

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

ACUTA Journal

ACUTA: Association for College and University
Technology Advancement

Fall 2004

ACUTA Journal of Telecommunications in Higher Education

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

"ACUTA Journal of Telecommunications in Higher Education" (2004). *ACUTA Journal*. 31.
<http://digitalcommons.unl.edu/acutajournal/31>

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.

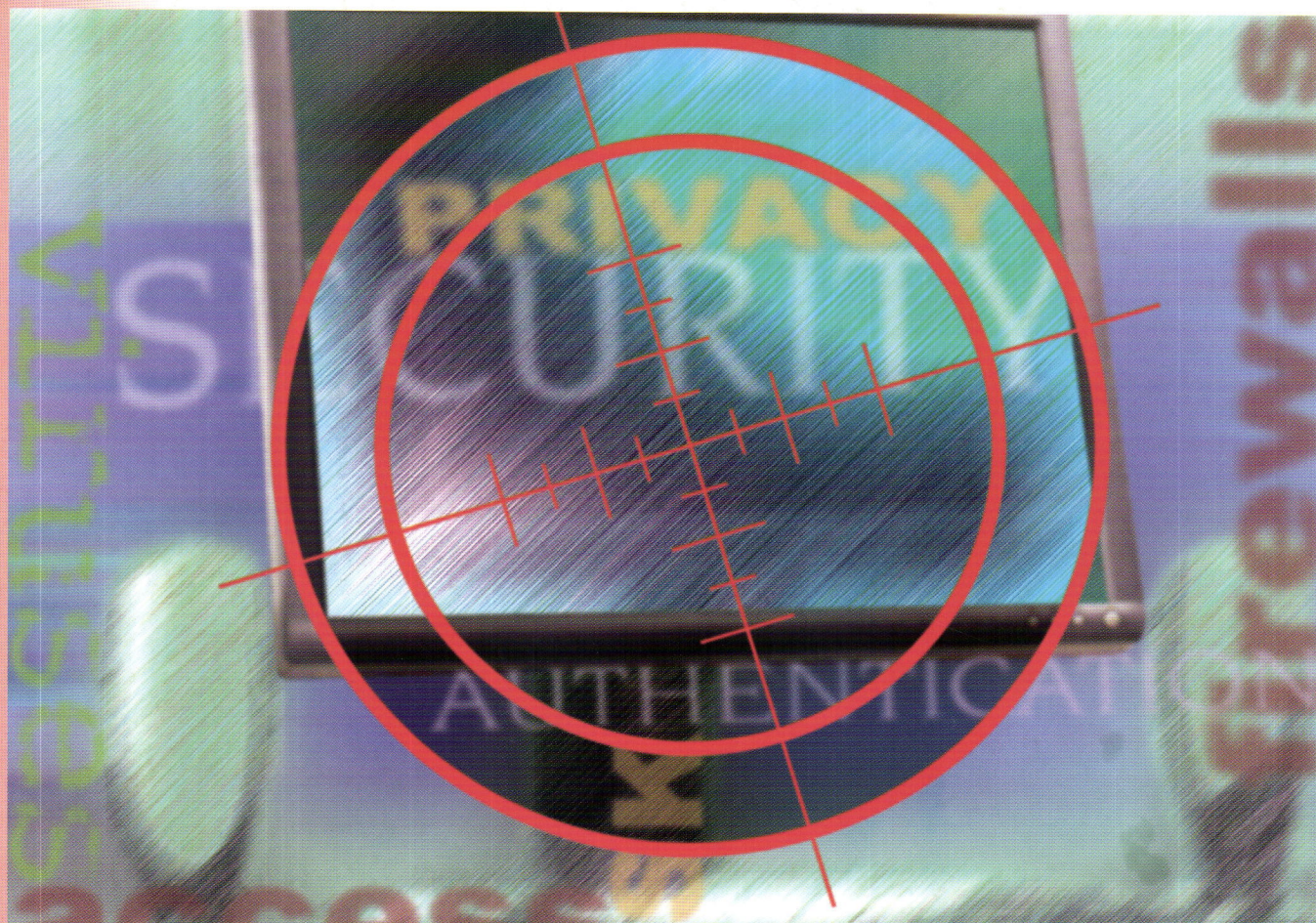
Fall, 2004
Vol.8, No.3

acuta

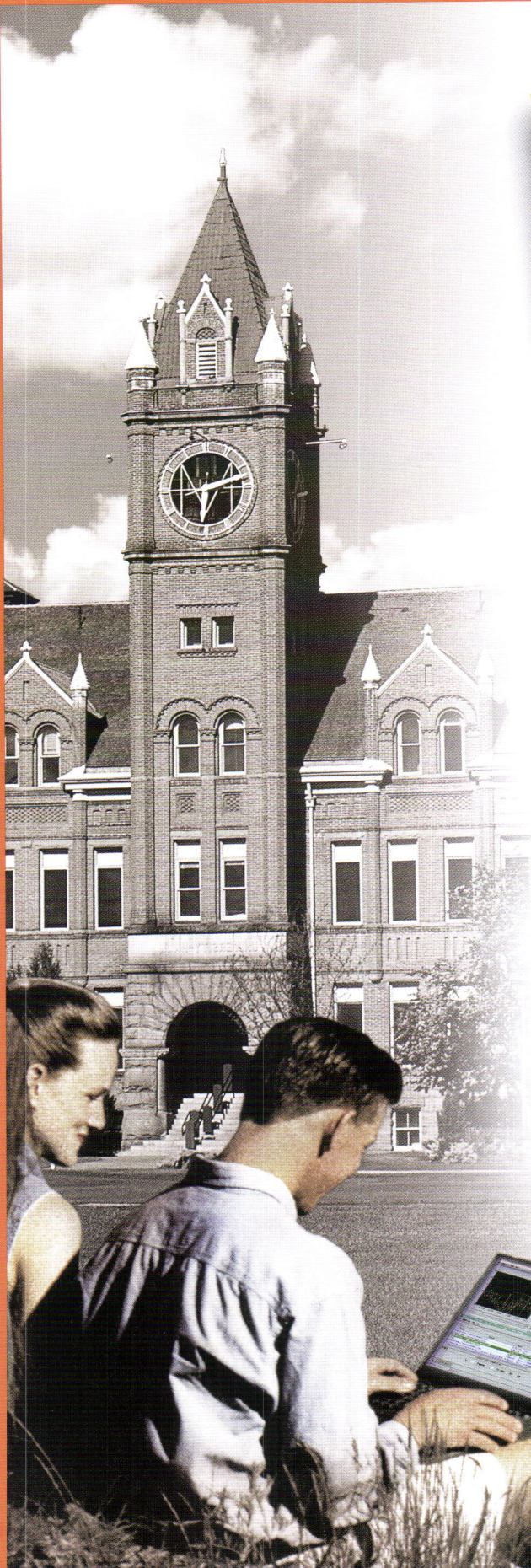
Journal

of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education



This Issue: Network Security and Management



*Can I secure, manage and
control my education network
with fewer resources?*

Yes!

Most educational facilities secure their private data from external threats by using WAN firewalls and VPNs. However, independent analyst studies show that up to 90% of security breaches come from inside the network – ranging from users attempting to access restricted data to students and mobile users signing on to the network with a virus they picked up in the outside world.

You need **internal security**

You need **continuous operation**

You need **wireless mobility**

You NEED Alcatel

ALCATEL DELIVERS



www.alcatel.com/enterprise

800-995-2612 (prompt #5)

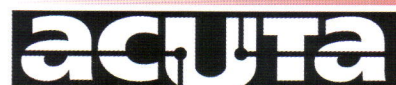
Events Calendar

Event	Date	Place
Fall Seminars	October 24 – 27, 2004	Hyatt Regency St. Louis, Missouri
Winter Seminars	January 30 – February 2, 2005	Hyatt Regency San Antonio, Texas
Spring Seminars	April 3 – 6, 2005	Wyndham Franklin Plaza Philadelphia, Pennsylvania
Annual Conference	July 17 – 21, 2005	Gaylord Palms Resort Kissimmee, Florida

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

ACUTA's Core Values are to:

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



Contents

Fall 2004 • Volume 8, Number 3
Network Security and Management

FEATURES

12

The Converged Closet: Considerations for VoIP

Gary Audin

For those who are planning to move to a converged network, Audin points out some hidden costs that will help calculate a realistic total cost of ownership.

18

Securing Your Wireless Network

Ron Walczak

From rogue access points to ad hoc hackers to troublesome neighbors, threats to the security of your wireless network are everywhere. What is industry doing about this problem, and what can you do about it yourself?

22

Legal Alternatives to Rich-Media Sharing

Curt Harler

The Internet is a great way to distribute content as well as music. But it has become a burden on networks and legal departments on campus. Two alternatives may bring viable solutions.

31

Basics of WLAN Security for Higher Ed

Glenn Taylor

Maintaining the security of your WLAN requires awareness of where the threats come from as well as a well-planned strategy. Taylor provides some basic considerations for achieving a high level of security.

34

Shaw University Upgrades Network to IP Telephony and Takes the Difference to the Bank

Martel Perry

Shaw University replaced an aging Centrex system with a converged voice, data, and video backbone to connect 10 satellite campuses. Read how they did this and are now saving money.

37

Instant Messaging on Campus: RU Secure?

Joe Licari

IM is a popular tool for extending communications capabilities on campus. How do you reap the benefits of IM without compromising the security of your network?

40

Network Assessments—The “Catch-22” of IP Telephony

Ron Walczak

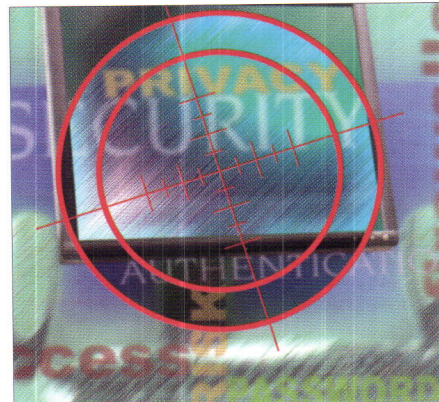
Walczak offers practical advice about assessing your network and avoiding a potential “catch-22” as you prepare for IP telephony.

42

Voice Lessons: Open-Source VoIP Finds a Home in University Networks

William Rich

A SIP-based, open-source VoIP platform may help your campus determine if VoIP works for you without major investment. Read about the experiences of Boston University, Swarthmore, North Carolina State, and Texas A & M.



INTERVIEW

28

with Doug Van Houweling

Internet2

COLUMNS

6

President's Message

Tamara Closs, Georgetown University

9

From the Executive Director

Jeri A. Semer, CAE

48

Here's My Advice

Geoff Tritsch, Compass Consulting Intl. Inc.



ADVERTISERS' INDEX

46

Thanks to the companies who support ACUTA by advertising in our Journal.



DON'T USE MUSEUM PIECES FOR YOUR WI-FI NETWORK.

BelAir Networks provides the most advanced and easy-to-deploy Wi-Fi networking solution available for university and college campuses.

Our unique mesh networking technology – deployed with outdoor Wi-Fi platforms – provides full carrier-grade Wi-Fi coverage, inside and out. It simplifies network deployments by eliminating the need to inter-wire access points. It provides greater range and capacity than any other option on the market. And it offers the lowest cost of deployment for campus networks.

So don't be old school. Use BelAir Networks to deploy your Wi-Fi network in days, not months; avoid drilling access points into buildings; and eliminate backhaul costs.

We invite you to study BelAir Networks in-depth. Contact us today.

BelAir 
NETWORKS

www.belairnetworks.com

1-877-BelAir1 (235-2471)

613-254-7070

info@belairnetworks.com

sales@belairnetworks.com



IT security can best be looked at as the balance between ease of access and protection of assets and information. The easier the access, the more vulnerable the information, especially considering that a significant portion of your threat (students) is inside your own firewall.”

Geoff Tritsch
Compass Consulting International, Inc.
page 48

THE ACUTA JOURNAL OF COMMUNICATIONS TECHNOLOGY IN HIGHER EDUCATION

Published Quarterly by

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

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

Publisher

Jeri A. Semer, CAE, Executive Director

Editor-in-Chief

Pat Scott, Communications Manager

Contributing Editor

Curt Harler

Advertising Sales

Amy Burton, Manager, Corp. Relations and Marketing
859/278-3338 or e-mail: aburton@acuta.org

Submissions Policy

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

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

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

Contents of this issue of *The ACUTA Journal* are copyrighted: © 2004, ACUTA, Lexington, Kentucky.

ISSN 1097-8658

POSTMASTER, send all address changes to:

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

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

Membership and Subscriptions

Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for \$80 per year or \$20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 22, or e-mail, kbowman@acuta.org.

ACUTA

2004–2005 Board of Directors

President

Tamara J. Closs, Georgetown University

President-Elect

Patricia Todus, Northwestern University

Secretary/Treasurer

Carmine Piscopo, RCDD, Providence College

Immediate Past President

Walter L. Czerniak, Northern Illinois University

Directors-at-Large

Phillip Beidelman, WTC

John Bradley, Rensselaer Polytechnic Institute

George Denbow, University of Texas at Austin

Corinne Hoch, Columbia University

Diane McNamara, Union College

Publications Committee

Walt Magnussen, PhD, Texas A & M University, *Chair*

Ron Kovac, PhD, Ball State University

Dale Lee, Biola University

Carole Sedlock, University of Toledo

Cindy Shortt, University of Texas Health Science

Center at San Antonio

Ex Officio

Tamara J. Closs, Georgetown University

Jeri Semer, CAE, ACUTA Executive Director

Board Advocate

Corinne Hoch, Columbia University

Staff Liaison

Pat Scott, ACUTA Communications Manager

Editorial Review Board

Dave Barta, University of Oregon

James S. Cross, PhD, Michigan Technological University

Jay Gillette, PhD, Ball State University

Steve Harward, University of North Carolina, Chapel Hill

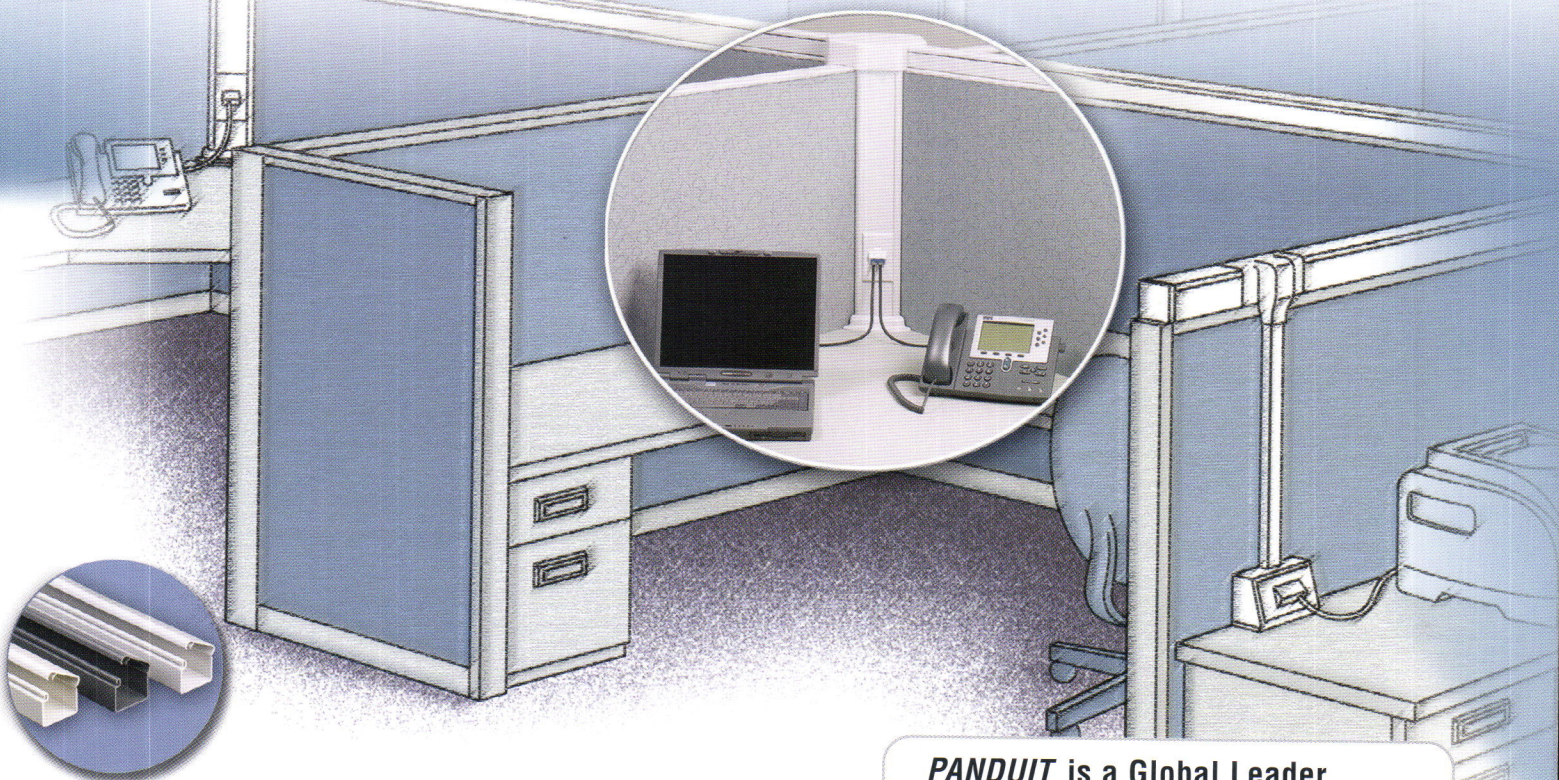
Ray Horak, The Context Corporation

Angela Imming, Southern Illinois University, Edwardsville

Jeanne Jansenius, University of the South

Dave Metz, Compass Consulting International, Inc.

Office Routing Solutions



Extend the life of your office furniture investment with PANDUIT Office Furniture Raceway.

Office Furniture Raceway is an innovative TIA/EIA compliant system that allows you to route, conceal, protect and terminate data, voice, video and fiber optic cabling. This non-metallic pathway solution is designed for routing data cabling to the workstation desktop of existing office furniture partitions. The superior corner termination option saves valuable workspace, while maintaining flexible and convenient access. Office Furniture Raceway is available in three popular colors to blend with most office furniture systems, creating an attractive cost effective routing solution.

- UL Listed in accordance with UL-5C requirements for Class 2 Communication Cable Management Systems
- Maintains bend radius control throughout the entire office furniture raceway system as required by TIA/EIA-568-B and 569-A
- Faceplates are compliant with the labeling requirements of the TIA/EIA-606-A standard
- Tamper resistant closure prevents unauthorized access to cabling
- Designed for fast easy installation



Service Provider
Solution Partner

PANDUIT is a Global Leader
Providing Innovative Networking
Solutions to Enable Technology.

- ***Racks and Cable Management***
- ***Network Identification Systems***
- ***Modular Twisted Pair and Fiber Optic Connectors***
- ***UTP Copper Cable***
- ***Outlets***
- ***Raceway Systems***
- ***Fiber Routing Systems***
- ***Physical Layer Management Systems***
- ***Zone Cabling Systems***
- ***Network Cable Ties and Accessories***
- ***Network Grounding Systems***



For more information, reference ad # ofr05

www.panduit.com/ofr05

cs@panduit.com • 800-777-3300

Maintaining Security at Georgetown University



Tamara J. Closs
Georgetown University
ACUTA President
2004–2005

At Georgetown University, network security and management requires the collaboration of many University departments including the University Information Services, Legal Counsel, Student Affairs, Office of University Safety, Internal Audit, and others. These departments work together to comply with applicable public policy and law and to develop internal policy; to implement procedures for enforcement of the policies; to monitor and coordinate response to internal and external threats and occurrences; and to provide user education.

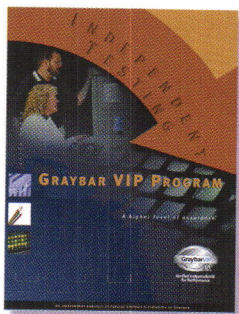
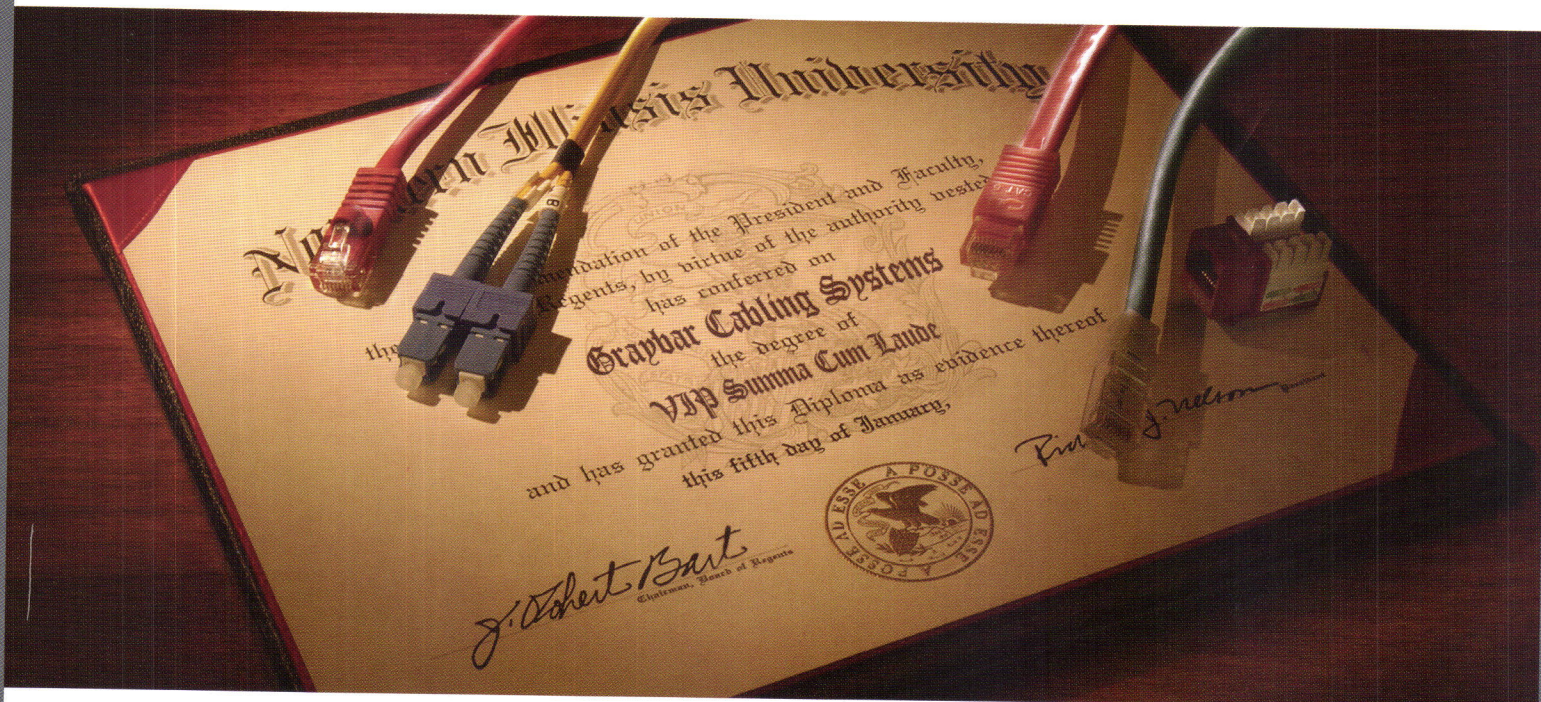
There are many non-technology federal regulations and laws that impact the management of network security, including Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability, Digital Millennium Copyright Act, Gramm-Leach-Bliley Act, and the National Strategy to Secure Cyberspace. When these policies and regulations are implemented through the development of University policies, there is an ongoing effort to balance the need for security with the need for privacy. While federal regulations may not directly implicate network security, they must be supported by the University's network security policy and procedures. As for policy enforcement, the key has been user education. According to Ardoth Hassler, associate vice president, University Information Services, "Typically when dealing with users, a 'first offense' of a policy is the 'last offense' once a user has been made aware of what University policy is. Our Student Affairs division is a wonderful partner in handling issues related to

student infringement of policy."¹ Georgetown University's policy process is available at <http://www.georgetown.edu/policy/technology/>.

"Security is a negative deliverable. You don't know when you have it. You only know when you've lost it," according to Jeffrey I. Schiller, MIT's security architect. August 2003 found most of us scrambling to respond to worms and viruses like MiMail, Blaster, Sobig, and Nachi. Georgetown University was successful in minimizing the impact of these worms and viruses through the tremendous efforts and long hours of many dedicated University Information Services employees. They developed and distributed a CD and supporting documentation that provided faculty, staff, and students the tools needed to patch and update their systems. Network alerts and firewall logs are an integral part of identifying and resolving problems before the users are affected, but once a problem is at the desktop, it requires an effective plan of action for developing and distributing the right tools to the affected users.

In gathering information to write this article, I interviewed the vice president of University Safety, the associate vice president for University Information Services, the University network security officer, and the director of Academic and Information Technology Services at Georgetown. They all agreed that a critical aspect of security is user education—evoking responsible actions and reaction to prevent and resolve security issues. While the worms and viruses of August 2003 were not a welcome problem, they

Your cabling system should earn the *highest honors – ours.*



For more information on our services and the VIP Program, call 1-800-GRAYBAR or visit www.Graybar.com/ac0904 for your FREE VIP Program information packet.

Before you upgrade your cabling system, wouldn't it be great if you could check its performance to ensure you are making the best investment for your university's future? With Graybar as your technology partner, we'll do that for you, as well as provide you with a higher level of assurance with our independent VIP Testing.

Graybar uses the third-party testing services of Intertek ETL SEMKO—the largest independent test lab in the world—to test interoperable combinations of the leading cabling system manufacturers' products in real-world scenarios. Only after these cabling systems are proven to **exceed** the performance standards of Category 5e, Category 6 and fiber* do they earn the Graybar-exclusive VIP designation. You can be assured of consistently superior performance because Intertek tests Graybar inventory randomly every quarter.

Graybar has a nationwide network of communications and data specialists at more than 250 locations to help you select the right cabling systems to support your educational applications today and, more importantly, tomorrow. Our knowledge and experience working with universities can save you time and money. Then you can focus on what you do best—educating the next generation of experts and leaders.

*TIA/EIA 568-B.3 and IEEE 802.3z

www.graybar.com
1-800-GRAYBAR (472-9227)
(During Normal Business Hours or After Hours for Emergency Service)
Graybar is ISO 9001:2000 Registered, ensuring consistent quality service.



Verified Independently
for Performance


GraybaR®
works to your advantage

President's Message

continued from page 6

did help to drive home the issue that all users are responsible for protecting information resources to which they have access. According to Brian Reilly, University network security officer, user education about strong passwords, patches, antivirus, and other desktop management tools is the best offense (or is that defense?) to providing network security.

Underlying the effectiveness of all aspects of network security is appropriate staffing. The scope of responsibilities for network security staff is changing as the policy and

technology issues become more complex. A recent ECAR *Bulletin*, titled "High Stakes: Strategies for Optimal IT Security Staffing," discusses the many metrics involved in determining the appropriate staff solutions that will be as unique as each institution but at some level must address the same issues.² The changes do not stop once staff is in place; training is essential for continued effectiveness. In response to a recent security breach, Senate CIO J. Greg Hanson says he could have offered more training and done a better job publicizing security best practices.³ One thing is for certain: Network security in higher education continues to gain importance and become more complex technically and legally.

References

¹ *Security Policies for Institutions of Higher Education*, presentation delivered on May 17, 2004 by Ardoth Hassler, assoc. vice president for University Information Services, Georgetown University; and Tracy Mitrano, director of IT policy and computer policy and law program, Cornell University.

² Judith A. Pirani, Educause Center for Applied Research, "High Stakes: Strategies for Optimal IT Security Staffing," *Research Bulletin* 2004, no. 6, March 2004), www.educause.edu/ecar/.

³ Ben Worthen, "Lack of Training Led to Security Breach," *Washington Watch CIO.com*, May, 15, 2004. http://www.cio.com/archive/051504/tl_washington.html.



Teamwork

Since 1983

*Consulting In Telecommunications,
Networks, & Information Technology
In Higher Education*



Talent



Technology

213-622-4444

www.wtc-inc.net

wtc@wtc-inc.net

From the Executive Director



Jeri A. Semer, CAE
ACUTA Executive Director

Annual Report to the ACUTA Business Meeting

Each year I present a report to the annual business meeting, highlighting key activities of the professional staff during the past year. This year, my report at the August 5, 2004, business meeting focused on accomplishment of the many goals and action items in the ACUTA strategic plan.

Since many members did not have the opportunity to attend the annual meeting, I would like to share highlights of my report and invite your comments and questions.

It is a continual pleasure to be able to work with a dedicated and service-oriented group of staff members in the Lexington office. This year saw some changes in our staff, as we wished Eleanor Smith, ACUTA's first business manager, a long and happy retirement. However, we were pleased to welcome Margaret Riley last November as our new business manager. Margaret has quickly assumed her duties and has introduced some great new ideas that are helping us move forward in that important area. In June, we welcomed Amy White as our new part-time accounting and administrative assistant. I hope that each of you has an opportunity to meet these new staff members in the course of your interactions with the ACUTA office.

As always, we were fortunate to have the leadership of a very talented and dedicated group of elected and volunteer leaders—our Board of Directors, committee chairs, and committee members—who continue to devote tremendous energy to setting a wise course and keeping ACUTA moving in the right direction. As members of this association, you can rest assured that your elected leaders are exercising their fiduciary and strategic leadership responsibilities with the utmost care and dedication.

Our president and secretary/treasurer shared their views on the state of the association, where we stand strategically and financially, and some important changes we have made to our membership and dues structures. These changes are all designed to strengthen our basic financial foundation going forward, while being fair to all sizes and categories of institutions with minimal financial impact on any individual college or university.

We all feel very positive about how much of the current strategic plan has been accomplished, and we are poised under the leadership of President-Elect Tamara Closs to move forward beginning this September with the development of a new plan for ACUTA.

As we embark on a new planning effort, I believe it is important to review the current strategic goals and highlight some of the objectives and action items that have been accomplished.

Since the strategic plan contains 6 goals, 24 objectives, and 96 action items, I am only going to cover a few. If you are interested in a complete status report, please e-mail me at the address at the end of this article and I will be happy to send it to you.



Goal A: ACUTA institutional and corporate membership will increase.

This has been an active area for the staff and Membership Committee.

A task force consisting of staff and volunteer leaders from the Board and Membership Committee was formed, chaired by John Bradley from the ACUTA Board. The task force recommended that we retain expert marketing consultants to assist in achieving this objective. An RFP was developed and the bidding process resulted in the selection of Marketing General, Inc., of Alexandria, Virginia. They will work with our staff to implement a sophisticated marketing effort to attract non-member institutions to membership in ACUTA. A direct-mail campaign to approximately 10,000 individuals in telecom and IT at campuses throughout the U.S. is scheduled to begin in August.

Goal B: Data Communications professionals will look to ACUTA for insight and information.

One of our objectives was to increase the participation of data communications professionals in our events and other ACUTA services.

We have devoted a great deal of staff and volunteer time to this objective, and our efforts continued this year with several educational programs, including audio conferences, seminar tracks, and conference breakout sessions that were designed to directly address the needs of these individuals. The scope of *Journal* articles was also expanded to incorporate additional data communications topics.

Another objective was to increase the number of data networking vendors who become corporate affiliates and are involved as exhibitors and speakers.

We have made a particular effort to attract vendors in the data networking area. The increased diversity of products and services featured at the conference and seminar exhibits is apparent to anyone who attends. Our committees and staff have also included data communications vendors as speakers and authors wherever appropriate.

Goal C: ACUTA will be a recognized leader in communications technologies.

Several activities stand out in our efforts to achieve this goal:

ACUTA was offered and accepted an invitation to join Internet2, and we became the first Association Member of that organization. Through this membership, ACUTA will be able to participate in Internet2's member meetings and workshops, working groups, strategic briefings and advanced technology initiatives such as digital video, middleware, and others. We will also work to strengthen our relationship with members of the Internet2 community through joint public policy initiatives.

We have created a special edition of the *ACUTA Journal* that is a compilation of Presidential interviews conducted over the past two years, and we plan to mail it this fall to the presidents of all member institutions and presidential associations. This will increase our visibility with institution presidents and will support ACUTA's role as a leader in communications technologies.

In addition, we developed a report based on the 2003 ACUTA Strategic Leadership Forum and distributed it to campus leaders throughout the U.S. We received good feedback on this publication, and plan to repeat it this year.

We created the "Press Room" on the ACUTA website, and it has been well received by both corporate and institutional members as a place to post their press releases.

We have also developed a multi-year plan of action for further increasing liaison with presidential associations and increasing ACUTA's media visibility.

Goal D: ACUTA will be a recognized source of insight on legislative/regulatory affairs in communications technology.

ACUTA members continue to value the information and insight they gain from ACUTA on regulatory issues, naming this as the most valuable benefit of membership in our most recent Member Needs Assessment.

A key objective under this goal is to serve the ACUTA membership with timely notification, analysis, and advocacy on relevant legislative and regulatory matters.

As the FCC increases its activities in areas that directly affect our members, we must be prepared to devote even more resources to representing your interests and keeping you informed. This will require a significant financial investment, but it is one of our highest priorities and provides substantial return on investment for your membership dues.

In support of this objective, we:

- Produced and updated the ACUTA issues matrix quarterly, as a resource on the current status of regulatory issues.
- Developed extensive comments to the FCC on IP-enabled services and E911 regulations.
- Allocated funds beginning next fiscal year to increase ACUTA's research, analysis, and advocacy in regulatory issues even further.

- We will also be increasing the distribution of the *ACUTA Journal* to include FCC Commissioners and other key officials.

Goal E: New technologies and applications will be developed to serve the higher education community.

We will be working with the Higher Education Advisory Panel—the group of higher education and industry leaders that helps us plan the Strategic Leadership Forum—to develop an annual survey to identify the top issues and challenges facing ACUTA members. This will help us identify the strategic activities that ACUTA might pursue with regard to technology development and other initiatives. It will also help guide the topics for future Leadership Forums and other educational programs.

Goal F: Member representatives will have the skills and abilities to succeed in a changing technology environment.

A great deal of the staff's time and energy are devoted to planning and producing educational programs. This year, with the help and guidance of the Program Committee, we developed several programs that directly respond to action items in the Strategic Plan:

- We offered an intermediate level seminar on data networking.
- We conducted two Regional Workshops (in Baltimore and New York) that were designed to make ACUTA education more accessible to local members. Both programs were well-rated on attendee evaluations and were financially successful. We will be developing a final report and recommendation on future regional workshops for the Board's consideration.
- We continued our practice of offering audio seminars featuring sessions from our quarterly seminars, and several other audio seminars on

hot topics and regulatory issues. They continue to be well received and well attended. Approximately 1,325 people at 440 sites participated in ACUTA audio seminars from August, 2003, through July, 2004.

- We also expanded online services. We enhanced the ability of members to manage their ACUTA membership and mailings online. We added links to valuable resources outside ACUTA. We are also in the midst of a major redesign and upgrade of our membership database that will provide even more functionality to our members.
- Finally, as part of the redesign of the membership and dues structure, membership benefits will be expanded to allow institutions to have additional "electronic members." These electronic members will receive the ACUTA

eNews and the Legislative/Regulatory Update, and will have access to all of the other Web-based resources of ACUTA.

It has been my pleasure to highlight some of our efforts to support the strategic goals of ACUTA.

None of these actions could have been accomplished without the dedication and energy of every member of the ACUTA staff and volunteer leadership team. I would like to thank every staff member for their professionalism and commitment to the continued success of ACUTA.

As always, I would be happy to respond to any questions. Please e-mail me at jsemer@acuta.org, or call me at 859-278-3338, ext. 225.



Emergency/Event Notification (EEN)

by Mutare Software

One-Call Communication System



- Easy to use. No special training class required.
- Deployment with a single call and flexible message delivery options.
- Members maintain their contact data optimizing accuracy.
- Simultaneously places live calls and sends emails for faster notification.
- Real-time web access for status of member notification and response.

Mutare Software
www.mutare.com

Call 847.781.2370 for more details
and to schedule a live demonstration.

The Converged Closet: Considerations for VoIP

by Gary Audin
Delphi, Inc.

Looking forward to a converged network? Are your LAN and WAN networks ready for converged data, voice, and video? The industry consultants are speculating that 40+ percent of the data networks are not ready for VoIP. Most of the attention has been directed to the wide area network (WAN). There will also be an investment in the closets, cabling, AC power, and air conditioning. These may be hidden costs that will make the organization and network designer think twice about the total cost of ownership (TCO) for VoIP.

The cost of procuring, operating, and maintaining any system or network must be predicted if financial approval is expected. When you choose to write a TCO it should include:

1. Maintenance over the installation lifetime
2. Depreciation over the installation lifetime
3. Replacement parts over the installation lifetime
4. Electrical power budget and possible UPS requirements
5. Floor/closet/rack space requirements
6. Training (salary, instructor fees, lost productivity, certification, staff testing)
7. Downtime factors (mean time between failures (MTBF), mean time to repair (MTTR), scheduled downtime)
8. Any changes necessary to implement or accommodate the expenditure
9. Monetary inflation over the installation lifetime

This article will focus on items 4, 5, and 8.

What to Consider: Elements of an RFP

If a VoIP request for proposal (RFP) is written for the closet, cabling, electrical power, and air conditioning necessary for the move to a converged network, the following issues must be addressed:

1. Will the IP phones require separate cables?
2. Will the existing LAN cabling have to be upgraded to Cat 5 even though the IP phones are supposed to work on Cat 3 cable?
3. How much of the legacy cabling and IDF and MDF closets will have to be retained for devices such as faxes, modems, alarm systems, security devices, telemetry and lifeline, and 911 connections?
4. Will there be a separate LAN or VLAN for VoIP?
5. Can the new closets and equipment support video over IP in the future?
6. What will be the power requirements for LAN switches, voice gateways, servers, and IP phones?
7. Will air conditioning have to be installed in the closets?
8. Will the closets have to support non-communications technology such as video surveillance cameras and environmental controls?

Cables, Closets and Space Planning

Unless the closets do not yet exist, as in a greenfield installation, there will be existing cabling, AC power, and air conditioning installed in the closets. The intermediate distribution frames (IDF)

VoIP Operational Goals for the Closet

Several operational goals for VoIP will be affected by the closet design including:

1. Produce reliability as high as the legacy telephone systems
2. Limit failures
3. Restore service quickly after a failure
4. Diagnose and reduce/prevent recurring problems
5. Ensure backups work

The cost of these goals should be included in the TCO calculation and planned for rather than become "gotchas" after the VoIP procurement decision is made.

WORLD-CLASS NETWORK.

FIRST-CLASS CUSTOMER SERVICE.

FOR STATE AND LOCAL AGENCIES, QWEST DELIVERS.

At Qwest,[®] we are fully dedicated to our state and local agency customers. From needs analysis and budgeting through implementation, testing and rollout, we're there for you every step of the way. And we don't disappear the morning after your solution goes up on our state-of-the-art network, either. You have

schools, emergency services and other critical public services riding on it. So we keep monitoring the network and helping you get the most from our services, long after the contract closes. After all, we want a long-term relationship. And that means earning trust and confidence every single day.

For more information
visit us at qwest.com/government



VOICE SOLUTIONS **DATA** SOLUTIONS **INTERNET** SOLUTIONS **MANAGED** SOLUTIONS

Services are subject to availability. Some restrictions may apply. Please contact your Qwest representative or see our Web site for details.

Table 1. Cables and Closets

Component	Legacy Phone	IP Phone
Legacy Phone Closet		
MDF	Use as is	Use for trunking only
IDF	Use as is	Abandon
LAN closet	Not used	Expanded
Cabling	1 Pair voice grade	2 to 4 Pair Category 3 to 5
Power	From switch 110/120 volts	From LAN switch, Gateway, Power Bar
Air Conditioning	Switch room, not MDF or IDF	LAN closet
Distances	1,000–2,000 meters	100 meters
Closets	Same as before	Multiple per floor

and main distribution frames (MDF) will be changed or possibly abandoned.

Table 1 compares the cabling environments for legacy and IP phones. Several conclusions can be drawn. The cables for legacy phones can be Cat 1 and span thousands of meters. The LAN cables will be 2 or 4 pairs of Cat 3 or 5 data-grade cable with a maximum coverage of 100m.

The LAN closet may assume the functions of the IDF for IP phones. It is unlikely that the IDF can be abandoned, because there will still be some requirements for supporting legacy devices. The MDF will be required for carrier connections. The voice gateways that connect to the legacy phones and other devices can be located in the IDF or centralized in the MDF. In any case, there will probably be some modifications required to both the legacy and LAN closets.

Space planning will be different for VoIP than it is for legacy phones and PBXs. Until all of the legacy phones and devices are moved over the VoIP gateways, the PBX will have to remain. The MDF room may then be oversized, because most of the VoIP cabling will be terminated in the LAN closets on each floor rather than running through the IDFs to the MDF. LAN closet space may have to be expanded, or more LAN closets will have to be arranged per floor. If the IDF is used, then rack space for the new equipment will be required.

Conduit space between floors is consumed with the legacy cabling. It is likely that LAN-to-LAN closet and server connections will use fiber optic cables. Is there room for the fiber cables, or does the legacy cabling need to be removed or new conduit installed? Abandoning the old cable and conduits may not be a viable choice.

Power over Ethernet

Power over Ethernet (PoE) can be implemented as a standard offering as defined by the IEEE 802.3af committee, or it can be proprietary like that offered by Cisco. In either case, the data cable carries the power to the device at the end of 100m of Cat 3 or Cat 5 standard cable. This is referred to as in-line power. The two standard versions of PoE use different cabling arrangements. When the power is generated by the LAN switch, called end span, the power is carried on the data wires used by the LAN NIC, pins 1, 2, 3, and 6. The spare pairs are not used.

The second standard configuration, called the mid-span design, uses the spare wires, pins 4, 5, 7, and 8. The mid-span version has an external power supply placed between the LAN switch and the end device (IP phone). The mid-span solution will probably require rewiring inside the LAN closet to accommodate the power supply. Cisco uses the end span design with negative voltage while the 802.3af standard uses positive voltage.

LAN switches are available in many configurations. Some support all three PoE versions. There are other LAN switches that provide PoE to some but not all the LAN ports. The standard is designed to deliver up to 12.95 watts to the end device. Power is lost passing through the cable, therefore the PoE LAN switch output is designed to deliver 15.4 watts at the LAN switch port. This is enough to power IP phones but not PCs or laptops. Working back to the AC side of the LAN switch, this means that a maximum of 17 to 18 watts may be consumed per LAN port. This seems like very little power until it is multiplied by the number of IP phones. Most IP phones need only 4 to 8 watts of power. The total power can easily exceed 1,000 watts per PoE switch.

A non-redundant Cisco Catalyst 6000 LAN switch requires 1,300 watts for operation supporting 240 PoE ports. The redundant power supply version consumes 2,500 watts for the same 240 PoE ports. The Avaya Cajun LAN switch supporting 24 PoE ports consumes 375 watts for the switch and an additional 150 watts for 24 PoE ports. This consumption of power will affect the air conditioning and backup power for VoIP. Are the closets powered by 110VAC? This is not enough power for larger PoE LAN switches. The closet must be upgraded to 220VAC with new receptacles, and the available amperage must be increased to support the larger PoE switches.

PoE should be thought of as a power utility rather than an IP phone powering system. The closet power designer must take a long view of PoE. The LAN switch is evolving into a significant provider of services. The LAN switch will be delivering QoS and security services that are also part of the IEEE 802 standards family. There are specific wireless LAN switches on the market that power wireless access points (APs) and deal with the problem of roaming wireless users. The WLAN

switch keeps the session or call up as the user moves from AP to AP.

There is more to PoE than just VoIP. Think beyond the IP phones and APs. (See Figure 1.) If the closet design does not anticipate the other devices that will eventually connect to the PoE switch, then another round of closet modifications, air conditioning extension, and AC power upgrades will be required. The future of PoE devices will include video cameras, surveillance devices, Bluetooth devices, security sensors and access devices, lighting controls, and environmental controls.

Safety Issues: 911, E911, Lifeline

Ensuring that a victim can be located quickly and accurately by EMS personnel in an emergency will depend on the functioning of the 911 and E911 services. Supporting 911 will require outside legacy circuits to the public safety access point (PSAP). These circuits will be terminated in the MDF

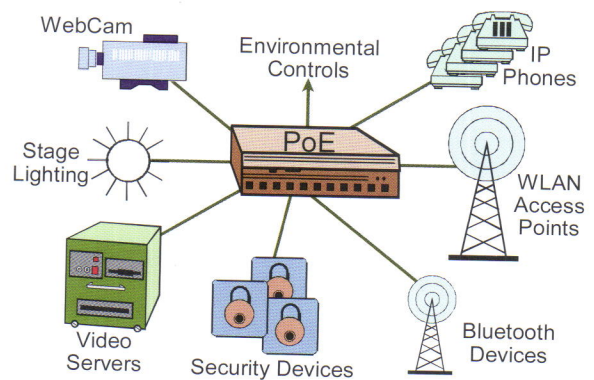
and then must be connected to the VoIP equipment that issues the 911 call.

This will not be a problem when the VoIP equipment and IP phones are all in the same location. When there are teleworkers and telestudents using IP phones on a WAN connection, which PSAP should be contacted? Even if the VoIP system can identify the caller's location, the VoIP system will probably not have a connection to the person's local PSAP. This is a problem yet to be solved. The solution will go beyond the closets on the VoIP site.

E911 produces an even greater problem. The ability of users to

physically move their phones without requiring a cable change to another LAN connection is attractive. This move, however, will require instant updating of the location information with the PSAP. PSAPs are not ready for this rapid change, nor are they ready for a direct VoIP connection. This problem will only worsen when a campus deploys voice over a WLAN

Figure 1. A power utility



The quality you need The service you demand



There is no time like the present for saving on your telecom equipment needs. Trust the professionals at 1 Nation Technology to deliver the highest quality products at a competitive price.

1 Nation guarantees quality and provides you with the most outstanding customer service in the business.

When you can't afford to wait for the products you want and the service you demand, turn to 1 Nation Technology.

Call us today for a complete stock list.

NORTEL AVAYA POLYCOM
PLANTRONICS AASTRA
GN NETCOM
REPAIR AND REFURBISHING
BUY BACKS ADVANCED REPLACEMENT
SAME DAY SHIPPING
5 YEAR WARRANTY
TECHNICAL SUPPORT

1
nation
technology

They make the products... we make the difference!
800-998-9862 www.1nationtech.com

Cooling the Closet

The IDF telephone closet has little or no equipment that produces heat. The light bulb, temporary test equipment, and humans were the heat sources. No air conditioning (AC) is required. With the advent of voice gateways and PoE LAN switches, the heat generated has increased to a point where attention must be given to AC. The following formula for determining the heat generated in watts was derived from White Paper # 69, found at www.apcc.com.

Determining Heat Output

1. Sum up the watts consumed by IT equipment _____
 2. Sum up the PoE LAN end-span switch input power x.6 _____
 3. If a mid-span PoE is used, sum up input power x .4 _____
 4. Sum up the full lighting in watts _____
 5. Multiply the UPS power rating by .09 _____
- ADD WATTS ALL TOGETHER TOTAL _____

The next question is what does the total of the watts mean. The answer depends on the result of the calculation. The table below provides guidance for the closet designer.

TOTAL WATTS	RECOMMENDATION
100 to 500 watts	Place grill vents at the top and bottom of the closet door that connects to an area that already has air conditioning (HVAC).
500 to 1000 watts	Place a ventilation fan above the closet door and install a grill at the bottom of the door that connects to an area that already has air conditioning.
1000+ watts	Install the equipment in an enclosed rack with a hot-air exhaust scavenging system so that the hot air does not recirculate. An air intake grill from a HVAC area will also be required.
1000+ watts	If the HVAC is <u>not</u> accessible, then a separate HVAC system should be installed adjacent to the equipment.

where there is constant location change during the call. Before these 911 and E911 problems are solved, a working solution is to have some legacy phones that do not pass through the VoIP system placed in strategic locations and connected to the carrier central office (C.O.). This will require that more of the internal legacy cable be retained, and the MDF will have to remain in use as well.

Lifeline is a different issue. Most telephone users expect the telephone to work during a power outage. That is because the PBX and C.O. have battery backup and possibly diesel power generators. A lifeline connection is a selected group of phones connected directly to the C.O. that will work when there is a total failure of the PBX and/or power. Unless all the associated VoIP equipment and LAN devices have backup power, phone service will cease to operate during a power failure.

Lifeline connections to the C.O. will still be required because the VoIP system—for example the call server—can fail.

Backup Power

Electrical power has actually become less reliable and has produced very long outages in the past few years. When the power industry published statistics on their reliability several years ago, an IT department would have about 15 interruptions a year. This would cause a reboot of the IT devices if no uninterruptible power system (UPS) were connected. Ninety percent of the outages lasted less than 5 minutes; 99 percent lasted less than 60 minutes. The overall reliability was 99.98 percent. (See American Power Conversion Technote # 26 at www.apcc.com.)

If the telephone service was restored at the same instant that power was

resumed, there might not be any complaints. However, this does not happen with VoIP systems unless UPS is installed. The budget for UPS grows as the number of supported devices increases. The VoIP server outage continues while it reboots its software after a power failure for 2 to 20 minutes depending on the configuration and vendor design. No phone calls can be made during the software reboot. Therefore all call servers must have UPS support to avoid this reboot period.

This does not include the voice gateways, IP phones, softphones, and LAN switches. When these are down, no calls can be completed. There is no dial tone. When power is restored, the IP phones, softphones, and voice gateways have to re-register to their server before a call can be completed. This re-registration time can vary greatly. The registration rate is vendor dependent and can vary from 20 to 60 IP phones and gateways per minute. The larger the network, the longer it takes to restore service to all users. At the moment there is no way to preselect which devices can register first. If the calls off campus pass through the routers, not through the C.O., then they must be included in the power backup plans.

There are three types of UPS on the market. The least costly unit just provides backup power and is called *Standby* or *Off-Line* UPS. This unit has no power regulation. Power regulation compensates for power fluctuations that are not outages but are variations in the voltage delivered by the power utility. Power fluctuations can damage the IT equipment. The next type, called *Line Interactive*, provides backup power and limited power regulation. The best unit, the *On-Line* type, provides full power regulation and backup power.

The next decision to make concerns the length of time the UPS will operate during a power outage. (See Figure 2.) As noted earlier, 90 percent of the outages are less than 5 minutes. A

minimum UPS power backup of 8 minutes would avoid most software reboots and would prevent device re-registration. If the backup requirement extends to an hour or more, the air conditioning, heating, lighting, and other power consumers must be operational. This leads to the decision to install a diesel generator. The small graph on Figure 2 shows that as the run time increases, the power available from the UPS decreases.

Air Conditioning

The typical IDF has no air conditioning. The MDF may have air conditioning for the PBX and associated equipment, but it will probably be inadequate for the new VoIP servers, gateways, and PoE LAN switches. Planning the air conditioning facilities depends on the closet equipment installation. This will then determine the heat output and whether the present cooling capacity is adequate. Guidelines for planning are provided on page 16, "Cooling the Closet"

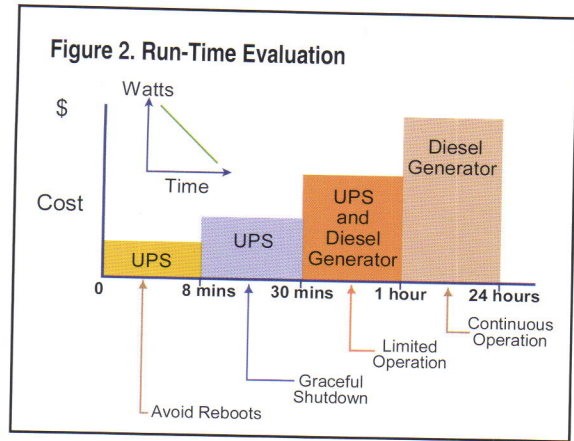
Closet Thinking

The investment in VoIP will expand to include a number of physical plant considerations: closet size and number of closets, power, UPS, air conditioning, cabling, and conduit space. It will probably be impossible to eliminate the IDF and MDF closets. Some of the legacy cabling will still be used, and the connections to the carriers will continue to exist in the MDF.

Once the design for the physical plant is finished, the questions you should ask yourself are:

1. How did you satisfactorily demonstrate that the physical installation works properly and to specification?
2. How long did this verification take, and was it worth it?
3. Could this effort be reduced in the future?

4. Were there incorrect assumptions made when planning the closet changes?
5. Did the vendor(s) forecast the physical changes necessary for their products?
6. Should a single closet be set up first to work out the problems? This would be very useful if there are going to be many closet changes in multiple building locations.
7. Is the closet design really future proofed? For how long?
8. Will changes in converged technologies antique the new design? As equipment becomes smaller, will the power consumed and heat generated per square foot of closet space increase considerably?



The institution has to build a better road (physical plant) before new types of vehicles (converged devices) can travel faster and safer on it.

Gary Audin is president of Delphi, Inc., a consulting and training firm based in Arlington, Virginia. He has spoken at numerous ACUTA events, contributed often to ACUTA publications, and delivered 2,000+ technology seminars. Reach Gary at delphi-inc@att.net or at 703/908-0965.



Save money and reduce FTEs!

Speech Recognition and "Live Operator" Call Center Solutions

The 1Call Just Say It and Infinity systems:

- ✧ Automate call processing
- ✧ Give operators instant access to important information
- ✧ Help you react quickly to emergencies, disasters, outages, and events when used in conjunction with 1Call's R.E.D. Alert module
- ✧ Integrate with your existing IS/IT infrastructure

Your perfect solution for handling:

Inbound/Outbound Fund Raising ✧ Directory Assistance and Switchboard ✧ Alarm Monitoring ✧ Enterprise-Wide Browser-Based Directories ✧ Dispatch ✧ Conferencing

1CALL

A Division of **amtelco**

(800)356-9148 • (608)838-4194

www.1call.com/acuta1

info@1call.com

4800 Curtin Drive • McFarland, WI 53558



Securing Your Wireless Network

by Ron Walczak
Walczak Technology Consultants

Is “wireless security” an oxymoron? At ACUTA’s annual conference in 2000, I gave a presentation on 802.11 wireless technologies and sternly warned that the products opened significant vulnerabilities that had to be addressed before we would be comfortable recommending deployment. I also wanted to know how all you folks planned to get the CFO and trustees to come up with the money to install radios with 5 Mbps shared throughput after convincing them to spend millions to install the latest wiring and 100 Mbps switches! Since that time, your creativity has been very effective, and I have witnessed a variety of approaches to rolling out wireless across campuses that include:

1. Implement it, check for signal (not actual throughput), cross your fingers, and spend the next weeks fighting viruses and attacks.
2. Install access points (APs) outside the campus firewall, protecting the LAN (but not the wireless end user) from intrusion, viruses, and trojans.
3. Install APs inside the firewall, activate Wired Equivalent Privacy (WEP), and cross your fingers.
4. Install access points inside the firewall, activate WEP and Media Access Control (MAC) filtering, and sleep without recurring nightmares every evening.
5. Install APs, security switches, password authentications, and MAC filtering, and sleep soundly after an exhausting day of main-

taining all the MAC tables and authentication schemes.

Security is *the* hot topic these days. Wireless technologies are under the microscope (rightfully so) because many of us have been voicing our concerns about vulnerabilities. Of course, active and accessible network connections all over campus pose as much risk to the network as your wireless system, but this article will focus on wireless only.

Who’s Threatening Your Network?

Security may be compromised by internal as well as external sources. Where do these threats come from? Following are some examples you may—or may not—have thought of.

- Rogue APs. Anyone can go to an office supply store and purchase an AP for as little as \$50. It’s not unreasonable to think that employees and students will spend the money for the added convenience of mobility or the impatience of waiting for the IT department to wire a new data outlet. After all, think about how many privately purchased telephone sets are on your PBX because the employee wants one-button speed dial.

Most rogues are installed “innocently,” but not all. If your network has MAC filtering, an innocently installed rogue won’t operate—but don’t forget that MAC addresses on APs can be changed to match a registered PC. And that suggests a

more questionable set of circumstances and motives.

Another internal problem results when end users set their clients to operate in an "ad-hoc" network—a network between local machines without accessing an AP. Again, done for convenience, this opens the network to all manner of intrusion and virus problems.

- Troublesome neighbors. Not all campuses have the luxury of being on a secluded parcel of land. Many have corporate neighbors who are installing wireless units that can interfere with the network, or that are close enough that their client cards are accessing your network by "mistake."
 - Malicious association. A hacker sets a client to be an AP answering the beacons from unsuspecting end users. The malicious AP authenticates the victim and gives the hacker access to the victim's PC. This permits the use of various hacker software for stealing MAC addresses, passwords, and so on.
 - Ad-hoc hacking. Your mobile users expose themselves to hacking when they associate to *hot spots* in airports, hotels, and other public network locations. You have to protect your network even when the wireless user isn't on your network.
- Think about it: If your mobile users gain access to public networks, they are no longer protected by your firewalls, e-mail virus software, or any other network-based security applications. When your mobile user goes off campus, hackers can gain access to his hard drive to steal passwords and data or to deposit malicious code.
- MAC spoofing. Some of our clients use MAC address filtering as a security measure. I think MAC filtering is as effective as WEP but with a whole lot more work. Software to "spoof" valid MAC addresses is available on the Internet, so don't assume that all is well.
-

Vo IP

Ivize™ is the Formula for Voice Network Management

Managing university voice networks is growing ever more challenging with changing numbers of voice mailboxes, PBX extensions, configuration information, and Grade of Service objectives. If that's what you face, the Ivize performance management suite is the answer.

Ivize manages messaging systems, and IP and TDM PBXs, at many of the country's most prestigious universities. It's the obvious choice for maintaining accurate records of PBX and voice mail resources as voice networking use changes over the school year. With these records, you'll gain greater control over your voice infrastructure and reduce management costs.

Many schools choose Ivize as a replacement for Octel's Decision Pro. Others buy Ivize for its unique unified view of telephony services such as IP and TDM PBXs as well as voice and unified messaging, running on platforms like Avaya Definity and 8700 PBXs, Nortel Meridian PBXs, and all Avaya voice messaging servers. You can choose the Ivize module or modules that meet your network's unique needs.

Visit our Web site or call us for more information.

Vitel
Software
inc.

67 Millbrook St. • Worcester, MA 01606
508-831-9700 • www.vitelsoftware.com

- Man-in-the-middle attacks. This attack can beat your virtual private network (VPN) security. Admittedly, this is more work for the hacker, but here is how it works:

1. The hacker observes the network to identify APs, SSIDs, authentication information, usernames, and so on.
2. The hacker then associates with the legitimate AP, asking for authentication. The AP sends the VPN challenge (which the hacker observes), and the legitimate user (victim) responds (which the hacker observes).
3. The hacker then acts like an AP and challenges the victim. The victim responds (picked up by the legitimate AP) and sends back an embedded sequence number. Now the hacker has everything necessary to violate the VPN.
4. The hacker then bumps the victim off the legitimate AP and keeps it from reassociating, allowing the hacker to access the network via the "secure" VPN.

Complicated? Not for a typical college-aged geek!

- Denial-of-service attacks. So easy to accomplish and so hard to defend against! Want to cripple an 802.11(b) or (g) network? Turn on a Panasonic 2.4 GHz cordless phone, one of several known troublemakers. The handset and base are in constant beacon communication, which floods the frequency and knocks you right off the network.
- Spanning tree infinite loops. In a more sophisticated scenario, a hacker abuses the spanning tree algorithm to trick the network devices into thinking

there are additional network paths (loops). The network devices keep attempting to communicate with these nonexistent paths, tying up the network and potentially freezing the switches and routers to the point that a power cycle reboot is the only fix.

Industry Response

The Institute of Electrical and Electronics Engineers (IEEE) is working on finalizing standards-based improvements to wireless security:

- IEEE 802.1x. This standard offers a means of authenticating and authorizing devices to attach to a LAN port. It defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network.
- IEEE 802.11i. This standard is intended to improve WLAN security. It describes the encrypted transmission of data between systems of 802.11a and 802.11b/g WLANs. It defines new encryption key protocols including the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). AES will require new hardware.
- IEEE 802.11e provides Quality of Service (QoS) support for LAN applications, which will be critical for delay-sensitive applications such as voice over wireless IP (VoWIP). the standard will provide classes of service with managed levels of QoS for data, voice, and video applications. This doesn't have much to do with security, but it is an important standard that you should be aware of as you consider the implications of VoIP and wireless.

Your Response

What can you do yourself?

- Combat laziness. For what the trade press would call "improperly configured access points," at a minimum, make sure every AP gets touched by an IT person who does the following:

1. Changes the management password.
2. Changes the name (SSID) and turns off the Broadcast SSID feature.
3. Enables MAC address codes.
4. Turns on the security features (WEP at a minimum).
5. Turns down the power and installs the right antennas to prevent the signal from going beyond your desired coverage area.

Don't forget that many low-end APs reset to default settings if they lose power!

- Beware of espionage. Are you a research facility? Do you work on government projects? Are you an incubator for new businesses or have some sort of partnership with local industry that makes you responsible for the security of important data? If so, you probably already have some sense of the risks of espionage. Don't make it easy for someone to steal your (or someone else's) secrets. Ask your security department to be on the lookout for cars/vans parked in your lots that have antennas on the roof.
- Learn about *war driving*. I have war driven and *war walked* every campus I have visited in the past 2 years, and I have never been questioned. Visit www.wigle.net to see just how much information is known about unsecured wireless networks and don't be surprised if you see *your* network listed.

In addition, the following recommendations will make your network as secure as practical.

1. Site surveys. Go find out what's *on the air* before, during, and after your deployment. Yes, it's lots of walking, but we all need the exercise.
2. Customize every AP, turning on security, changing passwords, and setting power levels to cover the area that needs coverage. Use the right antennas to further define the coverage patterns.
3. Use a layered approach to security:
 - Deploy internal AP security (WEP/EAP/LEAP).
 - Establish external authentication (RADIUS).
 - Invest in third-party security solutions (AirDefense, Blue Socket, Vernier, etc.), which can identify attacks and shut down access, identify duplicate MAC addresses in use, permit you to deploy radio sensors that will detect and report rogue AP activity, and identify man-in-the-middle attacks and shut down the attacker.
 - Implement strong application-level security.
 - Use end-to-end encryption to protect the confidentiality of the data (but, remember, it does not protect the network).
4. Develop and enforce written security policies. Those policies should be issued by a vice president or the president to have the necessary authority.

5. Educate your people about security and their role in maintaining it (no rogues, please).

Your mobile users should have software firewalls, virus protection, and a wireless card that is set to *infrastructure mode* to at least prevent the PC from networking directly to other wireless devices (ad-hoc mode); otherwise, they may contract a nasty bug that will contaminate your campus network.

6. Inventory control of wireless client cards—especially those in your MAC filter.

7. Set all client cards to infrastructure mode.

8. Educate your security force about the methods of wireless hackers—and what to look for when they are out patrolling.

9. Pray.

By the way, if you are truly concerned about security, you should go turn off those active-unsecured wired network connections all over campus!

Ron Walczak is the principal consultant with Walczak Technology Consultants, Inc., in Prospect, Pennsylvania. Visit his website at www.walczakconsultants.com.



MySoft.net

e-telemanagement

Compco = Results

MTSU – Ms. Ronda Vaughter: "MTSU is now able to provide online services and consolidate billings using MySoft.net. Not only has our efficiency improved, but we have also reduced billing errors, which in turn provides our customers with the best possible service using the latest technology."



U. Louisville – Ms. Karin Tyler: "From our search we determined that Compco suited our needs best due to their years of experience ... the support and assistance we have received during implementation assures us of a lasting partnership between UofL and Compco for our Telemanagement solution."



U. Maine – Mr. Les Shaw: "We have been very satisfied with Compco's host/server product that has served us for 10 years, so we went back to them to find out what was new. The new MySoft.net provides great functionality and will fill our needs well into the future."



Iowa State U. – Ms. Angela Bradley: "We evaluated the major telemanagement vendors and found that Compco's MySoft.net software is, by far, the best for tracking voice and data networks."

Compco
Vision.....Solutions.....Relationships

Compco, Inc.
615-373-3636
www.compco.com

MySoft.net, the only 100% web-based e-business software for managing voice/data services, charge backs, and vendor invoices.

Legal Alternatives to Rich Media Sharing

by Curt Harler

ACUTA members see rich media in different ways: They may view Napster-like services as a great way to circumvent greedy music companies. They may regard them as an illegal attempt to steal tunes from starving artists. Most probably view them as simply another pain that they wish their college's legal department could have handled without involving them.

On the other hand, everyone agrees that the Internet is a great way to distribute content—both coursework and entertainment. And it's a wonderful way to distribute videos, ranging from teaching tools to the latest Brad Pitt flick. But probably the biggest practical objection to students downloading music and video is the stress it puts on already overburdened servers.

Some schools—including Carnegie-Mellon, Case Western Reserve, University of Indiana, Kansas State, University of Montana, University of Nevada, Ohio State, Rochester Institute of Technology, University of Southern California, Wake Forest, Washington State, Washington University of St. Louis, and Yale University—have struggled with the question, not feeling comfortable simply leaving students to their own devices and monitoring usage. Two alternative approaches have emerged: a university consortium called CampusEAI Consortium (www.campuseai.org), based on Internet2; and a commercial effort offered by Cflix (www.cflix.com) and Ctrax (www.ctraxmusic.com), both part of the same Englewood, Colorado, firm.

It is no coincidence that the 25 CampusEAI colleges involved are all major television schools. All are looking at IP-broadcast (cable TV), movies and music on demand, educational assets, and the Open Student IP TV Network. OSTN encourages the exchange of ideas and digital video content contributed by college TV stations. It serves as an outlet for students to post their work and share feedback regarding their IP video content.

University Initiative

Prashant Chopra, Case Western Reserve University (CWRU), Cleveland, Ohio, co-chairs the CampusEAI Consortium with Jerry Gordon, Washington State University. It is no small project, and he is aware that there are parallel commercial interests.

"We are huge. We have hundreds of IT folks working on this, all committed to this project," says Chopra.

Chopra is the lead research and rapid application development architectural expert for business process reengineering, and he steers CWRU's Information Technology Services next generation of development on cutting-edge technologies.

"This includes sharing of assets between universities, digitization of curriculum assets (lessons and lectures), and entertainment," Chopra says.

In addition, the consortium presents a unified voice to content providers—a voice backed by about 3.5 million students. With Internet2 and 10-Gig services

linking the campuses, they also have a fearsome network for moving content around.

Pointing to the Internet2 links, Chopra says, "This is one way to demonstrate the value of Internet2. We have a group of universities facilitated by a [stable] backbone that is not going anywhere."

CampusEAI Consortium expects to provide broadcast services that deliver premium, compelling entertainment and academic content to students' PCs via the campus LAN. It plans to offer high-quality, easily accessible media over PCs and delivered through Internet2, effectively a closed-circuit, high-speed network bypassing the public Internet.

The consortium is driven by CIOs and provosts who see this sort of project as one form of validation of the huge investments being made in broadband.

CampusEAI notes that, with licensed movies, music, and TV shows available, campus networks are no longer conduits for piracy. This helps to avoid legal issues from illegal peer-to-peer networks.

Commercial Solution

Some colleges want to give teachers and students access to video without involving the school's IT department. Others feel that a college has no place messing around with commercial products like top-40 tunes and R-rated movies.

Those campuses might turn to Cflix, a 3-year-old company that provides digital media services, including current commercial movies, shorts, and sports clips, as well as educational media ranging from foreign language to historical clips. Ctrax, started in April 2004, provides access to 700,000 tracks from the five major music companies and about 70 independent labels. Students buy the material either by subscription or on a per-download basis.

"Cflix came to us a couple of years ago and offered to do a pilot at no

BORN TO PROVIDE TELECOM.

With service, quality, and pricing this hot, A1 makes your job a day at the
BEACH!



A1 sales representatives
Jaime Bouvet,
Maureen McAuliffe,
Joe Katz &
Rachel Page

A1

A Name You Can Trust™
since 1991.

TELETRONICS® Inc.

An Independent Distributor

✓ Inventory

Up to \$5 million in stock:
new/unused/refurbished
Nortel®, Avaya®, Mitel®,
Plantronics, Polycom®,
MCK & EDCO including:
Norstar®, Meridian®,
BCM® & VOIP solutions.
Along with Mitel's® new
SX200ICP
(Mitel® SX200ICP Florida
end users only)

✓ Quality Control

ISO 9001:2000 #006674

✓ Repair Services

Nortel® & Avaya®: First
repair free (\$100 value)

✓ Value Added Services

Excess inventory
solutions
Buy-back program
Consignment and trade-in
programs
Advanced replacement
Two-year warranty
Local installation in the
greater Tampa Bay area
Leasing options
Volume rebate programs

✓ Free technical support

✓ Cafe Telecom

Value added member
services available at
www.alteletronics.com

A1 Teletronics is proud to announce Independent Knowledge™: fast-paced, real world Norstar® product training FOR technicians taught BY a technician. Visit Florida to participate in this dynamic 3-day training class. For pricing and class availability please contact Melissa Roberts at 1-800-736-4397 ext. 190 or mroberts@alteletronics.com.

Independent Knowledge™

90012000
CERTIFIED
Quality System
006674

celebrating over a decade of service
1991 2001

1-800-736-4397
www.alteletronics.com

Nortel®, Norstar®, Meridian® and BCM® are registered trademarks of Nortel Networks, Ltd. Avaya® is a registered trademark of Avaya, Inc. Polycom® is a registered trademark of Polycom, Inc. Independent Knowledge™ is not sponsored or endorsed by, or affiliated with, Nortel Networks Ltd.

charge to see how their services would be accepted by students and to work out issues with their services," recalls Todd Edwards, director of media services at Wake Forest. At that time their only focus was offering movies to college students.

In January 2004, Yale University began a partnership with the Ctrax service. According to Chuck Powell, director of academic media and technology at Yale, the vendor approached the school in the spring of 2003. "We were already interested in trying to become more efficient in delivering multimedia to the classroom and the conversations took off from there," he says. They started with 25 courses engaged early on. By spring semester, the number was up to 30.

"Initial testing in the fall semester indicated that Cflix can be a real aid to instruction, allowing students a tremendous amount of flexibility in how, where, and when they interact with materials that are essential to their courses," Powell says.

"It also relieves faculty members of some of the more burdensome aspects of arranging for the materials to be viewed," he adds.

How the System Works

Cflix can provide access to video clips used as teaching tools, music, and entire Hollywood movies. It provides academic content to students in a campus (or closed circuit) environment. Company President Brett Goldberg says their primary mission is simple: to offer college students compelling content that they enjoy and frequently access.

Cflix provides the equipment and content for the school to deploy—

without requiring additional capital or operating budget approval from the Provost's office.

In a time when telecom departments are searching for a replacement for lost long-distance revenue, a video service could become a revenue-generating source. In any case, Cflix promises to provide the university with a state-of-the-art media delivery platform for its students.

"Our network has not had a problem," Edwards says, "but we have not had a large demand for these services yet."

Since the vendor provides the server, there was no problem there. There were some client issues with the OS (which is Microsoft) and Media Players.

"So far we haven't seen any major problems," Powell agrees. "Since Cflix/Ctrax has positioned hardware on campus there is no additional burden at the key juncture [the pipelines to the Internet] and the on-campus traffic is quite manageable."

Setup went well at Yale. "From our perspective it was pretty painless," Powell says. "They did all the setup and configuration. We provided technical information on our network topology and local authentication infrastructure, and they did the integration."

While there were small operational challenges throughout the process, Powell is pleased. "All in all it has been a very solid experience with very few support calls from end users."

"Cflix took care of most of the other technical issues," Wake Forest's Edwards says. "We also had some training issues linking Cflix with Blackboard."

"Since our founding, peer-to-peer networking has emerged as an alternative, albeit illegal, delivery platform for entertainment. Companies like KaZaA have provided methods for sharing content that ignores the content owner rights and supports a platform for piracy, perhaps unknowingly," Cflix President Goldberg says.

Since Cflix is not a peer-to-peer or file-swapping network, its delivery platform serves as a viable legal alternative to these topologies. "It is absolutely our responsibility," Goldberg says of copyright and royalty issues. They work with Music Net, a clearing-house, to handle such issues.

Architecture

The network uses a distributed architecture. Each campus operates primarily as a stand-alone. A Web portal server, Content Distribution Manager (CDM), and Content Engine are located at each campus. Management, monitoring, business support, and digital rights management (DRM) authorization are centralized. Multiple local content engines may be deployed to support the desired concurrent viewer capacity or to support network topology requirements on a campus.

The CDM uses this distributed architecture to route its high bandwidth content between individual campus content engines and the students accessing that content. This allows the system to leverage the existing bandwidth on a college's LAN to deliver high-quality media to desktops anywhere on the school's network.

One major problem with Cflix's system is that it is Microsoft based.

"Microsoft is a major problem," Chopra says. "Coming into the

university space with a Microsoft-only platform is a big no-no."

All media are digitally encrypted. The DRM is Windows media, which is not Macintosh compatible. They also do not support Linux or Solaris. Goldberg admits that this is an issue but notes a number of firms are working toward a solution.

Powell is aware of the problem. "The biggest (but known) issue was the lack of support for Macs, but we think that will be solved by fall," he says.

The campus consortium, on the other hand, is platform agnostic—not married to Microsoft.

Fee Structure

The typical student will pay \$3.99 for

24 hours of access to a current movie. Music runs about 90 cents per download. There is also a "permanent" download available that allows the track to be exported to an MP-3 player or a CD.

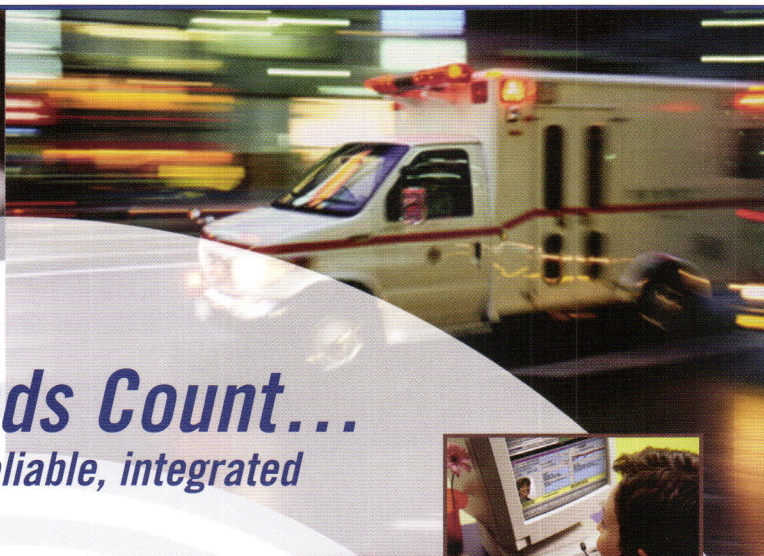
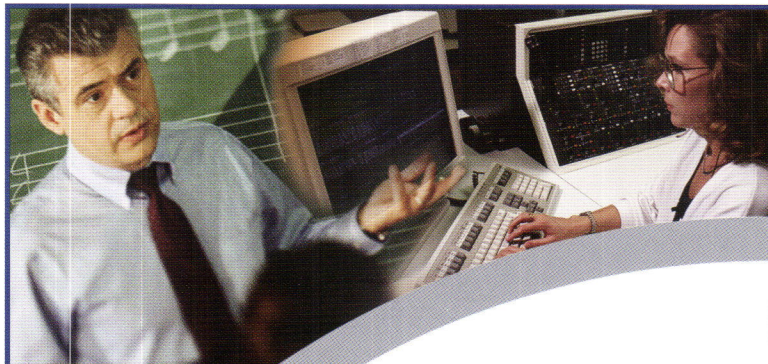
For music, a 10-song package sells for \$8, while 15- and 20-song options will be available for \$12 and \$15. The company is looking into a 2-month subscription plan available for \$4.

The cost to the network manager or IT staff comes up front. "We look to the IT people to help with the initial setup and deployment," Goldberg says. "After that, the load is less. We manage the system from our remote location."

"Yale (and my unit in particular) pays for the educational services and

therefore there is no charge to faculty or students," Powell explains. Both the Cflix and Ctrax entertainment services are voluntary and "opt-in" for Yale students, staff, and faculty, so they pay directly. "We do facilitate collecting the money through a secure local application, but that's mainly to keep standard e-business transaction costs to a minimum," Powell says.

Reception from faculty and students has been good. "Although we're still collecting data from faculty and students, it's safe to say that feedback on the educational services has been very positive. It's simply too early for a summary on the entertainment side, but early testing shows great potential.

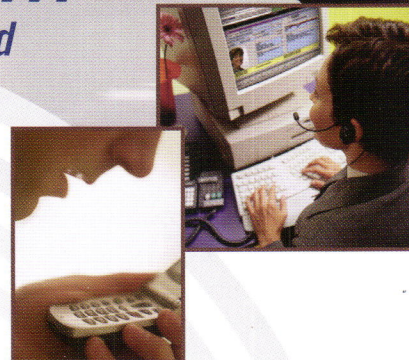


When Seconds Count... ***Only an automated, reliable, integrated solution will do.***

Amcom Emergency Notification and Response

- Group notification
- Response processing
- Escalation
- Alarms monitoring with group notification

*Scalable • Standards-based • Highly configurable
Supporting a multitude of protocols, devices and rules*



Amcom Software, Inc.
1-800-852-8935
www.amcomsoft.com

In the fall semester we should be able to get a much better assessment of usage and preferences," Powell says.

The music service, Ctrax, seems to be more appealing at Yale, but Powell says it is too early to draw a firm conclusion.

To date, Edwards says Wake Forest students have watched only 100-200 videos during a semester. At Wake Forest, Cflix hired two students as interns who handle most of the marketing, which has included flyers, advertisements in the student paper, and more.

Yale has proceeded more cautiously, working to known needs on the educational side. "In some sense to date, the way we have engaged faculty is simply by contacting the ones we know make heavy use of media and seeing whether they would like to try Cflix," Powell says.

The main, ongoing relationship between school and vendor is having the college act as a collection agent. "We bill the student's account, and we pay Cflix once a month for usage," Edwards says. Cflix identifies the transactions and reconciles accounts on a monthly basis, similar to a cable TV or phone service.

Academic material is paid for by the college according to the types of material, amount of space required on the server, and similar factors. Surprisingly in this day of scrambling for revenues, Goldberg finds that not all colleges want a percentage of the fees generated. "Some are more focused on quality of life and providing services," he says, "but others want to reap a cost savings."

Edwards says they started with about 20 faculty posting videos for class via Cflix. "The next semester only a couple wanted to continue," he says, explaining that "they have support people who can digitize and post the videos for them. Originally we wanted Cflix to take care of all of the copyright issues for us but that didn't work out."

Despite the slow uptake for Cflix, Wake Forest will test Ctrax this fall, Edwards says.

Other Savings

While dollars are important, the biggest area of savings that network administrators might realize is a lightening of the burden on the WAN-LAN interface.

"Our delivery platform originates at the LAN level," Goldberg says. "The most complicated part—the media content delivery—is within the school's walls."

Typically they set up a distributed architecture. One terabyte server might be at the network administration building. Another might be located elsewhere on campus. Since the movies or educational media reside on campus, there is no clogging at the margins.

"The only time we use [the WAN] is for off-hours downloads of media," Goldberg says. All video is on-campus before its availability is announced to anyone.

Music works differently. Rather than store 700,000 3 MB files, the music is downloaded to the campus server upon request. If one student requests a piece, it is delivered to the server and then stays on the server. The next student who wants the same piece

will get it from the campus server. This makes sense, since a Southern school might have heavy demand for country tunes while a school like Oberlin or Julliard would have heavier demand for classics.

Cflix provides a secure content delivery service that avoids the congestion of the Internet by providing local on-campus delivery of entertainment to student subscribers.

The Cflix solution for media delivery, developed with some of the world's leading technology companies, offers some of the highest quality digital media content available today. This media includes first-run feature films, TV programs, popular feature-length movies, sports content, and curriculum-based video content. A typical download will take 7-10 minutes on the college LAN. The student can watch the film as many times as they would like and at any time in the 24-hour period.

"We have been deploying the service in several select pilot environments over the past couple of years," Goldberg says. "We plan a general launch of our new digital music service this fall."

The Ctrax announcement actually was made in April, and activity got underway during the first half of 2004.

In addition to providing a content delivery platform, Cflix is contracting with major studios and media owners to aggregate entertainment that is of primary interest to the college student. While there is a significant amount of entertainment available to students today, very little of it is available on-demand or at hours that are suited to the student schedule. Cflix solves this

dilemma by offering entertainment when the student is interested, on-demand, or on a scheduled frequency level that minimizes pre-show wait times to less than 10 minutes.

The Longer Term

"It's a little too soon to tell if Cflix will pan out," Edwards says. "They have potential, especially at universities that do a great deal of video capture and want to outsource some or all of this work.

"Universities that have these services centralized would be most

successful with outsourcing to Cflix," he adds.

Powell agrees: "If a school is interested in finding a vendor or partner to help with delivering educational content and/or opt-in entertainment services, I'd recommend they at least consider Cflix/Ctrax as an option," he says.

On the other hand, colleges in the CampusEAI Consortium see a co-op, using their own resources, as the way to go. Much will depend on the resources at the individual college. Small schools

with few staffing resources may opt to outsource. Larger colleges, or those with Internet2 leadership and a technical bent, will probably opt for the Consortium.

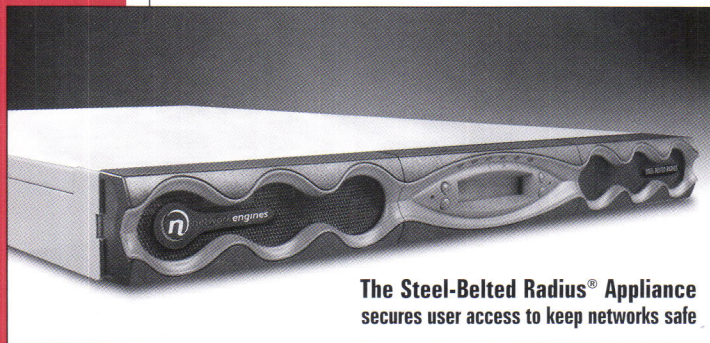
In either case, a college looking to deliver rich media with both course content and entertainment would be well advised to investigate both groups.

Curt Harler is a contributing editor to the ACUTA Journal and a freelance writer who writes and speaks on technology topics. Contact Curt at curtharler@adelphia.net.



WHO'S GETTING ON YOUR NETWORK?

Information is precious - make sure it stays that way



The Steel-Belted Radius® Appliance
secures user access to keep networks safe

Securing your networks - wired and wireless - just got easier. The Steel-Belted Radius® Appliance is a secure authentication solution that keeps networks safe. The appliance is the ideal authentication solution for local area networks (LAN) and wireless LAN - it is quick to install, requires minimal maintenance, provides support for most two-factor authentication solutions and delivers scalable, cost-effective secure authentication for any environment.

If securing access to your networks is a priority, ask about the Network Engines Steel-Belted Radius Appliance today.

Free download: Application note on Secure WLAN User Authentication Solutions for Higher Education at www.networkengines.com/acuta



networkengines

APPLIANCE SALES HOTLINE: 877-638-9323

Network Engines, Inc., 25 Dan Road, Canton, MA 02021-2817 ■ Tel: 781-332-1000 ■ Fax: 781-770-2000
e-mail: sales@networkengines.com ■ www.networkengines.com/acuta



Douglas E. Van Houweling is President and CEO of the University Corporation for Advanced Internet Development (UCAID), the formal organization supporting Internet2.

Dr. Van Houweling has played a major role in Internet development in the United States. He was chairman of the Board of MERIT, Inc., a Michigan statewide computing network, when the National Science Foundation awarded it responsibility for operation and management of the NSFNET national backbone in partnership with IBM, MCI and the Michigan Strategic Fund in 1987. Van Houweling was also chairman of the Board of Advanced Network and Services Corporation, a not-for-profit organization that implemented and operated the world's largest Internet backbone network from 1991 until 1995.

Dr. Van Houweling holds a faculty position at the University of Michigan as Professor in the School of Information. He received his undergraduate degree from Iowa State University and his Ph.D. in Government from Indiana University.

Walt Magnussen, Ph.D., chair of ACUTA's Publications Committee, is director of telecommunications at Texas A & M University at College Station. He is also co-chair of the VoIP working group for Internet2 and director of Texas A & M Internet2 Technology Evaluation Center.

Interview

Doug Van Houweling President/CEO, UCAID

Magnussen: Let us start out by saying how excited ACUTA is about the establishment of the relationship between ACUTA and Internet2. It seems that the Internet2 organization is stronger in the areas of application development and deployment while ACUTA's strength lies in the areas of understanding of legislation/regulation and business models. Can you share with us your vision of specific areas where these complimentary strengths can be joined to support our members?

Van Houweling: I'm delighted that we have established a relationship between Internet2 and ACUTA because I think that there are a lot of areas in which the two organizations complement one another.

I have always thought of ACUTA as the organization that gives people who have professional responsibility for telecommunications infrastructure in the higher education community an opportunity to share and gain expertise. And I've always been pleased with the extent to which ACUTA has taken as part of its mission not just trying to understand how to operate today's telecommunications infrastructure but has always tried to provide its members a window into the future and an understanding of the opportunities and challenges they will face as we move into the future. It's in this area, of course, that I think the relationship between ACUTA and Internet2 has the greatest potential because Internet2 is very much oriented toward the future of the Internet and the requirements that we

all understand will need to be met if the higher education community is to take best advantage of that future.

In particular, as our work at Internet2 has gone forward, we have discovered increasingly that the communications infrastructure on our member campuses is absolutely crucial. The Internet2 community is able to manage the core of the network to a very high level of quality because it's relatively simple and straightforward. However, when we move to the edge of the network and onto the campus, almost nothing is simple and straightforward. There are many different organizational entities and decision makers involved and a wide variety of equipment deployed. As a result, management of high performance network capabilities on campus is a big challenge as we look forward delivering the value of the high performance Internet.

It seems to me that an alliance between ACUTA and Internet2 to tackle what we call the end-to-end performance problem is perhaps one of the biggest opportunities we have working together in our respective organizational roles.

Magnussen: We have heard a lot about the middleware initiative. What is it and how do you feel that it will shape our future?

Van Houweling: As we think about the future of the Internet, one of the biggest challenges we face is how to deal with ease of use, security, and privacy. I don't know about you, but despite various spam filters and so on, my e-mail

includes a lot of messages that come from no one I know and are of no interest to me. I find it a challenge to keep all of my software updated so that when I browse the Web I'm not exposing myself to invasion of my personal computer by programs I never requested.

As Internet2 thinks about middleware, we think of creating an environment in which it is possible for both individuals and organizations to trust the sources of their connections on the Internet so that, for example, a library can trust that a person who is accessing their collection is authorized to access that collection. Or if someone requests a video conference with me, I can trust that that individual is from a community from which I would ordinarily entertain a video conference. As we move into these new application areas, like video conferencing or VoIP, we have to think in advance about the opportunities for "courtesy calls" and spam video encounters just as we have learned that we need to worry about those things with the standard telephone network and e-mail.

The middleware initiative is devoted to, first of all, creating a cross-institutional technological foundation that reliably authenticates individuals to manage access to particular resources. Secondly, the middleware initiative is about building communities in which that trust can be shared. It's our objective that eventually the higher education community will be a community in which trust relationships allow individuals at one institution to be authenticated in a way that they can be trusted by another institution and the people at that other institution. And thereby we can easily and securely engage in all types of Internet-based interaction with individuals across our community.

Of course, if we can accomplish that, we can also make the network easier to use, because each of our institutions can maintain information about each of us and use that information appropriately when we are engaged in some type of

interaction elsewhere. Personally, I now have somewhere between 50 and 100 user IDs and passwords that allow me to carry out my various activities on the Internet. I have to keep track of all those, and it's a real barrier to use. I would much rather have a trusted entity keep track of those relationships for me and provide the information required for each transaction. The middleware initiative should help resolve those issues.

ACUTA: Likewise, we have heard a lot about Internet2 involvement in the National Lambda Rail initiative. What is it, and how do you think that it will impact the ACUTA membership?

Van Houweling: First of all, I should say that Internet2 is a key member of National Lambda Rail. Internet2 has committed \$10 million to the National Lambda Rail effort. We are working hard with our colleagues in National Lambda Rail, who, by the way, are also Internet2 members, to make sure it succeeds. I think there's a general agreement among all higher education entities that we need to have a continued level of investment in facilities that allow the higher ed community to realize its future and meet its needs. National Lambda Rail, to me, is a remarkable example where a number of organizations have jointly contributed so that the higher ed community will have available to it a nationwide fiber capability that can be used for all manner of applications and research by the community.

In particular, at Internet2 we are looking forward to working with National Lambda Rail to advance Internet technology. We are now nearing the end of the period in which we can depend on routed networks as the sole digital connectivity for higher education and research. In fact, there are applications that require us to provide levels of service and capacity that will be difficult to meet with the traditional Internet structure. As a result, we are working with National Lambda Rail to develop a new hybrid

networking environment which takes advantage of both circuit and packet-switching technology to meet the future needs of the higher ed community.

From the point of view of the ACUTA membership, it is very important to note that it will become increasingly critical that institutions have direct optical connections between their campuses and points of presence on the national infrastructure. A number of universities and regional associations of universities working together—in many cases with the Internet2 Fiberco organization—have purchased or gained rights of use to dedicated fiber facilities from campuses to nearby points of presence. Having those fiber paths available will allow the institutions to participate in the evolution of the network to an environment which uses this hybrid of circuit and packet technology which I believe will be very important to the whole community over the coming decades.

ACUTA: ACUTA supports a program called the Strategic Leadership Forum that is intended to increase the level of awareness and understanding about Information Technology by our institutions CEOs. Are there complementary initiatives in the Internet2 community?

Van Houweling: As you probably know, the Internet2 board consists mainly of the university CEOs who are elected by CEOs of the member universities. That means that the university CEO community pays attention to Internet2 activities, and from time to time we do presentations for the various CEO organizations such as the American Association of Universities (AAU) and the National Association of State Universities and Land-Grant Colleges (NASULGC).

Even so, Internet2 does not have a program similar to your Strategic Leadership Forum, and as a result I would suggest that it may be useful to

ACUTA that Internet2 from time to time participate in your Forum as a means of providing the participating CEOs a view of some of the activities that are going on in Internet2, particularly those activities that are relevant to ACUTA.

ACUTA: Since September 11, our members have been increasing efforts to strengthen security in the areas of both physical and information security. In addition to the middleware initiative we've already discussed, what are the initiatives in the Internet2 community that are related to security?

Van Houweling: We agree that we need to devote increased attention to Internet security. Ken Klingenstein, who is also responsible for middleware at Internet2, has responsibility for our security activity.

As you know, we participate in the EDUCAUSE/Internet2 Computer and Network Security Task Force, and much of our work is done jointly with EDUCAUSE. That work has been primarily focused on helping campuses to understand best practices in security and helping us disseminate information about ways to manage and implement a more secure network environment.

The Task Force also works with other higher education associations, and the CEOs from those associations have made it clear that they view network security as a major priority for the higher ed community.

In addition, we have worked jointly with the federal government so that the federal government views us as part of the solution to their security problem rather than as a security exposure for the U. S. Fortunately those efforts have been quite successful, and I think we have a good working relationship with federal agencies, especially with the Department of Homeland Security. We also have an active Information Sharing and Analysis Center (REN-ISAC) that is operated for Internet2 and the research university community

by Indiana University which also provides Abilene's network operation center. The NOC takes advantage of some of the best security technologies from some of our corporate members. Internet2 is able to observe, monitor, and, when appropriate, take action against various types of denial-of-service attacks and other network security challenges that we can observe from the Internet2 backbone.

Finally, we have an effort to develop and deploy network security solutions compatible with high performance network infrastructure and applications. Many of the existing network security solutions compromise the utility and performance on the Internet, and Internet2 is working to find and deploy more positive solutions.

ACUTA: We heard a lot at our annual conference last month about how this upcoming information-savvy, wireless generation of students will change campus life as we know it. What do you think we will need to do to be able to meet their expectations of campus life?

Van Houweling: I believe that the generation of students that are coming to campus today are an enormous challenge for us as educators. The problem is not, frankly, a technical problem. I think that many of our universities have done an excellent job of providing students with access to good networking capabilities and to information services such as library access. In many cases these students come to campus having become used to a broadband environment, and they would be disappointed to find anything less than that available. And typically on Internet2 campuses they discover that they are actually in an even better position in regard to network connectivity.

The real challenge, though, isn't about technology; it's that these students have grown up in an information environment that is so radically different than the one that all of us

grew up in that they do not learn the same way that we learned. We learned, typically, in a sequential fashion, going from front to back of textbooks, having a field laid out carefully for us in linear fashion by a faculty member in lecture. Young people today have so much information available to them they don't need to learn *just in case* they're going to need to know something but learn *when* they need to know something. They just reach out for the information and they acquire it. As a result, the way that we traditionally pass knowledge along to the next generation at our universities is really not well suited to the way students of today are used to acquiring knowledge. Closing that gap is going to be an enormous challenge.

I believe that we need to get the students more involved in helping to create the learning environment on our campuses. While the faculty should continue to define the learning objectives and the content that needs to be included in a particular discipline, the students should help determine how that knowledge is acquired. They need to be actively involved in the creation of the system in which they learn.

One thing we've seen, for example, is that students who work together in high school, even though they go to different universities, tend to use the Internet to maintain contact when they get to the university. They depend on each other to help them learn new material. So we actually now have many small learning communities that are spread across multiple universities. Students are actively comparing the learning environment at their university with the one that friends are experiencing at another university. If our higher education community is to remain relevant, we need to tackle the learning environment head on.

ACUTA: Finally, what are the one or two leading issues that your member -

continued on page 36



Basics of WLAN Security for Higher Ed

by Glenn Taylor
Symantec

Here's some news that will grab any information security professional's attention: Of 500 firms recently polled by Jupiter Research, fewer than half had implemented security solutions for their wireless networks. That's a troubling discovery, especially given that wireless networking and mobile computing are two of the fastest growing technologies since the emergence of the Internet.

It's true that wireless networks have ushered in sweeping productivity gains at some organizations. With untethered network access, users can connect to the Internet and their networks not only from anywhere on campus, but also from any one of a growing number of hot spots in airports, restaurants, hotels, and coffee shops across the world.

Network administrators also benefit from wireless LAN (WLAN) implementations. By eliminating the need for costly and cumbersome wires and cables, wireless networks are more easily implemented, maintained, and reconfigured than their wired counterparts. What's more, connecting LANs between buildings is no longer a matter of running costly wires; instead, IT can simply use directional wireless relays. The result? Reduced total cost of ownership.

Despite these benefits, wireless networks have also increased organizations' exposure to security risks in ways not always understood. Universities are no exception. By now, the security

shortcomings of wireless networks are not a surprise. Walk-by hacking is no longer new; it doesn't take long for anyone who uses a wireless device to figure out how easy it is to connect to other networks and systems in an environment that relies on invisible and unrestrained radio waves. And, in a growing number of major cities across the world, walk-by hacking is made even easier by "war chalers" who roam city streets to find them and then mark the boundaries of corporate wireless networks on nearby sidewalks and walls.

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) published the 802.11b standard for a group of technologies governing wireless Ethernet connectivity. Because unauthorized users can receive wirelessly transmitted data, the 802.11b standard included Wired Equivalent Privacy (WEP) to encrypt the transmitted packets. Unfortunately, WEP utilized static keys as part of its encryption methodology, which made it relatively easy to intercept enough packets to discern the key and thus crack the coded traffic. Once hackers discovered this flaw, they developed automated cracking programs that soon hit the Internet and gave even inexperienced hackers the tools they needed to crack just about any WEP-based WLAN. Even worse, it's possible for an attacker to modify the packets, compromising the integrity of the data.



The good news is that the IEEE has developed a standard (802.11i) that is dedicated to providing solid security, although adoption is not yet widespread. In the meantime, the Wi-Fi Alliance, a nonprofit international wireless association, adopted an interim standard for wireless security called Wi-Fi Protected Access (WPA) in the fall of 2002 and began interoperability testing on it in the spring of 2003.

WPA is intended to address all the shortcomings of WEP; it combines user authentication (which WEP did not provide) with a stronger encryption element from the forthcoming 802.11i standard called Temporal Key Integrity Protocol (TKIP). TKIP includes Message Integrity Check, which protects against forgeries and so-called replay attacks.

Although WPA brings a boost to WLAN security, many view it as a temporary fix because future 802.11 equipment will likely use the Counter Mode with CBC-MAC Protocol (CCMP), which is also a part of the 802.11i draft. CCMP uses Advanced Encryption Standard (AES) to provide even stronger encryption. However, AES is not designed for backward compatibility.

Beware of the Back Door

Ensuring the security of wireless networks isn't just about standards, of course. Information security professionals are justifiably concerned with the many publicized types of attacks that can be launched against WLANs—including traffic interception, "man-in-the-middle" attacks, denial of service, and session hijacking, to name a few.

Fortunately, many risks can be mitigated by following basic wireless security practices using enterprise-class and client-protection technologies. Let's look at some of the steps involved.

The boom in wireless networking took many IT departments by surprise, with the result that much wireless equipment was introduced into organizations by individual employees and work groups, rather than through the IT department or other proper channels. The result of this "back-door" introduction was that wireless wasn't put through the normal process of understanding its capabilities and limitations before implementation. Consequently, efforts to secure wireless devices came as an afterthought, or were not sufficiently rigorous.

The first step in creating a secure WLAN is to establish a university-wide strategy for deployment and usage. The strategy should address these areas:

- Determine needs. What are the drivers and needs of your organization? Identify objectives clearly, and make sure that benefits outweigh risks.
- Integrate wireless policies into existing policies. Remember: Wireless solutions are an extension of the wired network.
- Clearly define WLAN ownership. This ensures control as well as response when security threats are identified. It also nips back-door introductions in the bud.
- Protect the existing infrastructure. This is critical: Do not place wireless devices directly on the internal network. Instead, provide a separate WLAN with highly controlled gateways to the main network.

- Educate users on wireless policies. This includes training students and faculty to configure their devices to securely access the network.

- Follow WLAN best practices.

In order to protect a WLAN from attack, universities need to be up-to-date with their security best practices. These should include the following:

- Control the broadcast area and lock each access point. Many wireless access points let you adjust the signal strength. Place your access points as far away as possible from exterior walls and windows. Test the signal strength so that you can barely get a connection at these locations. Next, make sure to change the default password on all access points. Use a strong password to protect each access point.
- To provide compatibility, purchase hardware from one vendor. While the IEEE standard should provide compatibility between wireless devices from different manufacturers, interpretations of the standards and proprietary extensions can prevent full integration between devices of different manufacturers.
- Use Service Set Identifier (SSID) intelligently. Buy access points that let you disable SSID broadcasting. This prevents access points from broadcasting the network name and associating with clients that aren't configured with your SSID. Also, immediately change an access point's default SSID. (And while you're at it, change the default user name and administrator password, too.)
- Regularly scan for rogue access points. Wireless network interface cards can be configured as access points, and

very little effort is required to turn a client computer into a rogue access point. Regularly scan for rogue access points on the network using a wireless scanning tool.

- Implement user authentication. Require access point users to authenticate. Upgrade access points to use implementations of the WPA and 802.11i standards. Also, as you implement user authentication on the access points, reuse any existing servers providing authentication for your other network services. This prevents former employees from using old user accounts to access the network.
- Secure the WLAN with IP Security virtual private network (IPsec VPN) technology or clientless VPN technology. This is the most secure way to provide user authentication, data integrity, and data confidentiality services on a WLAN. Additional VPN technology is not dependent upon the access point or the WLAN card; therefore, additional hardware costs aren't incurred as wireless security standards continue to evolve.
- Use Media Access Control (MAC) address authentication. If you have a manageable number of wireless users and just a few access points, MAC addressing lets you restrict connections to your access points by specifying the unique hardware address of each authorized device in an access control list—and allowing only those specific devices to connect to the wireless network.
- Restrict unnecessary protocols. Restricting unnecessary or redundant protocols from the LAN segment that connect the access points to the VPN

gateway reduces the possibility of unidentified holes and vulnerabilities. Retaining the Domain Name System and IPSec protocols is recommended to support the VPN.

- Turn on the highest level of security your hardware supports. Even if you have older equipment that supports only WEP, be sure to enable it. Whenever possible, use at least 128-bit WEP.
- Deploy personal firewalls and virus protection on all mobile devices. The Wi-Fi Alliance recommends using the corporate network security policy to enforce their continuous use.
- Deploy enterprise-class protection technologies. This includes employing a Layer 7 firewall on the demilitarized zone and client firewalls on each desktop; VPN services that encrypt all traffic to and from wireless devices; intrusion detection systems; antivirus software at the gateway, server, and desktop levels; regular vulnerability assessments of the WLAN; and policy compliance tools.
- Implement a university-wide strategy. Standards and technologies aside, perhaps the most effective tools for securing WLANs are an intelligent university-wide strategy and basic wireless security practices. Long considered the weakest link in both wired and wireless environments, users must understand the importance of security and know how to configure their wireless devices in order to protect the university network.

Conclusion

A recent study by Ipsos-Reid found that the typical mobile worker who accessed wireless e-mail was able to

gain an average of 53 work minutes per day. That spells improved productivity and flexibility for students and faculty—and extra work for IT departments. Like most advances, WLANs pose both opportunities and risks. The technology can represent a powerful complement to an organization's networking capabilities, enabling increased employee productivity and reducing IT costs. To minimize the attendant risks, IT administrators can implement a range of measures, including establishment of wireless security policies and practices, as well as implementation of various LAN design and implementation measures. Achieving this balance of opportunity and risk allows enterprises to confidently implement WLANs and realize the benefits this increasingly viable technology offers.

Glenn Taylor is Symantec's director of state and local government, hospital, and academic programs. He invites you to contact him at glenn_taylor@symantec.com.



Shaw University Upgrades Network to IP Telephony and Takes the Difference to the Bank

by Martel Perry
Shaw University

To say that Shaw University has taken its communications network from the 19th to the 21st century using Internet Protocol (IP) telephony technology is not an overstatement.

Where We Were Then

As the nation's oldest historically black college in the south, Shaw University had an awesome task: Take an aging Centrex communications system and build a University-wide communications system over a converged IP voice, data, and video backbone to connect 10 satellite campuses. Added to the challenge was for Shaw to eliminate busy signals, offer features such as voicemail for students and teachers, and reduce expensive phone service and Internet access bills.

The urgency for Shaw to revamp its communications system had been mounting for some time. We had no single telephone system on campus—there were 13 different phone systems—and the University was getting services from eight local telephone carriers, four long-distance carriers, and 15 different data and Internet service companies. The system was not only confusing to manage, but it was also expensive. The University's telecommunications costs, including a Centrex system, were close to \$40,000 per month, regardless of call volume.

Even worse, calls to the admissions or financial aid offices were frequently met by busy signals, which crippled productivity and lowered student satisfaction. In addition, the administration, faculty, and dormitory phones did not have voicemail capabilities. When 80 – 90 percent of your students are receiving financial aid, you have to create an environment in which students can reach the right people to get assistance. Because most students gauge the quality of service not by how much time you've spent on the phone with them, but by whether they've reached a live person when calling, we had to make improvements.

Shaw, which has 2,600 students, has a campus that spreads out across North Carolina. Along with our main campus in Raleigh,



Shaw operates 10 satellite campuses known as CAPE centers (Centers for Alternative Programs of Education). We needed to unify these campuses and make everyone feel connected. Previously, our CAPE centers also were not fully integrated from a communications standpoint. For instance, students had to dial long distance from the center in Ahoskie to the main campus in Raleigh approximately 140 miles away.

When it came to distance learning, the possibilities for CAPE centers were endless, but at the time, Shaw was not positioned to maximize those opportunities. We wanted to take advantage of technologies such as videoconferencing to truly connect CAPE centers with the main campus, create a more enriching classroom experience, and expose students to top instructors whatever their location.

Where We Are Now

With the flexibility of IP telephony technology, we have now created an integrated campus communications system that improves its educational offerings, supports students and instructors, and reduces costs while creating new ways for the University to generate revenue. We've also been able to strengthen our business and computer science programs.

Today, all of these technology upgrades have helped us to remain true to our University's original mission to provide quality education without barriers and to the leadership theme of our president, Dr. Clarence Newsome: "Strides to Excellence: Only the Best!"

At Shaw, our communications network now reliably connects its campuses, students, and faculty

through voice, Internet, and videoconferencing services. The network bolsters productivity, provides students and faculty with essential services such as voicemail and mobile online access, and enables Shaw to deliver distance-learning courses throughout the state through videoconferencing.

The new network also will help us gain return on our investment through revenue-generating services offered to communities surrounding its campuses, such as teleconferencing sessions and subscription-based Internet access. Shaw's monthly phone bills have been reduced by 50 percent, and thousands of calls per month are now answered by a live person or voicemail instead of a

busy signal as was often the case in the past.

The benefits of our new network include the following:

- Productivity and mobility up. Staff productivity improved with the use of IP phones, including the softphone. The softphone allows a computer to serve as a desktop telephone with the flexibility of connecting to the University network no matter where a person is. Administration and faculty also have greater mobility with the Avaya Extension to Cellular, which allows staff to move about the campus or telecommute and have their desktop calls transparently delivered to their cell phones.

Xtension Recorder

Recall every conversation using the power of your PC.

Features:

- Capture Caller ID/ Dialed Number
- Control from your phone
- Disconnect Alert
- Time & Date stamp
- E-mail
- Password protection
- Store calls locally or on Server

The Xtension Recorder simply connects in line with any Nortel PBX or key system telephone and plugs into the USB connector on any PC. Conversations are stored in the same high quality format as your digital telephone system ensuring excellent sound quality.

No sound card required, no handset cord connection, no complex sound card adjustment, simple Digital Connectivity.



Call Dees with your Nortel recording applications.

Dees

1-800-654-5604

www.dees.com sales@dees.com

- Distance learning enabled. With the installation of a new videoconferencing system, Shaw's voice, video, and data network has a footprint that covers the state of North Carolina. The University can offer a fuller lineup of courses to anyone in the world but has a local reach to its remote CAPE centers. These centers are located in areas that include Ahoskie, Asheville, Durham, Fayetteville, Rocky Mount/Wilson, Greenville, High Point, Kannapolis, and Wilmington. Most new students will come through the CAPE centers. This is huge for us, because the student population in rural areas of the state normally wouldn't have the opportunity to go to a four-year school. They would have to leave the area.
- Innovative communications for students. Students can even join a lecture via cell phone because the IP network allows links to as many as 24 videoconferencing sites and 48 audioconferencing sites.
- Travel time and staffing decreased. Staff and administration no longer have to travel to remote campuses for meetings because videoconferencing is at each site. The University has also decreased the number of adjunct professors needed at its remote locations.

- Network management eased. An IP telephony platform allows Shaw to more easily and centrally manage its network via the Avaya Integrated Management software. The school has also solved its urgent need for more bandwidth and reduced the myriad of carriers and service providers.
- Expenses cut. The school once paid expensive toll charges between locations and had no call accounting. Although all of the lines for Shaw's Centrex system were not being used, the University still had to pay monthly charges for the dorms' lines. That expense has now been cut in half.
- Enrollment and retention up. Shaw has already seen a 20 percent increase in enrollments at its remote campuses that are linked to the main campus via videoconferencing.
- Revenue generated. Shaw plans to become a videoconferencing provider for the towns surrounding the CAPE centers—currently such services are hard to come by. If the state government wants to hold a videoconference with state employees, or if banks want to perform staff training, they can do so in the 10 towns where our videoconference centers are located. And we can charge the same rates as a commercial videoconferencing network.

Shaw plans to reap monetary rewards from the new communications system. The University's phone bills have already dropped to half the amount the school previously paid each month. In total, Shaw is saving more than \$300,000 per year compared with its previous annual communications costs. We predict that over time, we will save 50 percent on payroll each month by being able to have fewer instructors cover more courses thanks to distance learning. In the next 5 years, we estimate an overall savings of \$1.5 million.

Conclusion

We've learned a lot of lessons from our implementation. If any university officials have to tackle overhauling any portion of their communications system, I would suggest they take a step back and consider an enterprise approach. In the end, coming up with a broader IP strategy that covers voice and data services could save money, time, and planning. In addition, an IP network could create new revenue sources and enable you to take your communications network as far as your imagination wants to go.

Martel Perry is executive vice president at Shaw University. Reach him at mperry@shawu.edu.



Interview with Doug Van Houweling *continued from page 31*

ship tell you are their concerns over the next few years?

Van Houweling: I think there are really two dominant issues. One is the issue of security, privacy, and ease of access. I believe that finding the proper balance and developing the proper tools to enable our students, faculty, and staff to continue to take advantage of continually developing facilities on the Internet is going to require that we

develop and implement better technology to deliver security and privacy in a user-friendly fashion.

The second issue is reinvestment in the campus and regional infrastructure. On many campuses today you can't use the latest Internet applications because multitasking and IPv6 are not available, and networks are poorly managed or congested. Internet bandwidth is too often less than many of the new applications require. The transition to Internet carriage of voice and video traffic will also demand an up-to-date

infrastructure, and I think we'll see this kind of reinvestment taking place over the coming years. I've also already talked about the importance of obtaining direct optical connectivity to major communication points of presence from each campus. Those are the two major areas that I would pick as focal points for our work together.

ACUTA thanks Dr. Van Houweling for taking time to speak with us and for his insights into the challenges we will be facing together.



Instant Messaging On Campus: RU Secure?

by Joe Licari
Sybari Software

Instant messaging(IM) has quickly become one of the most popular forms of electronic communication today, particularly for high school and college students. According to The Radicati Group, by year end 2008 there will be 670 million IM users. Most IM messages are being sent from public, unsecured IM platforms such as AOL, Yahoo!, and MSN. As IM usage increases in popularity, it presents a variety of challenges for IT managers who must protect campus networks and ensure that communication lines flow smoothly.

For example, Jenni, a college freshman and avid computer user, uses IM to talk with friends back home, get homework help from classmates, and make plans for the weekend. Since her friends often change screen names or have multiple accounts, she doesn't think twice about accepting a real-time message or files from a name she doesn't recognize.

Unlike e-mail, IM operates in real time, increasing the opportunity to receive and distribute viruses. As anti-virus products have become a ubiquitous part of the network security landscape, virus writers have turned to the largely unprotected IM applications as an open route for propagating viruses such as Bizex and Buddypicture.

In addition to increasing the risk of virus infection, users face increasing amounts of unwanted messages or "SPIM"—the IM equivalent to Spam.

According to Ferris Research, more than 4 billion SPIM messages will be sent in 2004. That represents a 100 percent increase from 2003. The Yankee Group estimates that 5–8 percent of corporate IM messages are SPIM.

In addition to the annoyance factor, SPIM messages can use hijacked identities to commit fraud or extract sensitive information from students who believe they are speaking to a friend or classmate. SPIM can also contain inappropriate or sexually explicit content that can leave colleges and universities vulnerable to potential lawsuits.

How can colleges and universities allow students, faculty, and staff to use IM without opening their network to attacks, unwanted messages, and SPIM vulnerabilities? IM success is built upon three key building blocks: policy, application management, and network protection.

Creating and Enforcing Policy

It is critical for colleges and universities to institute specific and enforceable IM policy regarding usage, content, and file-sending capabilities. IM may also give employees the opportunity to communicate more efficiently, but it can also be abused by employees making dinner plans or discussing J-Lo's most recent marriage without fear of reprimand. For both students and employees, absent any clear school policy guidelines, there is the potential



for the use of inappropriate language (which can lead to legal liabilities), the sharing of confidential information, and productivity losses through overuse by chat-happy employees as the IM client moves the water cooler to everyone's desktop.

Because of the delicate balance between "policing" students and giving them privacy and freedom, instituting policy for electronic communications can be difficult, particularly when it comes to enforcement. Because many students exchange messages from the relative privacy of their room in the residence hall, institutions need to put the right tools in place in order to ensure proper IM usage through effective policy enablement. Policy enablement is a means for facilitating

specific policy in an organization based on pre-determined criteria, such as minimizing communications or IM traffic based on the content of a message and/or its size. The ability to enforce these policies is one of the key elements of instituting a high-level IT security strategy and creating a successful IM deployment.

One of the easiest and most effective ways to institute automated and continual policy enforcement is to use best-of-breed solutions that allow administrators to configure document filtering by type, size, and name. This ensures that inappropriate or confidential information is not being sent to parties outside of the school and that potential viruses are stopped before entering the network.

In addition, administrators need to have the ability to institute real-time, rules-based content filtering of IM messages. Having text-based dictionaries for profanity, sexual harassment, and racial discrimination allows schools to provide a safe environment for the exchange of messages both inside and outside of the school community.

Application Management

Currently, organizations are taking one of two approaches to the management of IM applications: using a dedicated IM server or managing public IM platforms. Both are effective solutions within specific environments. With the release of products such as Microsoft's Live Communications Server (LCS), some organizations have chosen to streamline the IM process and create a centralized enterprise IM application.

The Microsoft LCS is an IM server that delivers enterprise-ready, secure IM, text logging, archiving, and encryption, and it integrates these features within an existing Microsoft Windows Server 2003 infrastructure.

By creating an internal IM environment, schools can maintain maximum control over IM usage, set effective policy, and limit the ability to send and receive potentially harmful viruses or malicious code. For schools and organizations that are experiencing a high degree of IM usage among faculty and staff, this can be an effective and manageable solution.

Since most students use their own computers or Internet accounts, third-party IM applications such as MSN, Yahoo!, and AOL are used frequently, so being able to manage these applications is essential to network protection.

REGISTER ONLINE AT WWW.ACUTA.ORG



ACUTA Fall Seminars

October 24-27

St. Louis, Missouri

**Track 1. Campus Wireless
Networks**

**Track 2. Cost Savings and
Revenue Generation**

St. Louis Convention & Visitors Commission. All rights reserved.

By creating a directory of logon names, having the ability to filter IM conversations based on pre-determined policy, and managing the flow of messages, schools and institutions can maintain control without limiting their students' or employees' access to IM and potentially cutting them off from important classmate or colleague contact.

Application management products such as IMlogic's IM Manager bring centralized control, reporting, and security to traditionally unmonitored and uncontrolled IM usage. Network administrators are able to continue to allow IM usage while minimizing the risks and challenges associated with the use of public IM platforms.

Protection

Many users view IM applications as unrestricted, and conversations tend to be less inhibited and many times inappropriate. Recently, a corporate executive was fired after a virus sent his buddy list a record of his IM conversations containing disparaging remarks about several coworkers.

Network administrators responsible for the messaging and collaboration servers that support their school's IT infrastructure need to implement a server-level solution that preemptively protects communications, data, and file exchanges being sent via IM, while providing the features and functionality needed to implement a strong policy management system.

Antivirus protection becomes critical for schools, since the type of software or filtering capabilities students use is not easily controlled or monitored. Even for schools that have antivirus software in place at both the

desktop and server level, IM sidesteps many of these solutions and requires specific IM-focused protection in order to ensure total network security. Recent viruses have used both e-mail and IM-type applications for propagation, making IM security essential. With the right tools, IM security can enhance the centralized security and message-logging capabilities of their IM server or management application and allow them to secure their network and apply

content and file-filtering policies to these real-time communications.

IM is a popular and useful tool for extending the communication capabilities of students, employees, and schools. When designed and managed effectively, institutions are able to reap the benefits IM has to offer without opening up their network to exposure and attacks.

Joe Licari is Director of Product Management at Sybari Software. Reach Sybari at 631/630-8500.



**Be Seen.
Be Heard.
Be Known.**

Dux
PUBLIC RELATIONS

**Business-to-business public relations
and marketing for technology and
other innovative companies**

www.duxpr.com

e-mail us at info@duxpr.com

Network Assessments— The “Catch-22” of IP Telephony

by Ron Walczak
Walczak Technology Consultants

As the pressure continues to install IP telephony on your data network, a potential “catch-22” has surfaced that could have serious impacts on your budgets, timelines, and careers. The issue is network readiness, and the problem is that most vendors will require it (and any unforeseen required network upgrades) before they commit to installing a new IP telephony system that will work to your satisfaction.

I have listened to all the major vendors cheerfully tell the consultant community that they will conduct a network readiness assessment as part of their installation project after the client signs up for the new system. Some even say they will do it for “free.” But at what real cost?

Consider that 90 percent of data networks over 1 year old will require some sort of attention—whether it is software upgrades, institution of VLANs and QoS, or hardware replacement—and the costs are unknown until the assessment is complete. The vendors are asking customers to accept a price proposal for a VoIP system with the caveat that any network upgrades are the responsibility of the client. Of course, the vendor will gladly sell you the equipment, software, and services to fix your deficient network.

This is unacceptable for the following reasons:

- How do you budget dollars for unknown upgrade costs (and whose budget does it come out of)?
- How do you budget timelines for unknown network upgrades?

Start at the Beginning

Most large technology projects begin the approval process with a preliminary budget. Often a consultant is retained to conduct a business case analysis to project costs and timelines for executive management to consider and approve. Will your CFO accept a business case with a line item called “potential network upgrades” that has a question mark in the dollar column? I hope not!

To further exacerbate the problem, most of my clients schedule system replacements around planned events: Schools have students return in mid-August; corporations have leases that expire or begin on certain dates. Technology projects must be scheduled to coincide with fixed deadlines; there is no schedule or budget room for the last-minute inclusion of major ancillary efforts (such as replacing a data network).

Independent telephone technology consultants (not to be confused with integrators) have traditionally designed and priced solutions based upon the ability to conduct a preliminary assessment of a network (wiring distribution, equipment rooms, wide area network resources, etc.). The equipment required to conduct an accurate VoIP readiness test is beyond the financial reach of independent consult-

ants (\$50,000–\$100,000), and most really do not want to become network technicians. So you and we have a problem with the current paradigm of procuring telephone systems: There are now two major unknowns that can most certainly lead to disastrous consequences. So what is the solution?

A Two-Step Process

Buying a VoIP system properly has become a two-step process, and you must build in the time and expense of the two distinct phases: (1) independent, standards-based network assessment and (2) RFP for the VoIP system to include any recommended upgrades to the data network.

1. Independent network assessment. By crafting an RFP that includes your network details and parameters, you can solicit pricing for a network assessment that will provide standards-based test results. These results will permit the vendors such a level of comfort that they will not be surprised when they arrive, which will reduce the protective “padding” they have to add to their bid price and timelines. The bids will be more competitive and the timelines realistic.

Understand that even after a network assessment is completed, any vendors who know what they are doing will conduct at least a high-level assessment before they begin the installation to limit their liabilities; but there should be no surprises if you haven’t made major changes to the network since the first assessment. This process adds costs and time up front, but I believe it is crucial to ensure success. Contemplate adding 2–3 months to the process up front, and you won’t miss your deadline on the back end. I heard someone say “you can always put an ‘out’ clause in the VoIP RFP that says if the network upgrades cost too much, you don’t

have to proceed with the installation.” Tell that to the returning students or your corporate executives who are planning to move into their new offices on a predetermined date. Then start looking for a new job.

2. RFP for VoIP system. Now you have an independent network analysis and you can build a business case to buy a new VoIP system. If the true dollar amounts (you now have accurate cost information) and the schedule permit, you are in good shape to solicit bids for the new system. Vendors who receive your RFP will have the test results and can now engineer their solutions with a high level of confidence—and isn’t that important to all of us involved?

By the way: Do a network assessment even if you *aren’t* planning for

VoIP in the immediate future. The least painful way to justify a VoIP installation is to have little or no network upgrade costs involved. That means that the network should be evaluated for voice quality as a way of ensuring that if the organization wants to evaluate VoIP, the network will be ready. If the organization never considers VoIP, you still end up with a high-quality data network and higher user satisfaction. A network assessment should be considered an ongoing maintenance expense and an absolute requirement after any new network (or upgrade) is completed to make sure you get what you paid for.

Ron Walczak is the principal consultant with Walczak Technology Consultants, Inc., in Prospect, Pennsylvania. Visit his website at www.walczakconsultants.com.



CONNECTING ACUTA MEMBERS WITH COST SAVING PROGRAMS	
TELECOMMUNICATIONS <ul style="list-style-type: none"> Long distance Local Telephony Equipment Cellular Products - Services 	Qwest • Sprint • AT&T • MCI • CMC Telecom • Wireless Frontier Internet • LDMi - (MI Only) Qwest • Sprint • AT&T • MCI • Wireless Frontier Internet Avaya • Sprint • Innovative Technologies Group • PC Mall • Anixter Sprint PCS
NETWORK / INTERNET SERVICES & PRODUCTS <ul style="list-style-type: none"> Internet Access Wireless LAN/WAN Network Equipment 	Sprint • Qwest • AT&T • MCI • Merit Innovative Communications Inc. Sprint • Avaya • Wireless Frontier Internet • Qwest Innovative Technologies Group • PC Mall • Anixter
VIDEO SERVICES & PRODUCTS <ul style="list-style-type: none"> Integration Network Services Video / A-V Equipment 	Innovative Communications Inc. Sprint • AT&T • MCI Innovative Communications Inc. • Sprint • Innovative Technologies Group • PC Mall • Office Depot • Brodat
LEARNING MANAGEMENT SOLUTIONS <ul style="list-style-type: none"> eLearning Course Management 	Desire2Learn • WebCT
COMPUTER SERVICES & PRODUCTS <ul style="list-style-type: none"> Computers - Peripherals - Software Hosting Content Filtering 	Gateway • Innovative Technologies Group • PC Mall • Tech Depot Qwest Stratacache • Innovative Technologies Group • PC Mall
ADDITIONAL PROGRAMS <ul style="list-style-type: none"> Office Equipment & Supplies Library Equipment & Supplies Power Conditioning Consultants Security - Backup Systems Cable - Connectors - Wire - Fiber 	Office Depot • PC Mall Brodat Coffman Electrical Equipment Company Digby 4 Group • Communication Advisors Inc. New Visions Network, LLC • Total Solutions Group InfoCore • Wireless Frontier Internet Anixter



CALL (888) 870-8677 or visit www.micta.org

Voice Lessons: Open-Source Voice over IP Finds a Home in University Networks

by William Rich
Pingtel Corp.

Open-source computing and Web server platforms such as Linux and Apache are commonplace in university networks, classrooms, and labs. But the promising idea of a Session Initiation Protocol (SIP)-based, open-source voice over IP (VoIP) platform is just beginning to gain interest among forward-thinking university telecommunication departments and labs.

Not only is open-source VoIP an enticing technology because of its inherent cost-effectiveness and flexibility, but open source is also a valuable learning platform for students. Because the whole idea behind open source is its open nature—meaning programmers can obtain the code and adapt it to their needs—open-source VoIP is also finding a place in the classroom and lab as undergraduate and graduate software engineering programs become involved in open-source development.

In addition, open-source organizations such as SIPfoundry (www.SIPfoundry.org) have evolved in order to organize the open-source code as well as support developers and create educational forums for students and university technical professionals, providing a valuable learning opportunity for all.

Opening Up to Open Source

Open source means software in which the source code is open for public view and modification. With open-source SIP-based VoIP, universities would receive their call control software, such as PBX, call routing, and messaging software, for free, without licensing fees. They would be able to run their VoIP communications software on off-the-shelf Linux servers, use media

gateways and standards-based phones from multiple vendors, and pay only for customer support or professional services, if desired.

In addition, they would be able to modify the solution in order to enhance their own VoIP services, either by working with professional organizations that package and support open-source SIP, by working with third-party programmers including those in the open-source community, by taking advantage of the undergraduate and graduate student body, or by creating the code themselves.

Within the current market model, incumbent players provide proprietary solutions packaged with their own hardware, including phones, media gateways, chassis, line and trunk cards, and their proprietary applications, including voicemail and call-center applications. This locks the university customer into a vendor relationship for hardware, software, maintenance, support, and professional services.

Establishing a true standards-based solution, based on SIP, will turn the current model upside down. Universities will no longer be tied to one vendor for their hardware and software applications. And almost immediately, customers will notice a cost savings because with open source, the VoIP application software is free, or is available in low-cost packages that include TAC support, documentation, and training from vendors.

Moreover, colleges and universities reap substantial additional savings because open-source solutions (free or packaged)

operate on off-the-shelf "LinTel" platforms versus expensive Windows boxes or proprietary cards and can be matched with low-cost SIP gateways, phones, and softphones from any vendor. The relative price of open-source solutions will continue to drop as Linux servers become cheaper and new SIP hardware enters the market: Moore's Law at work.

In addition to reaping the financial benefits, universities will be able to assist student developers who are eager to work with the support of their professors to develop something worthwhile and solve real-world networking problems. Ultimately, universities could use any technology development as incubation for small companies.

Securing the Code

In order for open source to work, one or more organizations must oversee, enable development of, and maintain the source code. The backbone of open source's benefits is its inherent freedom but also its safety and security as the source code is watched over, monitored and reviewed by open-source communities and projects, including SIPfoundry; Vovida.org (www.vovida.org), a community that creates SIP infrastructure; and reSIProcat Project, which creates open-source SIP stacks.

Because open-source software is built using some of the key elements of the scientific method with published results and peer review, open-source development not only attracts freelance programmers working in their spare time, but also full-time programmers who are employed by industry and who focus on developing the source code to enhance their firms' businesses. Undergraduate and graduate students are also able to participate through the support of their universities and professors.

The possibilities of open-source VoIP are endless and so are the opportunities for universities, natural early adopters of new technologies, to evolve their telecommunications systems into something innovative as well as useful, as the following cases demonstrate.

Innovating Based on Demand

Swarthmore College, in suburban Philadelphia, had no choice but to use a VoIP system when it set up new offices in a 50-year-old train station near its campus. With no right-of-way to run cabling to the station, and train tracks in the way, the college had to find a way to run voice and data services to the 12 people in the new station offices,

according to Mark Dumic, associate director of networking systems at Swarthmore College.

For over a year, the college has been running a pilot based on open-source VoIP technology. Using point-to-point wireless to cross the tracks, the college then used VoIP phones and standard network connections to provide voice and data services.

In addition to the train station office, the college also has several small houses at the edge of campus that were turned into residence halls. In those cases, where the run was too long for copper, the college decided to use fiber instead, and put voice and data over that fiber, says Dumic.

Notify thousands in minutes!

1Call R.E.D. Alert (Response to Emergencies and Deployment)

Use for everyday notification needs, and those times that you need large-scale notifications!

- ✧ A must when an immediate response is vital
- ✧ Send alerts automatically via pager, e-mail, mobile phone, home phone – *any or all!*
- ✧ Monitor progress in real time
- ✧ Use *Just Say It* speech recognition to automate the communication process



Your perfect hosted or on-site solution to handle:

Emergency/Disaster Situations ♦ Help Desk/Maintenance Dispatch
♦ Special Conditions and Events ♦ Outages ♦ Alarms

1CALL

A Division of **amtelco**

(800)356-9148
www.1call.com/acuta2
info@1call.com
4800 Curtin Drive
McFarland, WI 53558
(608)838-4194

A third scenario where Dunic hadn't anticipated using VoIP was with campus construction causing a lot of office moves. "We've had to get creative about creating office space out of little niches on campus," he says. "It's very convenient to run data cabling and give the customer voice on that. It gives us a lot flexibility."

The ease of implementation and cost saving over having to run copper for voice has enabled the college to provide phone service quickly, sometimes with only a few days' notice, adds Dunic.

And while Dunic currently doesn't anticipate any student involvement with regard to the open-source code development because of college resources, he is anticipating replacing the college's 14-year-old ISDN PBX with a SIP-based platform. "We are anticipating as early as the summer of 2005 needing to implement new technologies," he says.

"We are interested in SIP because of its promise of open standards, mainly having control over when and how we transition from old to new technologies," says Dunic. "We don't want to be at the mercy of a vendor and a proprietary system that's calling all the shots."

Saving Money and More

North Carolina State University has also been running a VoIP system for more than 3 years now and has open-source technology in its lab, according to John Streck, director of networking research and development at the University and a professor of networking.

Streck is interested in using the SIP-based technology for multimedia

because of open source's flexibility and freedom for development and creativity. "It's nice to be able to get in there and get at the kernel and not be restricted, and be creative," says Streck, referring to the ability to access the open-source code. "But I also want the stability of knowing that community knows where it is, has tried it, and got most of the bugs out," he adds.

Streck's ultimate goal is to have a platform that allows him to offer multimedia service offerings, not just voice, so that as other new technologies and applications come along, including teaching technologies, he can seamlessly integrate the new features, such as peer-to-peer video, into the platform at an off-the-shelf-cost.

One project Streck is currently researching with the help of students is contextual computing tied to VoIP, which would enable callers to see where the person they are trying to communicate with is—at home, at the office, or in a meeting. "You could use that information to tailor what you do with the call," says Streck. "You could add in privacy, security, messaging. We are barely scratching the surface with presence information. Open source opens up a whole myriad of applications."

Working with open source literally opens up a once closed world to new minds that don't know what they are not supposed to do—but in a good way, says Streck. "You don't have artificial boundaries that have been established over time."

Having a supportive community of developers not reigned in by any type of boundary also means users will be able to go to the source and ultimately

have faster access to what they need.

"Maybe one developer can see something valuable that another does not and get in there and develop it," says Streck. "We can get out and get what we need and don't have to wait in line."

Not having to depend on one vendor means universities have the vehicle to force the competition to get better quality for lower prices, he adds.

Lowering the Initial Cost

With many universities struggling with strict budgets and the challenges of keeping up-to-date with the latest technologies, open-source VoIP is an attractive offering, according to Susan Lehto, senior analyst of telecommunications and information technology at Boston University. "In a list of the advantages of an open platform compared to a proprietary platform, you get flexibility and functionality," she says. "You can look for the vendor that develops the best or most suitable peripheral system, you get faster development response from feature developers, you can run an open standard on any operating system," adds Lehto. "Plus there are a lot of guardians of the SIP and open-source codes that work to protect the integrity of the platforms and additional software."

Boston University is currently evaluating open-source VoIP for peer-to-peer calling in order to become familiar with the technology and see how it works. "We wanted to become familiar with VoIP in the pure OS model," says Lehto.

The low initial cost of open-source VoIP, as well as the ability to shop

around for the best features and value, were key factors to Boston University's trial. "We can buy systems from one party and the support from another," says Lehto, referring to considering open-source VoIP platforms. "There's not the lock-in from the vendor, no ownership, and the pricing is scaled to be much lower. And as far as managing them, if you don't like the one, the contracts are only 1 year at a time, so you can go to another one."

In addition, Lehto says the ability to develop their own features based on University demand was also an important factor to their trial. "If a user asks for feature and it doesn't exist on a proprietary system, we'd normally have to tell them that the phone system doesn't do that," she says.

With open source, Lehto can look to a third-party developer for that feature or a website that sells or develops software and know that because it's based on standards and monitored by the open-source community, the software is safe. "There is always the danger of adding software to the mix, but with the open-source community out there bug-fixing and enhancing, we'd probably get more of a shake-out on any particular piece of software in the open-source market than we'd ever get out of the proprietary," says Lehto. "With proprietary we don't even know how it works."

Considering the Student Advantage

While saving money on actual hardware, software, and contracts is an important factor in many universities' decisions to allow open-source VoIP into their labs and networks, another important factor is the ability to have students solve real-world networking problems as part of their curriculum and acquire valuable

skills at the same time.

"Universities don't have extra people sitting around to do the research," says Walt Magnussen, director of telecommunications at Texas A&M University. "I'd have to hire a whole lot more people within my staff to be able to go ahead and do the research we are trying to do here," he says. "The questions we are asking the students to answer are questions that the University *has* to have answered."

In addition to being the Internet2 evaluation center, which evaluates new technologies and applications for higher education, Texas A&M also asks its senior engineering students to solve some of its own networking problems as part of the graduating course work. Students work with outside companies, get more than just a textbook education on VoIP networking, and then the companies often end up hiring those same students upon graduation.

Texas A&M uses its own intellectual resources to have its networking problems solved: Students find jobs, and the University builds its contacts in the industry. "It's a win-win situation," says Magnussen. "The students are working on state-of-the-art real-world problems, and we are getting problems solved."

Texas A&M knows about networking problems. With over 100 remote locations across Texas and several international sites, the University's network is primarily VoIP now. "We were moving a lot of offices off campus and leasing more and more space in the surrounding community," says Magnussen. Rather than running a T1 for voice and a 10 or 100baseT Ethernet connection for Internet, or ATM over

Links to find out more about SIP and the open-source effort

www.pingtel.com
www.SIPfoundry.org
www.vovida.org
www.ietf.org/html.charters/sip-charter.html
openuss.sourceforge.net/openuss
itec.tamu.edu
www.internet2.edu

an OC-3, Magnussen says simply, "now that VoIP is out there we just do VoIP."

A lot of universities would like to get their feet wet and figure out whether or not VoIP works for them, says Magnussen. "Open source gets them started without a significant investment. The initial and ongoing costs are lower because they are not paying for the code itself," he says. "VoIP standards are rapidly evolving and most are happening within higher education."

Indeed, higher education seems to be the perfect test bed for open-source VoIP thanks to the wealth of knowledge and innovation found in the sector and its natural early adopter tendencies. Labs like Internet2 and university networks like those of Boston University, North Carolina State University, Swarthmore College, and Texas A&M University will be the proving ground for open-source VoIP solutions, and their innovation and support will lead to the adoption of technologies in the enterprise market.

William Rich is president and CEO of Pingtel Corporation. Reach him at brich@pingtel.com.



Advertisers' Index

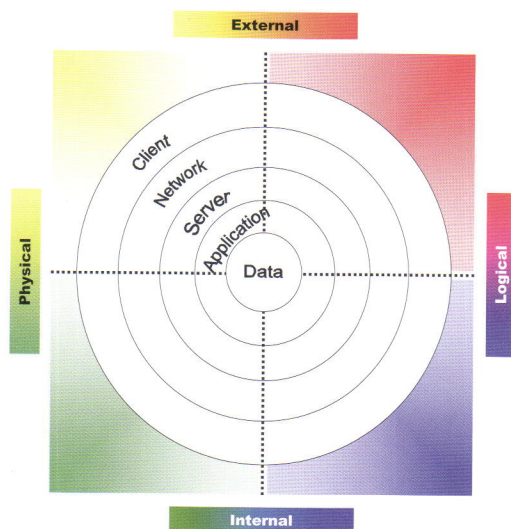
★ Indicates ACUTA Corporate Affiliate

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

- ★ **1 Nation Technology** 15
Sales (800/998-9862)
4027 Tampa Rd., #3000, Oldsmar, FL 34677
info@1nationtech.com
www.1nationtech.com
- ★ **1Call, A Division of Amtelco** 17, 43
Matt Everly (800) 356-9148
4800 Curtin Dr., McFarland, WI 53558
info@1call.com
www.1call.com
- ★ **A1 Teletronics** 23
Don Sturiano (800/736-4397)
1010 118th Ave. N., St. Petersburg, FL 33716
acuta@a1teletronics.com
www.a1teletronics.com
- ★ **Alcatel Internetworking Inc.** Inside Front Cover
Bob Colbert (800/995-2612)
100 Main St., Suite 108, Dover, NH 03820
end-enterprise-data-solutions@ind.alcatel.com
www.alcatel.com/enterprise
- ★ **Allot Communications** Back Cover
Derek Peterson (877/ALLOT-CO)
7664 Golden Triangle Dr., Eden Prairie, MN 55344
edu@allot.com
www.allot.com
- ★ **Amcom Software** 25
Kathy Veldboom (952/946-7715)
5555 West 78th St., Minneapolis, MN 55439
kveldboom@amcomsoft.com
www.amcomsoft.com
- ★ **BelAir Networks** 3
Joe Aragona (613/254-7070)
603 March Rd., Ottawa, Ontario, Canada
jaragona@belairnetworks.com
www.belairnetworks.com
- ★ **Compco** 21
Randy Burns (615/373-3636 x148)
5120 Virginia Way, Brentwood, TN 37027
rburns@compco.com
www.compco.com
- Dees Communications** 35
Louis Champan (425/869-1963)
4130 148th Ave. NE., Redmond, WA 98052
lchampan@dees.com
www.dees.com
- ★ **Dux Public Relations** 39
Kevin Tanzillo (972/889-9577)
5713 Maidstone, Richardson, TX 75082-4970
kevin@duxpr.com
- Graybar** 7
Robert Weiland (314/573-9356)
34North Meramec Ave., Clayton, MO 63105
robert.weiland@gbe.com
www.graybar.com
- ★ **Micta** 41
Clancy DeLong (989/772-2623 x203)
1500 W. High St., Mt. Pleasant, MI 48858
cdelong@mictaservice.com
www.micta.org
- ★ **Mutare Software** 11
Ben Crown (847/781-2387)
2401 West Hassell Rd., Ste. 1510, Hoffman Estates, IL 60195
bcrown@mutare.com
www.mutare.com
- ★ **NEC Unified Solutions, Inc.** Inside Back cover
Sydney Burton (214/262-2430)
6535 N. State Hwy. 161, Irving, TX 75039
sburton@necunified.com
www.necunifiedsolutions.com
- Network Engines** 27
Erika Batten (877/638-9323)
25 Dan Rd., Canton, MA 02021
sales@networkengines.com
www.networkengines.com
- Panduit** 5
800/777-3300
17301 South Ridgeland Ave., Tinley Park, IL 60477
cs@panduit.com
www.panduit.com/rs06
- ★ **Qwest** 13
Pat Williams (952/848-7651)
4206 Salem Ave., St. Louis Park, MN 55416
patricia.williams@qwest.com
www.qwest.com
- ★ **Telecom Technology Resellers** 47
Michael Forst (636/527-7100)
440 Sovereign Ct., St. Louis, MO 63011
mikeforst@teltechresellers.com
www.teltechresellers.com
- Vitel Software** 19
(508/831-9700)
67 Mill Brook St., Worcester, MA 01606
sales@vitelsoftware.com
www.vitelsoftware.com
- ★ **WTC** 8
Shelley Hasselbrink (213/689-5314)
801 South Grand Ave., Ste. 700, Los Angeles, CA 90017
shasselbrink@wtc-inc.net
www.wtc-inc.net

We like to look at network security as a quartered onion. There are layers within the network. Clients connect to the network, which accesses servers. The servers house applications through which data is accessed. The quarters represent the threats, which can be internal or external, physical or logical (viruses, DoS, etc.). Your security must address all aspects of all layers and all quadrants.

Start with an audit and risk assessment of your business processes, critical areas, systems, and policies. Evaluate and prioritize your risks. Find appropriate technical solutions.



But, at the same time, you cannot ignore the harder tasks of developing strict security policies and providing security education, training, and awareness at all levels. Security policies must be proactive, adaptive, and on-going. And of course, there is the even harder issue of enforcement. While enforcement is often avoided in higher education, policies without teeth are merely polite suggestions and will do little to improve IT security.

Geoff Tritsch is president of Compass Consulting International, Inc., an ACUTA corporate affiliate for 19 years, and a

frequent speaker at ACUTA events. Reach Geoff via e-mail at tritsch@compassconsulting.com or visit www.compassconsulting.com for more information.

Vendors leaving you a little... stranded?

Call
On

Telecom Technology Resellers, LLC

36 Month Advanced Replacement Warranty
Additional Warranty Two Year Warranty for \$100/card, \$30/phone

Don't miss this month's specials!

M2616D NT5D12 NT8D14 NT8D09 M7208 M7310 M5008 M5312

\$149.00



\$950.00



\$650.00



\$750.00



\$89.00



\$125.00



\$109.00



\$145.00



Where Quality Never Comes Up Short. The Best Nortel Buy-Back Program.

Call 636-527-7100 or Fax 636-527-7127

Email mikeforst@teltechresellers.com

Visit www.teltechresellers.com

NT8D14 is a registered trademark of Nortel, Inc. NT8D14 is an independent model of equipment designed by Nortel to meet

Here's My Advice



**Geoff Tritsch, President
Compass Consulting
International, Inc.**

IT Security and Management

IT security can best be looked at as the balance between ease of access and protection of assets and information. Daily operations require on-campus access to information and systems. Collaboration, researchers, visitors, students, traveling faculty, and telecommuters demand ready off-campus access. In both cases, the easier the access, the more vulnerable the information, especially considering that a significant portion of your threat (students) is inside your own firewall.

As technologists, we tend to approach problems technologically. While a strong technical approach must provide the foundation for any security initiative, we have come to realize that technology alone is not enough.

As part of a recent focus group that we coordinated for a statewide university system, we worked with the attendees to develop a list of critical IT security issues and then to rank those issues first by importance and then by risk. Everyone went into the session focusing on the technical aspects of security. However, when it was over, topping the *importance* list were support/compliance/enforcement, patch management, and rogue devices (servers and wireless APs). Topping the *risk* list were "The Human Element," physical security, and data downloads, storage, and use.

Clearly, all of these are primarily people issues dealing with use and abuse of the network, not the "behind-the-curtain" technologies like firewalls, authentication, and access control. Generally, we found that the technical issues were less scary because they were controllable—the people issues more scary because they were not. Below are some of the findings and suggestions resulting from that focus group.

Issue	Risk	Mitigation
"The Human Element"	People will always be the weakest and the strongest link in security. There are increasing numbers of stories about how employees' helpfulness can be used to facilitate unauthorized access.	Training, education, communications
Governance	Inconsistent management and security practices; too many other things to be done	Set priorities with the assistance of CIOs and peers; communicate and share information and best practices; internal consulting; IT Security Officer
Nontraditional employees (student workers, temporary help, and hourly workers)	Password sharing; poor enforcement of password policies	Policies; education
"Temporary" situations	Creates holes in security to accommodate occasional and temporary access; rogue servers and clients; rogue APs	Policies; education; communication; flexibility
Support/compliance/enforcement	Without enforcement, compliance will be spotty	IT security policies and practices need to be formulated with the participation of clients and upper management
Security awareness	All of the above	Training, education, communications

continued on page 47


$$1 + 1 = 3$$

**NEC brings more
to the equation than
the traditional answer.**

Just adding up the pieces of your network won't necessarily give you the greatest competitive advantage.

Whether deploying reliable IP Telephony across a campus environment or providing a comprehensive set of services to help you get the most of your network performance, NEC Unified Solutions will help you achieve a total solution that is greater than the sum of its parts.

NEC

NEC Unified Solutions, Inc.

Building Communications Solutions. Delivering Excellence.

www.necunified.com/education



Allot®

Communications

The Brains Behind Some of the World's Most Advanced Networks



*Allot Communications—
P2P Traffic Management
Solutions That Have No Peer*

At Allot Communications, we're committed to helping colleges and universities solve their network traffic management problems. With a few clicks of the mouse, our award-winning appliances can block or control P2P file transfers, dramatically improve network performance, and keep your infrastructure costs in line. The decision is infinitely clear...

- *Industry-leading P2P control (music and video downloads)*
- *Intelligent Layer 1-7 traffic monitoring and reporting*
- *Advanced QoS for reliable VoIP and video*
- *Infinite control and optimal bandwidth efficiency*
- *Frontline protection against malicious worms, viruses and DoS attacks*
- *Real-time alerts of impending network problems*
- *Industry-leading performance scalable to 1Gbps*

edu@allot.com
877-P2P-GURU
www.allot.com



Allot®
Communications
The Traffic Management Company™