Fall 2006

ACUTA Journal of Telecommunications in Higher Education

Fall, 2006
Vol.10, No.3

ACUTA

Journal

of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education

This Issue: Infrastructure: The Building Blocks of Communications

Intelligent PoE

From the most trusted name in power.

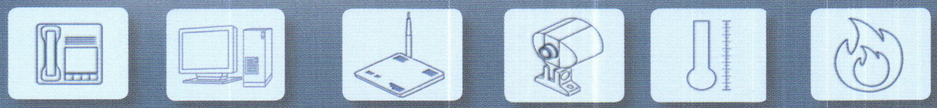
Hubbell PowerTRAC™. Power Over Ethernet.

Today's most intelligent approach to delivering PoE with capabilities to track and manage critical assets.

PowerTRAC™ is a Midspan panel solution that saves valuable closet space and its modular design allows you to select the configurations that meet your requirements.

Whether it's delivering PoE for access points, security cameras, building access controls, or tracking valuable assets like personal computers, **PowerTRAC**™ delivers.

- *Full power to every port.*
- *Reliability and security.*
- *Business critical applications that work.*
- *Rock solid asset management.*
- *Lower cost of ownership.*



Voice over IP | **Asset Management** | **Wireless and Wireless Devices** | **Security Systems IP Cameras** | **Building Automation/ HVAC Control Systems** | **Life Safety Control**

HUBBELL®

Hubbell Premise Wiring

14 Lord's Hill Road
Stonington, CT 06378
Tel: (860) 535-8326; 1-800-626-0005
Fax: (860) 535-8328
Internet: www.hubbell-premise.com

Events Calendar

Event	Date	Place
Fall Seminars	October 22–25, 2006	Marriott Portland Downtown Portland,Oregon
Winter Seminars	January 21–24, 2007	Hilton Austin Austin, Texas
Spring Seminars	April 1–4, 2007	Baltimore Marriott Waterfront Hotel Baltimore, Maryland
Annual Conference	July 29–August 2, 2007	Westin Diplomat Hollywood, Florida

ACUTA's Core Purpose is to support higher education communications technology professionals in contributing to the achievement of the strategic mission of their institutions.

ACUTA's Core Values are:

- Encouraging and facilitating networking and the sharing of resources
- Exhibiting respect for the expression of individual opinions and solutions
- Fulfilling a commitment to professional development and growth
- Advancing the value of communications technologies in higher education
- Encouraging volunteerism and individual contribution of members

Contents

Fall 2006 • Volume 10 Number 3
Infrastructure: The Building Blocks of Communications

> [A] good technology design should be concerned about flexibility and the ability to easily install new technologies and not just meeting the needs of the occupants on opening day.
>
> *Geoff Tritsch*
>
> *Acentech – Compass Consulting Division*

pg 12

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 communications technology managers and staff.

ISSN 1097-8658

POSTMASTER, send all address changes to:

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

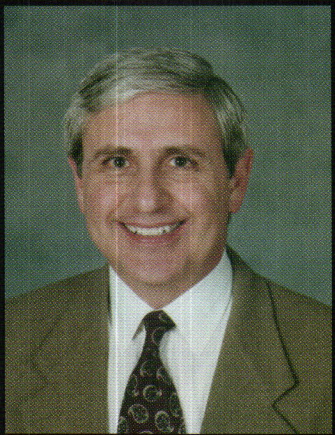
Visit the ACUTA site on the World Wide Web:

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 Adkins, Membership Development Manager, 859/278-3338, ext. 222, or e-mail kellie@acuta.org.

PRESIDENT'S MESSAGE



Carmine Piscopo, RCDD
Providence College
ACUTA President
2006–2007

Focusing on Infrastructure

I'm constantly amazed at the number of devices that are now dependent on our campus communications infrastructure. At the ACUTA Annual Conference last month, I attended a preconference seminar entitled "The Convergence of Communications and Construction" that, among other things, reminded me of how many systems—other than traditional voice and data—are dependent on our cable infrastructures: important devices such as copy machines, surveillance cameras, access control, building automation instrumentation and control systems, cable television, intrusion detection systems, distributed antenna systems, and even fire alarm systems. All of these are critical to the mission of our respective institutions, and all of these are becoming more and more IP enabled. Tom Rauscher of Archi-Technology, who conducted the preconference session, has contributed an article to this issue of the Journal that addresses this subject in some detail. (See page 52.)

As technology progresses, these systems are being engineered to work with newer and faster networking hardware, requiring higher and higher bandwidth. This further reinforces our need to build and maintain a solid cable infrastructure to support the mission-critical systems that travel over our networks. Would you buy a Ferrari if there were only dirt roads to drive on? Probably not, but that is what our networks would feel like if the wired infrastructure didn't keep pace or was poorly maintained.

If we examine the seven layers of the OSI model, it is easy to see that the physical layer is a critical and essential foundation of building any data network. At Providence College, we are very conscious of this issue and continue to improve and document our existing outside and inside pathways and cable plant. Simultaneously, we expect to create a new inside and outside plant wiring standard for all future communications infrastructure projects. Part of our standard will be to remove all unused cable per the latest revision of the National Electrical Code published by the National Fire Protection Association (http://www.nfpa.org). Ric Simmons of LSU provides additional details on this subject in his article that begins on page 20.

Our entire campus and each building already have a complete set of "T" (telecommunications) drawings. The drawings are in a tiered structure showing the entire campus view followed by floor layouts, serving zones, telecommunications equipment rooms, and the detailed information of each room. All of these drawings are web-based, allowing for easy access and eliminating the need to store large architectural drawings—although we do have the ability to print them if the need arises.

This ongoing project is expected to result in a completed communications management program by sometime in 2008. However, the documentation process to create the T drawings is very time consuming. It involves the physical inspection of all communications manholes, building entrance facilities, and all telecommunications rooms. We're currently photographing all such facilities and recording all cable information pertinent to each voice and data device on campus.

As we construct new buildings and renovate existing space, we are also re-evaluating and re-establishing a standard specification consistent with Division 27 of the Construction Specifications Institute (CSI) master format for our administrative and residential buildings.

The most influential organizations for standards that govern communications cable are the Telecommunications Industries Association (TIA) and the American National Standards Institute (ANSI). Copies of these standards are available from IHS on line at http://global.ihs.com.

This issue of the journal is focused on infrastructure. The term "infrastructure" covers much more than the wire and cable to connect devices, and there are literally thousands of products and services that fall into this category. I hope you find the articles to be of high educational value.

In addition, at the ACUTA Winter Seminar that will be held January 21–24, 2007, in Austin, Texas, one of the two educational tracks is "Convergence and Infrastructure: What it Takes." This track will cover ways that campuses are structuring their cabling, switches, routers, network architecture, power, and other infrastructure to prepare for converged technologies and applications. If it's time to re-evaluate your campus infrastructure, please make plans to join us in Austin.

▼

FROM THE EXECUTIVE DIRECTOR

Jeri A. Semer, CAE
ACUTA Executive Director

The Year in Review

For those who were unable to attend the 2006 annual business meeting in San Diego, I am pleased to have this opportunity to report on some of the highlights of activities by the professional staff in the ACUTA office over the past ACUTA administrative year.

ACUTA is fortunate to have a dedicated corps of elected and volunteer leaders—our board of directors, committee chairs, and committee members—who devote tremendous energy to setting a wise course and keeping ACUTA moving in the right direction. The staff's role is to support their efforts by implementing policies and programs to serve ACUTA members and fulfill the mission of the organization.

Strategic Planning

We have been actively working with the committees to implement action items in the strategic plan. (You can view the current strategic plan on the ACUTA website.) Of the 43 action items targeted through the second quarter of 2006, 37 are either completed or underway by staff and committees. I believe that we have made excellent progress in all five of the goals in our strategic plan.

Public Policy and Regulatory Affairs

As the staff liaison to the Legislative/Regulatory Affairs Committee, I spend a great deal of time monitoring and analyzing regulatory proposals and actions at the U.S. Federal level and key state developments. It has been an extremely active year in this arena, with much of our efforts focused on universal service, CALEA, net neutrality, VoIP, and other information and communications technology reform issues. We continue to face formidable challenges in each of these critical areas, with the potential for increased regulatory compliance requirements and costs to colleges and universities.

There is strength in numbers in the legislative and regulatory arena, and ACUTA works closely with other higher education organizations in these areas. In May, I was appointed to represent ACUTA on the Network Policy Council (NPC). This is a group within EDUCAUSE that is analogous to the ACUTA Legislative/Regulatory Affairs Committee and includes representatives of higher education institutions; national, state, and regional networks; consultants and EDUCAUSE national policy staff. The NPC meets biweekly, including several meetings in Washington that involve visits to key members of Congress and Federal agencies

ACUTA has continued to benefit from the increased involvement of legal counsel on regulatory and legislative issues, made possible by the commitment of our members' and Board of Directors' support for making this important investment.

We continue to provide quarterly updates of the online Regulatory Issues Matrix on the Legislative/Regulatory section of the ACUTA website. I hope that you are accessing and using this matrix to advise your campus on the important ▶

issues we are currently following at the Federal level.

We have also published twelve issues of the Legislative/Regulatory Update, our online newsletter which is a joint effort with Wiley, Rein and Fielding, in addition to submitting comments to the FCC on issues of interest to our member institutions.

Public and Media Relations

It has been a successful year for ACUTA in accomplishing our objective of increased positive visibility in the media. We have continued our efforts to position ACUTA and our institutional members as valuable sources of information about communications technology in higher education. This year, we sent out 13 different press releases, resulting in at least 50 articles (that we are aware of) in which ACUTA was mentioned or acknowledged as a source of information. This effort also included surveys of attendees at our seminars and the Annual Conference, on selected topics of high media interest. Press releases were written and distributed on the survey results, and generated quite a bit of interest among editors and reporters.

Research Projects

Two major research projects were coordinated by teams of ACUTA staff members, with input from our committees and Board and execution by independent research firms. During months of advance planning, a great deal of time and effort was invested to ensure that these surveys would yield meaningful and useful results. These projects included:

- We conducted a study of attendance patterns at the ACUTA Annual Conference. This study measured the opinions of members who had and had not attended the ACUTA summer conference within the past two years regarding such issues as program content, the exhibits, networking opportunities, time of year, location, return on investment, and how our members prefer to receive information about the conference. We are pleased that the conference was rated very high. Based on the preferences indicated in this survey, we are working on changing the conference to the springtime beginning in 2009. As soon as those plans have been finalized, we will give you plenty of advance notice for planning.
- We conducted a comprehensive needs assessment survey of ACUTA members as part of our efforts to be as relevant and indispensable as possible in a changing technology and academic environment. While there were no major surprises in the results, some of the key findings were:

1. Respondents indicated very positive satisfaction with ACUTA and its programs, services and publications.
2. The top three programs and services considered most important to continued participation in ACUTA were: access to updates on regulatory changes, efforts to influence regulations, and the ability to network with other communications technology peers. These were followed closely by access to the latest technical information, benchmarking with similar institutions, online information from the resource library and listservs, access to training, information on vendor products, and opportunities for leadership development.
3. Increasing security threats to campus networks was identified as the most critical issue to campuses over the next two years, followed closely by meeting increasing student expectations and regulatory compliance.
4. Respondents are senior and experienced. Ninety-six percent have five or more years experience in communications technology, and 50 percent have 20 years or more experience.
5. They have a wide range of responsibilities, but the majority of members are responsible for institutional telephone services, management of all or portion of telecommunications or networking, moves/adds/changes/trouble tickets and voicemail support.
6. In addition to their communications technology responsibilities, our respondents have significant management responsibilities. These included department management, strategic planning, purchasing/contracting and RFPs, billing or accounts payable, financial/business planning, and staff training and development.
7. Directors, managers, assistant/associate directors, and CIOs are the primary audiences for ACUTA programs and services.
8. Sixty-one percent felt that their institution's senior administration views communications and information technology as an important strategic asset.

Our board, committees, and staff will be using these results extensively in planning our programs and services.

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 the Board as well as every staff member for their professionalism and commitment to the continued success of ACUTA.

▼

Don't Make a Million Dollar Voice Messaging Mistake

How much money can you expect to spend if you change to a new family of messaging systems? Our customers tell us that it's twice as expensive to purchase a new messaging system versus upgrading their current system!

Why?

- There is a huge time and expense commitment in training new users, re-recording greetings and auto attendants and rebuilding distribution lists.
- Users resist learning new user interfaces, and get little help from confused employees and overwhelmed help desks.
- Database conversions can be more complicated than anticipated.

At **CommuniTech Services**, we've specialized in providing and supporting voice messaging systems since 1983. We have the answers that solve your most critical concerns, including these:

Have you made sure that that the critical features you use now are available on your new system?
New "state-of-the-art" systems often lack the features you expect. Some don't even offer automated attendant.

Does your vendor know both the voice messaging applications and the capabilities of the new technology and can bridge the old with the new?
We know messaging intimately in both the TDM and IP worlds along with *Find Me, Follow Me, Unified Messaging, IVR,* and *Speech Recognition* and other productivity enhancers. Don't pay for your vendor's learning curve.

Does your vendor know how to proactively monitor and optimize systems that have heavy demand, high up-time requirements?
This is part of our standard support service. Don't wait for your system to malfunction...we'll make sure it never does.

If you're considering a messaging product from your PBX vendor, is their experience limited to just integrating their own messaging system to their own phone system? What if you need to integrate with other PBX's, e-mail or Presence servers, Speech Recognition, IVR or other Voice Messaging platforms?
As a messaging focused systems integrator, we can handle all of your future needs.

Does your system have the latest design considerations for up-time and high security requirements?
Our systems are built for maximum reliability and up-time. From the operating system to the CPU and power supplies, we are focused on insuring your up-time.

Can your vendor help devise marketing programs to help you get your user communities to use your services and to help you sell your services?
We'll help you sell your users on the services you provide (and offer special revenue generating programs that target students.)

What other hidden costs of ownership are there?
Many vendors are inexperienced in sizing systems which leads to spending more than is necessary. We'll help you make the right decision the first time. Needs change - an expert in messaging can ensure that your messaging platform can adapt and thrive in an ever changing, complex environment.

CommuniTech Services can help you avoid potentially costly mistakes with your messaging systems needs. For more information, call us at 847.981.1200 extension 480.

CS

COMMUNITECH SERVICES, INC.

www.communitechservices.com

The Strategic Accommodation of Change

by Geoffrey C. Tritsch
Acentech – Compass Consulting Division

I was meeting with a group of faculty to discuss technology in the classroom and other related technology issues. The meeting was being held in one of the university's newest technology-enabled classrooms. As the faculty filed into the room for our discussion, I looked around at the millwork, lighting, electronic lectern, and work surfaces. "Nice room," I remarked. "Yeah," came the chorus of responses.

"... too bad no one uses it."

"... too bad nothing works."

"... too bad I can't run it."

"... too bad I have to completely redo all my course materials."

It was a classic case of technology disconnect. Since the technology obviously did not connect with the needs of the users, the users disconnected themselves from the technology. Clearly, there is more to putting technology in a classroom than putting technology in a classroom.

Planning Rooms That Meet Users' Needs

The most common shortcoming of technology is failure to understand the needs of the intended users. The *Oh, wow* factor tends to draw occupants and designers toward the latest and greatest technologies. But what users want are systems that are reliable and easy to operate with an intuitive user interface. Anything less is rejected out of hand by many users.

In addition to the ease-of-use issue, a number of physical design issues contribute to the success or failure of a teaching space. The room design must take the following into account:

- Room use
- Room size/shape
- Acoustics
- Program audio
- Presenter audio
- Decor
- Mechanical systems (i.e., power, HVAC)
- Camera locations
- Projector locations
- Screen size and locations
- Viewing angles and sight lines
- IT requirements
- Lighting
- Safety/security

But a room does not exist in a vacuum. The process must go beyond how technology fits into the room and also address how the room fits into the building, how the building fits into the campus, and how the campus fits into the environment. Even the best-designed high-tech classroom will suffer from a noisy air handler directly above the room unless proper noise and vibration control measures are taken, from noise in adjacent corridors that is not mitigated, from wireless networking that is not properly designed, from the sun reflecting off an adjacent building unless there are shades to shield the projection screen, from windows incapable of attenuating exterior traffic noise, or from the sound of aircraft from the local airport. To solve these problems, the design team must include acousticians, architectural/mechanical noise specialists, audiovisual specialists, IT specialists, and sound-system designers. It is "convergence" in its physical manifestation and in the truest sense.

The Impact of Convergence

Integrated designs must also deal with convergence in the technical sense. There is considerable hype in technology circles centered on "convergence," and the term has come to mean different things to different people. In the context of this article, convergence refers to the transport of multiple systems, formerly allocated to separate networks, onto a common infrastructure—typically the TCP/IP-based data network. The highest-profile example is voice over IP (VoIP), where the traditional infrastructure for telephones (dedicated copper wire pairs arranged in a "star" configuration radiating from a central point or points on campus) is replaced by carrying the phone conversations over the data network infrastructure. There are both more mundane and more "speculative" examples of using the data network as transport for such services as:

- Access control
- Audiovisual (A/V) systems
- Cable television
- Clocks
- Environmental monitoring and control
- Fire alarms
- Paging systems
- Security alarms
- Streaming (on-demand) video
- Surveillance video/audio
- Videoconferencing

The applications described above are not innovative uses of technology but are standard practice and increasingly common at the majority of colleges and universities across the country. These applications are almost universally Ethernet network –based and assume a network with high availability (uptime in the region of 99.999 percent), negligible packet loss, low latency (less than 100 milliseconds), and low jitter (variability in latency).

As Scott McNealy of Sun Microsystems put it: "The network is the ▶

computer." But in order to operate in that type of environment the infrastructure needs to support the illusion that all network devices are local to the user. That means that there must be little delay added to access times because of the network. Large files need to be transmitted across the network as if they were on local disks. A reliable, high-throughput network is central to such technologies. This becomes increasingly more difficult as more converged traffic is added to the network.

For example, the addition of an A/V management system to the network can add as much as 3 Mbps of consistent background traffic to a network as devices exchange status information such as projector status, lamp life, temperature, and so on. While 3 Mbps may not seem like much, it does add up, especially as other systems such as access control and building management add their "chatter" to the network as well.

The following list identifies some attributes of a 21st-century network:

- No maintenance/upgrade down-time
- Secure
- Redundant devices in diverse locations
- Redundant and diverse routing
- Adaptive (self-healing)
- Redundant and reliable power and backup power
- Profile and directory-driven management
- End-to-end management
- End-to-end quality of service (QoS)[1]

Convergence is definitely a tide sweeping technology before it. While we do not urge clients to move toward convergence before they are ready, we do strongly suggest that all new buildings be designed in such a way as to be "convergence ready."

In order to accomplish this, one must have a multidisciplinary, interactive design process that integrates technology into all building functions. The advantages of this approach include the following:

- Lower building life-cycle costs
- Improved energy efficiency
- Lower energy costs
- Improved life-safety features
- Lower than average operational costs
- Improved and more flexible technology services
- Occupant-specific environmental and operational control
- Increased physical security, access control, and visitor tracking
- Improved occupant satisfaction

Today's approach to new construction does not often allow for this. The common design team consists of the architect and numerous design-team members in various disciplines such as mechanical, electrical, plumbing, acoustics, furniture, millwork, and others. Technology, while acknowledged as significant in the design, is often an afterthought. The problem is that all of these disciplines are interrelated and this approach randomizes and suboptimizes interaction. The architect is rarely in a position to coordinate technology procurements and implementation. Coordination is voluntary and minimized.

While any project is a compromise among technical, financial, design, and operational objectives, the goals of IT are often in conflict with construction budgets based on today's needs. A building is designed based on a 20- to 100-year life. Technology is based on a 3- to 5-year life. One can easily expect technology to "churn" between 4 and 30 times over the building's lifetime. Therefore, a good technology design should be concerned about flexibility and the ability to easily install new technologies and not just meeting the needs of the occupants on opening day. But large tel/data rooms, cable trays, riser chases, and the other design considerations that increase flexibility also increase construction costs. Since the architect and general contractor are responsible for the construction budget and not the life-cycle building costs, it is all too tempting for them to eliminate long-term value in return for lower up-front costs.

The Standard Construction Process

To understand IT's role in the process, we need to take a quick look at the process itself. The standard construction process consists of five phases.

- Programmatic phase. What do the occupants want to do with the space? How will it be used? Is it classroom, lab, offices, library, or something else?
- Schematic design. Various design options are put forth and refined. Where will the building be located on campus? Will the building be L-shaped or rectangular? Is it functional or grand? This is where the trade-offs between ideal and reality begin.
- Design development. The selected schematic design is further defined and refined. Alternatives are priced and selected or rejected. The objective is to arrive at a single design and specific definition of the building to be constructed. Trade-offs continue.
- Construction documents. The architect and team members prepare drawings and specifications for the final selected design. These drawings and specifications are used to select the contractor to construct the building.

• Construction administration. This includes the construction process itself as well as all oversight, testing, changes, and documentation.

IT must be involved "early and often" in all major construction and renovation projects. In fact, a representative from IT should play an active role in all projects from day one. IT's design role should begin early in the Programmatic phase of a project (what do the occupants want the building to do?) and should be as critical to the schematic and design phases as plumbing, electrical, and HVAC. This kind of early and in-depth involvement ensures that the design will meet the needs of the building occupants and maximize the invested resources.

The major thrust of technology in the design of any new building must be to ensure the provision of the spaces, pathways, and infrastructure required to support high-quality wired and wireless communications throughout the facility. These spaces and systems need to be designed to support present applications and emerging technologies over the lifecycle of the facility. This includes provision for adequate equipment rooms to house the hardware and terminations; conduits, ladder racks, and raceways for wire and cable; and adequate connectivity to other buildings and to networks outside the building. The quantities, types, and technical specifications for copper twisted-pair cabling and fiber-optic cable as well as wireless access points must also be set forth.

The objective is not future-proof design, but the strategic accommodation of change. Despite the fact that technology is finally recognized as an important factor in construction and renovation, and despite the number of years that the telephone company has *not* installed cabling, the architectural community has been slow to grasp the basic design principles. We continue to run into architects who think that everything is wireless and communications rooms can get smaller and smaller.

Isn't Everything Wireless?

One question commonly voiced in association with infrastructure projects is, "Why are we spending money on cabling and infrastructure? Isn't everything wireless now?"

While there is an increasing application for wireless voice and data, it is our view that wireless is an "overlay technology" and not a replacement for wired solutions. Wireless works well for casual access for libraries, classrooms, cyber cafes, meeting spaces, and break-out rooms and for the mobile professional. It offers mixed results in high-density, high-usage applications such as residence halls. And it offers little advantage for fixed office workers, researchers, or those with high-bandwidth applications. For every increase in wireless capabilities, there is a tenfold increase in wired capabilities.

▶

> One cannot assume that the fact that IT services are critical automatically translates into recognition that IT must have a significant role in all new building and major renovation projects.

For example, present wireless data transmits at up to 108 Mbps for 802.11a and the newer versions of 802.11g. Subtracting overhead for collision and flow control, this provides a usable bandwidth of about 60 Mbps. However, this is a shared technology, and the bandwidth is divided among the number of users connected. With 10 users (a small number), the average bandwidth per user would be less than 6 Mbps. Compare this with a wired solution in which the user is provided a *dedicated* connection of 100 Mbps, with 1 Gbps (1,000 Mbps) now available and 10 Gbps just finalized. For accessing e-mail, checking stock quotes, or surfing the Web, wireless is sufficient. However, in educational applications, which often include high-resolution graphics, video, CAD files, GIS applications, and large downloads, one can see that the difference is significant.

Anyone who has had recent experience with the implementation of wireless can tell you that while the implementation is easier (or at least more expedient), problems that occur after the fact can be much harder to solve. User density, coverage overlap, bandwidth, interference, security, and a host of other issues all need to be taken into account when designing and implementing wireless. Like any tool, wireless is an excellent solution in the right application and a failure when applied incorrectly.

Call It the Tel/Data Room

Over the last two years the latest versions of both the EIA/TIA Cabling Standards and the BICSI Telecommunications Cabling Installation Manual have begun to use "Intermediate Cross Connect (ICC)" in place of "Intermediate Distribution Frame (IDF)" and "Tel/data Room" in place of "Telephone Closet." This change in terminology makes it much easier when dealing with architects to get them thinking, early in the process, on a room scale rather than on a closet scale.

Obviously, tel/data room sizes need to be driven by the number of cable terminations in the room and the amount of equipment to be housed there. Given the inexorable move toward convergence, more and more equipment (HVAC control, alarms, CATV, access systems, security systems, etc.) seems to be moving into the tel/data rooms.

We are strong proponents of including communications infrastructure in the Construction Specifications Institute (CSI) specs. However, the issue is not just getting your specs into that format, but getting your specs incorporated into your institution's standard construction boilerplate. The advantage of the CSI Division 27[2] format is that architects and engineers are familiar with the CSI construction specifications and are more likely to take seriously specifications organized that way. This not only legitimizes tel/data in the eyes of architects and facilities managers, it also gives you the chance to establish overall policies on use (no storage or slop sinks in communications rooms) and get the basic requirements for space, HVAC, power, and UPS built into the inherent design requirements. Given that everyone seems to hate "wasted" space (that is, not usable for the building occupants), you can fight your battle once and then just have to tweak the requirements for each building.

In addition to communications spaces and pathways, design must also take into account the various communications systems required to support the activities planned for the building (e.g., voice, data, video, access, intrusion, fire, PA, CATV, environmental monitoring and control). The universal trend toward convergence (in this context, carrying all the systems listed above over the data network rather than over separate networks) should drive the design of spaces, pathways, and infrastructure.

The one shortcoming of Division 27 is that it lumps all technology together and assumes that everything should be part of the building specs. Logically, communications infrastructure needs to be divided into three components: the spaces and pathways, the cabling and terminations, and "what hangs on the end of the wires." The spaces and pathways must be part of the building design and construction; the cabling and terminations may or may not be part of the building specs (we usually prefer to bid it separately but allow the general contractor to respond if so desired); and the network and desktop components really should be kept separate.

Due to the rapid rate of change in communications technologies and prices, and the time between building design and occupancy, we recommend that final decisions concerning specific networking and systems be deferred until as late as possible in the process—certainly no sooner than 9 to 12 months before planned building occupancy. Our approach is to use Division 27 only for the parts of the project the institution wishes to include in building construction.

One cannot assume that the fact that IT services are critical automatically translates into recognition that IT must have a significant role in all new building and major renovation projects. You need to educate everyone involved in these types of projects regarding the role of IT. The message to all involved is this: "Communications infrastructure is vital to the ongoing provision of technology services to this institution. We have spent a considerable amount of money, time, and effort constructing and implementing cabling infrastructure (conduit, closets, and riser systems). Communications spaces must be viewed as a limited, nonrenewable resource, vital to the long-term technological health of the institution. Since this resource must serve ever increasing numbers of voice, data, and video applications, improper design, management, and use of these spaces can waste this resource and make future connectivity unavailable or more expensive."

As a final note, we can thank the upswing in environmental awareness for making our technology infrastructure design activities easier. Recent trends in LEEDS certification and energy conservation have shifted the focus of building design from construction costs to life cycle sustainability. More than anything, this ensures that our message supporting the strategic accommodation of change will no longer fall on deaf ears.

[1] Quality of Service (QoS) is a function of a converged network that allows voice and video traffic (which is sensitive to delay or to being received out of sequence) to obtain priority routing through the network ahead of data traffic, which can be buffered and re-transmitted without loss of information content. QoS is a way of ensuring that the network can handle isochronous traffic at peak periods. The downside of QoS is that it does adversely affect all other traffic on the network.

[2] Originally, communications cabling specifications were usually contained under Division 16-700 as part of the electrical specifications. After several attempts to give cabling its own section, cabling has finally come to rest as CSI Division 27.

Geoffrey C. Tritsch is director of communications technology consulting at Acentech, Inc. – Compass Consulting Division. He frequently presents at ACUTA events and has been a member of ACUTA for 21 years. Reach Geoff at gtritsch@acentech.com.

▼

Good Advice: Clean Out Your Closets (and More)

Ron Walczak, RCDD/OSP, CWNA/CWSP
Walczak Technology Consultants

"A chain is no stronger than its weakest link." This adage can be applied to many aspects of our lives—and to our networks. Networks have many components that must come together to create a reliable and robust platform for the delivery of information and applications to your end users.

Years of travel through telecommunications rooms of clients have provided moments of both humor and outright fear. We have been in closets housing telephone PBXs and data network equipment that exceeded 100 degrees with no air flow and closets that would require a technician to stand in water while working on active electronics. We've seen electrical service to a rack provided by an extension cord that had no plug on the end—just two stripped wires jammed into a receptacle. Many closets would not pass a fire inspection or an OSHA safety review.

Yet the equipment in these rooms (sometimes no more than a janitor's closet) is expected to provide reliable service to business-critical information services. With the reality of voice over IP (VoIP) comes the increased importance of having an infrastructure that is reliable and robust. So here's my advice when it comes to infrastructure:

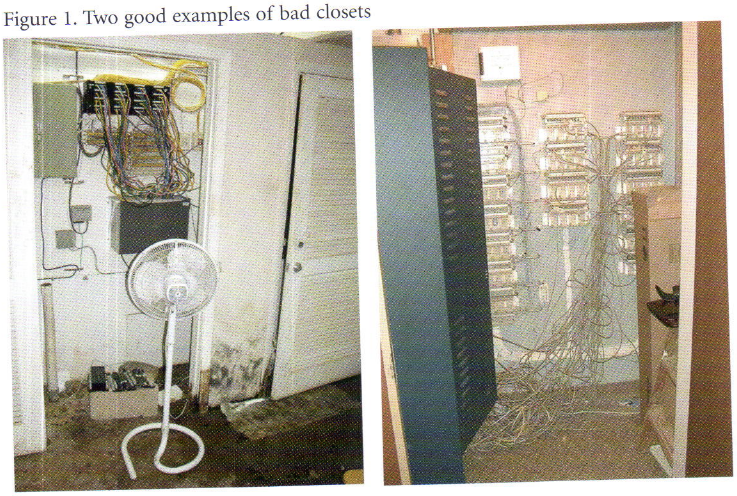
Take a Walk

When was the last time you actually inspected and documented the condition of your telecommunications facilities? Even though you have 200-plus closets, all it takes is one failure to ruin your day. Create a checklist of standards. The first time you complete it, you may be amazed at what you find. Visual inspections will identify the most egregious issues, and that's a start. Here are five points to consider.

1. Conduct inspections.

- Security/safety
  - Working door locks
  - Cameras/intrusion detection
  - Appropriate lighting
  - Firestopping
  - Walls that go to the floor decking above (no drop ceilings that let people crawl into the room from the hall)
- Equipment protection from the following:
  - Water leakage
  - Electromagnetic interference
  - Heat (Is the air-conditioning turned off at 5:00 P.M.?)
  - Dirt/dust
  - Chemicals (I've seen 55-gallon drums of corrosives stored in telecom rooms.)
  - Other people's stuff (Your room is *not* for storing beds and desks from residence life.)
- Electrical systems
  - Are there enough circuits in the room or do you have daisy-chained power strips to get all your equipment plugged in?

Figure 1. Two good examples of bad closets



- When was the last time you checked/tested your UPS? (You *do* have an appropriately sized UPS in each closet, right?)
- Just in case you hope to implement VoIP, will the electrical system and UPS handle the additional load? You may find yourself upgrading the UPS to a 208V unit from a 120V unit.

2. Clean house.

- Racks and cabling should be orderly to facilitate access and changes.
- Equipment should be securely mounted and supported. (Folding chairs are *not* an acceptable method of supporting servers and switches).
- Repeat: The room should *not* be used as storage. People moving stored items present a security risk and can inadvertently bump something that shouldn't be bumped.
- Room should be clean. Dirt and dust get sucked into equipment, shortening life cycles. The best closet design has positive air pressure forcing air out of the closet, not sucking it in.

3. Take pictures.

This is especially important if you have a large number of closets on campus and want a quick reference for each. Photographs will document conditions and help you bring your case to the powers that be (they sure aren't going to go look at your closets).

4. Find out what's in the conduits and manholes.

Do you have accurate documentation of the conduit system? Accurate butterfly drawings of manholes provide you with an understanding of existing facilities and the ability to add capacity across the campus. Assuming you have space can become a showstopper when it turns out the four-inch conduits are really only two-inch conduits—and they're full.

What is the condition of your conduits? Are they properly sealed against water and vermin? Here's a tip: Avoid using "touch-n-foam" expanding foam sealant as a means of sealing your conduits. Contractors get testy about having to dig three feet of expanding sealant out of conduits when its time to pull more cable.

Time to get rid of old and unused equipment and cabling. The 2002 revision to the NFPA/NEC requires you to remove abandoned cabling. Be ruthless: If you don't need it in there, get rid of it.

5. Verify your documentation.

Do your records accurately reflect reality? Now is the time to update campus maps, network diagrams, and capacity records.

Now that you know what you have, you can intelligently start the process of improving areas that need attention and upgrading for planned initiatives.

Upgrade Capacities

The introduction of new technologies and the inevitable increase in demand for power and access mean you must regularly upgrade capacities.

1. Fiber backbone

Fiber is the only media that has not undergone significant technical changes over the years. Operating characteristics of 62-micron multi-mode and single-mode fiber installed 10 years ago will work just fine with today's electronics. The same cannot be said for copper or, now, 802.11 wireless. Fiber provides the fastest and most reliable and secure path for communications, and the price is right.

We have often encountered fiber networks that can be significantly improved with the addition of some links to create redundant loops. The star topology installed by most campuses (and recommended by BICSI) has the defect of lacking alternate path capabilities. Study your physical network. Where can a link or two be installed that would provide a ring—or multiple rings? If you have a network that has buildings daisy-chained, it's time you rethink the layout.

2. Power

VoIP will increase the power draw of your network switches by a factor of five. Phones that used to get their power from a centralized PBX now are fed from your edge devices. Make sure your room has adequate power and air-conditioning to handle the load and BTUs.

3. Wireless

Your infrastructure already includes or will soon include 802.11 wireless technologies. The 802.11 wireless environment has created a plethora of challenges that include adequate coverage patterns, adequate throughput, security, QoS for voice, VLANs, and, most frustrating, interference from other systems.

Despite all the challenges of wireless, your constituents will continue to demand increased mobility, and it will be your job to provide it. The complexities of wireless network design demand a separate article, but for now, remember that this component of your network is increasing in importance while remaining a potential weakest link in your infrastructure.

Ron Walczak is the principal consultant at Walczak Technology Consultants, Inc., and a frequent contributor to the *ACUTA Journal*. Reach him when he's not in a telecom closet at ron@walczakconsultants.com.

▼

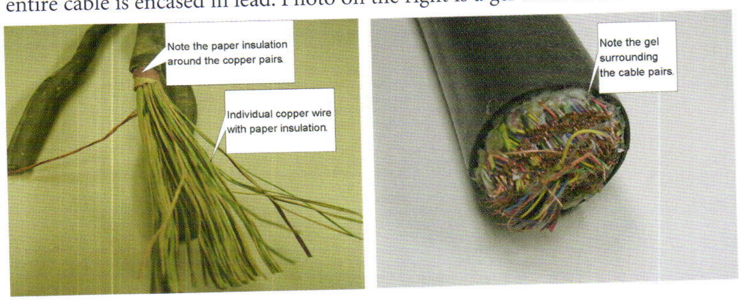
Making Decisions to Remove Legacy Cable

by Ric Simmons, PE, RCDD
Louisiana State University

Like many large organizations, Louisiana State University (LSU) maintains a complex outside plant cable system consisting of copper, multi-mode fiber (mmf), and single-mode fiber (smf) cables. This infrastructure supports a 10 gigabit Ethernet core, approximately 1,500 wireless access points (WAPs), 30,000 network connections, and more than 14,000 telephone stations. Faculty, staff, and students have access to Internet2, the National Lambda Rail (NLR), and, of course, the commercial Internet. In the near future, LSU users will have access to the Louisiana Optical Network Initiative (LONI) network—a high-speed fiber-optic backbone network connecting research institutions around the state, which enables grid computing and other applications.

As a basic utility, the campus network must stay at the forefront of current and future expectations of the campus. For example, within each building our current standard installation guidelines call for two Cat 6 cables and one Cat 5e cable (for voice) to each desktop. Where a 10 Gbps connection is needed within a building, fiber is pulled to the desktop. Each Cat 6 cable is installed to a patch panel set in a rack, and each rack is equipped with a network switch—typically 10/100/1000 Gbps capable. Each network switch array in turn is connected via fiber to an aggregator switch at 1 Gbps Ethernet or, where necessary, 10 Gbps back to the network core. Off-campus locations are connected to the LSU core via T1 or carrier Ethernet service. The same structured inside wiring standards are followed whether a building is on or off campus.

Figure 1. The photo on the left shows a piece of air core paper cable. Each wire is wrapped in paper, and the bundle of cable pairs are wrapped in paper. The entire cable is encased in lead. Photo on the right is a gel-filled PIC cable.



In addition to standard network access for printers and workstations, facility management systems access the network for HVAC control, security camera control and storage, and building security access systems. All of these applications depend upon a solid infrastructure within the building and a solid outside plant cable system. As voice over IP (VoIP) and other applications continue to saturate the campus, our standard installation guidelines evolve to meet anticipated needs.

The cable infrastructure is one of several critical components of the campus network. Although VoIP is more commonplace today than in the past, the majority of the telephone services provided on campus remain traditional POTS service. LSU administration has long recognized that part of the aging copper cable plant needs to be replaced. In evaluating replacement options, we have considered whether or not to install VoIP technology.

The LSU Cable System

There are two types of outside plant copper cable in use on the LSU campus: air-core paper-insulated cable and gel-filled plastic insulated conductor (PIC) cable (see Figure 1 on page 20). The air-core paper-insulated cable is part of a cable system that consists of cable, splices, and air pumps. As the name implies, air must constantly be pumped through the cable system in order to keep moisture out of the cables. The air-core cable is old technology while the PIC cable is newer technology.

The majority of the copper cable pairs are used to connect telephones from around the campus to the LSU ▶

Figure 2. Air pumps Frankenstein and Godzilla pump air 24 x 7 through the LSU copper cable system.

Figure 3. Another part of the air-core system is the distribution panel, which directs air pressure to different cables. On the left-hand side are backup nitrogen tanks, which are an additional backup in case both air dryers fail.

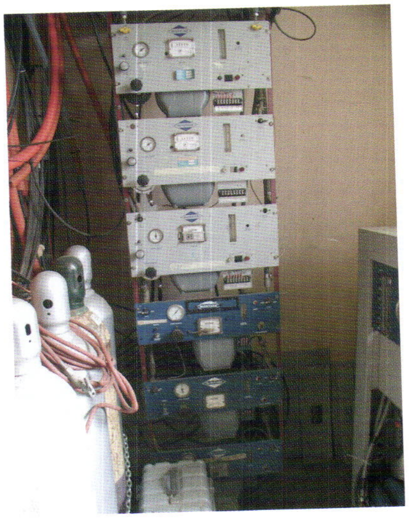


Figure 4. All cables end up at the main distribution frame (MDF). The MDF houses over 30,000 cable pairs from around the campus and is where the local exchange carrier (LEC) drops off trunks and network services to the university.

telephone system. Since the cables are connected to the telephone system, the cable pairs have a constant voltage applied (-48 VDC). If water enters any part of this system, the cable pairs short-circuit, creating transmission problems. Ultimately, the section of cable that shorts must be replaced.

Air is circulated through the air-core cable system via two air dryers (air pumps) affectionately known as Frankenstein and Godzilla (see Figure 2). These two machines operate 24 hours per day, seven days per week. At any given time, one machine is always active—busily pumping air through the cable system—while one machine is in hot standby mode. These machines are expensive to operate from maintenance, electrical, and cooling perspectives.

The other type of cable considered—PIC cable—is gel-filled and does not require air circulation. Gel-filled PIC is commonly used underground, as a thick gel surrounding the cable pairs prevents moisture from entering the cable.

The air-core cables on the campus are approximately 50 years old. At the time this cable system was installed, air core was considered the "in" thing; it was really the only type of underground cable system offered. This type of cable is still in use nationwide. In 1994, LSU had priced a cable replacement strategy at $10 million. This project would have replaced the air-core cables and increased cable counts in buildings already short on cable pairs. This project proposal was put on the back burner as more pressing needs around the campus were addressed.

As new projects and renovations to the campus were proposed over the years, we have taken every opportunity to install gel-filled PIC cable wherever possible in order to avoid expanding the air-core system. However, a large amount of air-core paper cable remain, and both Frankenstein and Godzilla continue to work hard keeping the cables dry.

The Flood of 2000

In the last week of November 2000, a major cable system failed. Baton Rouge was deluged with huge amounts of rain (about 10 inches), and the manholes on the LSU campus filled up with water. The pressure on the underground air-core cables increased, and leaks quickly developed in the cable system. Frankenstein and Godzilla could not keep up with the demand. Approximately 15 air-core cables failed and shorted out due to water entering the cable system. More than 20 buildings on campus, including residence halls, lost dialtone.

At the time, most students at LSU did not come equipped with a cell phone as they do today. Without dial-tone in the residence halls, we were concerned about life safety and immediately began a major publicity campaign informing the campus of what had happened. For the most part, we used e-mail to spread the word since the majority of the buildings were connected to the campus network via fiber. Unfortunately, the university was not VoIP capable as it is today. With VoIP capability we could have deployed phones to key areas.

The cable contractor worked around the clock for two weeks to restore most services to most buildings. In some cases, the damaged cables could not be removed and replaced. Instead, new conduits were installed along with new cables. Damage was so widespread that it was two months before all services were restored to preflood levels. Fortunately, final exams were fast approaching, so the students did not miss their phones too much before leaving for the Christmas break.

Figure 3 shows the distribution panel which directs air pressure to different cables plus the nitrogen tanks which give us a backup in case both air dryers fail.

Moving Forward

Although this event, which occurred in November 2000, reminded us that ultimately we would have to replace the air-core cable, money remained a stopping point. The university continued to install PIC cable for new projects where possible. However, the air-core cable was so widespread that it remained necessary to continue installing air-core cable in some instances, even on new projects.

Staff have continued to examine how we could abandon the air-core cable and consider other options. VoIP was one potential alternative. Several factors have been considered in the process of evaluating VoIP, including the following:

- Power. Whether you're implementing VoIP gateways in the telecommunications room to handle analog telephones and applications, or installing VoIP telephone sets on the desktop, phones need to continue to work when the power is out. This requires more than simply backup power in the specific building where the VoIP service resides; backup power needs to be applied to all routers and switches upstream from the VoIP service.
- Cooling. With a power outage, there is no cooling available in most of our telecommunications rooms. If a UPS needs to keep a router upstream from the VoIP service up during a power outage, cooling must be considered.

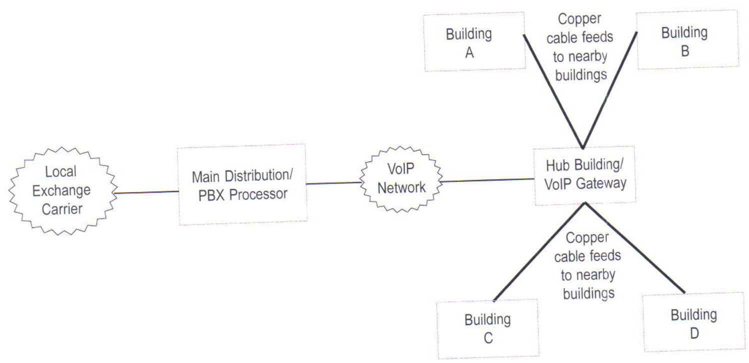
- QoS. Quality of service must be considered from the VoIP phone or gateway through the campus network to the call server.
- Backup copper. We have a requirement in several buildings for services that require copper. For example, some organizations on campus have a T1 from the local exchange carrier (LEC) for a variety of services. We have chosen to transport T1s on copper for several reasons, including cost.

After evaluating costs and other requirements, we chose a two-pronged approach to rid the campus of the air-core cable system:

First, install gel-filled copper from the main distribution frame (MDF) to nearby buildings in place of the air-core cable. For the most part, this approach involves short cable runs with minimum-size copper cable to nearby buildings. The air-core cable originally installed was a large-count trunk cable that fed multiple buildings. As this cable passed a building, smaller copper counts were peeled off and installed to the telecommunications rooms of each building. This new strategy negated the need to install large, expensive trunk cables in lieu of shorter, smaller-count cable runs. (See Figure 4.)

Second, we looked for buildings with large telecommunications rooms that were located near clusters of buildings being fed by air-core cable. We identified two buildings that would act as hub locations to house a VoIP gateway and serve copper cable to nearby buildings. The VoIP gateways were connected to the VoIP network for communication back to the PBX processor. This design eliminated the need to purchase VoIP telephone sets (thereby protecting current investments in electronics and existing telephone sets), sustained our requirement for some copper in buildings, and minimized the need to ensure adequate UPS/generator capacity as well as cooling to every building on campus where a switch or router is located. Each hub building serves anywhere from 5 to 10 buildings. (See Figure 5.)

Figure 5. A typical hub building connects back to the MDF. The hub building serves dialtone and copper requirements to nearby buildings.



Current Status

Godzilla and Frankenstein soon will be retired after serving nobly for many years. By the end of this year, air-core cable will no longer serve any building on campus. This project has positioned us to move users off the air-core cable and onto the gel-filled PIC cable. As stated, we are not ready to do away with our current investment in telephones and equipment andreplace them with VoIP.

We are about to embark on the Network 2010 project (N2010) in order to ensure QoS throughout the campus —something currently available only on a case-by-case basis. N2010 also keeps us ahead of the curve on meeting the expectations of our end users. As we all know, it is vital to take advantage of opportunities as they are presented, and this particular cable project enabled us to take care of a problem before N2010 started.

This has been a long process. We were fortunate in that over the past several years, every decision we made for new projects and renovations around the campus involved eliminating air-core cable where possible. As technology has changed, including the addition of VoIP, more options have become available. We were able to significantly reduce the cost of a $10 million–plus project to under $800,000; protect our current PBX investment; and position ourselves to offer VoIP as we see fit. We're looking forward to having a little less to worry about and more opportunities to serve.

Ric Simmons is director of voice, video, and network installation at Louisiana State University. Reach him at rsimmons@lsu.edu.

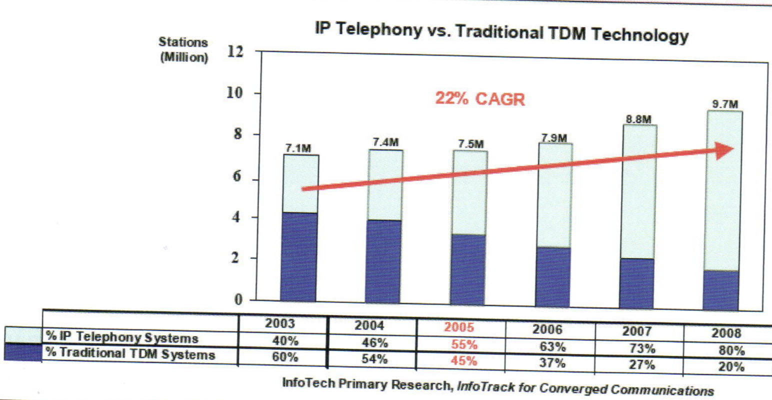
▼

Best Practices for IP Telephony Implementation

by Rod Johnson
Manager, Services Solutions
NEC Unified Solutions, Inc.

Many campuses are considering migration toward IP-based telephone systems. In fact, according to InfoTech, a leading communications analyst group, 2005 marked the first year that the sale of IP telephony systems exceeded that of traditional phone systems. (See Figure 1.)

Figure 1. IP Telephony vs. Traditional TDM Technology



	2003	2004	2005	2006	2007	2008
% IP Telephony Systems	40%	46%	55%	63%	73%	80%
% Traditional TDM Systems	60%	54%	45%	37%	27%	20%

There are many reasons why campuses are considering such a migration, including the following:

1. Lower operational cost
   - Reduced long distance
   - Easier moves, adds, and changes
   - Common infrastructure
2. Improved worker productivity
   - Unified messaging
   - Easier and faster moves, adds, and changes
   - User administration of various changes
   - Remote phone use through IP soft-phones
3. Enhanced IT efficiency
   - Common infrastructure and technology
   - Integration with other network technologies, such as LDAP
4. Enhanced competitive positioning: Reduced communications costs (allow investments in other core initiatives)

Campuses must carefully evaluate reasons for migrating to IP telephony and understand the anticipated advantages. The ability to lower operational cost proves a good example. Minimal savings will be realized in long-distance expenses, but if there are interoffice connections over traditional telephony lines, voice over IP can achieve remarkable savings. Today, the greatest advantage of IP telephony is likely within inter-office connectivity and worker productivity, especially in relation to remote workers.

Once a campus decides to move to IP telephony, an IP telephony assessment is essential. The purpose of an IP telephony assessment is to evaluate the current campus network infrastructure and determine if it is ready to support IP telephony or to determine the changes required to support an IP telephony system. The IP telephony assessment baselines network performance, evaluates network infrastructure for VoIP readiness, stress-tests the network with VoIP traffic, and measures call quality (based on ITU G107 recommendation) and the Quality of Service (QoS: delay, jitter, packet loss) performance of the network. The assessment provides recommendations to configure the network infrastructure to meet the delay-sensitive demands of an IP telephony system with the highest possible voice quality.

Assessments are a critical part of the planning and design of an IP telephony system because voice is a "real-time" ▶

UNM's IP Telephony Migration Pilot and Strategy

by Mark Reynolds
Telecom Operations Manager
University of New Mexico

In an age of rapidly evolving technology, a strategic plan is the best "hedge" to keeping institutions at the forefront of innovation. The main components that allow institutions to complete and successfully accomplish their strategic plan are to identify your direction and intended ROI, create an RFP to articulate your needs, and select a vendor(s) to partner with.

The University of New Mexico has proven to be successful at developing a strategic plan and implementing it to meet the campus's communications needs. The university identified the following criteria as critical when migrating to IP telephony:

- Strategies and goals must be aligned between the telecom and IT departments.
- A network baseline is imperative to evaluate network performance before and after implementation.
- The staff needs to be prepared in advance with education on both the new technology and the products, applications, and services.
- ROI calculations must be considered early in the process to facilitate gathering the correct data during the migration process.
- During planning stages, security must be addressed to avoid creating new vulnerabilities.

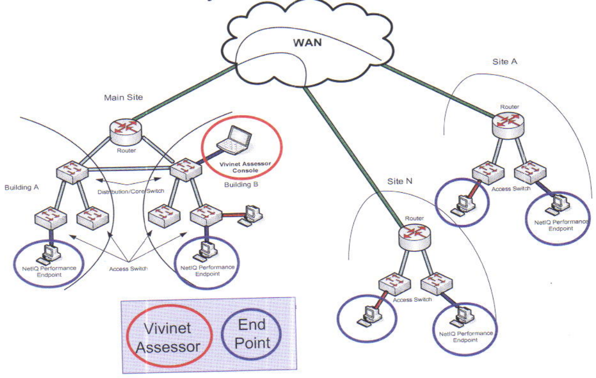
The university is currently using these lessons learned and the experience we developed to successfully upgrade our extensive network.

application; therefore, it's highly sensitive to network delays and other network problems such as jitter (caused by voice packets arriving "out of order," which can cause conversations to be incoherent) and packet loss, which can cause conversations to sound choppy. Poor voice quality can negatively impact higher education revenue through the poor communication experience delivered to alumni, administrators, and students. It is critical that a campus's network be carefully evaluated prior to deploying any type of IP telephony.

A typical IP telephony assessment, as conducted by NEC Unified Solutions, Inc., includes the following steps:

1. Customer Interview / Site Survey
   - On-site interview covering assessment questionnaires designed to catch any potential problems or anything out of the ordinary
   - Site walk-through
   - Network diagramming of components involved in the transport of IP Telephony
2. Network Baseline
   - Place network analyzer on WAN/LAN segment(s)
   - Collect data
3. Call quality & QoS test measurements
   - Load software agents on testing PCs placed at specific locations within the environment
   - Generate VoIP traffic load in accordance with expected traffic patterns
   - Measure call quality MOS (Mean Opinion Score) and QoS statistics
4. Analyze the Test Results
   - Network infrastructure
   - Equipment configurations
   - Call quality/QoS reports
5. Make Recommendations
   - Equipment upgrades (platform, IOS, memory, etc.)
   - Equipment configuration tune-up
   - QoS policy configuration
   - Network architecture
   - Implementation plan regarding recommendations
6. Customer Presentation
   - Provide a detailed written report regarding testing parameters, test results, and recommendations
   - Provide a customer presentation regarding test results and recommendations

Call Quality and QoS Test Measurements



The typical tools used in such an assessment are illustrated by the tool-set utilized by NEC Unified Solutions. NEC uses the most advanced multi-protocol network analyzer and application performance measuring tool-set available from Agilent Technologies, NetIQ, and Ixia. These tools may be used separately or collectively to adequately and objectively identify the current data/voice environment and recommend actions to enhance performance and reduce down time.

In summary, it is important to clearly understand the anticipated advantages to be gained by moving to IP telephony and to thoroughly evaluate the campus's network infrastructure via an IP telephony assessment prior to deploying VoIP. But additionally, since an assessment is merely a *snapshot* in time and networks are always changing, those implementing IP telephony must incorporate into their planning an ongoing monitoring and management solution, which will continually evaluate the network to ensure proactive responses to any voice quality issues that might arise.

▼

VoIP Security: New Frontier, New Challenges?

by Llewellyn Derry CISSP, CISM
Director, Security Solutions
NEC Unified Solutions, Inc.

You're entering a world, not of sight or sound, but of a new state of mind—a world of converged networks, real-time applications, and unprecedented yet equal demand for bandwidth and QoS. Next Stop…VoIP.

You are the IT manager of a midsize university, and it's late on a Wednesday afternoon. Rogue IP phones are popping up across the campus. Someone is "plugging into" your network—you don't know who or where, but they are disrupting normal business operations. Your new VoIP PBX is operating normally, but dropped calls and sporadic dial tones are problematic today. How do you respond when your management console says "all systems go," but your end users say "all systems stop"? As the VoIP Expert on the IT staff, you are dumbfounded… and today feels like your third Monday this week.

Yesterday brought an extremely large PSTN bill. Was it toll fraud? How can you verify who did this? Do you need to call the police or FBI? Was it an inside job, a total stranger, or both? Even worse, is this an international culprit? How can you be sure? (Also, are you liable for those calls?)

The help desk receives calls from the network, but it cannot call out to the network. No obvious reason or explanation will satisfy your end users who disagreed with your efforts to replace their comfortable TDM phone that "worked fine" over the last 20 years. How do you protect and manage against an invisible nemesis? When you ascended into the role of IP Telephony Expert, a Superman cape might have come in handy.

These all represent security issues that cross organizational boundaries. That these problems have already occurred on campuses across this country demonstrates that secure VoIP is not a technology requirement, but rather, a business requirement.

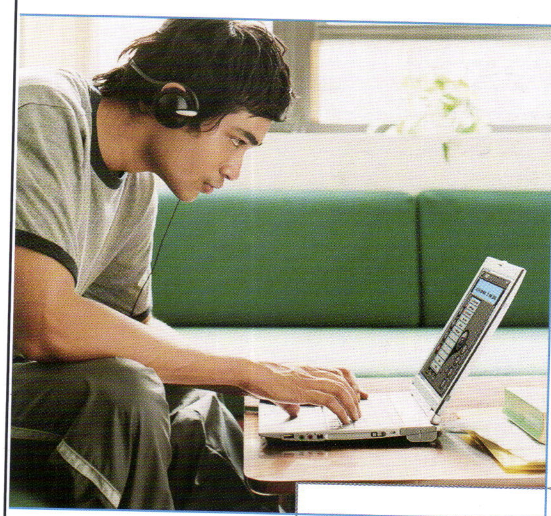
These and even more severe issues can arise and damage the institution's reputation, embarrass the board members, reduce alumni contributions, and possibly cause litigation expenses. Therefore, the entire campus VoIP/data network should be protected from attack, abuse, and negligence by security professionals using state-of-the-art tools, vendor-neutral assessment methods and procedures, and 24/7 monitoring and management services.

VoIP Security Solutions

Security solutions include a thorough vulnerability assessment to avoid the issues described above and the implementation of various tools to quickly detect and mitigate new forms of attacks. Since the Internet is a 24/7 operation with both 0% responsibility and 100% accessibility, the need to monitor Internet-borne activity and IT devices becomes essential for understanding the health and posture of your network infrastructure.

As voice becomes an application on the data network, responsible parties (including IT/telecom management and staff) must understand that VoIP vulnerabilities are similar to data vulnerabilities. Depending upon a campus's structure, it may be beneficial to use independent services to validate your security posture and identify, triage, and remediate vulnerabilities in your IT architecture that can be deliberately or accidentally exploited.

▶

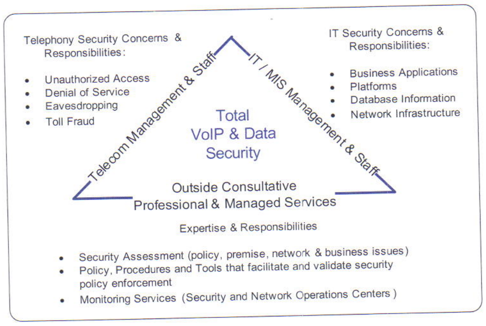


may be beneficial to use independent services to validate your security posture and identify, triage, and remediate vulnerabilities in your IT architecture that can be deliberately or accidentally exploited.

The New Total Security Domain

VoIP solutions are part of the overall voice and data network infrastructure and include the VoIP platform, VoIP applications, and VoIP/TDM gateways, along with preexisting business applications and infrastructure. Figure 1 illustrates a model of how staff and outside managed services can provide risk mitigation and management across your campus IT network.

Figure 1. An end-to-end risk mitigation and management program



If not properly installed and maintained, VoIP systems open a new set of security risks similar to traditional applications and network vulnerabilities. Internal and external attacks may be due to the challenge of breaking into a network (a.k.a. bravado), extortion and/or embezzlement, or a "for hire" model for specific tasks or revenge motives. Also, students themselves may be the source or the conduit of these and other IT security risks.

A vulnerability assessment should be performed periodically to ensure adequate protection has been established and maintained to minimize your campus's security risk profile. Neglecting this form of network checkup marginalizes your campus's exposure to threats from the Internet.

24/7 monitoring of your IT infrastructure highlights the visibility and details of what's happening on your network while you are there, as well as when you are not (after 5 P.M. or weekends/holidays). The growing number of access methods to your network (laptop, PDA, cell phone, Vonage, etc.), underscores that your need to know who is on your network is not optional, it's mandatory.

NEC's Total Solution Provider Methodology brings security professionals and managed services together. These services are available to campuses of all sizes for the express purpose of assessing, monitoring, and managing a campus's IT network security risk posture, and ensuring compliance to and enforcement of your predefined security policy. NEC's security offerings are based upon our best-of-breed tool set, experienced, trained, certified engineering staff at 24/7 NOC/SOCs, as well as our established reputation within the global IT industry. The crossroads of these offerings, matched with 24/7 visibility, enables your campus to focus on strategic projects without expending resources on ad hoc firefighting to defend your network from who-knows-who, coming from who-knows-where. At NEC we pride ourselves on acting as an extension of your staff, open and working 24/7, to protect your IT infrastructure.

Visit NEC online at www.necunified.com/highered.

Austin Peay State University – Meeting the Needs through VoIP

by Jim Spriggle, Telecommunications Manager
Austin Peay State University

More and more universities are evaluating and implementing VoIP on their campuses. However, before determining that VoIP is right for your campus, it is important that a good strategic plan be in place and the right people available for implementation. All justifications, issues, and logistics need to be addressed beforehand as well, such as TCO, deployment strategy, off-campus locations, and crossing state lines.

To be successful in VoIP implementation, these elements should be included in strategic planning:

- Understand your university's purchasing regulations and processes. If your purchasing regulations allow, get an extended pricing catalog which will allow you to purchase extra equipment as needed during and after deployment.
- Ensure that your RFP clearly reflects your requirements and preferences—be sure to state what you want and what you don't want.
- Identify all of the options and alternatives that would constitute your optimal solution—even if you don't implement everything initially, it can still be available for later implementation. Get bid pricing on options and alternatives in case your bids come in lower than expected.
- Build extra time into your project schedule to proactively address any potential delays.
- If at all possible, use an experienced consultant to help evaluate your needs, help write a comprehensive RFP, and help evaluate the proposals.

Austin Peay State University recently and successfully upgraded to a new telephone system which includes IP trunking between three on-campus switches, and a total IP solution at their downtown Clarksville offices and the Fort Campbell campus.

In-Room Phones: Nice or Necessary?

by Curt Harler
Contributing Editor

This fall, Notre Dame will still have its rigorous education. It will still have Touchdown Jesus behind its football stadium. But, effective June 30, 2006, Notre Dame no longer has mandatory telephone service in the residence halls.

"Removing (mandatory) phone service from our 27 residential dorms will affect about 7,000 on-campus students and free up more than $1 million in room and board revenue to be applied to other ResNet IT services," says Dewitt Latimer, deputy CIO and chief technology officer at the University of Notre Dame, South Bend, Indiana.

Notre Dame is just one of many schools making the transition from providing in-room phone service to making it an option. Over the past decade, and for a variety of well-documented reasons, students have shunned college-provided phone service and moved to other providers, mainly cellular carriers.

That leaves open the question of providing emergency services in residence halls and other campus buildings. Unlike stationary systems, cell phones—by nature mobile—are difficult to pinpoint when the user dials 911.

Cellular service is not the only vexing option when it comes to 911 service. IP phones also are quite transportable across a campus and can be plugged in just about anywhere there is a terminal.

Calling 911

John Ourada of DePaul University notes that there are products that provide automated E911 service. "For our administrative implementation, it is a requirement," he says.

"A particular phone number can now appear on different campuses and in different buildings," he continues. "With the current state of the E911 system, location zones would have to be set up unless you had a DID number to dedicate to every single Ethernet port on your data/voice network."

At DePaul, the administrative implementation included setting up three DIDs per zone, with a number of zones per floor of a building.

"The only way for something like this to work is by designating IP address ranges to a zone, which would mean each zone would be its own VLAN subnet," Ourada explains. He gives another option: allowing the system to be able to query the switches to find out to which port a particular MAC address was connected.

Ourada is happy with the solution DePaul implemented. "It works well for our environment so far," he says.

In discussing plans for VoIP at Oakland University in Rochester, Michigan, Theresa Rowe, assistant vice president for University Technology Services, says several options are being considered. Some are making service changes, such as the following:

1. Phone drop but no phone
2. No service at all
3. Campus-only service (house phones)

"Others are keeping services, but making technical changes," Rowe says. Among the options she sees are:

1. VoIP with a "reslife" phone assignment (students' Cisco 7940 phones)
2. SIP phones
3. Analog voice gateways
4. Keeping PBX for the res halls

▶

"We have virtually eliminated traditional MACs. Service calls to the dorms, once commonplace, are nonexistent."

John Turner, Brandeis University

Customer Expectations

When a student from, for example, Cleveland, Ohio, goes off to school in Columbus or Toledo, her main concern is probably cost of calling. She can take her cell phone 130 miles from home and still have local calling in her home areas of 216 and 440. It works just as well if she goes to Philadelphia or Phoenix.

Yet, what is the school's responsibility to get emergency services to her location if she has an accident?

Not to be flippant, Latimer says, but he feels that Notre Dame needs to be ready to give students whatever they want. "It is an end-user and, to some extent, a market-driven service model."

He explains that the change is not as drastic as some telecommunications administrators might fear. "First of all, the only thing Notre Dame is doing is removing 'mandatory' phone services from room and board charges. The business model has been flipped to be an 'opt-in' model," Latimer explains.

"If the student and/or mom or dad feel they really need landline service, then they can 'opt in' and pay semester to semester. Those who truly value landline service can pay for it without penalizing those who don't."

But, when it comes time to put pen to a contract, "My guess is that we won't see many takers," Latimer says.

To ensure adequate cellular coverage and capacity, Notre Dame is deploying a carrier-independent distributed antenna system throughout campus comprised of 10–12 microcells. Two major carriers committed to late-spring deployment for the system.

Still, does the university not have some sort of responsibility or requirement to provide a localized version of universal public safety access?

"If you have a safety or 911 question lurking in the back of your mind, yes, we are putting one or two safety phones per hallway," Latimer says. "Moreover, full-time rectors and assistant rectors as well as the RAs will retain landlines as part of their housing contract," he says.

"Notre Dame's general counsel and our risk management group (two of the more conservative entities known to man) have both signed off that we have not exposed the university to any unnecessary risk," Latimer states.

Ron Walczak, principal consultant with Walczak Technology Consultants, Inc. (www.walczakconsultants.com, Prospect, Pennsylvania), recommends that before any school goes to gateways, it do a cost/benefit analysis of SIP phones versus gateways.

"We are working with a university that will be deploying 100 percent IP, including dorms (1,200 phones), and it will be placing SIP phones in the dorms. Inside plant and outside plant costs should be factored!" he cautions.

Not everyone is as far along in finalizing plans as Notre Dame. But most schools, including the University of Buffalo, are working on the myriad problems. "We haven't decided what to do with the dorms yet," says Mark Deuell. Today analog service is provided throughout the university.

"But few students—maybe 20 percent—even bother to plug a phone in the jack," Deuell says. "They all have cell phones, and we have seen a significant growth in the use of Skype."

Keeping Phones

Not ready to give up his PBX, Bill Lamb at the New Mexico Military Institute (NMMI), Roswell, New Mexico, is considering a sort of hybrid approach. He is considering phasing out having NMMI provide phones as part of the room package. He would rather have the students bring their own phones.

"I know that students mainly use cell phones now," he admits, "but we still provide a standard 2500 analog set in each room. Our switch is a Definity G3Si."

Lamb has pondered the legality of the situation but says he never received a definitive answer about it. "We provide a jack to the wall, but it is up to the student to bring in the phone," he says.

One more immediate concern he has about allowing students to bring their own phones is whether there are potential problems with the telephone switch supporting them.

Paul Valenzuela, associate director and operations manager for communications services in the office of information technology at the University of California, Santa Barbara, does not see that approach as a problem.

"We 'require' students to bring their own phone for use in the residence halls," he says. The university's switch is an NEC 2400 IPX.

"We have so few students who want telephones anymore that supporting the few that they bring is not an issue," Valenzuela says.

Valenzuela has gone through the E911 question pretty thoroughly. Those students who do bring phones and tie into the 2400 automatically are logged into the system, and their 911 services work just about the way they always did.

"They subscribe to my service. I'm responsible. We have their locations mapped. It's a piece of cake," Valenzuela says.

911 Cell Calls

Not so straightforward is dealing with those students who bring cell phones from home. The office of information technology has made a real effort to show, on its website, all of the carriers who serve campus. Santa Barbara is a fairly rural location, so not all carriers provide equal levels of service. The webpage tells which carriers have the best service in which areas of campus.

However, no matter which carrier a student selects, all cell-phone-based 911 calls from the campus do not go to the university police. Rather, they are routed to the California State Police. "We tell them that right up front," Valenzuela says. "But nobody has ever said 'no' to cell-phone service based on that."

A good working relationship between the state police and the university is a big boost here. "We have a lot of good interjurisdictional support," Valenzuela says. The state police are very good about transferring calls to the right department on campus, he adds.

That provides peace of mind, both for the users and for Santa Barbara's office of information technology.

Joe Morvan, director of user services at Norwich University, Northfield, Vermont, agrees with Valenzuela that support for students' phones is not a major hurdle. Like UC Santa Barbara, Norwich requires students to bring their own phones.

"There are occasional issues such as your 2.4 GHz phone interfering with my 2.4 GHz phone, but overall it works well for us," Morvan says. "Students have such varied tastes in telephones that it's just easier to let them bring whatever they prefer."

He reports that they have not had any compatibility issues with their Siemens PBX.

"I would not say that troubleshooting is simpler, but tracking the cost of repairs is easier since we eliminated telephone sets from the picture completely," he adds.

At Brandeis University, Boston, the decision was made to give all students Cisco 7940 phones. "Use is not mandatory," emphasizes John Turner, associate director for networks and systems at Brandeis, "but they are financially responsible if the phones are lost or stolen. We offer a 7940 to every single student on campus.

"I would guess that about 85 percent or more take a phone," he continues. "We have only had about two or three in almost three years that were lost."

At Brandeis the phone number is assigned to the student, and it stays with the student for all four years. The phones can be plugged into any power-over-Ethernet (PoE) jack on campus.

The heart of the emergency response network at Brandeis is the Cisco Emergency Response (CER) system. Every one of those PoE jacks across campus is mapped with either a building location or room number.

Anyone who dials the internal emergency number or 911 is immediately linked to the on-campus public safety office. "The call appears with the caller's room number and location," Turner explains.

Brandeis has its own on-site medical response team. However, if the call requires help from the community police or emergency units, the university's campus public safety office has a direct line to town. They also share the same radio frequencies.

There are other benefits to the unified phone system. "With VoIP the students do their own moves. They take their phones with them over the summer and bring them back to their new rooms," Turner explains.

In the fall, the university hands out phones to new students. Turner's people program them on the fly with a bar-code reader and a special application written specifically for that use.

"We have virtually eliminated traditional MACs [moves, adds, changes]," Turner says. "Service calls to the dorms, once commonplace, are nonexistent.

"We have about 10 VG248s and have been reasonably happy with them, but we still have copper problems that require troubleshooting," he continues. "My hope is to get that number WAY down or deploy them in buildings with generators."

One school that is in the process of a 100 percent switch to VoIP is South Plains College, Levelland, Texas. Tim Winders, associate dean of information technology, says, "When that migration is complete (approximately 600 phones), I will revisit the dorm situation. At this point, we are planning on keeping the PBX to use solely for the dorms, but it might make more sense to completely retire the PBX and move toward analog voice gateways."

Like others, Winders says it is unreasonable to expect students to evacuate their residence hall room in case of a power failure. "We sure don't," he says.

South Plains College has not decided what to do with the residence halls yet. "Today we provide analog service but few students (20 percent) even bother to plug a phone in the jack," Winders says. "They all have cell phones, and we have seen a significant growth in the use of Skype."

Canisius is heading along a path that will lead to the retirement of its old 9751 PBX. "The new dorm was the latest and greatest, so I had to offer telephone service," says Frank Kirstein, director of network services.

"Before the new dorm was built we 'tested' the idea of no phone lines (except in the halls or for those who wanted to pay extra) and got an earful," Kirstein says. He says they had some experience and problems with the VG248 in another location (emergency phones, alarm voltage that ran low), and thus opted to use the VG224.

"So far, so good," he says of the VG224.

Conclusion

Even as the method of providing services changes, most campuses appear to be able to provide the same emergency and 911 service they always have offered. Many have found added bonuses when they offer alternative services. That scores points for everyone.

Curt Harler is a freelance writer and frequent speaker who specializes in technology topics. He is also a contributing editor for the *ACUTA Journal.* Reach Curt at curt@curtharler.com.

▼

Voice and Network Department Convergence

How to stay afloat when IP telephony comes to your neighborhood

by Peggy Fischel
Middlebury College

A successful IP telephony project requires the cooperation and collaboration of the voice and network staff. Many who have been through the process of implementing voice over IP (VoIP) observe that the technology is often easier than the human side of the equation. If your campus has not yet gone through departmental convergence, here are a few lessons learned by some institutions that have.

Bryant University Works from Within

Richard Siedzik, director of computer and telecommunications services at Bryant University in Smithfield, Rhode Island, believes that one of the challenges of departmental convergence is getting the two groups to talk the same language and learn from each other how to approach an issue.

"The data side is used to e-mail and Web applications," Siedzik says. "The technician would go in the closet and change a cable and not adversely affect either application. But with voice, they can no longer just change the cable without first considering the implications."

To help overcome some of the differences in perceptions between the groups, Bryant's telecom staff were included very early in meetings that discussed data/networking security and operating systems upgrades. According to Siedzik, "This occurred six months prior to our VoIP project approval. Together, the voice and data staff received shoulder-to-shoulder training throughout the project."

In addition, more formalized training developed by the university's VoIP partner was done in-house over an intense six-day period. Siedzik feels it is important to do this in a nonsterile, real-world environment where knowledge transfer between the groups and the partner takes place more comfortably. Once the system went live, the voice staff began taking over many of the functions that the network staff had performed before.

In retrospect, Siedzik would have done more to prepare the data side for some of the changes the new system brought. He had conditioned the telecom side to be ready for change and a new way of operating. Siedzik also feels it is important to do the same with the network staff so that preparatory matters, such as a network assessment, are welcomed and not met with skepticism.

In the end, though, Siedzik believes that staff on the data side have more of an appreciation for voice. There is a heightened awareness and understanding of the critical nature of voice applications.

The six-person telecom and network staff is now integrated, and Siedzik believes that the distinctions between ▶

the two former groups will eventually disappear. Bryant University, with an enrollment of 3,200 students, is a useful departmental convergence model for any college or university that has similar staff numbers and skill sets.

Swarthmore Seeks a Partner

Swarthmore College, with 1,450 students and limited staff resources, solved its convergence issue by actively seeking a strong relationship with its partner vendor. According to Mark Dumic, associate director of networking and telecommunications, as the college sought bids for a new system, "Our primary factor in choosing a bidder became the capabilities of the maintenance provider and its willingness to be flexible in working with us. We also realized that we had a preference for a local reseller with whom we could establish a close relationship." During the bid process, the team found few resellers with both strong voice applications and networking support experience, and finding one that had those combined strengths was central to Swarthmore's goal.

"In the past, we had complete responsibility for running our own network—which we did fairly well," Dumic says. "But the two people involved with the network have to cover a wide spectrum of activities. We don't have the luxury of maintaining the kind of expertise that certified, full-time network engineers bring to the table. One of the big positive changes made with our new arrangement is that the 24 x 7 monitoring and maintenance of the campus network is also covered by the contract."

Dumic notes that, typically, many smaller organizations outsource the PBX maintenance and manage the campus network internally. He refers to this arrangement as a vertical split. Swarthmore instead did a horizontal split by outsourcing the monitoring and maintenance of both the campus network and voice system. This provides access to specialized technical resources to draw upon for hardware failure issues and for more project-oriented network activity requiring specialized knowledge that is impractical to develop internally. Swarthmore's three-person system staff can now concentrate on activities that require an on-site presence, including network planning. Swarthmore co-manages its systems with its maintenance provider, and both have administrative access. This provides them the flexibility of using the best and most cost-effective resource for each task.

Since the staff involved with the new VoIP system was small, little restructuring took place. The telecommunications position was already part of the ITS department. Both the telecom and network administrative staff members are now support for each other and attended vendor training together.

Penn Builds a Team for Open-Source Environment

The University of Pennsylvania, an institution of 20,000 students and 17,000 faculty and staff members, is in the midst of an ambitious project to replace a Centrex system with open-source IP telephony, with approximately 35 staff members working on the VoIP project.

According to Michele Narcavage, voice services project leader, one of the major challenges was bridging the organizational gap. Putting together such a large, diverse group of people who spoke different technical languages was daunting.

In the early stages, the VoIP project team was small. Narcavage was the voice person selected to work with Steve Blair, the data engineer on the project. "Some of the early conversations must have been comical when observed by our coworkers. Steve and I handled one misunderstanding at a time, and it continued until we hit a level playing field, at least in terms of acronyms and definitions of technical terms," she said. With entirely new concepts to absorb, she and Blair taught each other a great deal.

They were willing to work and learn from each other, Narcavage said, and without that drive the project might have failed early on. "There was a huge amount of give and take. Some days were frustrating, as almost everything I touched was new. We ended up with a profound respect for each other."

After the initial phase, the two began cross-training the rest of the staff involved in the project. "Everyone attended an initial course that simply covered the basics of networking and telecommunications. That really helped kick-start the understanding among everyone that we didn't speak the same language, but it also provided a realization that there is a lot of expertise on both sides of the department," Narcavage said. "At the same time, it forced us all to be in the same room at the same time." Regular group meetings were held to explain the merger process, and later to build teams and brainstorm.

One of the critical lessons learned from the project was developing the knowledge-transfer process, but she cautions that this process takes time to properly develop. Sharing information with the entire project team—from the developers to the network operations center staff to the communications team and the customers—is necessary for success.

Having been a phone-oriented person for many years, Narcavage initially brought to the project her normal work philosophy: "Let's fix it first, then figure out why it didn't work." But in the VoIP world the impact of a decision may reverberate. Narcavage and others quickly learned that a wider range of staff must be consulted, for instance, before a patch is installed or a server rebooted. The consultation and communication point becomes even more important if the organization is creating its system in-house, such as Penn is doing. The development, testing, feedback, and documentation procedures in an open-source environment require people to rethink the way they function day-to-day.

As Narcavage points out, "The process itself is not new, but the list of stakeholders involved has changed. People need to be willing to reconsider decisions and make adjustments."

While the Penn team is now fully integrated, they continue working on integrating some of the service and delivery processes. Responsibilities among the former voice and data staff now overlap to a great degree. Narcavage says she's proud of this integration, believing the staff deserves a lot of credit for being willing to learn, but also ready to change day-to-day thinking, where appropriate.

Middlebury Contemplating Change

Middlebury College is in "preconvergence" mode. The PBX is maintained by an outside vendor, but the network is primarily self-maintained. Consequently, there is a disparity in the number of staff and the technical skills. As the college migrates toward VoIP and other emerging communications technologies, it plans to use its internal knowledge base and some combination

▶

of strategic consulting and outsourcing.

While voice and network systems are still administered separately, the staff of both groups are in the same department. Thomas Cutter, area director of systems and infrastructure, heads up this new combined area. He is enthusiastic about the efficiencies convergence will bring, new applications, and uses yet to be imagined. These advances are only possible with a converged communications infrastructure and staff.

"We are moving from a past that had a distinct separation of duties and even separate management and reporting structures," says Cutter. "There are some history and differing cultures that present unique challenges, but both sides need to understand each other's points of view and work toward outcomes that are the best for all involved and the institution as a whole."

Cutter believes that some of the responsibilities of existing telecom, server, and network staff will be modified as they work ever more closely together. To that end, his desire is to encourage greater staff development and teamwork now to prepare for the future.

Conclusion

The experiences of the staffs at these four schools indicate that there is no one way to build voice and network department convergence. It is clear, however, that the earlier the two groups start talking and working together, the better off they will be long term.

Geoff Tritsch of Acentech – Compass Consulting Division believes that the culture of the organization also plays a critical role in the success of convergence. He says that typically organizations take existing staff and reallocate, retrain, and cross-train, or some combination. Tritsch asserts, "Cross-training has to work." Each organization must find a way for it to work. However, it does largely depend on the people and how they are managed. Tritsch continues, "If they are interested and excited about new opportunities, and if management is supportive, it will work. If you get the 'that's not my job' attitude, you have a problem."

Tritsch comments, "Though IT has won the technical battle of VoIP, telecom has won the business model battle." While current telecom staff needs to learn about routers, switches, port status and the like, the issues of customer service and support remain telecom's strong suit.

At the ACUTA Spring Seminars in Providence in April (where representatives from the schools discussed in this article made presentations), the benefits of VoIP were the topic of an open discussion. When participants were asked to identify the biggest challenges that VoIP brought to the campus, the list of five included the following:

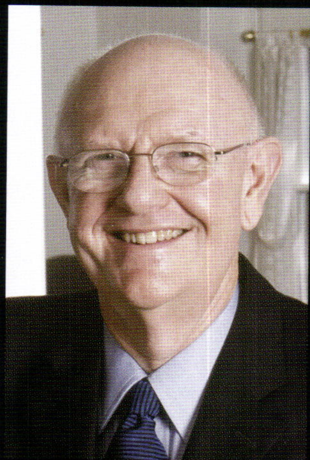
- Changing the support model: converging help desks
- Redesigning workflow and trouble-shooting checklists
- Supporting triage arrangements
- Handoff to the vendor
- Training staff

These will likely be key administrative areas of emphasis for many of us as we modify our way of doing business.

Convergence is not easy, but the commitment of everyone involved can make a difference. When staff with different skill sets come together, ideally they learn to appreciate each other's abilities and what they can contribute to the project. As important is that everyone knows what he or she will be doing once the system is cut over. Providing a stable work environment and telling people what to expect before you transition them and your systems will pay off. As these examples illustrate, the right combination of cross-training, knowledge transfer, and inspired management do indeed result in an integrated team.

Peggy Fischel is manager of telecom services at Middlebury College in Middlebury, Vermont. She can be reached at fischel@middlebury.edu.

▼



As the 16th chancellor of the University of Kansas, Robert E. Hemenway is the chief executive for the university, which spans the main campus in Lawrence, the Edwards Campus in Overland Park, the Medical Center campus in Kansas City, and its clinical branch in Wichita.

Since coming to KU in 1995, Hemenway has streamlined KU administration, made the university more student-centered, and overseen KU's growing national reputation. Under Hemenway's leadership, KU has set a goal to be recognized as a Top 25 public university within the next five years. A growing list of nationally ranked academic programs and achievements of faculty and students support this goal.

Research funding at KU, a major source for Kansas economic development, has climbed steadily, reaching a record $274 million in fiscal year 2004. KU students win several of the nation's most prestigious awards every year, including the Rhodes, Goldwater, Marshall, and Udall scholarships.

In Kansas, Hemenway has performed a complex balancing act, positioning KU as a major player in the movement to make the Greater Kansas City area a national center for life sciences and information technology, while at the same time forging stronger connections with the rural counties of western Kansas.

Interview

Robert E. Hemenway, Ph.D.

University of Kansas

ACUTA: Some say campus IT infrastructures are now more of a commodity and have diminished in strategic importance. Others say IT is more of an integral part of the delivery of education than ever. Which position do you take, and how do you see IT becoming a greater contributor to the educational mission? As the chancellor and chief executive, what do you see as the unique challenges for IT at a university that spans multiple campuses and includes a medical center?

Hemenway: An increasingly frequent and essential aspect of leading the university is engagement with technological leaders on matters relevant to our educational mission. I confer periodically with our Chief Information Officer, Denise Stephens, on issues and challenges driven by the influence of IT and the criticality of the network to the work of the University of Kansas. My perceptions are influenced by what I continue to observe and learn in this area.

The basic services have, indeed, reached a commodity state. However, the deployment and customization of these services still holds importance for the higher education environment. Researchers are now able to access equipment, laboratories, and data from new sources. Additionally, they are now able to collaborate and share their findings, often in real-time with their peers. Students have a more ubiquitous access to class materials than ever before. Whether in the classroom, the library, or their dorm room, students can connect to whatever resources are required.

When interconnecting geographically dispersed campuses, it can be difficult to offer the same online experience at each location. Fundamentally, we are challenged with the need to maintain some services centrally, while addressing the need for specialized resources and interfaces across campuses. KU is one university. Still, like other multi-campus institutions, we face complexity in both our diverse, distributed programs and in our approach to providing effective technology solutions. This is especially true in the case of a medical center, where heightened security measures due to federal regulations are a must.

ACUTA: What role does the basic campus infrastructure play in helping KU attain its goal of being a top 25 public university within the next five years?

Hemenway: From the standpoint of telecommunications and the network, advances in wireless will allow students to be more mobile and have access to information wherever it is needed. Advances in the wired network will allow KU to connect to and participate in research initiatives taking place across the globe. Advances in content delivery will allow instructors to use rich media more effectively in the classroom (whether physical or virtual). Our people will have greater access to the tools and data resources they need to be productive ▶

from wherever they are. The convergence of voice, data, video, and applications over networks is where the future is rapidly taking us. Our intelligent and innovative deployment of these capabilities will help make KU a leader technologically, as well as instructionally and in the research arena.

ACUTA: With frequent news reports of both malicious and unintended information security breaches from all over the spectrum, is there a role for higher education in developing national policy initiatives to protect our critical infrastructures such as telecommunications and information technology? If so, what will it be?

Hemenway: As a frequent target of such attacks, educational institutions are in a key position to learn from these attempted incursions. As a community, we have had to quickly ramp up our technology security knowledge and institutional protocols to safeguard institutional data resources and to minimize the risk to our people from cyber harm. All universities invest in securing their technology environments as an operational necessity—and we are learning a great deal. With this vast and growing experience at its disposal, the higher education community is in a good position to recommend how to best defend against digital hostility. Campuses are much like small cities. They are complex places where the need to bring both understanding and change is constant.

ACUTA: After events such as the devastating storm you experienced last spring, there are opportunities to learn and make changes in order to be better prepared and to weaken the impact if another similar event were to occur. What key lessons did KU learn, and how has that affected your prioritization of activity and resources? Were there pleasant surprises that enhanced the recovery efforts?

Hemenway: We are working toward minimizing our vulnerability to power surges or loss. Previously, it was assumed that redundant feeds, one from each side of Lawrence, would be sufficient to supply power to the critical infrastructure. However, we lost both feeds in the March 2006 microburst event. We've also experienced other less dramatic power events since then. As a result, we are making significant investments to our power infrastructure with added emergency power for our data center and at other critical locations on the KU campus.

The identification of the most critical services has allowed us to prioritize and to conserve resources in times of emergency. By focusing on maintaining a smaller subset of services, the crisis becomes more manageable. Further, recovery efforts are focused on these critical services, allowing the university to return to a productive state more quickly. During the damaging storm event in March, we successfully brought up the network and all services within 12 hours. If another event like this one occurs, we hope to have even better recovery time.

ACUTA: Does KU have a current business continuity plan, or will you be developing one? Will/Did you manage this in-house or call upon external expertise to integrate with your campus personnel? What methodologies are in place for formal plan review and refresh to ensure the plan's viability? Following the storm, what immediate actions were taken to assess the damage and put forward a plan for recovery?

Hemenway: KU has an emergency operations plan and had begun work to revise its existing emergency response plan prior to the storm in March. Based on what we learned from that event, the plan is being further improved. Our computing services developed a technology-specific continuity plan with expert outside consultants and knowledge inside assistance. It is reviewed every six months, and a "table top" exercise was being considered at the time of our last disaster. While it gave us an excellent starting point, there were weaknesses found that have been addressed.

During the storm event, our Emergency Operations Center was assembled, and essential staff from across the university were on site and in action very soon after the event. Damage reports came directly to the EOC, and recovery efforts were directed from there by key university personnel. We had regular monitoring and updates on the telecommunications situation, which played a large role in getting the university back on its feet.

ACUTA: How are priorities for infrastructure technologies established and implemented for short-term needs versus long-term goals? How are funding mechanisms established to support the levels of prioritization?

Hemenway: Basic technology refresh is being introduced as part of our funding model. This captures the funding necessary to move to newer generations of hardware and software in the existing systems. For investments into different technologies and services for the campus at large, the university administration is called upon for funding assistance. Individual departments are also free to fund new services if they have a unique need.

Long term improvements are essentially major priorities that require planning and a fresh look at how major capital projects can be implemented in a timely way, given the real world fiscal limitations faced by all universities. The short life span of the communications infrastructure (requiring frequent refresh or replacement) forces us to think aggressively about the future in order to maximize our institution's scholarly, research, and productivity gains through technology investment.

ACUTA: How does KU work with the community in the provision of services, and how does that impact the decisions you make on the development of your overall infrastructure?

Hemenway: Many functions within our Information Services division operate as cost-recovery units, and therefore charge for the services they provide. The service subscription level directly drives how much money is put into the infrastructure. Onetime funding is also used to execute specific network-related projects that address current needs, or facilitate near-term infrastructure improvements. Other services are funded centrally. These groups hold assessments within the user community periodically to check their effectiveness and rely increasingly on regular user engagement to anticipate communications technology needs.

ACUTA: Wireless technologies are bringing new strategies for all facets of operation from disaster preparedness to everyday voice communications. In what ways do you expect wireless technologies will impact the education and the administration at KU in the next couple of years?

Hemenway: Wireless holds the greatest potential for significantly changing how the infrastructure is used. As wireless speeds increase, it becomes possible to run more bandwidth-intensive applications, even video. As wireless coverage grows, students and researchers alike will have the ability to go where it is convenient to conduct work. Cellular is adopting data capabilities just as Wi-Fi is adopting voice capabilities, further converging these previously distinct networks. Not only will students be able to move freely about campus with access to their academic systems, but soon they will also have the freedom of roaming anywhere with the same level of access.

Students are not the only likely beneficiaries of expanded wireless capabilities. Faculty increasingly use wireless in teaching (podcasting) and for generally enhancing communication with students. Staff and administrators will continue to adopt these technologies to promote time management, decision making, immediate response to issues, and the real-time management of institutional assets in the field or on the road.

ACUTA thanks Dr. Hemenway for taking the time to share his thoughts and insights with us on this important topic. Learn more about KU when you visit their website at www.ku.edu.

▼

Making Communications Accessible

by Paul Spicer
Spicer & Associates
Debra Ruh
TecAccess

On the last day of Sean Stapleford's junior year in high school he dived into the James River—and broke his neck. The year was 1972, and he was paralyzed from his shoulders down.

Today he lives in the Virginia Home, an adult residential-care facility within eyeshot of Byrd Park, in Richmond, Virginia. The park contains three lakes and teems with children, wildlife, and picnicking city dwellers.

Inside his home, Stapleford skillfully operates a "mouth stick" to navigate his computer screen, jumping from website to website while communicating with others using a host of assistive technologies. A computer monitor, suspended from an overhead swing arm, is mounted on his headboard, and an environmental control unit (ECU) operates as a universal remote control—accessing his TV, VCR, stereo, phone, the nurse call bell, and his electric bed.

Despite limited use of his hands, Stapleford can press keys, turn pages, and operate switches and speakerphones with ease. This ability to navigate the world of technology has allowed him to experience meaningful recreation, socialization, employment—and education.

In recent years advancements in electronic and information technology have helped Stapleford and others around the world become more integrated into day-to-day life. However, it wasn't always that way. A long rehabilitation process followed Stapleford's high school accident. He spent a year and a half in the early 1970s being rehabilitated, learning to operate a motorized wheelchair, and continuing his education.

Stapleford was trained in, among other things, computer science, binary and hexadecimal number systems, and other fundamentals of computers. He also learned to operate electric typewriters and computer terminals using a mouth stick, a lightweight wooden dowel or metal tube with a plastic mouthpiece on one end that was held between the teeth, and a rubber tip at the other.

Now, working for Richmond-based TecAccess, Stapleford telecommutes each day from his room at the Virginia Home. He is taking advantage not only of a recent move toward telecommuting in the government, business, and educational sectors, but also of a general push throughout the world to make technology more accessible to disabled computer users and the elderly. As many advocacy and technology experts agree, we build ramps and elevators in lieu of stairs, so it's high time we made electronic and information technology accessible as well.

How Does This Affect Higher Education?

According to the 2000 census, more than 20 percent of the 281 million people in the United States have functional disabilities. More than 56 million people with functional disabilities in the United States earn $1.2 trillion in income and have more than $175 billion in annual discretionary income.

What this means is that people with disabilities are fast becoming a very significant portion not only of the technology market, but also of the growing e-learning landscape. With increasing disposable income, advancements in assistive technology, and the desire to further their education, students with disabilities are likely to be part of your next online classroom.

Understanding how best to use assistive technology is a crucial step in accommodating this growing student base. To help make this happen, TecAccess and Stapleford's team of accessibility experts are currently collaborating with such institutions as George Washington University, the University of Kansas, Oklahoma State University, and Virginia Commonwealth University.

While many schools are following their lead, there are still many institutions that have not taken the simple and cost-effective steps to make education inclusive for all. In fact, according to a recent study by the National Center for Education Statistics, 95 percent of postsecondary institutions use the Web to offer distance education, yet only 18 percent of institutions make the content accessible to students with disabilities.

While there is no magic bullet, accessible design is a very real possibility when a number of basic steps and factors are considered, as evidenced by these institutions. Stapleford and TecAccess are proving that the concept is not difficult.

Here's How They Do It: Best Practices in Telecommunications

For many people with disabilities, access to basic telephone service is still nothing to take for granted. People who are deaf, hard of hearing, or speech-impaired cannot use the voice-based telephone system. Telecommunications relay services are now developing to address some of these needs; yet they are a type of technical Band-Aid, requiring the user to first acquire an extra device (text telephone or telecommunications display device) and then communicate through an operator to another party. Many text telephones use Baudot code, an extremely slow mode of transmission. Technologies are now emerging that could eventually replace this system.

There are nontechnical barriers to telecommunications as well. For example, people who use text telephones have little assurance that they can communicate with educational institutions and government offices, even those that are listed as having text telephones. Workers, who are often untrained in text telephone use, hang up the phone because they don't recognize the sound of a text telephone call.

Other telecommunications considerations include the following:

- Nonproprietary standard signal protocols. Telecommunications systems must transmit in Baudot code at 45.5 baud or in ASCHII at 300 baud. These two protocols are nonproprietary, which implies that they are not part of a product's standard functionality.

▶

• Interactive voice response system. Interactive voice response systems (IVRSs) pose a definite obstacle to TTY users since they cannot hear the options provided. Voicemail also has to be accessible to TTY subscribers who want to check their voicemail boxes.

To render accessibility, special software can be applied to IVRS so the user can recognize TTY tones. Another technique is to route TTY calls. The IVRS presents a voice message followed by a pause and then TTY tones. The hearing caller is thus routed to the audio prompts while the TTY caller is routed to TTY prompts. A third method is to have two interactive response systems—one for hearing callers and another for TTY callers.

• Time response. Individuals who have cognitive or dexterity impairments may not be able to complete a phone transaction quickly enough since they may have difficulty accessing the telephone buttons. TTY users who call through a TRS also may have problems since the calling assistance may not have enough time to relay the caller's message on to the answering system. Therefore, alerts should be provided on the IVRS asking users if more time is needed.

• Caller ID. Persons who have vision or other impairments may be unable to read caller ID information on liquid crystal displays (LCDs). To resolve the issue, voice caller IDs should be implemented. Until recently, caller IDs also presented an obstacle for TTY users, who could only use analog phones. However, new telephone systems are TTY compliant.

• Adjustable volume. Persons who suffer from hearing loss have difficulty comprehending words, yet they are sensitive to loud noises. Therefore, telephone systems must have adjustable volume controls with the intermediate setting at 12 decibels (db) and a maximum setting of 20 db.

Best Practices in Video and Multimedia

• Caption decoders. Captions are written text that appears on the bottom of a monitor or computer screen. They reflect dialogue being spoken during a presentation or program and sound effects, such as laughter and off-screen noise. Captions benefit individuals who would like to learn another language as well as those whose hearing is limited.

Captions can be open or closed. Open captions appear automatically on the screen without viewer selection, whereas closed captions only appear when the viewer selects them. To enable closed captioning, the multimedia product must come with a decoder.

Analog and digital televisions, along with computer screens, must have closed-caption circuitry. However, analog screens that are 13 inches or less and digital screens that are 7.8 inches or less are not required to have decoding capabilities.

• Audio descriptions. An audio description of a video presentation enables individuals who are blind to experience the visual content. Audio descriptions are synchronized with the presentation's soundtrack. Portions are narrated at points where otherwise silence would occur naturally.

Audio descriptions usually are broadcast through the secondary audio program (SAP) feature of stereo televisions. SAP enables each channel to have a secondary audio channel where audio descriptions or foreign translations of the channel's programs may be transmitted.

• User selection. Televisions and other multimedia systems that have closed captions should provide user-selection features. Viewers can select or deselect the features and choose the position of captions. Since these options are presented through a menu prompt on the screen, an equivalent audio prompt should accompany the visual one.

• Self-contained products. Self-contained products are technological systems that have embedded software. Examples of such systems include copiers, calculators, fax machines, and printers. Persons with disabilities must be able to access and operate self-contained products without connecting assistive technologies, such as a screen reader, to the systems. Examples of accessible self-contained products include printers that have easily reachable controls and fax machines that have identifiable buttons. However, assistive technologies such as mouth sticks and head pointers still can be used without attachment to the products.

• Timed response. As with webpages and telecommunications products, self-contained products often have functions with timed responses. If a user does not enter a fax number within a certain amount of time, for instance, the fax machine disconnects. This scenario may occur frequently with persons who have dexterity impairments.

Self-contained products must provide alerts that the time for an interaction to be completed will expire soon. An option also must be given for extra time.

• Controls and keys. Besides telecommunications products, self-contained systems also should have controls that are tactilely discernable and operable with minimum effort. A good example is a touch screen where an area does not have to be pressed for a certain period in order to be activated. Furthermore, the controls should have audio and visual indication when they are selected or deselected.

- Biometric forms of identification. Biometric forms of identification or control are prints of an individual's physical aspect, such as a fingerprint or a voiceprint, that are implemented as security measures.

Persons with disabilities may not be able to access such self-contained systems biometrically. For instance, a person with cerebral palsy may not be able to hold a finger on the screen so a print can be taken. In those circumstances, the system must accept a non-biometric alternative (e.g., a personal identification number).

- Nonproprietary audio signals. Users must be able to manipulate audio output on information kiosks in schools, for instance, if they would like to hear the audio again or stop it. Furthermore, these self-contained systems must be compatible with the standard connector of nonproprietary headsets or earplugs that individuals with visual impairments carry sometimes.

- Incremental volume control and reset. The Occupation Health and Safety Administration and the American Speech-Language-Hearing Association have determined that the standard volume level of speech is 65 db. Information kiosks, such as those in museum displays, must have a minimum volume level of 65.

If background noise interferes with the audio output of the self-contained product, individuals with partial hearing may have difficulty comprehending the information. The minimum interference level is 45 db. To override ambient noise, the self-contained product must provide an option to allow users to raise the volume 20 db higher than 45 db.

- Color coding. As with software and Web applications, color alone should not convey information regarding self-contained products. This guideline benefits all users, not only those with cognitive or visual impairments. Different colored buttons on a printer, for instance, must have text labels to identify their functions.

- Color contrast. Users may need to adjust color and color settings in self-contained products. Some people may be sensitive to brightness and thus cannot distinguish text. Others may need a sharp contrast between background and foreground colors.

- No flashing or flickering. Flashing or flickering on the screens of self-contained products may cause persons with photosensitive epilepsy to have seizures. To prevent episodes from occurring, an option should be provided that would stop the flickering.

- Reachable controls. Persons in wheelchairs may have difficulty reaching operable controls (e.g., the print or stop button) on equipment such as printers and copiers. Once again, controls and parts that involve maintenance or repair of self-contained products are exempt.

The following guidelines prevent operable controls from being too high, too low, or out of the reach of the user:

1. The front part of the self-contained product, otherwise known as the vertical plane, must be a maximum of 48 inches high.

2. The reach range of an operable control should not be more than 10 inches if the self-contained system is a maximum of 54 inches and a minimum of 15 inches above the floor.

3. The reach range of an operable control should not be more than 24 inches if the self-contained system is a maximum of 46 inches and a minimum of 15 inches above the ground.

- Desktop and portable computers. Unlike self-contained products, desktop and portable computers can contain assistive technologies, such as screen readers and magnifiers. Like self-contained and telecommunications products, however, desktop and portable computers must have accessible controls and keys.

Additionally, computers must have nonproprietary connectors so developers of assistive technologies are assured that their devices can interface with computer systems. Standard connectors include RS-232, Centronics, SCSI interfaces, PCMCIA, or USB.

Communication for All

Access to information is the critical core of education. Those who provide communications technology services on campus have far more resources today than ever before, and thus also have a greater responsibility to provide access for the disabled to all the opportunities of higher education.

As president and CEO of TecAccess, Debra Ruh brings over 20 years of experience creating technology solutions for private firms, government agencies, universities, and non-profit organizations. Inspired by her daughter, Sara, who has Down's syndrome, Debra has built a successful, award-winning company with more than 60 associates worldwide, most of whom are people with disabilities. Contact Debra at druh@tecaccess.net.

Paul Spicer, speaker, author, and founder of Spicer & Associates, regularly advocates for people with disabilities and accessibility issues worldwide. Paul can be reached at paulspicer@spicerassociates.com.

▼

Sinclair Community College Secure LAN Strategy Project

Scott McCollum from Sinclair Community College accepted the Award for Institutional Excellence in Communications Technology at the Annual Conference in San Diego. Left to right: ACUTA President 2005–06 Patricia Todus, McCollum, Awards Committee Chair and Immediate Past President Tamara Closs, and Rick Cunningham, PAETEC Communications, sponsor of the Award.

The Sinclair Community College Information Technology Services (ITS) team is responsible for maintaining a secure, manageable, and scalable IT system that facilitates a balance between secure and collaborative network computing for the college's students, faculty, and staff. Information Technology Services had completed a great deal of work researching, testing, and implementing technologies that address specific issues for the college network; however, the college faced some complex challenges in achieving a truly secure LAN solution.

Most network infrastructures allow unrestricted access once a connection is made by a client with the assumption that the only necessary security is to protect the resources on the network servers where there are very sophisticated authentication and access control mechanisms. The main goal is to route communication on the network as fast and efficiently as possible. This leaves the entire network exposed to any software that can take advantage of this openness to find and exploit vulnerabilities in the connected systems.

The growth in wireless networking on the Sinclair campus, the need to provide protection from the introduction of wired and wireless "guest" computing devices, and the need to protect the network from the proliferation of network-borne viruses and worms caused the ITS team to develop a strategy for a Secure LAN Solution. This strategy was completed in October 2004, and it has provided a road map for the implementation of network switch port-based authentication; the authentication, verification, and provisioning of guest and unknown devices; and the identification, isolation, and remediation of problems with unpatched or virus-infected PCs and other devices.

This project was initiated to build intelligence into network devices so they can limit the type of communication that they will forward. These limitations vary based on the type of user and the type of device that is attempting to connect to the network. This puts the control over the network's security into the hands of the college rather than at the mercy of the various devices that can be connected.

A unique approach used in this system was the creation of a partnership between the college and a provider of free wireless services. Because the partner uses the same wireless equipment as the college, the partner's wireless network has been designed with the ability to access the college's secure wireless access over the same equipment. This has been beneficial to both the college and the wireless partner as the college obtained additional wireless services and coverage areas at no cost using its secure wireless access system, and the wireless partner gained additional installation areas and customers.

The Secure LAN Strategy defines a clear path toward a network where access to network resources on the entire Sinclair Community College campus is based on the role of the user, the configuration of the computing device he or she is using, and the verifiability that the device is problem-free. When the plan has been fully implemented, no computer will be able to communicate on the Sinclair network, via wired or wireless connectivity, without the user of the device passing an authentication process. The plan also provides for different levels of access based on whether the device is a Sinclair-imaged computer or a device with an unknown configuration.

Planning, Leadership, and Management Support

ITS was already working toward a secure LAN solution, but to address the significant challenges involved, the team defined the Secure Network project for inclusion in the IT division's master plan, a major component of the division's planning and budgeting process. The college's administration provided the funds to proceed, and the project began with exploration of the IT marketplace to get a broader view of available products and to acquire additional expertise. Blue Spruce Technologies, Inc., was selected to help develop the Secure LAN Strategy because much of the infrastructure and tools that were in place were from Enterasys Networks and many of the Blue Spruce staff were former Enterasys employees.

The development of the strategy began with a vision of the desired end state which included these components:

- Role based access
- Separation of users/systems by risk level
- Differentiation between known and unknown
- Definition of what is unallowable
- Quarantine of policy violators
- Registration of unknown devices

The definition of the Secure LAN Strategy allowed us to evaluate existing resources for their ability to fit within the framework and identify gaps where other products or new procedures were needed. The college's administration has been very supportive of security initiatives and maintaining up-to-date technologies, so there was already a significant investment in products and technologies that could meet the goals of the strategy, including the following:

• *Enterasys Matrix E7/N7 Switches.* A total of 29 seven-slot modular switch chassis connected at the edge via gigabit fiber uplinks to Enterasys 8600 core routers. Each edge switch is connected to two separate core routers using VRRP to provide redundancy in case of link failure. Each building contains at least one edge switch supporting one to three separate networks.

• *Enterasys X-Pedition 8600 Router.* The network core consists of one 8600 router in buildings 2, 5, 12, and 13 connected in a meshed topology via single-mode fiber to provide full redundancy. The X-Pedition 8600 delivers full-function, wire-speed IP routing using OSPF and IGMP and DVMRP.

• *Enterasys Dragon IDS.* The Dragon provides high-speed sensors to detect security events such as network misuse, network intrusions, system exploits, and virus propagations. In addition, it facilitates the analysis of forensic data to determine the impact of network attacks. It combines events on the network with those on the hosts, switches, and routers to help provide automated threat detection, isolation, and containment.

• *NetSight Atlas Management Suite.* This suite of software products enhances the security, management, troubleshooting, and control of all infrastructure devices. The products used are:

1. NetSight Atlas Console. The command and control console from which all NetSight management products are launched. It also provides a centralized console for enterprise wide monitoring of all infrastructure equipment.
2. NetSight Inventory Manager. This component enables the centralized management of all infrastructure components cohesively as a system, keeps a centralized database of all infrastructure components and provides for data collection and reporting.
3. NetSight Policy Manger. This component allows policy rule sets to be defined and allocated at the port level of each switch, across the entire enterprise. These policies define the types of communication allowed on each port.

• *McAfee VirusScan and ePolicy Orchestrator (ePO).* Virus detection and removal is a critical capability within any network to ensure uninterrupted availability of services. However, the ability to ensure that every computer has the software loaded and that the software continues to function as it should is a nearly impossible task. ePolicy Orchestrator is a software solution that enables ITS to centrally manage and enforce antivirus policies transparent to the users. According to policies that are enforced VirusScan is

▶

installed and constantly running, and virus definitions are updated within one hour of their release by McAfee. Memory scans take place every hour, and every file is scanned when it is opened. If any of these policies are not detected, they are enforced within 5 minutes.

In addition to detecting viruses, McAfee VirusScan 8.0i includes firewall capabilities, spyware detection and removal, and buffer-overflow prevention. ePolicy Orchestrator distributes updates to VirusScan settings to all campus users without any user or technician intervention.

• *Altiris.* Desktop workstation images are deployed using software from Altiris that uses IP multicasting to install an entire lab of computers concurrently via a single stream of data that is sent across the network infrastructure. Processes are also in development to use Altiris to install individual applications or updates to applications over the network.

• *Microsoft's Windows Server Update Service.* Keeping desktop operating system software updated is critical in order to prevent the exploitation of vulnerabilities that are regularly discovered and patched within the Windows operating system. With the increase in network-based attacks, the removal of viruses and spyware from a computer is not sufficient. Other computers can take advantage of vulnerabilities in the operating system through its network connection. ITS uses Microsoft Windows Server Update Service (WSUS) to distribute patches to the operating system that are made available as vulnerabilities are discovered.

ITS maintains a standard "core" workstation image for employee computers and builds lab-specific images that contain the software required in various departmental academic labs. The software tools listed above are all part of this core, so the ability to identify imaged workstations from other devices allows the network to treat imaged PCs as trustworthy.

The Five-Step Plan

Once we had created the Secure LAN Strategy and identified existing technologies that could be used within that strategy, we needed to develop a plan for implementing the strategy, identify gaps in our existing technology, and determine how to plug these gaps. The resulting plan consists of five phases:

Phase 1: Acceptable Use Policy. During this phase the various roles were defined that would be used to categorize network users and the type of access that they would be given. Initially the roles would be manually assigned to ports based on the type of user connected to that port. However, once the authentication phases were implemented, the role would be dynamically assigned using groups within Active Directory.

Phase 2: Network Management System (NMS) Application Configuration. The NMS applications assist in the administrative tasks necessary to quickly perform tasks such as device management, switch configuration backup and restore, firmware upgrades, device inventory management and change control, and policy configuration and deployment.

Phase 3: Dynamic Intrusion Response (DIR). In this phase, response processes to network security events were implemented. This phase brought together work that was done in the two earlier phases by dynamically changing the user role assigned to a switch port to a quarantine role when a security event is identified as being sourced from that port.

Phase 4: Authentication of imaged devices. This phase addresses the authentication steps for imaged PCs (a Sinclair PC with standard set of software including antivirus and security patches). After the imaged PC is recognized by the system, the user's role is defined upon login to a network switch-port and the policy that enforces that user role is applied.

Phase 5: Authentication of non-imaged devices. In this phase, non-imaged PCs are scanned by the system, and if the PC has problems, the system places the PC in a predefined quarantine role. If the PC has no problems or its problems have been remediated, it is provided "Web only" access.

Some challenges that needed to be addressed in these phases included the following:

- Creating policies that allow secure communication between network users and systems while simultaneously preventing threats from spreading.
- Mapping the Sinclair business functions which are modeled in the Windows Active Directory OUs with effective and manageable network usage policies.
- Identifying imaged versus non-imaged PCs and assigning "gold" network access to imaged PCs.
- Redirecting non-imaged PCs to a registration/remediation server for the purpose of validating PC configuration.
- Ensuring that the machine meets an acceptable level of security or complies with Sinclair's Acceptable-Use Policy.

• Identifying a viable 802.1X client for non-Windows-XP systems that will be compliant with the security goals of the Sinclair network.

• Determining the best EAP type for desktop 802.1X authentication.

Additional technologies that would need to be implemented to meet the requirements of the plan included:

• NetSight Automated Security Manager (ASM). This additional component of the NetSight suite integrates the Enterasys switching and routing infrastructure with the Dragon IDS to automatically take action on the network, down to the port level, when an attack is identified using NetSight Policy Manager to dynamically modify the role assigned to a switch port, thereby changing the allowable communication for the connected device.

• Microsoft Windows Server 2003 Internet Authentication Service (IAS). The Microsoft IAS Server is a Remote Authentication Dial In User Service (RADIUS) server. A RADIUS server accepts authentication requests from network devices and forwards them to an authentication server, which, in a Windows Server 2003 domain, is the domain controller. The authentication server confirms or denies the authentication request and forwards the result to the RADIUS server, which in turn forwards it to the device requesting authentication.

• Cisco Clean Access. This is a system that authenticates, authorizes, evaluates, and remediates wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, personal digital assistants, or even game consoles are compliant with the network's security policies and repairs any vulnerabilities before permitting access to the production network.

Figure 1. Sinclair Network Access Levels

Access Level	User	Device
Level One: This is the highest level of access. The user must login with their Sinclair network username and password.	College Employees: This includes all faculty, staff, and student employees. It also includes student use of login IDs that are assigned to campus lab computers.	College-Owned Laptops and tablet PCs with the Sinclair Administrative Software Image
Level Two: "Web Only" access similar to the type of access when connected to the Internet off-campus. The user must login with their Sinclair network username and password.	College Employees: This includes all faculty, staff, and student employees. It also includes student use of login IDs that are assigned to campus lab computers .	Devices without the Sinclair Administrative Image or not owned by the college: PDAs, non-imaged laptops, personal laptops, smart phones, etc.
Level Three: This is a "Guest" access granting "Web Only" access similar to when a user is connected to the Internet off-campus. A login is NOT required.	Anyone: This includes all students and the public.	Any Type of Device

Once the plan was defined, it became clear that a different wireless technology would be required to implement the same controls placed on the wired infrastructure for wireless access. In order to meet the requirements of this strategy, a new wireless technology from Airespace, which has since been acquired by Cisco, was selected through an RFP process. This system uses a "thin" access point with a central controlling switch. The roles of the Acceptable Use Policy, which are implemented on the wired ports using VLANs, are made possible on the wireless network using multiple WLANs, each with a different SSID and authentication method.

The Acceptable Use Policy that was developed in Phase I of the project defined an access framework based on three levels of service. Each level provides a different level of service based on the type of user and the type of device that is being connected. Level One would provide authenticated users on college-owned, imaged devices to connect with the highest user access. The second level access allows authenticated users to use non-college owned or non-imaged devices to connect, but at a lower level of "Web only" access to the network. The third level of service is what can be thought of as "guest" network access. (See Figure 1.)

Even though we defined the Level 3 access within the plan, we had no immediate interest in providing the guest access due to the costs of the infrastructure as well as the cost of supporting this type of access. This led us to investigate vendors that would be willing to bear these costs and provide the service that our customers would require. In August 2005, the College signed a contract with Harborlink to provide the guest wireless access in various public spaces in all of Sinclair's Dayton campus buildings.

▶

Because Harborlink uses the same wireless equipment as the College, Harborlink's wireless network has been designed with the ability to access the college's secure wireless network over the same equipment.

The contract with Harborlink not only provides the guest wireless access at no cost to the college, it also allows ITS to extend wireless access into 30 more areas on the Dayton campus at no additional cost. Harborlink is also working with the City of Dayton to provide free wireless access throughout downtown Dayton. This would eventually expand the guest access available inside Sinclair campus buildings to the outside areas around the campus buildings.

Promotion of Technology and Maturity of Effort

The Secure LAN Strategy, completed in October 2004, has provided (1) a road map for the implementation of network authentication for all computers that connect to the Sinclair network; (2) controlled access for unknown devices; and (3) the isolation and remediation of problems with unpatched or virus-infected PCs. The plan defines a clear path toward a network where access to network resources is based on the role of the user, the configuration of the computing device they are using, and the verifiability that the device is problem free.

Implementation of the plan began in December 2004 with the definition of the various authentication roles for users and devices. The next 2 phases, NMS and Dynamic Intrusion Response, were completed in February 2005. These 3 initial phases were all fairly easy to implement in short time-frames due to their minimal impact on existing services. The authentication phases have both been implemented but will take several months to make fully functional due to the changes that must be made to the computers and other network attached devices. These changes are currently underway using documented processes, and the network grows more secure with every step toward the project's completion.

The first three phases of the project are complete, and all 20 of the campus's buildings are protected by the Acceptable Use Policy. We currently have the full plan implemented on the network switches that support two of the college's buildings. One of the buildings is on the downtown Dayton campus and the other is a newly opened Learning Center in Englewood, a suburb of Dayton. All network switch ports in these two buildings are not only protected by the Acceptable Use Policy, they also require authentication of devices and users trying to connect to the network.

As soon as a connected device is powered on, it is required to authenticate using 802.1x. The network switch passes the authentication request to IAS and if it is successful, the user is required to authenticate. If the user authentication succeeds, he or she is provided with the access defined by the Acceptable Use Policy. If the device authentication fails, the device is isolated into a quarantine VLAN. This separate network authenticates the user and then requires the machine to be scanned and remediated if it is found to have vulnerabilities. The user who is able to be authenticated on a device that was not authenticated is provided with Web-only access but only after the scanning and remediation steps are performed.

Initial wireless access for college-owned laptops and tablet PCs began in August 2005. The contract with Harborlink for the guest wireless access was completed in late August 2005. The guest wireless access and the expanded wireless access areas were implemented in early November 2005. The wireless access control process is functionally the same as the wired process that was described above, even though the technologies and methods used are different.

ITS extensively promoted the expanded wireless services to the campus community. A Web page and other documentation were created to provide information about wireless services to Sinclair faculty, staff ,and students. Sinclair's publications department created posters, flyers, and table tents to advertise the expanded wireless services around campus.

ITS also worked with Sinclair's Web systems team to create a virtual tour of wireless services on the Dayton campus. The tour is found at http://tour.sinclair.edu/. The wireless tour was integrated into the existing campus virtual tour, and it includes maps of wireless access areas and user support information. The campus wireless project was featured in the Dayton Daily News as an economic development innovation for downtown Dayton.

Though another institution may use different tools, the problems that all networks are faced with are similar, and the concepts employed by Sinclair to develop a secure LAN could be adapted and used by any institution.

Quality, Performance, and Productivity Measurements

The greatest quality, performance and productivity measurements are those experienced by users who are not impacted by the secure LAN system itself but by the system's results. The positive impact of a secure, dependable, and available LAN on the productivity of campus faculty, staff and students can't be measured in dollars. However, a system that is not secure and dependable can have a huge impact on productivity, which is directly related to costs.

Every person who uses, or attempts to use, the Sinclair Community College network including current and future students, alumni, and conference/seminar attendees, develops an opinion about the network. This experience contributes to user opinion of Sinclair as an educational institution and ultimately affects enrollment and funding.

In today's IT climate, users expect the network to be everywhere and available at all times, but they expect it to be secure as well. This is the balance that must be maintained through the implementation of this plan. In addition, Sinclair Community College will be able to protect and enhance its reputation of the institution as one who leads the way in IT innovation.

Cost, Benefit, and Risk Analysis

Enterasys acknowledges Sinclair as an important partner in the use of its technologies and agreed to combine the ASM software with a large purchase of equipment as a donation to a fundraising campaign run by the Sinclair Foundation.

ASM is a key component in creating a secure network due to its ability to recognize inappropriate network communication and dynamically change a computer's ability to communicate over the network. After the acquisition of ASM, ITS had all of the tools necessary to complete its vision, but there was much planning that needed to be completed to ensure that the new and previously installed technologies would be integrated into a single, interactive system.

BlueSpruce Technologies, a company founded by some of the creators of the ASM product, was selected to help develop the plan. Once the plan was complete, ITS and BlueSpruce began discussing its implementation. This developed into a second commitment with BlueSpruce in which the company would assist ITS in all of the plan's project phases.

The contract with Harborlink not only provides guest wireless access at no cost to the college, it also allows ITS to extend wireless access areas into additional areas on the Dayton campus at no additional cost.

Security incidents can create intangible costs to the college such as lost productivity or lack of customer satisfaction. In addition, they can create breaches of confidential information that could cause financial penalties for the College. Minimizing the possibility of these types of incidents is absolutely critical.

Customer Satisfaction and Results to Date

Changes within the network infrastructure are being phased in to ensure that each set of changes are thoroughly tested before the next changes are applied. The result is an increasingly secure network that protects user productivity from the malicious or accidental spread of network-borne threats.

All wireless access and wireless devices are now 100 percent secured by this system. This project increased the number of wireless access locations, allowed faculty and staff to be more productive by accessing the campus network wirelessly, increased student satisfaction with the college, and benefited guests and visitors.

ACUTA congratulates Sinclair Community College, winner of the 2006 Institutional Excellence Award. The information presented here was taken from the documentation they submitted for this award. If you have questions about Sinclair's Secure LAN Strategy, contact Scott McCollum, Director, Information Technology Services, at scott.mccollum@sinclair.edu.

▼

Advertisers' Index

★ **Indicates ACUTA Corporate Affiliate**

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to communications technology 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 and that you appreciate their support of ACUTA.

For complete details about advertising in the ACUTA Journal, contact
Amy Burton, Manager, Corporate Relations & Marketing

Phone: 859/278-3338 x240 • e-mail: aburton@acuta.org
www.acuta.org

Here's My Advice

continued from page 52

As the construction industry increasingly adopts the 2004 edition of the MasterFormat, the number of requests from the construction industry for assistance with planning and designing CLA systems will increase. The key to success is participating as early in the process as possible.

"Participating" can range from ensuring that a CLA consultant is brought on board to work alongside the architect and engineers to assigning someone from your staff to prepare the drawings, specifications, and estimates for the project. This person should be well versed in AutoCAD, product specifying, and cost estimating. Ideally, the CLA consultant or staff person should be familiar with backbone and horizontal cabling systems, voice and data systems, distributed and integrated audiovideo systems, and safety and security systems, as well as building automation systems. In addition to understanding how buildings are designed and constructed, this person should also understand related building systems such as mechanical and electrical systems.

Another important effort will be to establish a solid working relationship with the department on your campus that facilitates the design and construction of new buildings. Historically, the communications technology department has been outside the loop during the design and construction process and often at odds with the design and construction team. This can no longer be the case.

As you look for useful resources, CSI (www.csinet.org) has a number of certifications and publications, in addition to the MasterFormat, that can help you and your staff get up to speed with the processes and methods used by the construction industry. In particular, the CDT certification and Project Resource Manual (PRM) are excellent resources.

In the communications industry, groups such as BICSI and TIA are releasing publications and standards that help to define the CLA requirements and provide guidance when planning the CLA systems. BICSI's (www.bicsi.org) series of design manuals and TIA standards 569B for pathways and spaces and 606A for administration are tremendous resources when planning and designing CLA systems.

Tom Rauscher specializes in design and documentation services at Archi-Technology. Reach Tom at tomr@archi-technology.com.

▼

Here's My Advice

Thomas C. Rauscher, President
Archi-Technology, LLC

Planning, Designing, and Constructing a Building

Technology and communications systems have become commonplace in a typical building. The network has become an information transporting system (ITS) that is very capable of transporting more than just voice and data. As a result, many new systems are beginning to seek access to the IP network.

These systems can include CCTV, access control, intercom, audiovisual systems, digital signage, and building automation systems. If your campus includes a hospital or medical center, there are even more systems in the clinical arena that need access to the IP platform. These new systems need to be accommodated even while we roll out our own enhancements such as VoIP and wireless services.

While provisioning network service for this new group of customers can sometimes be a pretty big task, that is only half the impact of these new systems coming on to the network. We also need to learn how to better integrate the ITS into a building.

With the number of systems using the IP platform increasing, the size of the communication equipment rooms (CERs) that support these systems also needs to increase. This translates to an increase in the amount of power and HVAC capacity needed to support the CERs and the systems they house. The pathways from the drop locations to the CERs also need to support more wires and, therefore, must increase in capacity as well.

The pathway and space requirements associated with modern networks have evolved to a point that they can no longer be figured out during or after construction.

Communications, life safety, and automation (CLA) systems and the mechanical, electrical, and plumbing (MEP) systems that are needed to support them often represent 10 to 15 percent of the construction cost of a building. CLA systems no longer represent an inconsequential dollar amount in terms of construction costs, and many institutions are beginning to realize that there are substantial cost benefits when these systems are planned for earlier in the process.

Here's my advice: **Learn how the construction industry plans, designs, and constructs a building.**

In 2004 there was a substantial change in the construction industry that will facilitate the integration of ITS systems and infrastructures into the design and construction of modern buildings.

The Construction Specifications Institute (CSI) released its 2004 edition of the MasterFormat. The MasterFormat is a master list of work results associated with a construction project (essentially a big table of contents for a new building).

The 2004 edition includes three new divisions (chapters) addressing communications systems, electronic safety and surveillance systems, and integrated building automation systems. These divisions are 27, 28, and 25, respectively. CLA is the common name often used for the systems included in these divisions. These new divisions are a result of the communications industry's Division 17 initiative.

continued on page 51


A mathematical formula for converting wind to megawatts doesn't move anyone. But if I can give an undergrad a virtual tour through 3,000 whirling turbines, his instructor can renew his energy for physics from anywhere.
Dynamic Networking from AT&T delivers Services over IP through our secure MPLS-enabled network. And that helps Anna do more with less, as increasingly media-rich curriculums require greater bandwidth flexibility. For more about e-learning, go to att.com/edu.
THE WORLD ACCORDING TO
ANNA
The new at&t
Your world. Delivered.
att.com/edu

Are you ready for the Digital Generation?

Digital Generation \'di-juh-tuhl je-nuh-'ray-shun\

Definition: 1. a group of contemporaneous individuals with cultural or social characteristics, technological experiences and attitudes. **2.** individuals who see limitless possibilities through the use of technology - to imagine, to dream, to envision new possibilities, to create and of course, to learn!

Today's students have grown up in a digital world along with a sea of electronic digital devices. Naturally, when selecting a school, they expect the latest in cutting-edge technologies to be offered.

Let NEC show you how to meet the communication needs of the Digital Generation. Our solutions for higher education provide a full range of the latest cyber-infrastructure technologies, enabling campuses to offer innovative teaching methodologies, drive new sources of revenue and manage costs. NEC's solutions are comprised of voice, data and video products, applications and services built on the latest IP communication technologies. These solutions address campus needs ranging from mobility to network security and campus safety.

www.necunified.com/highered

Empowered by Innovation NEC