly for the lower-income areas. Some places may need an annual subsidy; others can do fine with the up-front grant. If they do it annually, as the e-rate does now, it ought to be structured in a way that’s administratively workable. On the other hand, it’s kind of like health insurance: You have to have a co-pay so that there’s at least some disincentive to prevent people from just going and getting it because it’s there. Price point ought to be such that it’s affordable yet doesn’t invite wasteful consumption.

ACUTA: Our second question is of particular importance to some of our members. What are your views on current regulatory policies and procedures for handling slamming and cramming?

Of course, a lot of the universities get phone bills that are literally thousands of pages long. Trying to uncover and figure out where these charges are coming from is a real time-consuming process, and unfortunately now for some of the larger institutions it’s almost becoming a monthly event.

Wood: I think we’ve got the right amount of authority here in Texas from our legislature to address these issues. In addition, the FCC has deferred to the state on slamming issues. I believe some 31 or 32 states have taken primacy over slamming complaints from the FCC for the people in their states. So the FCC has worked pretty well with states to make it easy for a customer to place just one call to get all this dealt with.

As for the cramming issue, unauthorized billing for charges, I don’t know how broad the federal authority is on that. We got clear authority on that from our legislature in 1999, and we handle more cramming than slamming complaints as of year-end 2000. For your customers, it may be hard to even identify slams or crams because of the bill’s complexity. We did get a bill-simplification mandate from the legislature last year and implemented the rule, but quite frankly I don’t see that as your silver bullet. There are diametrically opposite views about how simple a bill ought to be. What’s simple to one person is concealing to another. And so “You’re hiding something from me” would be the response from a person who didn’t like our rule. I consider our bill-simplification rule one of my few defeats here as a regulator.
We don’t even reach the exercise of our authority over slamming and cramming if we don’t get complaints from the customer. So if your customer is having difficulty reading a bill, then God help him because we can’t. That’s where I think the bigger customers may be able to use their attractiveness to new competitive providers to negotiate bill format as well as rates. Bigger customers can say to their provider, “Each month or each quarter when I get a bill from you, I want it to look like this.” Many of your readers are big enough where they don’t have to just take the bill off the shelf.

**ACUTA: What will be the role of the FCC and PUC with regard to colleges and universities? What kind of interaction do you see between regulatory agencies and higher education?**

Wood: Well, one, selfishly, when I went to Texas A & M recently I did use that as an opportunity to try to poach some of your brightest talent to come work for me! But I don’t think that’s what your question was. I met Mr. Farber, the FCC’s chief technology officer who was “on loan” from the University of Pennsylvania to the FCC for the last year or so. His job was basically to be a resource for the FCC so that they have the benefit of the most current engineering and technological view of the world. Good engineers can tell regulators a whole lot about the telecom industry.

On the service provision side, regulators should make sure the embers of competition continue to ignite and grow and create more of a robust competitive market so that you folks have choices. Quite frankly, you are very attractive customers to an ILEC and a CLEC, so anything we can do to make sure you have the maximum number of choices from those providers is a good thing for you. Also important is the ability to integrate all this technology into a complete service package—getting the RBOCs into long distance so that there’s nobody out there who cannot legally provide you with the services you want. That’s why I was glad when Southwestern Bell opened its local markets here in Texas. They, along with everyone else, can provide you and everyone else in Texas with a full panoply of alternatives on voice, video, and data, as well as local and long distance. That’s what I think the FCC and PUC can do for all your members, and also listen to you when you’re trying to tell them what the outside world is thinking and looking like. You’re big customers that matter a lot.

**ACUTA: What should be the role of the federal government in policing the Internet, especially with regard to providing voice services over the Internet?**

Wood: I think the general direction of voice regulation has been toward deregulation, so I don’t envision that there will be any move to regulate the price of services provided over the Internet. I think that would be a move in a very surprising direction. This debate began when VoIP started and access charges were relatively high. Now with the acceptance of the CALLS petition and the resulting low access-charge rates, the use of VoIP is less threatening to ILECs’ access-charge cash flows. So as far as pricing services over the Internet, I don’t see a regulatory role in that at all.

**Policing the Internet: Here at the PUC we have an Internet screening program that the IT staff uses to prevent any user from logging onto adult content pages. Putting that kind of software in place makes a whole lot of sense. It’s hard to tell Grandma Jones why her e-rate money ought to be used to help somebody go get porn pages. That’s just bad PR and bad policy.**

That kind of “policing” the Internet is not going to be offensive. I think you have problems when you go international and certain countries try to restrict certain kinds of content and others that say it’s not regulateable. I don’t know what the future’s going to bring on that.

The Internet was designed to be an anarchic medium, and I don’t think it is or should be subject to a lot of government. Just a medium whereby people can share their ideas, and if you don’t like those ideas, you don’t have to listen to them. If kids are picking up on it, then parents ought to watch what their kids do or don’t give them a computer. I think there are a lot of ways for a parent to do something about the content, but we don’t have to regulate the actual conduit in order to get at the content. I think that gets you back into a regulatory world where we haven’t had a whole lot of success.
ACUTA: What role will the FCC and the federal government take in policing and monitoring wireless calls?

Wood: I'm not a Big Brother fan. I think the more you can do for general customer privacy in this day and age, the better. I know the FBI has a role to protect national interests. I assume they will continue to have the same authority as they have today. I would be reluctant to expand that beyond what's necessary to protect national security.

ACUTA: Let's look at a companion issue—tracing caller to location on cell phones. My understanding is that cell phones will have a GPS chip in them, or we'll be using triangulation. But for the most part that location information isn't going to go anywhere outside the public safety arena anyway, so that's pretty much subject to the same restrictions that your police records and everything else are right now. It's not going to be something anyone can readily jump in and grab, right?

Wood: Yes, but certainly there are plenty in our society who wonder if law enforcement should have that sort of information or not. I think it ought to be the minimum amount of intrusion necessary to fulfill very narrowly drawn national security goals and people ought to be able to rely on the security of a phone line to have a private conversation, although, quite frankly, I don't anymore. Too many times I've overheard calls made by neighbors of mine on a handheld wireless. It's unfortunate we can't depend on that technology after all these years, but we don't need to encourage wire tapping or any of the other intrusions.

ACUTA: What are the social obligations of the incumbent LECs and LDCs for the build out of broadband services in rural and nonurban areas?

Wood: The obligation ought to be whatever it is on any other business. If Sears or Wal-Mart is obligated to put a store out in rural Texas, then maybe Southwestern Bell ought to be obligated in rural Texas as well. But Sears is not under that obligation, without a specific economic development subsidy. That's what I was talking about before about having a competitively neutral universal service fund. If you're going to do something, make sure that not only the incumbent but the competitor and the alternate technology also have the ability to get that same subsidy. I don't believe that laying on financial obligations for somebody just because they're already out there is appropriate.

One of the things we have indicated at the Texas PUC is that, for broadband deployment, we may want to make the traditional phone company an agent for a nonaffiliated company that provides broadband. In other words, if the only way you can get broadband out in the rural part of Texas is through satellite, but the local telephone company does not offer satellite, then perhaps you can put the obligation on the telco to have a business or partnering arrangement with somebody else. Think about what the customer might want. This setup is a little different from a financial obligation: I would make that slight distinction. Companies won't be thrilled about it, but they can comply without putting themselves at a financial disadvantage. And if there's a subsidy out there for any of this stuff, that subsidy is available to anybody, not just to the incumbent.

ACUTA: What are your views on a telecommunications consumer bill of rights and protection of consumers, simplification of billing statements, etc.?

Wood: Billing, again, is my lost battle. It's one thing to give someone some rights; it's another to actually implement them. Saying that you've got a right to a clear and intelligible bill is one thing, but actually translating that into something that can work is a whole other kettle of fish. That's where, certainly in concept, you're going to have a telephone customer bill of rights, but make it something that's actually meaningful and actionable and not just some broad principle.

ACUTA: At A & M we're acutely aware of this. We see the billing aspect from both sides. In my case, as a telecom director, not only am I the recipient of a large number of bills from various telephone companies every month, but we also have a very complex internal billing system that, in turn, re-bills my end users, my departments. So we take what we learn from our providers and try not to do the same thing to our customers that, unfortunately, is being done to us. But then again, too, in the case of the university, like a lot
of other institutions, they have created the organizations that have the expertise to be able to read those bills where most of them really don't.

Wood: That's a good point. Every different local customer has different needs with regard to what some of these rights actually mean.

ACUTA: Overall, what do you see as the role of government in the process of training future generations in the appropriate use of technology and assuring an adequate supply of talent to sustain our high-tech industry?

Wood: I learned a lot about computer programming in high school and at Texas A & M. Of course, we had punch cards back in the '80s. Once you have a mindset to figure that sort of thing out, you can pretty much figure out the next software package. DOS wasn't a household word back in the '80s. You have to make sure that our educational institutions teach those basic skills and general technological issues.

I think even a liberal arts major ought to be required to meet basic requirements. As an engineer I was required to take English and history. I think liberal arts majors ought to be required to take basic engineering and technology just so they have a basic understanding of technology—not how a prism splits light but just basic principles of sound and light. What's a laser? What's fiber-optic? What are the basic things that drive the communications industry? How does a telephone call actually happen? Everybody needs to have some level of understanding because it's such a big part of our culture—much more than our parents', certainly, but even a bigger part than when I was in school.

Certainly through our public educational institutions the government has an obligation to familiarize students with technology, as your question implies. The only way to reach anyone is through the parent or a teacher. An educator is second to a parent as far as stimulating interest. You can't force them to learn, but you've got to make it interesting enough for them to want to learn for themselves.

ACUTA: What are your views on the short- and long-term implications of deregulation in the telecommunication industry based on the last 25 years' experiences? How do these experiences apply to other industries, such as energy?

Wood: When I give a speech on deregulation and competition, I always go back to my timeline comparison. In 1984 Reagan was still in his first term. We had the Olympics in Los Angeles, and a country called the Soviet Union (remember them?) boycotted those Olympics. Bruce Jenner won those Olympics, and there was just beginning to be competition in the phone industry.

That competition was, "Do you want your rotary-dial black phone hanging on the wall or sitting on your desk? Or do you want a fancy new Princess phone to set in your daughter's bedroom?" And that was competition. But at the time the courts created the long distance/local bifurcation, they also did a quiet but important thing: They deregulated the phone equipment. From the phone jack in the wall outward became something that was no longer owned by AT&T. It could be rented from them or bought at Radio Shack and used in the same jack. When I look at what has happened since that time, just 17 years ago, and all the types of innovation that have happened with the Internet and faxes and wireless phones, I think, you know, that would not have happened if AT&T still had that rotary phone regulated from the phone jack out.

So to me the whole drive toward deregulation is to get government out of the way so that the entrepreneurs and the venture capitalists and the creative ideas that come out of somebody's head can enter the marketplace and win or lose based on how good that product is. That's been true since time began, and it's clearly true in the telephone industry today. I think the same thing will happen in the energy sector as well. Yes, you do it for price. Yes, you do it for better customer service. But at the end of the day the main reason you do it is because you're unleashing technology to see what it can do.

ACUTA: What are the hot issues on the horizon for the regulators under the new administration?

Wood: The hottest issue is sitting on our hands so that some of the things in my last answer can happen.

ACUTA: It's one of those things where if you've done your job, you sort of put yourself out of business.

Wood: Yes, I was hired by Governor Bush six years ago to put myself out of a job. Quite frankly, we're still going to have a big role in maintaining the electric infrastructure because it's not being deregulated. And we will also monitor the marketplace as antitrust cop, anti-trust policeman.

That's a real different role than we've had to play before. We've got to be smart on the technology, we've got to understand it as it's unwinding and happening, and that's a role that certainly you folks in higher education can help with—keeping us smart in what we do and making sure we understand the trends and direction of technology.

So we've got to sit on our hands, but we've got to keep our eyes, ears, and minds open. Listen
attentively, watch closely, and think very carefully about current trends so that if the government needs to get involved, it can do so in a thoughtful way but in the least intrusive way possible. If there is a need to involve ourselves on the Internet and security issue, we will have people who understand what the implications are rather than just rushing in.

That's like what we did on slamming. We had mild experience in Texas with slamming before we had any statutory authority. So when we went in and asked for authority on slamming, we knew pretty much what we needed, and we asked for it and we got it and it worked out just fine. Such a focused approach to government involvement hasn't forced us to basically be in the position of re-regulating the whole industry, which would, I think, have worked to its detriment.

ACUTA: With the announcement of the American-TWA buyout and others, there's a lot of talk about the airline industry being down to just three airlines which handle some 80 percent of the market. We've seen a trend toward mergers and acquisitions in the telephone industry as well. Will that have a long-term negative impact?

Wood: I hope it does settle down. My bogey is that there be five equal players. Our state legislature set that number as our mandate on the electricity market here in Texas. That's 20 percent market share each. That's not a bad standard for these other industries.

In long-distance telephony, we had the big three long-distance companies for a long time. That didn't create the big pricing pressure that even a fourth provider provided. A fourth provider (Southwestern Bell) came into the Texas market, and it certainly kind of shook things up and dropped prices.

We don't want to end up like the railroads. We're down in Texas to two big railroads. Re-monopolization is not super for the customer, and that's what we actually tried to get away from when we went to deregulation. Competition first, then deregulation. Let's make sure that what we're putting in is better than what we had.

ACUTA: Any other comments for ACUTA members?

Wood: Having seen the potential when bright, smart people in the academic world contribute to the broader debate, I don't know that we have played enough toward that relationship. I had that conversation with chief technology officer Farber over at the FCC when I was in Washington, and it really impressed upon me how important it was to make sure that the smart people in the industry are interacting with regulators on a daily basis.

The more I interact with the leading, cutting-edge people—whether they're from industry or the academic world or even from our own staff—the better I can do my job, and that's always going to be important for regulators, whether it's in this world or in the future. If we don't stay abreast, we're fighting yesterday's battle, and that wastes a lot of people's time and money.

ACUTA: From our end, the universities cherish that kind of role, too, because we want to do anything we can to help in the legislative and regulatory process, such as providing background information. We like to feel that we are folks you can look to who don't have a fixed agenda in terms of products to sell. We typically use any type of technology that networks well, so we have nothing to sell, which makes us a little less biased than most of the others.

Wood: Right, and that's hard to find.
Middleware:
Core Network Services

by John Roman, PhD
Washington University at St. Louis

Over the last 10 years the network has become an indispensable component of the infrastructure of universities, corporations, and other enterprises. Its initial growth was largely due to electronic mail and the World Wide Web, and these are obviously important functions today; but the network still has unrealized possibilities. New applications are constantly being developed which have the potential not only to add value and provide a competitive advantage, but also to quickly become critical to the success of an enterprise. A partial list of these applications includes Web portals, privacy-enhanced e-mail, streaming video, e-commerce, and digital libraries.

These applications have several features in common:
- First, they require identification and authentication. The applications need to determine the user’s identity and classify him or her. Is this a student? Prospective student? Faculty? Staff? Alumnus? Friend?
- Second, the applications require authorization; they must be able to determine if the user has the authority to perform a particular operation (for example, view a particular Web page).
- Finally, they require privacy and security for such actions as sending e-mail, searching a library, or making a purchase.

Traditionally, these features have been provided on a per-application basis. Each new application must create and maintain a database with the names of people authorized to use the application and their privileges. Privacy and security, if considered, are done in a stand-alone fashion. Because the applications are unrelated, the wheel must be reinvented every time, limiting innovation and the value of the network.

Middleware is the name for the set of core services and data that provide identification, authorization, and privacy. Middleware provides the critical layer of the enterprise IT infrastructure between the network and application levels. It allows the core data and services to move from their multiple instances into a coordinated institutional offering. As Kenneth Klingenstein points out,
"This central provision of services eases application development, increases robustness, assists data management, and provides overall operating efficiencies."  

Core Middleware Services  
Middleware provides the core services that allow applications to use network services. Middleware provides identification, the set of codes that uniquely identify a subject; authentication, the process of a subject electronically establishing that it is, in fact, associated with a particular identity; and authorization, those permissions that drive transaction handling, administrative applications, and automation of business processes. 

- Identification  
An identifier is generally a character string that maps a real-world object to a set of computerized data. Objects can be almost anything about which one would want to store and retrieve information, such as persons, organizations, computer applications, online services, and network components. Identification is critical, as each object has a number of different identifiers. A person may have both a username identifier and a user ID identifier, for example. Identifiers differ from names in that unique identifiers are designed to be just that—unique identifiers. However, just as names are not unique and may change, so identifiers may be unique at any given moment but not be unique over time.
cate is a public key that has been digitally signed by a recognized authority attesting that the owner of the key is who he says he is. It is a tiny, coded file with identifying information about an individual or institution.

The software, protocols, and legal agreements that are necessary to effectively use certificates combine to form a public key infrastructure. PKI has several components:

1. A certificate authority (CA) that manages and signs certificates for an institution.
2. Registration authorities, operating under the auspices of the certificate authority that validate users as having been issued certificates.
3. PKI management tools, including software to manage revocations, validations, and renewals.
4. Trust models that extend the realm of secure communications beyond the original certificate authority.
5. Policies that identify how an institution manages certificates, including legal liabilities and limitations, standards on content of certificates, and actual campus practices.
6. A directory to locate and store certificates.

One compelling reason that digital certificates are important for libraries and campuses is the national movement to use digital certificates for authentication and authorization for secure interactions over the network. Digital certificates provide a single method of authentication and access control for remote faculty and staff and for remote applications, such as access to databases and electronic copies of journals outside of their campus collections.

PKI has been developing more slowly than directories. There are much larger issues related to organizations, legal issues, and politics.

**Where to Start?**

How does an institution get started? First, do some research. A number of organizations and institutions are leading the way with middleware. For example, Internet2 and CNI have been working in this area for several years. Internet2 has created a program called Early Adopters in which a number of institutions are pioneering in implementing middleware. Check the references below for more information.

Second, identify stakeholders—people within your own organization or institution who would benefit from this. As a group, these people can start to identify sources and flows of data, determine who owns the data, and identify potential applications and their needs.

Third, consider a pilot project for “proof of concept.” A possible project would be to set up an LDAP directory to perform functions of the white pages services. This would require relatively few resources for hardware and software but would allow you to start understanding the issues required to develop an enterprise middleware service.

**Conclusions**

Middleware is a core component of the infrastructure and consists of a set of robust, online services that support a broad set of institutional applications. It has well-defined technology standards with established interfaces. It is consistent with institutional structures.

Middleware can be both distributed and centralized, depending on the organization and its needs. It is interoperable across communities of interest. An institution can interoperate with other universities as well as with commercial organizations. It is scalable: Middleware will grow and evolve as the needs grow.

Middleware is something you, as a technology leader, should investigate for its potential for your campus.

**John Roman is senior manager, systems and planning, within Network Technology Services at Washington University at St. Louis. He can be reached at jrn@wustl.edu.**


**Additional Resources:**
- Internet2: [http://www.internet2.edu/middleware/](http://www.internet2.edu/middleware/)
- Sample certificate: [http://www.cren.org/ca/sample.html](http://www.cren.org/ca/sample.html)
How do you know if your school is getting income from all student telecom revenue sources? Not sure?

Just Ask.

We're connected with nationwide services to find your university hidden income on calls leaving your PBX.

- Operator Service Commission offerings from the majors carriers including AT&T
- Income on outbound 800 calls
- Discounted Directory Assistance

We'll connect you.

SPECTRACORP
TELEMANAGEMENT GROUP

1-800-375-7945
e-mail justask@spectracorp.com
www.spectracorp.com
Network to Go:
Wireless Computing at the University of Southern Mississippi

Under the shade of a large oak tree, in the parklike setting that so much defines the character of Southern Miss, a graphic arts student intently studies the Web site of the Louvre Museum in Paris on her laptop computer. She selects the last item to be included in the paper she is completing for her art history class. Finishing the project—seated on a blanket on the lawn instead of at a carrel in the library—she quickly attaches the document to an e-mail message and sends it off to her instructor. Seconds later, she points her browser to www.planes-n-trains.com to check on her spring break tickets to Daytona.

EagleAir—named for the Southern Miss Golden Eagles, of course—brings the promise of ubiquitous computing to the whole campus community. At the end of the year 2000, some 30 buildings have been fully equipped with wireless network technology and 70 more will be added by the end of the spring semester. The common spaces between buildings will also be blanketed with wireless network access.

The Motivation to Go Wireless

In addition to making mobile computing a reality, the wireless network will also save the University more than $9 million in wiring costs. These savings have allowed the campus to achieve advances in technology that would have taken many years using conventional methods. Although wireless is not a substitute for wired connections in all cases, it

by Scott Montgomery
University of Southern Mississippi
is a very effective and flexible option for the majority of users whose needs center on basic Internet connections for e-mail, research, and entertainment.

The substantial savings come from the fact that, in the conventional wiring process, cable must be manually installed in each wall of each room of a building where network connections are required. This is both labor- and material-intensive. With the wireless approach, access points are strategically placed in ceiling spaces so that complete signal coverage is provided. The access points provide the wireless connections for properly equipped computers anywhere within or near the building. On average, the cost of using wireless is about 15 percent of the cost of hard wiring.

While this technology is still relatively new, it is rapidly being implemented in businesses, institutions, and even homes. Industry statistics indicate that use of wireless technology is increasing faster than network use in general. The reasons for this rapid growth become clear the minute you actually begin to experience the advantages yourself. Even for desktop users, the freedom to place the computer anywhere without regard to the network jack is a definite plus. For laptop and other mobile users, the ability to obtain network access anywhere on the campus will allow much more effective use of their computers.

Increased productivity is, in fact, one of the most significant benefits of going wireless. Messages can be composed and sent on the spot. Questions can be researched and answered when they arise.

Planning

While these advantages and others yet to be discovered are a good thing, getting there is not a simple task. At Southern Miss, the wireless project grew out of ongoing efforts to get pervasive network improvements implemented on a campus that was largely unconnected. The initial project called for implementation of a new campus network backbone and rewiring of many buildings.

The implementation of the new backbone was a project unto itself and included the placement of fiber-optic cable reaching to most buildings on the campus. The core of this backbone consists of three asynchronous transfer mode (ATM) network switches operating at OC-12 (622 Mbps). From this high-speed core, OC-3 (155 Mbps) connections fan out to the various buildings where switches provide the connection to the in-building network infrastructure, including our new wireless network components. (See Figure 1.)

As the planning for this progressed, it became apparent that while the backbone implementation was necessary and could be accomplished, the wiring of buildings was going to be very difficult to afford. As luck would have it, at about this time, the

Figure 1: New wireless network
commercial release of products using the industry standard for wireless technology (IEEE 802.11b) occurred, providing 11 Mbps connectivity.

Our planning group at Southern Miss redirected its focus to studying the feasibility of using this technology as an alternative to hard-wired connections in at least some buildings. The research was done, and a pilot building was equipped with the wireless technology to begin testing. While these tentative first steps were encouraging, they also taught us that there was considerable work required on the planning and implementation side that was not required with traditional hard wiring.

Establishing a wireless network is not just a matter of putting enough access points in a building; many factors affect the range and strength of the wireless signals. The technology operates within a range of radio frequencies. Each access point can be set to operate on one of several specific frequencies within this range and uses a smaller range centered on that specific frequency. If two access points operating on the same frequency are placed too close together, they can interfere with each other and defeat the network operation. So careful testing is required. Frequency selection and placement of the access points must be balanced to give overlapping coverage to expected numbers of users (about 30 per access point) without causing interference between access points.

These lessons in hand, we expanded our testing to a few other buildings and began the process of planning for general deployment. All of our planning for outside network plant remained entirely valid. Inside the buildings, though, both the equipment in the closets and the conduit and wiring installations had to change dramatically.

Our deployment plan included services by the University’s physical plant department, our department (Office of Technology Resources), and third-party contractors. Project activities included logical and physical network design, design of wiring closets, installation of equipment, installation of conduits and wiring, placement of access points, integration with the legacy network, and testing. All of this work had to be done in a coordinated way while maintaining services on the legacy network.

**Implementation**

Procurement of services and equipment required considerable work. This included preparing specifications and an RFP, selecting equipment types and vendors, managing receiving, and staging the equipment. We found that writing highly detailed specifications, especially for the provision of implementation services, was crucial in the vendor selection process.

We had completed a full campuswide survey of existing physical plant, including all installed cabling, conduits, wiring closets, and in-building facilities. We then extended this documentation to include the required modifications and additions. This work specified placement of all new facilities, designs for wiring closets, and routing for all new conduits. We also stipulated all materials and certifications required. These details allowed a fair and level comparison of the RFP respondents for this work.

Further, upon completion of the work, these detailed materials facilitated verification that contractors had met specifications in all cases.

Avaya Communications (formerly Lucent Technologies) won the contract for provision of the wireless equipment for our project. Their access point (Avaya model AP-1000) and related equipment, along with their willingness to partner with us in supporting our deployment, made them the best alternative in our case.

An important aspect of the project revolved around controlling access to the network. After considerable head scratching, we determined that the best way would be to use dynamic host configuration protocol (DHCP) and Radius authentication. When a student, faculty, or staff member wants to obtain an access account for the wireless network, he must first register the media access control (MAC) address of his wireless network interface card (NIC) through our help desk.
His status as student or employee is verified and tied to the MAC address for later authentication. Then, each time he attempts to access the network, his MAC address is authenticated before a session can be started.

A frequent question about wireless networking has to do with the security of the radio transmissions between computers and access points. To protect against electronic eavesdropping, there is an optional encryption capability available in the wireless technology to provide the needed security at this level. We chose to employ the 128-bit RC-4 encryption option, which provides the greatest level of security. A 64-bit WEP encryption option is also available at a slightly reduced cost per wireless NIC.

In order to establish a user-based revenue stream to support ongoing maintenance of the network, students are currently charged a monthly fee for network access services.

**Conclusions and Lessons**

As we view our project presently, we are satisfied with its progress. The time from inception to rollout was less than six months. We are bringing new buildings online almost daily now, and a high percentage of the work is being done by our own staff. The technology is stable and performs well in nearly all areas. Administration and maintenance overhead has remained within the levels anticipated. Feedback from our user base has been very positive, although that base is not yet very large.

Still, there are a few things that we know we could have done better. We have not put adequate resources into either the end-user support, marketing and public relations, or customer service areas.

As technologists, we sometimes pay inadequate attention to the human factors of our projects. In the case of the wireless network deployment, these factors are very important and must be given adequate consideration up front. For example, our field service technicians did not previously provide any computer support for students. But with the wireless network going into the residence halls, it has become apparent that unless we can provide direct assistance to students in getting their wireless cards installed in their computers and getting them online, we won’t get the student buy-in that is so critical to our success. We are having better success now as we implement these extended support services.

Also, attention to preparing our user community for the changes earlier in the project would have led to more rapid growth of the user base. A promotional effort aimed at both awareness and education of the various user communities would have garnered internal interest and acceptance of the technology more quickly.

Another concern has been the cost of the wireless NICs for students. Equal to the cost of a couple of textbooks ($170–$200, depending on computer configuration), the cost represents “just one more extra expense” to students. We are currently exploring options to allow these costs to be charged to the students’ general accounts. This spreads the cost over a semester and bundles it with books and other school supplies.

Our user base is expanding now, and many are reporting very positive experiences using the network that is becoming available. This project promises to make Southern Miss one of the most “unwired” campuses in the country.

Scott Montgomery is director of technology infrastructure at the University of Southern Mississippi in Hattiesburg. Reach Scott at scott.montgomery@usm.edu.
Old Cables Out —
New Cables In:
Improved Fire Safety Ahead

by Frank Peri
Communications Design Corporation

A number of entities such as the National Fire Protection Association (NFPA), the National Fire Protection Research Foundation (NFPRF), and others make fire safety their business. From time to time these groups mandate new standards as technology improves and our knowledge increases.

Get ready—it’s time to take a look at the fire safety standards on your campus again!

If adopted, proposed changes to the 2002 National Electrical Code (NEC) will effect some major changes in how colleges and universities manage their communications cabling infrastructure. In addition, recent research into the fire safety performance of communications cables means new, safer LAN cables may be increasingly specified in critical applications.

While bandwidth—the information-carrying capability of the cable—will continue to be a major factor in cable selection, the cabling plant must, above all, be safe. Those responsible for the cabling infrastructure in institutions of higher learning know that fire safety performance cannot be compromised. Students, staff, property, and sensitive and expensive electronic equipment must be protected from the ravages of even a small building or residence fire. And that’s what proposed changes, likely to be adopted by the NEC in May 2001, are designed to address.

The Hazard

Reducing the fire hazard from building facilities is a combination of sound engineering design and a variety of active and passive systems working together to protect people, property, and equipment.

Unfortunately, deaths due to fires in nonresidential buildings have been trending up in the past few years. The 136,000 nonresidential fires, 170 deaths, and $2.3 billion in losses reported by the NFPA in 1998 are unacceptably high by any standard. (See Table 1.)

Clearly, all fires are dangerous, but those that originate in or spread to the plenum space above the ceiling or below a raised floor are of special concern to facility and cabling professionals and firefighters alike. Because of the high-volume airflow in these horizontal open spaces, fires can spread with alarming speed and introduce copious amounts of smoke and combustion products into the
Table 1: Non-residential Fire Statistics

<table>
<thead>
<tr>
<th>Year</th>
<th>Fires</th>
<th>Deaths</th>
<th>Injuries</th>
<th>Direct Dollar Loss in Millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1989</td>
<td>174,500</td>
<td>220</td>
<td>3,275</td>
<td>$4,326</td>
</tr>
<tr>
<td>1990</td>
<td>157,000</td>
<td>285</td>
<td>3,423</td>
<td>$2,888</td>
</tr>
<tr>
<td>1991</td>
<td>162,500</td>
<td>190</td>
<td>3,125</td>
<td>$3,087</td>
</tr>
<tr>
<td>1992</td>
<td>165,000</td>
<td>175</td>
<td>2,726</td>
<td>$3,342</td>
</tr>
<tr>
<td>1993</td>
<td>151,500</td>
<td>155</td>
<td>3,950</td>
<td>$2,703</td>
</tr>
<tr>
<td>1994</td>
<td>151,500</td>
<td>125</td>
<td>3,100</td>
<td>$2,636</td>
</tr>
<tr>
<td>1995</td>
<td>148,000</td>
<td>290*</td>
<td>2,600</td>
<td>$3,257</td>
</tr>
<tr>
<td>1996</td>
<td>150,500</td>
<td>140</td>
<td>2,575</td>
<td>$2,971</td>
</tr>
<tr>
<td>1997</td>
<td>149,500</td>
<td>120</td>
<td>2,600</td>
<td>$2,502</td>
</tr>
<tr>
<td>1998</td>
<td>136,000</td>
<td>170</td>
<td>2,250</td>
<td>$2,326</td>
</tr>
</tbody>
</table>

* Reflects 166 civilian deaths that occurred in the explosion and fire at the federal office building in Oklahoma City on April 19, 1995. Source: National Fire Protection Association.

ventilation system. Return air plenums can present an especially hazardous fire environment, as has been tragically demonstrated in several building fires.

The NFPA has no records on the number of nonresidential fires that involve plenum spaces and cable, but they do occur. The report on the 1975 fire in New York’s World Trade Center (issued by the New York Board of Fire Underwriters Bureau of Fire Prevention and Public Safety) sums up the hazard: “Cables passing from one closet to another closet on the same floor pass through the plenum above the hung ceiling. The exposed cable is combustible and constitutes a hazard because fire will be drawn into the plenum and the insulation will intensify the fire at this point.”

Although today’s code-compliant cables are an improvement over what was used in 1975, we can do better.

**Safer Cable Options Ahead**

Cables listed and labeled as CMP (communications plenum) are acceptable for installation without metal conduit in plenum areas according to the NEC, which is adopted by most jurisdictions in the United States. Underlying the NEC is NFPA 90A, Standard for Air Conditioning and Ventilation Systems. This powerful standard recognizes the potential hazard associated with plenum spaces and requires that all materials exposed to air flow shall be “noncombustible” or “limited combustible,” as measured by the NFPA 259 fire load test, and have a maximum smoke developed index of 50, as measured by the NFPA 255 Steiner Tunnel test. CMP-listed cables, however, do not comply with either of these primary requirements. Instead, they have been allowed in NFPA 90A, under a lesser exception adopted in 1975, if they meet the less stringent smoke requirements of the NFPA 262 Steiner Tunnel cable test. How much less stringent was not known until now. (See NFPA Standard 90A on page 38.)

Although CMP cable designs have reduced the fire hazard, they have been with us for more than 20 years. New cable designs offer superior protection.

Major research conducted on the fire safety performance of horizontal communication cables has been made public. The result: new, safer LAN plenum cable designs from leading cable manufacturers that provide new options for colleges and universities that have special concerns and want an extra margin of fire safety.

The new breed of cables meet all of the primary requirements of NFPA 90A and are identified as CMP-50 limited combustible (LC). Underwriters Laboratories (UL) and Engineering Testing Laboratories (ETL) now provide a listing service for these cables. Based on proposed code changes, both combustible CMP and limited-combustible CMP-50 cables may be recognized for plenum applications in the 2002 NEC, along with other possible code revisions that may require the removal of abandoned cable in plenum spaces.

What makes CMP-50 limited-combustible cables so appealing? Very low flame spread and extremely low smoke, according to new findings published this June by the National Fire Protection Research Foundation (NFPRF).

**New Research**

As a result of concerns of fire-load buildup and smoke production resulting from concentration of cables in plenums …, the NFPRF report provides new data on a variety of plenum-approved cables. The 16-member Technical Advisory Committee, consisting of material and cable manufacturers and fire science consultants, sponsored the project and tested cables for flame spread, smoke generation, and potential heat.

Under the NFPA 90A exception, only the NFPA 262 Steiner Tunnel cable test is used to measure flame spread and smoke generation of communication cables. In this test, cables are placed on trays and exposed to flame in the tunnel. Cables qualify for plenum installation without conduit (i.e., listed as CMP) if they demonstrate a maximum flame spread...
distance of 5 feet, peak optical density due to smoke of 0.5 or less, and an average optical density due to smoke of 0.15 or less.

The NFPRF study expanded testing beyond NFPA 262 to determine how cables and materials perform under the primary requirements and test protocols of NFPA 90A. Using the NFPA 255 Steiner Tunnel test and the NFPA 259 test for potential heat, more information was revealed on the burning behavior of cables and the fire load of cable insulation and jacketing materials. The fire load, or potential heat, of a material is the heat produced by a sample when burned under conditions used to classify a material as noncombustible or limited combustible. NFPA 259 produces complete combustion of materials and measures the heat produced in the process. In effect, potential heat measures the extent to which a product may contribute to the speed and size of a real fire—that is, how fast does it burn and how big does it get?

Tests were conducted at UL and Intertek Testing Services/ETL Semko, well-recognized independent test laboratories. A detailed interim report presenting test data is available from the NFPRF, Quincy, Massachusetts.

Compared to typical, combustible CMP cables, especially those which contain PE (polyethylene) insulation on one wire pair and which are jacketed with LSFR PVC (low-smoke, flame-retarded polyvinyl chloride), the CMP-50 limited-combustible cable designs demonstrated less flame spread (zero in some test series).

Even more startling was that the typical combustible CMP design described above generated about 20 times more smoke than allowed by the primary requirements of NFPA 90A (See Figure 2) and had over 2.5 times higher fire load compared to the CMP-50 limited-combustible cable. These results aren’t surprising since PE can be considered a solid fuel with almost as much potential heat as gasoline.

As a base polymer, both PE and LSFR PVC would be considered "combustible" by NFPA standards. In other words, they are fuels.

Despite these dramatic differences, it should be noted that the typical combustible CMP cables tested in the NFPRF study meet the current requirements of

---

NFPA Standard 90A-1999

NFPA Standard 90A-1999 requires materials used in the construction of wire and cable for location in plenums to meet the following:

2-3.10.2 Ceiling Cavity Plenum. The space between the top of the finished ceiling and the underside of the floor or roof above shall be permitted to be used to supply air to the occupied area, or return or exhaust air from or return and exhaust air from the occupied area, provided that the following conditions are met:

(a) All materials exposed to the airflow shall be noncombustible or limited combustible and have maximum smoke developed index of 50.

Exception No. 1: The following materials shall be permitted in the ceiling cavity plenum where listed as having a maximum peak optical density of 0.5 or less, an average optical density of 0.15 or less, and a maximum flame spread distance of 5 ft. (1.5 m) or less when tested in accordance with the specified test method:

(a) Electrical wires and cables and optical fiber cables—NFPA 262, Standard Method of Test for Flame Travel and Smoke of Wires and Cables for Use in Air-Handling Spaces.

2-3.10.6 Ceiling Cavity Plenum. The space between the top of the finished floor and the underside of a raised floor shall be permitted to be used to supply air to the occupied area, or return or exhaust air from or return and exhaust air from the occupied area, provided that the following conditions are met:

(a) All materials exposed to the airflow shall be noncombustible or limited combustible and have maximum smoke developed index of 50.

Exception No. 1: The following materials shall be permitted in the ceiling cavity plenum where listed as having a maximum peak optical density of 0.5 or less, an average optical density of 0.15 or less, and a maximum flame spread distance of 5 ft. (1.5 m) or less when tested in accordance with the specified test method:

(a) Electrical wires and cables and optical fiber cables—NFPA 262, Standard Method of Test for Flame Travel and Smoke of Wires and Cables for Use in Air-Handling Spaces.
NFPA 90A and the NEC, which means they are fully code complaint for plenum applications. Unlike combustible CMP cables, CMP-50 limited-combustible cable designs typically use fluorinated ethylene propylene (FEP) for both the electrical insulation and the cable jacket (illustrated on page 36). 1FEP, commonly known by the DuPont trademark Teflon, has outstanding fire performance and would be considered a “limited-combustible” material by the NFPA. CMP-50 limited-combustible cables are fully compliant with the original intent of NFPA 90A, which was to allow only low-fire-load, low-smoke products in plenum spaces.

Although the combustible CMP cable designs tested by the NFPRF are likely to remain acceptable for plenum applications without conduit, what’s new is that facility personnel have another option representing the best available technology to provide extra building safety. For example, those responsible for public buildings, hospitals and healthcare facilities, university buildings, and buildings containing mission-critical computer operations and sensitive switches and equipment may find CMP-50 limited-combustible cables most useful for protection and peace of mind.

Damage from Smoke Can Be Extensive

When it comes to sensitive electronic equipment, we have a better understanding today of the effects of smoke, which are much worse than previously suspected. Recent studies show that very small amounts of smoke containing fine conductive carbon particles result in current leakage and irreversible damage to digital electronic equipment. This is believed to be one of the major reasons why the AT&T central office fire in Hinsdale, Illinois, several years ago caused so much damage to equipment.

According to a paper presented by Lucent Technologies, a leading manufacturer of communications cable, new CMP-50 limited-combustible cable presented the lowest current leakage and no damage to electronic equipment using the UL 1985 test protocol.

More Cables than Anyone Anticipated

Adding to fire hazard concerns is the sheer amount of cables accumulating in plenum areas. It seems that some type of cabling or recabling project is always underway, due largely to MACs—moves, adds, and changes. The result is layer upon layer of cables in plenum spaces, including generations of abandoned cables, cables that are no longer in use. Removing a few ceiling tiles for a glimpse at cable density can be appalling, to say the least. The concern is fire load. Every 1,000 feet of 4-pair UTP LAN plenum cable installed puts approximately 11 pounds of plastic material for insulation and jacketing in the plenum area. As mentioned above, certain plastic materials used in combustible CMP and other older cable designs can contribute to high fire load.

Buildings typically use tens of thousands of cable feet, but many use hundreds of thousands. A little math will quickly show how much potential fuel may be “up there,” hence the concern over which materials are limited combustible and which are combustible. Limited-combustible materials can have up to 400 percent less fire load. Furthermore, to reduce the buildup of fire load, the NFPA is also considering code proposals mandating the removal of abandoned cables from plenum areas.

What does it all mean? In the next six months expect new codes to be written which provide safer LAN plenum cables. New CMP-50 limited-combustible cable for improved fire safety has already been announced by two leading manufacturers. Also expect to remove all abandoned cable from horizontal areas and even risers. The language of the proposed new NEC code is intentionally nonspecific as to precisely when and under what conditions abandoned cable must be removed. Your local inspector or jurisdiction will have authority to guide you on when removal is mandated. What is clear is the intent: Abandoned cable must come out to reduce fuel load.

Frank Peri is president of Communications Design Corporation. A member of ACUTA since 1997, he has more than 20 years of experience serving college and university campuses.

Figure 2: Plenum type cables tested to NFPA 90A primary “limited-combustible” requirements at UL.
When Michigan Technological University faced an explosion in demand for network services, their first instinct was to review the existing voice and data infrastructure to determine if the existing network could be extended to support both voice and video traffic. The challenge was to find an architecture that was both flexible and scalable enough to enable growth and to support new network applications. The University's information technology professionals partnered with Mitel Corporation to provide a solution that met and exceeded the expectations of students and staff.

**About Michigan Tech**

With a total enrollment of more than 6,300, Michigan Tech graduates a majority of students with degrees in engineering or science. These demographics meant Michigan Tech needed to excel at the technological solution in order to attract forward-thinking students. Michigan Tech has nationally ranked undergraduate programs in civil, environmental, mechanical, and materials engineering, and all of the academic programs make extensive use of computing and educational technology.

The IT department at Michigan Tech supports students, faculty, and staff in various endeavors, providing telecommunications and network services, videoconferencing and video programming, maintaining student labs, facilitating test scoring, and providing hardware maintenance. Dr. James Cross leads the IT department and has responsibility for both the telecommunications and the data networks on campus. This makes the department one of the newly emerging converged IT organizations responsible for centrally managing and delivering voice, data, and video services to their users.

Dr. Cross observes that one of the key challenges his department faces is delivery and auditing of the different voice and data network services. The telecommunications services department provides a variety of network-based services and facilities for the entire campus.
社区，包括本地和长途电话服务，语音邮件，网络访问，拨号访问， cellular phone service，以及 pager services。The department also operates a cable TV system for the University's residential housing. According to Dr. Cross, there are currently 6,000 devices on the University’s data network, and it’s growing at the rate of approximately two devices per day.

All faculty and professional and administrative staff of Michigan Tech have network access through their offices and labs, while students are guaranteed access to computers with spreadsheet and graphing capability, e-mail, and printing facilities. Most academic departments support student computer facilities with a wide variety of software for communication, academic coursework, and research. The University supports ResNet, a residence hall network in all residences and apartment complexes for the approximately 2,300 students living in University housing. This link enables students to connect anytime to academic labs and servers—and expensive technical software—as well as to the Internet.

Michigan Tech is four years into a five-year project to upgrade the wiring in all the residence halls to Category 5 or Category 6 UTP cabling for data network service. To complete the system, there are links to remote campus sites (wireless and ISDN), dial-in access points, and two T3 connections to the Internet and Internet2 via MichNet, Michigan Tech’s regional network provider.

The IT department at Michigan Tech recognized the need for a voice solution that would leverage a significant investment in their high-speed backbone and data network. In an effort to contain costs, acquire more control, and provide simpler centralized management, the IT department committed to migrating from the existing Centrex network to a fully converged voice/data solution in stages over the next three years. In 1998 they chose a distributed PBX solution from Mitel Corporation to provide voice services to the student residence halls. It was important to the technology team that migration paths to an IP-based platform protect their current voice investments. As their voice infrastructure evolves, the IT staff will be able to capitalize on the current investment in equipment, training, and infrastructure and avoid the cost and frustration of learning a brand new voice system in the future.

**Toward IP Telephony**

In early 2000 Michigan Tech took the first steps toward IP telephony, beginning with a trial of enterprise VoIP technology in the IT department. The Mitel Ipera 2000 solution provided an opportunity to pilot VoIP technology in a small adjunct implementation by allowing both users and support staff to get comfortable with the technology and build expertise in voice over the LAN while minimizing risk and maximizing use of existing products and knowledge.

With this migration, the IT department can easily track IP phones in the same manner that it tracks PCs and other intelligent network devices. Through the use of an integrated directory (Netscape Directory Server), the IT department can add any new service, including phone and network connections, using a single application. This makes it easier to track services, and it reduces the time it takes to add a new user.

The IT architecture is based on a switched IP core with an embedded TDM bus that provides native support for legacy TDM switches and devices without the need to employ multiple external gateways and conversion boxes that would add cost and complexity to the voice infrastructure.

**About the Installation**

The first step in the Michigan Tech installation involved connecting the IP platform and 20 IP phones to a dedicated 10/100 Ethernet switch. The switch was, in turn, connected to the ATM backbone through a 100-Mbps connection from a bridge/router. In order to use the IP platform in a workgroup adjunct mode, the device was connected via an MSDN link to the existing SX-2000 NT server. The successful execution of this task demonstrated that an IP platform and IP phones can offer excellent audio quality when connected to a single dedicated IP subnet.

The second step was designed to test the system’s ability to work across two IP subnets connected by a bridge/router. This test was important because even small enterprises use subnets to control unnecessary network broadcasts, improve performance, and provide easier management. To test the cross-subnet installation, the IT staff connected 16 IP phones and Ipera 2000 to a dedicated 10/100 Ethernet switch. In order to prevent unwanted network broadcasts, the IT department implemented virtual LANs (VLANs), which provide the capability to break a single LAN into segments and eliminate unnecessary chatter between network devices. With a VLAN, traffic only leaves the virtual segment if it is destined for a remote IP or MAC address.
This test was also successful, and the users were able to complete calls to the phones located on the second subnet, calls to the digital phones on the legacy PBX, and outside calls to the PSTN. There was no degradation in voice quality, which is comparable to traditional voice solutions.

The third step involved locating IP phones on a completely different IP LAN segment connected via the ATM backbone to test the product’s ability to work across a large enterprise while providing the same call features and toll quality. To perform this test, two of the initial 20 IP phones were connected to a 10/100 Ethernet switch located on a remote bridge/router connected to the ATM backbone. The remaining 18 IP phones and Ipera device were left on the original LAN segment. This test was also successful and is indicative of how the IP platform will eventually be deployed throughout the campus and other sites.

After successfully installing the IP phones across different subnets and VLANs, the Michigan Tech IT staff is moving on to the task of using Mitel OPS Manager to cluster IP with the legacy systems to provide centralized management. Once the clustering is complete, a single administrator will be able to perform moves, adds, and changes on all digital and IP phones wherever they are located on the Michigan Tech campus.

**Future Plans**

With the successful implementation of an IP solution, Michigan Tech anticipates the ability to enable desktop videoconferencing and real-time data acquisition to easily tailor voice applications and to implement voice-to-text alphanumeric paging and voice-activated network management.

In addition to installing IP phones, the University has plans to add more capabilities to the converged network in the future, specifically in developing Internet2 Advanced Network Services. One of the most exciting expectations of Internet2 and IP telephony initiatives at Michigan Tech is the ability to enable new applications that will extend the capabilities of the IP voice desktop to enable it to talk to any IP device and become a real-time portal to network-based services. This opens the network to the possibility of applications such as speech recognition, WAP/WML, and PDA integration.

**Business Case for IP Telephony Throughout the Campus**

Network efficiencies are a key driver behind Michigan Tech’s move to converge its voice and data networks. Deployment of an IP solution is not expected to have a significant impact on the number and type of existing staff supporting the network, even as voice is routed across the network. Instead, Tech anticipates that the move to IP will reduce staff workloads, particularly when MACs are necessary. This will enable IT staff to focus on higher-level roles.

Likewise, the ability to include voice-related user data, such as telephone and extension information, into the global LDAP directory server will cut by almost half the time required to add new people and telephones to the system. According to Dr. Cross, IP telephony will decrease the cost and complexity of providing telecommunications services, increase service levels and technology integration, and leverage network Quality of Service support for both IP telephony and Internet2 applications.

In terms of voice quality, the IT staff at Michigan Tech is very satisfied with using an IP platform and IP phones. Through the use of VLANs, they are able to achieve the same voice quality they received using their Centrex service and legacy PBX. The IT department was also pleased that the ease of use was comparable to digital equivalents because this simplifies the training process.

The IT department benefited from reliability provided by the call control, which used a system it is already familiar with. This, in combination with a full PBX feature set and ease of integration within the existing network, common dialing plans, common centralized management, and feature transparency, provides Michigan Tech with an IP solution that leverages its data backbone while delivering the functionality and benefits of a traditional high-performance voice communications solution.

With the migration to IP telephony, Michigan Tech has ensured that a framework will be in place for future growth and development. In adapting its network, Michigan Tech wanted to build expertise in new converged voice/data technologies to deliver efficiencies and new capabilities for its users, while also providing high levels of service and features. With this successful progression, Michigan Tech has taken substantial steps in maintaining its standards of high-quality engineering and innovative service offerings.

Kevin Johnson, director of product marketing at Mitel, has 19 years’ experience in the telecommunications industry. He is respected as a speaker by the voice and data industries in North America.
Where Voice, Video and Data Become One Choice...

NetVoice Technologies, Inc. is an IP communications company and a partner with the ability to meet all your communication needs.

- **Scalability**
- **Interoperability**
- **Reliability**
- **Accountability**

Experienced in all facets of Integration, Design and Engineering, NetVoice can help simplify your organization's unique integration process.

**Hardware:**
- Cisco Architecture for Voice
- Video and Integrated Data (AVVID)
- IP Telephones
- PSTN Gateways
- Callmanagers
- Data Networking Equipment

**Software / Applications:**
- Unified Communications
- E-Learning & Distance Learning
- IP Television Video Conferencing
- Video on Demand
- IP Call Center
- E-Care

**National IP Network:**
- Converged Voice, Video & Data
- Point-to-Multipoint Fixed Broadband Wireless (last mile and campus LAN)
- VPN
- State-Of-The-Art NetVoice N.O.C.
- Local and Long Distance
- Prepaid VoIP Calling Cards

**Professional Services:**
- Consulting and Planning
- Installation
- Support and Training
- Business Development
- NetVoice Certified - IP Trial Integration Lab Testing

To Request Additional Information About NetVoice Technologies Products or Services Please Contact Us at http://www.netvoice.com/acuta/journal/ad/winter00
Or call (800) 997-2988 x1258
Campus Profile

Institutional Excellence in Telecommunications

Honorable Mention

Two schools, Binghamton University and Florida State University, were recognized at ACUTA’s Annual Conference in July 2000 as winners of honorable mentions for the Institutional Excellence in Telecommunications Award. Both schools are to be commended for their fine efforts, details of which are provided below.

Binghamton University

Binghamton University is a full-service provider of voice, video, wireless, and Web-enabled services to more than 15,000 customers. The entire platform is owned and maintained by the campus and is fully complemented with staffing in technical operations, information systems, the business office, and the call center.

Some of our defining processes and services are:
1. Creation of telecommunications mission and vision statements
2. Creation of a world-class information call center
3. Implementation of technology services
   a. I-81 Distance learning consortium
   b. Interactive voice response
   c. Web-based services
4. Creation of training program for users of communications services
5. Ongoing organizational and institutional services

Everyone understands that before you can construct a building you need a sound foundation upon which to build. The same principle holds true for running a successful telecommunications operation. Several years ago we were faced with some difficult demands and no effective way to determine priority. Then it hit us: Define a mission statement creating a visual sense of what we do and supporting statements of how we’re going to do it.

A day-long retreat of the staff produced a working document that serves as our guiding principle on a daily basis. Almost overnight our tasks and planning processes became easier. This is a direct result of understanding and operating by our principles at all levels of the organization.

The Information Center

In the summer of 1998 we began a comprehensive review of several processes we oversee. One of these is the campus operator service, which includes switchboard and department no-answer or busy-call-revert duties. We noticed a steady increase in the number of calls coming back to the switchboard after reaching busy signals or departmental voicemail services. These calls came mostly from our busiest offices, such as financial aid and admissions. Using our focus on customer service, we explored new ways of handling these calls.

Our initial meetings included the offices mentioned above and our center for quality. We were able to align ourselves with the values of the involved offices and map out the necessary steps to satisfy our callers. Our decision was to create a call center.

By June 30, 1999, we had senior staff approval to move on our plan. The response was strong in favor of a call center, now named the Information Center. Our ongoing operative is to provide basic information and answers to frequently asked questions. This relieved the specialist in each area to handle more personalized caller needs.

Before implementing this solution, we needed benchmarks and a goal in terms of service and
productivity measurement. We visited existing call centers to gain a better insight into the effective implementation of human and technology resources. The information center, though small in appearance, is overwhelming in terms of creating and adding value to the University.

**Distance Learning**

In the fall of 1995 we were asked to propose a distance-learning solution for I-81 corridor schools (schools located near U.S. Interstate 81). Within a matter of several weeks we had joined with other campuses in the design of program and technical support for a robust effort.

The first of its kind in New York, this program, which uses H.320 videoconferencing technology, became the benchmark for what other institutions are doing in terms of distance learning. Westnet and the SUNY United Colleges of Technology are just two groups that have emerged as a result of the efforts set forth by Binghamton.

Our campus and community share in the benefits of having this technology available to them. Faculty have been able to synchronously interact with diverse resources all over the world. For example, a theater class brought in a live Japanese Butoh performance from Tokyo and through an interpreter learned of centuries-old art from world-renowned performers.

**IVR**

Another new technology we deployed is interactive voice response (IVR). In 1996 we developed our first application for the busy financial aid office to report aid packages and status. The response was overwhelming. Even though terminal access still exists for the same purpose, we are finding that IVR provides a critical component of the student services portfolio. In our ongoing developments with other campus offices, we are finding new ways to use IVR.

The buzz word of the day is Web. Beginning in May 2000, student and convenience account holders were able to post payments to their accounts online, with real-time authorization and posting. With Web payment capability, we can develop a new host of services for our customers, including credit limits, prepayment, and more.

**Technology Training Center**

Binghamton University hires around 350 new employees per year. We developed a training program for new employees in order to educate them as users of our communications services. The campus Technology Training Center (sponsored by the Educational Communications Department) was developed using some of our guidelines for training.

They offer at least 10 workshops per month on everything from html development to PowerPoint.

Binghamton University Telecommunications is positioned to travel the road of change with confidence and integrity. It will be a remarkable journey for everyone, defining new traditions in learning and operating, and we look forward to our trip.

---

**Florida State University**

Florida State University is indeed “wired” for technology. Due to the creative and innovative thinking of several departments—including the Office of Telecommunications (OTC)—we have come out of the dark ages of paper processing into the electronic world of Web sites and online order processing.

**A Process Problem**

In the past, multipart order forms for OTC products or services were either hand-delivered or sent via campus mail to OTC. OTC would enter the orders into a database that assigned sequential numbers to each order. The order number would be written on the order form, and a copy of the form would be returned to the originating department. This provided confirmation of OTC’s receipt of the order, as well as a reference number for follow-up.

Lost orders were a significant issue. Since OTC was the last in a long line of delivery, orders often failed to reach their final destination, and departments would not realize that the order had not reached OTC for several days or even weeks.

**A Paperless Solution**

The OTC has developed an online Web order application, the Telecommunications Services Request (TSR), that provides University departments with an automated method to submit orders for products and services. The application provides immediate confirmation of OTC’s receipt of the order. This automated process has, for many customers, replaced the cumbersome paper process.

Key goals and objectives of this project were:

1. To reduce the number of lost orders sent through campus mail or by fax
2. To streamline the process and reduce the time it takes for orders to be placed in queue for processing
3. To provide customers with a simple and convenient method of submitting orders
4. To reduce the costs of processing in terms of time, human intervention, and costs of multipart forms
5. To reduce the number of errors in information on order forms by limiting the choices available for certain data elements

In early 1998, OTC employees were well aware of the shortcomings of the order process system based on their own experiences as well as on customer feedback. The seven-member team (representing OTC's customer service, accounting/billing, and Web development areas) developed a more customer-friendly process which would streamline internal procedures for OTC order processing. In October 1998, the new system was ready for testing. Select customers were advised of this new option for placing orders and were trained to use it. OTC then solicited feedback and evaluated and modified the new online order system.

With the new online application, departments can easily submit an order for all types of OTC products and services using drop-down boxes, links to relevant OTC Web pages for information, and a few other tools. Using the new system, a customer enters the order and clicks submit. The order is sent via e-mail to OTC where the order data is imported into the order tracking system and is ready for processing. Multipart forms have been completely eliminated. The department representative receives not only a confirmation of receipt immediately upon submitting the order but also the Web order number, the OTC consultant assigned to the order, and a brief description of OTC procedures for processing orders (e.g., expectations for follow-up calls, completion of order, etc.). What's more, OTC receives the order and can begin processing immediately.

The automatic upload of records will reduce clerical data entry time by approximately 95 percent. It is also expected to eliminate errors resulting from manual data entry by OTC staff into the order tracking system.

Obviously, OTC sought to reduce the time and costs involved with processing orders and increase customer satisfaction as a result. The first two elements were easy to measure. OTC was able to reduce its processing time from approximately three weeks to a "guaranteed" 13-workday turnaround—but 90 percent of orders are actually completed in less than 10 workdays, 50 percent in less than five.

Probably the single most important result of this project is that customers have experienced and demonstrated a much-improved level of trust and confidence in OTC, its processes, and its staff. The automation of OTC's product and service orders is a prime example of exemplary or best-practices business processes. Not only has it saved the University dollars, it has resulted in more streamlined processes; faster, more efficient services to customers; and better customer relations between OTC and other University departments. The team continues to evaluate and process feedback, from both internal and external customers.

Saving time has not only opened the door for OTC to investigate and introduce newer technologies, products, and services, but has also opened a gateway through which OTC has and will continue to develop new and better Web applications. A critical part of OTC's mission is to deliver excellent customer service, stable service offerings, and the continued expansion of new and existing technologies to the University. The introduction of the online Web order application has been the impetus for development of other Web applications here on the Florida State University campus.

Executive Director

Continued from page 48

wireless services. However, some of the spectrum being considered for reallocation is currently being used by many campuses for instructional television fixed service (ITFS), which is used for educational programming and was recently authorized for two-way data transmission. Alternative spectrum being considered is currently used by the Defense Department for undisclosed purposes. We anticipate that many campuses and associations representing the cellular industry and ITFS license holders will weigh in on this complex matter. A report was due from the FCC on March 1 and will be available at the ACUTA Web site.

At ACUTA's Winter Seminar in New Orleans, attorney Jeffrey Linder reported that we might see a complete turnover in membership at the FCC within a year due to term expirations and resignations.

As always, ACUTA will continue to monitor and inform our members on the shifting sands of telecommunications regulation and will act as an advocate on issues that we believe will have a significant impact on higher education.
Advertiser Index

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.

Applied Digital Solutions ......................... 8
David Crowell
540 North Commercial St.
Manchester, NH 03101
603/645-1616
sales@ip-acd.com

★ AT&T ................................................ Back Cover
Glen Fleishhacker
Product Development Director
2350 Green Rd., Ste. 100
Ann Arbor, MI 48105
gfleishhacker@acu.com

Centrinity ................................................ 5
Dean Hannaford
100 Allstate Parkway, Ste. 800
Markham, Ontario, Canada L3R 6H3
905/415-7000
dean_hannaford@centrinity.com

Compco ................................................ 7
Randy Burns
Vice President, Sales & Marketing
5120 Virginia Way
Brentwood, TN 37027
615/373-3636 x148
rburns@compco.com

MHT Executive Search ......................... 27
Cathy E. Tidmarsh
631/243-1735
cathy@jobmagician.com

★ MiCTA ................................................ 15
Clancy DeLong
Vice President/Treasurer
PMB 304, 2020 S. Mission
Mt. Pleasant, MI 48858
517/772-2623
cdelong@micta.org

★ NetVoice ............................................. 43
Eileen Schloss
Marketing and Product Development Mgr.
3201 West Royal Lane, Ste. 160
Irving, TX 75063
972/788-2988
eschloss@netvoice.net

★ Optus, Inc. ........................................... 11
Lori Smith
Vice President, Sales and Marketing
P. O. Box 2503, 3423 One Place
Jonesboro, AR 72401
870/974-7747
lsmith@optusinc.com

★ PaeTec/Pinnacle ................................. 17
Rick Cunningham
Vice President, Sales and Marketing
1530 Eisenhower Place
Ann Arbor, MI 48108
734/975-8020
rick.cunningham@paetec.com

★ PCR, Inc. ............................................. Inside Back Cover
Dan Ross
4635 N. Breton Ct.
Kentwood, MI 49508
616/354-0000
danr@pcr7.pcr.com

★ SpectraCorp ........................................ 31
Wendy R. Pyne
President
8131 LBJ Freeway, Ste. 325
Dallas, TX 75251
972/671-1700
wpyne@spectracorp.com

★ StarTel .............................................. Inside Front Cover
Maribeth Dorman
National Sales Director
17661 Cowan Ave.
Irvine, CA 92714
949/863-8700
maribethdorman@startelcorp.com

★ United ................................................ 35
Kenneth Allison
6608 Joy Road
E. Syracuse, NY 13057
315/463-5500
kallison@ucc.com

★ Williams ............................................... 33
Gene Barnette
12069 Connell Dr.
Overland Park, KS 66213
913/897-1551
gene.barnette@wilcom.com

★ WTC .................................................. 12
Shelley Hasselbrink
Business Development
801 South Grand Ave., Ste. 700
Los Angeles, CA 90017
213/689-5314
shasselb@ix.netcom.com

★ Indicates ACUTA Corporate Affiliate

For information about advertising in the ACUTA Journal contact KCS Intl, LLC.
717/397-7100 • www.kcsinternational.com
From the Executive Director

Public Policy in a New Administration

With a new administration in place in Washington, D.C., my thoughts naturally turn to public policy and changes that might be on the horizon that could affect higher education telecommunications in a major way.

Commissioner Michael Powell has been appointed to replace William Kennard as chair of the FCC. Powell, a Republican appointed by President Clinton, has served on the commission since 1997. Previously, he was chief of staff in the Justice Department’s Anti-Trust Division, and before that he was a private attorney who practiced telecommunications law, among other specialties. He was an army officer, and yes, he is the son of Secretary of State Colin Powell.

From our observation, in his four years on the commission, Powell has supported deregulation as a prerequisite to increasing competition in telecommunications. He is deeply interested in issues related to accessibility of telecom equipment and services for the disabled and has generally supported efforts to promote the deployment of advanced telecommunications capability to all Americans through the removal of regulatory market barriers and encouragement of private sector investment. He has spoken out strongly against “slamming” and other fraudulent practices. He is also an advocate for law enforcement and national security issues, cautioning the commission and Congress to make the safety of life and property and the national defense priorities in the FCC’s strategic plan.

Some observers have speculated that the commission under its new chairman may not place as much scrutiny on mergers of companies in the telecom industry. Chairman Powell has not, to my knowledge, been particularly outspoken on higher-education-specific issues.

On January 23, the Bush administration’s education package was sent to Capitol Hill for introduction. In a section of the report called “Enhancing Education through Technology,” the president calls for several changes in the e-rate program, which provides telecommunications discounts to K-12 schools and public libraries. The proposed changes include combining the e-rate program with other federal technology grant programs and providing funds to schools based on a formula rather than the current cumbersome application program.

It is not yet clear what the effect of the Bush proposal would be on the rates currently paid by telecom carriers and passed on to end users (including colleges and universities) to support the e-rate. In addition, it is too soon to tell whether the proposed modifications would eliminate the corporate structure put in place by the FCC to administer the program. These proposals face review by the House Telecommunications Committee and other committees prior to enactment.

As we go to press, two major regulatory issues before the FCC could have a far-reaching impact on colleges and universities. The first is the competitive networks proceeding, in which the FCC is considering whether to require owners of multiple-tenant dwellings to allow competing providers of residential telecom services to enter their premises. ACUTA and a number of other higher education associations have asked the FCC in comments submitted January 22 to exempt college student housing from any such requirement.

The second major issue for our members is the numbering resource optimization proceeding, which will affect the length of time and terms under which institutions may reserve telephone numbers for future use. ACUTA plans to comment on this matter prior to the deadline date of February 14. It is not yet clear whether the change in leadership at the FCC might delay any decisions by the commission on these two matters.

A third issue that will have long-range implications for some ACUTA members is the FCC’s inquiry into third generation wireless, or 3G. 3G is being implemented in other countries but has not been introduced yet in the United States. The federal government has launched an effort to study how advance wireless broadband services can be introduced in this country, and they are searching for spectrum to use for this purpose.

3G will provide opportunities for campuses to make broader use of more-reliable, higher-bandwidth

continued on page 46
telemanagement + WEB = COMIT WebCenter

PCR proudly introduces COMIT WebCenter, the first full function telemanagement system available via the Internet.

**telemanagement**

Take advantage of the proven power of the COMIT Telemanagement System. The COMIT WebCenter provides the first full-function telemanagement system available via the Internet, offering:

- Call Accounting
- SMDR Call Collection
- Service Order & Trouble Ticket Processing
- Equipment Inventory
- Cable Inventory Management

**+ web**

- Secured access from any location
- Access COMIT via an Internet Explorer or Netscape enabled PC
- Avoid the cost and support associated with a stand-alone system
- Eliminates the need for paper reports
- Take advantage of COMIT's powerful UNIX architecture via the Web

**- hassles**

- Risk-free trial
- Minimum commitment; the COMIT WebCenter is provided at a **low monthly cost of less than 20¢ a line.**
- No startup costs
- Eliminates capital expense – pay via corporate credit card
- No more implementation headaches; sign up today and start entering data tomorrow

**COMIT WebCenter**

It all adds up to a no-brainer.

---

Want to pick our brains about the COMIT WebCenter?

Go to [www.comitwebcenter.com](http://www.comitwebcenter.com) and sign up today for your risk-free trial.

Stop by our booth at ACUTA
You know more than anyone, gone are the days where your community can be contained on a campus map. The information revolution not only connected your college or university with the entire world beyond, it made the world your campus. Don’t worry about how you’re going to deliver cutting-edge technology and communications services to your world. AT&T can do any of it or all of it for you.

Whether you’re simply adding popular creature comforts to enhance campus living arrangements or creating internet-based avenues for teaching and research, AT&T can put technology to work for you.

The AT&T Campus Advantage brings together the best people, technology and resources to meet the unique needs of higher education in today’s world. Your World. Your Campus.

Wireless Services, Broadband, Long Distance, Pre-Paid Calling Cards, Integrated Billing and Management Services, Internet Service Provider and eSolutions... Get the AT&T Campus Advantage for your campus, your world.

For more information, contact your AT&T representative at www.att.com/campusadvantage or call 1 800 ACUS-YES.