Fall 2016

ACUTA Journal of Telecommunications in Higher Education

2016
Fall
Volume 20
Number 3

*Association for
College and
University
Technology
Advancement*

ACUTA JOURNAL

IoT NENA SIP DAS

POTS FCC &

What's Cooking in the IT Kitchen?

PANs

VoIP LTE ITSM WIFI BYOD AN/ALI SD-WAN E911 PSAP

IN THIS ISSUE

POTS and PANs: What's Cooking in the IT Kitchen?

IT-Style Alphabet Soup

IoT: The Internet of Things

Is the LPWAN in Your Future?

Ingredient for Wireless Success: DAS

1,200+ Educational Institutions Rely on AVST

AVST

Interoperability

Future-proof both today and tomorrow's telephony platform choices – Premise to Cloud

Resiliency

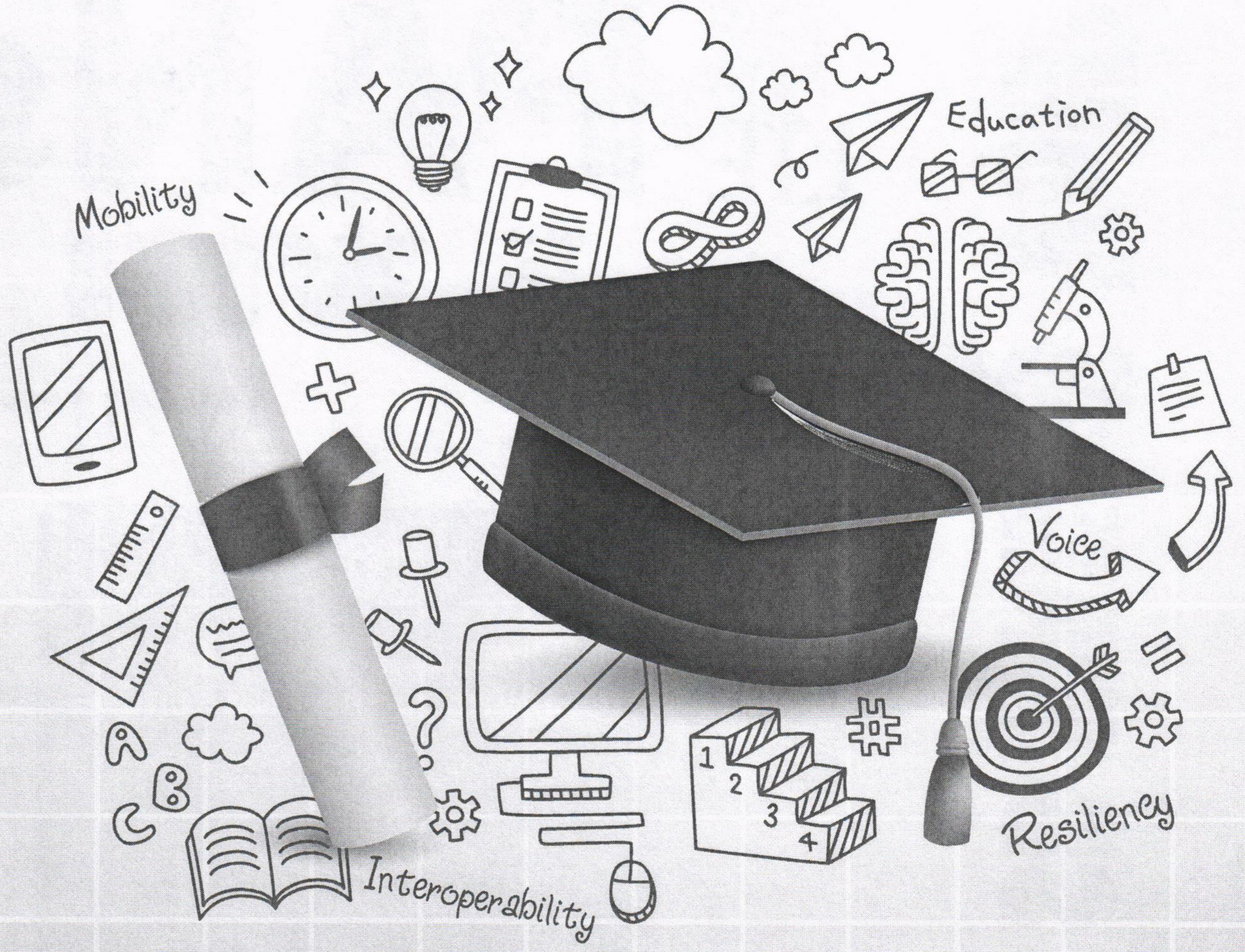
IT continuity assured – unmatched scalability, virtualization, disaster recovery

Voice

Speech auto-attendant and secure voice messaging for regulatory compliance

Mobility

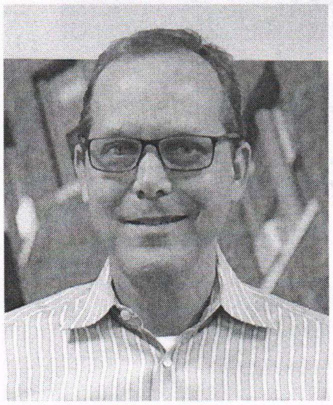
Secure mobile client and first context-aware personal assistant



www.avst.com/education For over 30 years, AVST has been ***Unifying Communications***

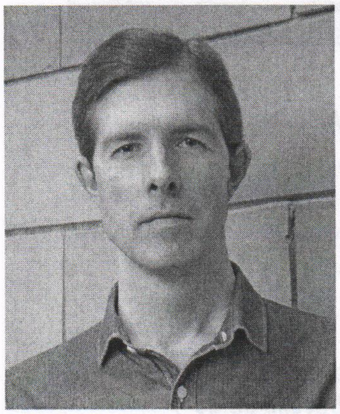
THE ACUTA CONNECTION

Quotes of Note



When considering today's evolving technology demands, we should strive to be proactive in capitalizing on potential integration points across the systems and services we offer our university communities. This forward thinking will help us implement better problem avoidance, mature change, and incident management practices and will also empower effective, relevant service delivery.

Chris Megill
Assoc. Director Customer Support Services
The George Washington University



The nature of today's higher ed customer ensures that tech trends will appear on campus. Small campuses face an especially tough challenge, trying to provide an agile and forward-thinking IT environment that can attract students and faculty while staying in budget and without outstripping the capacity of a small staff to provide support.

Robin Burns
Network/Telecom Engineer
Principia College

The Year Ahead

Winter Seminar	January 8–11, 2017	Wyndham Grand Hotel Orlando, Florida
46th Annual Conference	March 19–22, 2017	Hilton Chicago Hotel Chicago, Illinois
Fall Seminar	October 1–4, 2017	Hilton Palacio del Rio San Antonio, Texas

Core Purpose and Values

ACUTA's mission is to advance the capabilities of higher education communications and collaboration technology leaders.

ACUTA's core values are to:

- encourage and facilitate networking and sharing of resources
- exhibit respect for the expression of individual opinions and solutions
- fulfill a commitment to professional development and growth
- advocate the strategic value of communications and collaboration technologies in higher education
- encourage volunteerism and contributions by individual members

ACUTA

Association for College and University Technology Advancement

Fall 2016

Volume 20 Number 3

THE ACUTA JOURNAL

INSIDE THIS ISSUE

page 10

You can imagine a top kitchen using "containers" to organize ingredients, keeping them fresh, avoiding cross-contamination, ensuring the best flavor and outcome of any recipe. The CIO needs to use these same strategies to protect the elements that make up a successful university IT environment.

Neal Tilley
Cisco Systems

ADVERTISER INDEX

Thanks to the companies that support ACUTA by advertising in this issue.

AVST
page 2
www.avst.com

MiCTA
page 23
www.micta.org

Talkaphone.com
page 5
www.talkaphone.com

Telecom Reseller Magazine
page 13
www.telecomreseller.com

ADVERTORIAL
Cisco UCS for HPC
page 26

COLUMNS

7
President's Message
Articulating the Value of IT
by Arthur Brant

9
From the Editor
What's the Meaning of This Issue?
by Pat Scott

FEATURES

10
IT-Style Alphabet Soup
by Neal Tilley
Universities Need TOP CHEFs as well as Top CIOs to Meet Demands of IoT in Education

12
Software-Defined WAN (SD-WAN)—Moving Beyond MPLS
by Michael Finneran
SD-WANs can reduce costs and improve performance for network applications

14
IoT: The Internet of Things
by Ron Kovac, PhD; Dominic McClung; & Ryan Patterson
The IoT is the future. What are we to do with it?

17
Is the LPWAN in Your Future?
by Gary Audin
Wearable technologies and the IoT are bringing new demands to the campus.

19
Ingredient for Wireless Success: DAS
by Scott Gregory
When Wi-Fi is not quite enough, add DAS to the mixture.

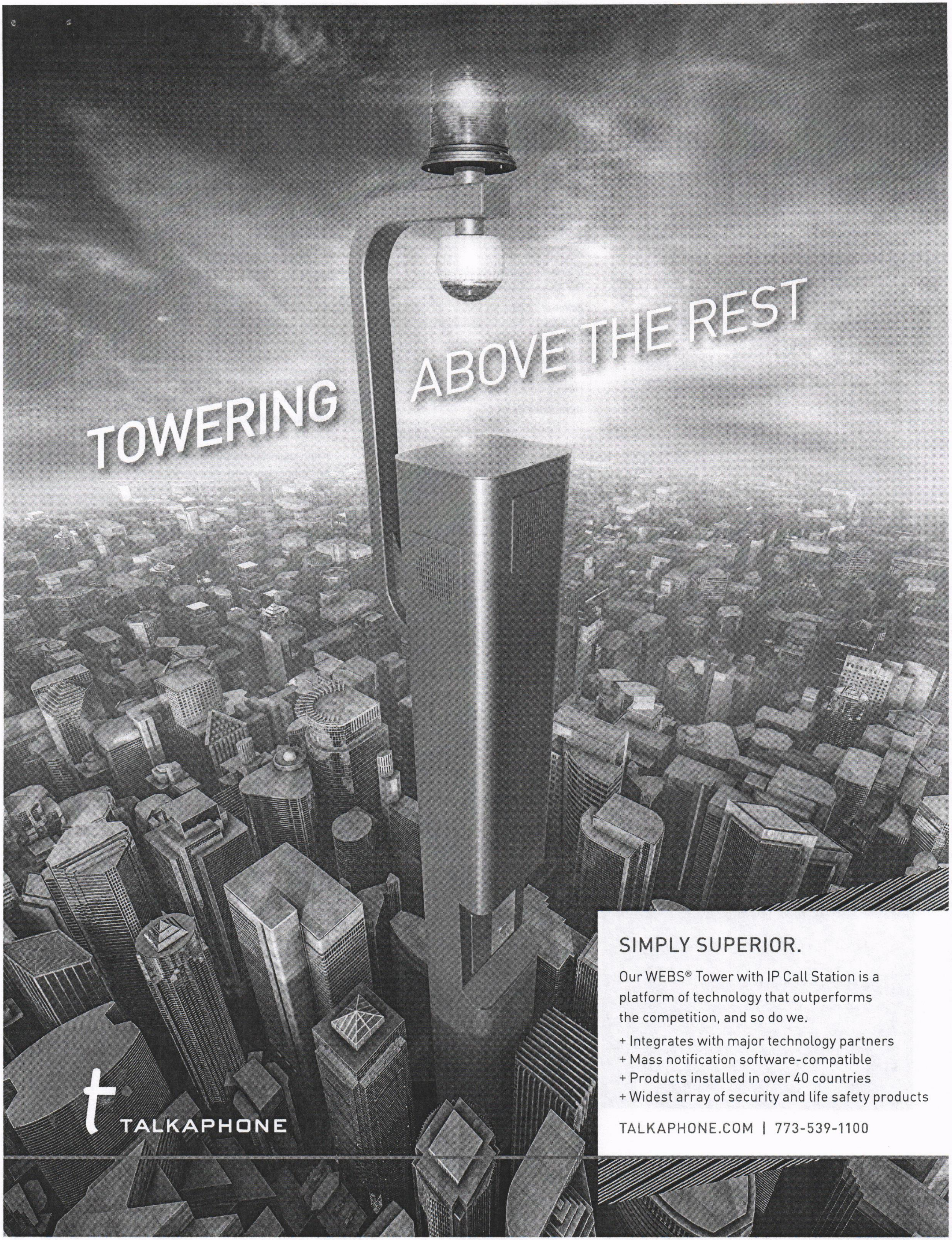
22
Hot Issues in Communications Technology Law
by Martha Buyer
Martha Buyer takes a look at TCPA, Kari's Law, E911, FCC, FTC and more.

29
Institutional Excellence Award:
CSU Fullerton's Shared Cloud Services

SNAPSHOTS

21
DIDs for ELINs?
by Geoff Tritsch

25
ISE...ERP...KnowBe4
by Dave Lutes


TOWERING ABOVE THE REST
TALKAPHONE

page 14

One of the biggest hurdles standing in the way of data collection is the question of how to store all of the data generated by IoT devices. Not only will data centers have to increase in size in an effort to hold the massive amounts of data, but the methodology of data centers will also have to change to object-based storage to meet the analytics requirements of IoT.

Ron Kovac, PhD
Ball State University

Welcome to the ACUTA Journal!

We hope you find our digital format convenient and enjoyable, the content interesting and useful. We welcome your comments at any time.

To share a story with our audience, please contact Pat Scott, ACUTA communications director, at **859-721-1659 or pscott@acuta.org.**

For next three issues, our *Journal* will focus on the following topics:

Winter: 2020: Vision of the Future

Spring/Summer: Providing Telephony on Today's Terms

Fall: The Business Side of IT/Telecom

THE ACUTA JOURNAL

Publisher
ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

859-278-3338 general office
859-278-3268 fax

Interim Executive Director
Lisa Thornton, CMP

Editor-in-Chief
Pat Scott, Director, Communications
pscott@acuta.org

Contributing Editors
Curt Harler
James S. Cross, PhD

Advertising Sales
Drilon Gojani, Manager, Business Development

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 on 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 electronically by ACUTA, a nonprofit association for institutions of higher education, represented by communications technology managers and staff.

ISSN 2151-3767

Postmaster, send all address changes to:

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

For more information: www.acuta.org

Membership and Subscriptions

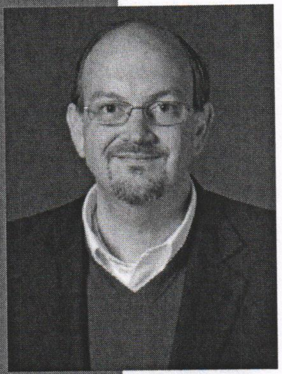
Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for $80 per year or $20 per issue. For information, contact Lori Dodson, Member Services Coordinator, 859/721-1658, or e-mail ldodson@acuta.org.

Do a Friend a Favor: Invite a Colleague to Join ACUTA!

MESSAGE FROM THE PRESIDENT

Our Challenge to Be Innovative

by Arthur Brant
Abilene Christian University
ACUTA President, 2016–2017



In my household, my wife and I share cooking duties. I mostly take the weekend meals, while my wife handles the weekday meals. This arrangement works for us because my wife is more creative with food preparations that I am. While I can follow directions on the outside of a box, I rarely veer far from grilling something, tossing a salad, and baking a potato. On the rarest occasions, I can make lasagna, but I'm lost without my mother's carefully detailed recipe card.

This Journal's theme of "What's Cooking in the IT Kitchen" I find intriguing because so often I find myself comfortable with time-tested procedures and policies related to Information Technology. However, one of the words that I often hear associated with technology is "innovation." Many times this word is leveraged to describe a new piece of software or the latest hardware platform, and the word is accompanied by a promise to disrupt preconceptions of what is possible.

In January 2015, Abilene Christian University's Information Technology department embarked on an Innovation Challenge. Each member of the department, from our BI specialist to the switchboard operator, were distributed into three teams, led by one of the IT directors. The challenge was to come up with an innovative project. Simple enough. The teams would be tasked with presenting their project to a group of university vice presidents, who would judge the projects based on three criteria: feasibility, scope of impact, and creativity. With these guidelines and four months to prepare, the teams began to meet.

The team I lead started by attempting to quantify the three criteria. Dissecting "feasibility," we deduced this could imply cost, time, resources, and the likelihood that the project would move beyond the pitch. Dissecting "scope of impact," we thought of impact, reach, and benefit. During this discovery exercise, we also attempted to quantify groups of people who could be affected. Beyond the typical faculty, staff, and students, we also considered campus visitors, alumni, the local community, family members of those associated with the university, university divisions, and prospective students.

Finally we dissected "creativity" and discerned this could include things new, uncommon, unusual, contrary, and resourceful, and the idea of challenging "the norm," "status quo," or "conventional wisdom." Before soliciting ideas, we also went through an exercise to identify struggles, annoyances, or obstacles various groups faced. Attempting to apply the idiom "necessity is the mother of invention," we figured that these struggles, annoyances, or obstacles could provide us insight as we consider an innovative project.

Each team's process was different, but one common element we observed was that each team solicited input from folks outside of IT. For instance, one team met with the director of enrollment management, to better understand the student recruiting process. Another group met with the director of student retention to better understand important trends associated with keeping students enrolled and ensuring they graduate. My own group met with representatives from alumni relations to understand how the university leverages and engages alumni. This also included the importance of university donors, alumni and student connections, and career placement. My group also solicited input from the university's director of facilities, to better understand some of the challenges our facilities folks face in supporting faculty, staff, and students.

[I]nnovation can come from anywhere, but for it to take hold, someone has to be willing to champion the innovation.

At the end of this process, three different projects were pitched. One group had an idea of an attendance check-in application that incorporated Bluetooth beacon technology and smartphones. The primary premise for this idea was to eliminate the need for professors to take attendance and enable students to "check-in" to class.

Events Calendar

Winter Seminar

Orlando, Florida
Wyndham Grand Hotel
January 8–11, 2017

• • • • • • • • • • • • • • • • • •

46th Annual

Conference & Exhibition

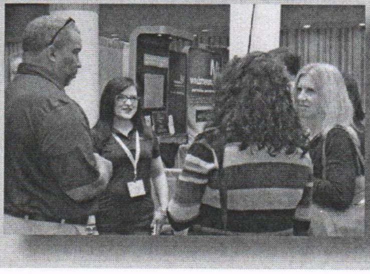
Chicago, Illinois
Hilton Chicago
March 19–22, 2017

You Should Come...

For the Education

For the Networking

For the Information



Another team offered the idea of a student graduation success algorithm or score, which would incorporate several data points the university already captures about prospective students. This algorithm could then help identify areas where university assistance could be leveraged to help ensure the student graduates in five years. Finally, the group I lead offered the idea of replacing every traditional keyed door with electronic door locks that could be unlocked with a smartphone app, using bluetooth.

In a 2013 Fast Company article, Google's chief social evangelist Gopi Kallayil highlighted nine principles as being Google's secret sauce for innovative success. One of the principles is that innovation comes from anywhere. To paraphrase the point, the article states that innovation can come from anywhere, but for it to take hold, someone has to be willing to champion the innovation. The notion that innovation can come from anywhere is precisely the perspective of ACU's IT executive director, Kay Reeves. Kay is convinced that we have smart people, who accomplish some amazing things, each and every day. However, often these individuals are regulated to focus on desktop support, networking engineering, or programming. By commissioning the challenge, and placing employees in a context outside of their daily responsibilities, the hope was that they would be empowered to think beyond their box and explore synergies with others who were operating outside their areas of influence.

Have you ever had an idea that you considered would benefit your institution, but failed to act upon it, because you didn't know how to get traction? Have you ever prohibited an employee from running with an idea, because it was outside their job description or area of responsibility? Have you ever chided someone not to challenge the status quo or uttered that dreaded phrase "that's not how WE do things?" I'll be honest, I have experienced all of these.

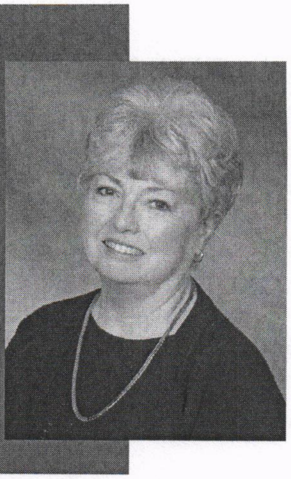
As we think about what's cooking in the IT kitchen, I would encourage and challenge each of us to look around our organizations and ask how we can expand our repertoire. Maybe there's an opportunity to conduct an innovation challenge. Instead of formalizing a challenge, maybe we can subtly diverge from the norm and be creative with the IT ingredients. Maybe there's a new clientele base who could benefit from our regular menu of IT services and products. I will confess, I'm a creature of habit. Being creative isn't something that comes easily, whether we are talking about preparing meals for the family or embracing new methods or technologies at the office. That said, I see the benefits of establishing a healthy balance of maintaining the familiar and exploring unproven solutions or ideas. One of my professional goals this year is to establish a new habit of being accepting of the new and willing to champion these ideas.

Share your comments and ideas with Arthur at branta@acu.edu.

MESSAGE FROM THE EDITOR

POTS and PANs: What's This Issue All About?

by Pat Scott
ACUTA Communications Director



This issue of the ACUTA Journal departs somewhat from our usual collection of articles built arouond a topic as we bring you articles chosen because they define or elaborate on a topic relevant to higher ed that is commonly known by an acronym or its initials. It's IT-speak, or it's telecom-speak: POTS, for example, is how we say plain old telephone service. PANs are not always cooking vessels but may be, in our office, personal area networks.

If someone on your staff is new to our community and may not know all the linguistic shortcuts, this issue can help clue them in. If you already know what DAS, SIP, BYOD, VoIP, and IoT are, you will still glean some useful information from the sources we found. I hope you enjoy this issue; we had some fun with it! Let's start with a few basic definitions.

B/C/L/M/P/WAN

All those areas a network covers:
Body Area Network, Campus Area Network, Local Area Network, Metropolitan Area Network, Personal Area Network, and the Wide Area Network.

BYOD

Bring Your Own Device
From meetings to staff luncheons, the business world continues to stay connected through everything. Students today bring everything on campus. How does this affect technology services?

DAS

Distributed Antenna System
When your mobile device is running slow, coverage might be the cause. DAS can improve that coverage.

IoT

Internet of Things
What we are calling the networking of all things electronic—from appliances to utilities to vehicles to computers and everything in between—so that they all communicate in what is assumed will enhance our lives.

ITSM

Information Technology Service Management
A broad term for organizing the technology framework.

LTE

Long-Term Evolution
The next generation of a stronger, wireless technology

LTE-U

Long Term Evolution in Unlicensed spectrum. Supplements LTE for faster connections!

Li-Fi

Visible Light Communications
A wireless connectivity technology that relies on the visible light spectrum to transmit data at high speeds over short distances. Big at the research level now.

M2M

Mobile to Mobile
Is IoT really just the M2M on steroids?

PON

Passive Optical Network
In a PON, one host connects to as many as 32 optical network units.

SIP

Session Initiation Protocol
This is the layer in technology that helps carry out media messages and sessions. SIP is the meat of the technology sandwich.

Wi-Fi

Wireless Fidelity
Remember when you played records on the Hi-Fi system in your room? Now we complain about weak Wi-Fi connectivity. Let's go to Starbucks and talk about it.

IT-Style Alphabet Soup

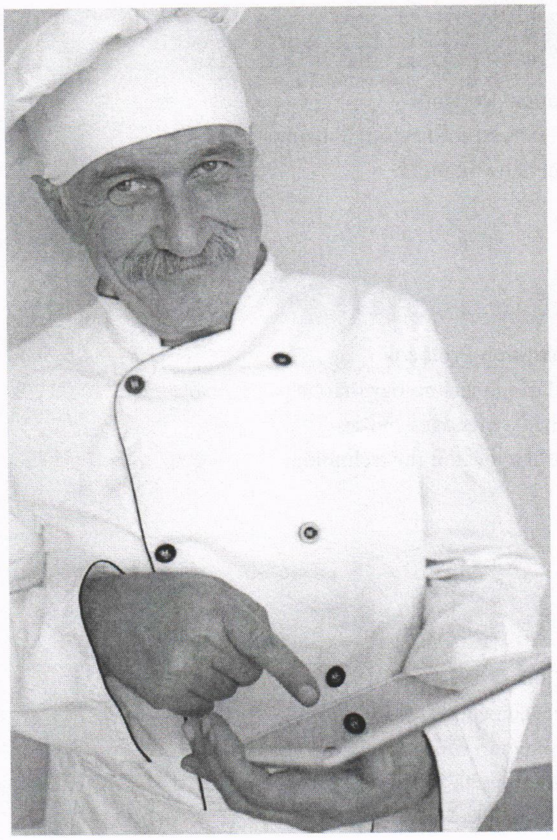
Universities Need TOP CHEFs as well as Top CIOs to Meet Demands of IoT in Education

by Neal Tilley

Budget cuts, tuition up, resources tightened...How can a university cope with IoT and rising expectations with all these "chopped" ingredients?

I am a self-professed foodie and like to watch cooking shows. I marvel at the way chefs can take a wide range of ingredients, deliberately apply techniques that often seem difficult, and make something amazing!

Coincidentally, I have noticed that same level of mastery in the IT departments of universities. Just like those intrepid chefs, the CIO and team have to work with a diverse mix of factors to support the business strategy of the college. For Internet of Things (IoT), read *the latest chef fascination or trend*; for budget cuts, read *any ingredient no chef wants to cook with*; for resource tightening, read *the chef must use only a hand whisk and a blunt knife*. I think you get my point.



www.graphicstock.com

This view was validated at a number of events I attended in the last few months. At the ACUTA Annual Conference in San Diego, the main topics aligned with the view that IT is becoming even more strategic and even more important to student satisfaction and success. Unfortunately, this direction is hampered by lack of budget and lack of resources. Many sessions discussed the importance of continued professional development, ways to find funding, and optimizing resources in need of supporting the IT demands of faculty and students.

The overarching theme was the need for better understanding by executives of cyber security, and the rapid escalation of threats brought on by the race of each college to be competitive.

University IT Knows Security Is Vital

The keynote at ACUTA was given by the former Bell Labs head of cyber security / former White House CIO, Carlos Solari, now CIO of Mission Secure Inc. His delectable session was a journey through the threats and solutions that many CIOs have lived through in IT. The universities know this too well as they have experienced most of the consequences of new hacks, virus or breaches ahead of the majority of companies. It's the nature of education environments that creates this breeding ground for hacking.

The most important message was the proactive steps that Colleges need to make, especially if they are supporting the explosion in smart connected devices as part of their university strategies (including BYOD, IoT, online virtual services, even EDTECH). Carlos called this the Third Wave of threats. See The Internet of Things: Security by Design.

I took this to indicate that although universities have been building solid IT security foundations (for example firewalls, access control), more resources need to be applied to "wave 3" threats (internet of things, smart connected devices) that are appearing in the higher education space.

In fact, the internet of things is far more evident in universities than you might think. Not just smart phones and laptops and STEM devices (robotics, computing kits, 3D printers) but lots of sensors have been enabled with IP capabilities like irrigation systems, washing machines, geo-fencing services, RFID tagged equipment, dorm room motion sensors, security systems, refrigeration equipment in the kitchens...even cooking equipment is Bluetooth and WLAN enabled for remote access!!

So in addition to worrying about student and faculty mobility, the need to support cloud learning applications, and the complexities caused by the criss-crossing of digital footprints with social media, CIOs now have to add IoT to the list. If IoT wasn't on the university's IT strategy menu, it needs to be, and quick!

I also attended this year's INTEROP 2016 in Las Vegas, and was lucky enough to see Arthur Brant, Director of Infrastructure at Abilene Christian University (and current President of ACUTA) do a talk on "Is your network ready for Internet of Things?" You can view his Interop presentation here: http://presentations.interop.com/events/las-vegas/2016/conference-presentations.

He made some excellent points about what you need to consider when every device is IP connected, carrying a MAC address, an IP stack and the ability to transport information across the network. One great point is that IoT is made up of not only connected devices, but of smart connected devices. This difference needs to be understood – however unthreatening a device, gadget, or capability is, there is still a potential threat that needs to be considered.

Those Raspberry PI kits or programmable robots are a way in, a weakness to exploit for any hacker. They can punch holes in the security of a network with their natural open source roots. Like a fleck of egg yolk in a meringue base, the smallest element can cause a catastrophe in the kitchen.

This type of threat isn't news to a university. In fact, recent studies show that education organizations top the lists for cyber attacks: Higher education actually comes out at 105 percent above the national average in terms of cost per breach. (See http://www-03.ibm.com/security/data-breach/)

What is the best practice? The best recipe?

So what's the right balance? How do universities adopt the innovations that students, faculty and stakeholders demand without compromising security? Offering the highest IoT security without compromise could deliver the learning environment that they demand.

First, there needs to be a realization by the executive level of a college on the repercussions of a breach through lack of action. Many states are looking to bring regulations to penalize and fine organizations for any data breach or incident that occurs under their watch.

The best chefs get inspiration and guidance from reading cook books. So too should the CIO and their team.

What are the right steps for building the right network to help cut the threat?

There is no one-size-fits-all magic solution, no out-of-the-box product that fixes everything, protects everything, and makes this issue disappear. As a vendor, we look to develop architecture that will help an IT department deliver a strong level of defense, while enabling the latest innovations. The range of cyber security features and technology that are supported inherently in the equipment itself are ones that should be at the foundation of the university network.

The recipe is simple but effective, inherently increasing the security of the IP network as a whole:

- Policy management, user network profile and virtual network profiles
- Unified access capabilities (wired and wireless connections seen as one environment)
- Seamless integration with security tools (Firewalls, AAA, 801.x, etc.)
- Secure operating code and software diversification

This "Cyber Infrastructure" is now necessary for every university. They must protect against breaches and attacks without stopping progress with education technology for student success.

What is a cyber infrastructure?

Over the coming weeks we will be making recommendations on how to build the new cyber infrastructure for universities, one with faculty and students at the heart, and one that is protected to the highest level. We will be introducing the concept of software diversification, the use of virtual containers across the network, using Intelligent Fabric (iFab), Unified Access (UA), Software Defined Networking (SDN) and networking standards such as Shortest Path Bridging (SPB).

You can imagine a top kitchen using "containers" to organize ingredients, keeping them fresh, avoiding cross-contamination, ensuring the best flavor and outcome of any recipe. The CIO needs to use these same strategies to protect the elements that make up a successful university IT environment.

See the latest information on the latest technology steps we and our partners are developing at http://enterprise.alcatel-lucent.com/?solution=security&page=overview.

What will you cook?

Like the dishes chefs produce under pressure, it's the recipes selected and the experience to execute the right techniques that will lead them to success. Every CIO in every higher education institution will need to leverage that approach for a safer future. Bon Appétit!

Neal Tilley works in US Higher Education, Business Development, with Cisco Systems. Reach him at ntilley@cisco.com. This commentary was originally written for and published on the Alcatel-Lucent Enterprise blog. It is printed here with permission from the author.

•

Software Defined WAN—Moving Beyond MPLS

SD-WANs can reduce costs and improve performance for network applications

by Michael Finneran

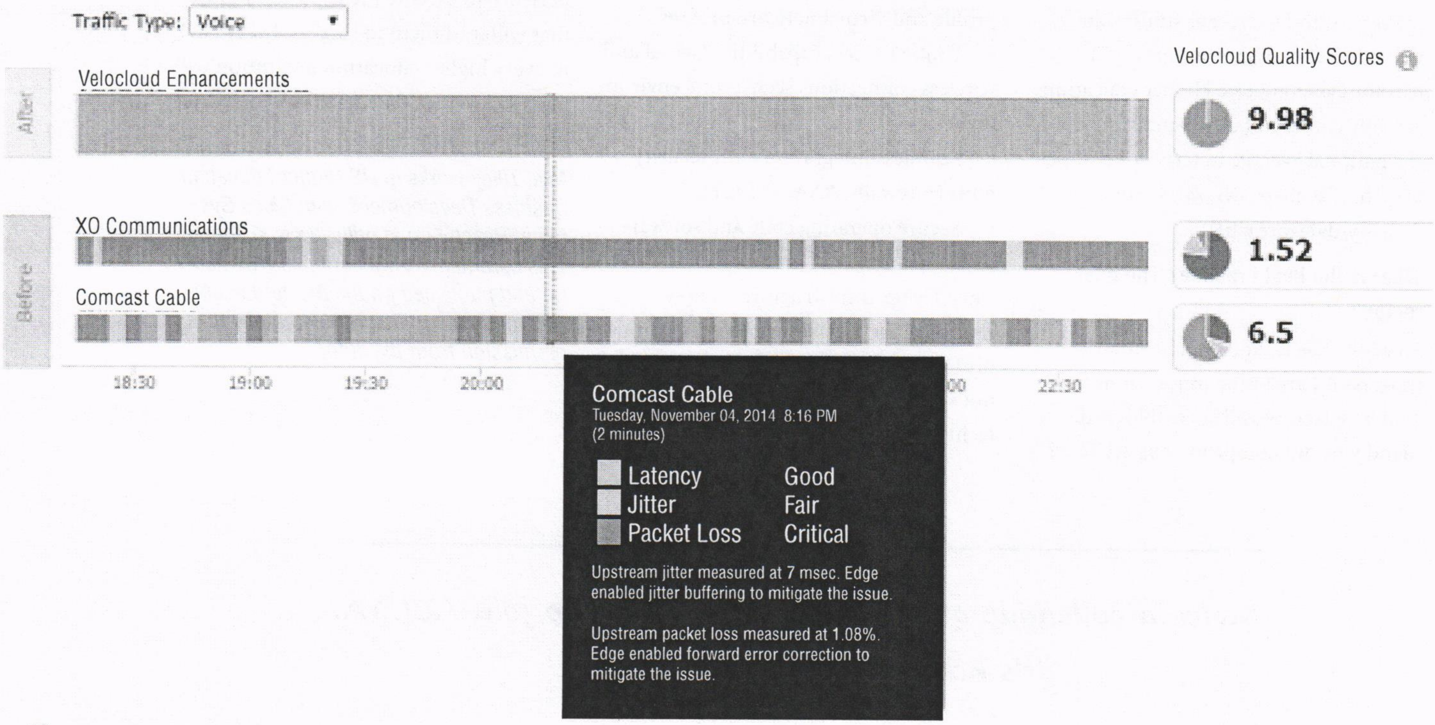
One concept network managers are being faced with today is the software-defined WAN (SD-WAN). Hailed as the first major advance in wide area networking since MPLS, SD-WANs can make better use of MPLS services in conjunction with traditional Internet and wireless LTE data services to reduce cost and improve performance for the full range of network applications.

While many companies have built extensive MPLS networks to connect their headquarters and data centers to branch offices, those MPLS networks often represent a significant ongoing cost. With their inherent security and the ability to provide quality of service (QoS) for real-time applications such as voice and video, those MPLS networks were typically implemented to support site-to-site voice over IP (VoIP) calls and mission-critical applications run in the data center. However, Internet traffic originating in those branch offices is often backhauled to the data center and then "hairpinned" out to the Internet, resulting in costly and suboptimal Internet access.

However, today we are seeing a shift in network requirements. One major change is the move to the cloud for both voice and data services. Unified communications as a service (UCaaS) is now growing at a rate several times greater than premises-based UC systems. Further, more and more applications are being migrated to cloud services such as Amazon Web Services or Microsoft Azure. And, organizations are taking a second look at whether it makes any sense to backhaul branch traffic over an expensive MPLS service, just to dump it back into the Internet.

SD-WAN provides a new way to address these requirements while simultaneously reducing cost and improving service quality. The essential idea of a software-defined network (SDN), of which SD-WAN is a subset, is to decouple the packet-forwarding decision from the hardware that actually does the forwarding. To those who come from a telephony background, the idea is not unlike common channel signaling in a telephone network.

Figure 1: Comparison of network performance before and after Velocloud SD-WAN



Traffic Type: Voice

Comcast Cable
Tuesday, November 04, 2014 8:16 PM
(2 minutes)

Latency	Good
Jitter	Fair
Packet Loss	Critical

Upstream jitter measured at 7 msec. Edge enabled jitter buffering to mitigate the issue.

Upstream packet loss measured at 1.08%. Edge enabled forward error correction to mitigate the issue.

While there are some differences among the implementations, an SD-WAN typically comprises network services, edge devices, and a network controller; in some cases, the network controller is an on-premises server, while in others it is cloud based. If VoIP calls are part of the traffic mix, MPLS will likely be one of the network services involved, along with traditional best-effort Internet and potentially LTE, which is often used as a fail-over.

All of the services coming into each site are terminated on the edge device; as the network "smarts" are in the controller, the edge device is far simpler, and the vendors claim that they are simple plug-and-play so there is no need to dispatch techs from headquarters to install and configure them. IT administrators responsible for establishing the network policies do so through the controller.

The edge devices use deep packet inspection (DPI) techniques to identify the various application flows passing through them. The policy settings for the various application types, combined with the performance of the available network connections—which is sensed automatically, determine which network, typically MPLS or basic Internet, the next packet should be routed over.

As well as reducing network cost by replacing some amount of MPLS capacity with basic Internet services, the application-aware intelligent packet routing can have a significant impact on network performance. The illustration in Figure 1 from SD-WAN vendor VeloCloud below shows the improvement in the performance for a site with links from XO Communications and Comcast Cable. At the bottom is a representation of the performance prior to implementing the SDN (red indicates trouble), and at the top, the performance over the same two links when used in an SD-WAN.

Conclusion

Meeting the performance requirements for wide area traffic, particularly real time traffic like voice and video, has been an expensive and time-consuming challenge to network managers. That journey has led us through frame relay and ATM, and now users are faced with a choice between expensive MPLS services or less costly Internet connections that cannot guarantee latency, packet loss, or jitter that are so critical to real time traffic performance. SD-WAN offers a new option to use the less costly Internet service but use intelligence embedded in the network to optimize the performance of the network.

SD-WAN is one of the first big deliverables to come out of SDNs, and it's a technology that every WAN manager should be taking a look at.

Michael Finneran is a consultant with dBrn Associates in Hewlett Neck, NY, and industry analyst with over 40 years of experience in the networking field. He is a frequent contributor to NoJitter.com and UCStrategies.com and chairs the Mobility track at Enterprise Connect.

•

by Ron Kovac, PhD
Ryan Patterson &
Dominic McClung

IoT: The Internet of Things

What are we to do with it?

The Internet of Things (IoT) is poised to be the third generation of the Internet and a revolution in the technology industry. Experts predict that by the year 2020 there will be over 50 billion IoT devices that generate over $8 trillion in revenue over the course of the next decade. These numbers highlight the large changes that are on the way not only for industries but for academia as well. To help prepare for this upcoming change, the Intelligent Networked Devices institute (INDi) was started at Ball State. INDi is working to research human interactions with IoT devices and to explore how IoT will affect academia. INDi conducted a study during the spring of 2016 to estimate the readiness of colleges for the rise of IoT.

What Is It and Why Are We Concerned?

The formal definition of IoT is the network of physical objects embedded with software, electronics, software, sensors, and network connectivity to collect and exchange data. A simple way to think about this definition is that it brings Internet connectivity to ordinary devices that we use every day, such as cars and home appliances. The proliferation of these devices will also introduce several new hurdles in realms of IT that are already challenging—including security, privacy, and data management.

The greatest concern for IoT is security. The lack of any standards for IoT devices places security in the "Wild West" of technology. This has led to many devices completely disregarding security in an attempt to reduce costs, therefore putting consumers and businesses at risk. This means that the IT staff handling implementation of IoT devices must take every precaution possible to ensure that IoT devices do not negatively compromise the security of their network. Surely the students will bring them and expect their full integration into their lifestyles.

Another major concern with IoT is privacy of data. Privacy of data involves a series of challenges from the sharing of consumer data to maintaining data security in high-risk areas such as health care. Industry and academia alike must adapt to the privacy concerns presented by IoT to ensure that they keep employees as well as students safe. There are currently several college campuses around the United States that have open webcams, allowing anyone to spy on what is taking place within the university. While it may not seem like this is a major issue, it could result in major legal implications for med schools that handle large amounts of patient data, for example.

Another major component of IoT is data management. Data collection and analysis is one of the biggest benefits to IoT implementation, but it comes with its own set of problems. One of the biggest hurdles standing in the way of data collection is the question of how to store all of the data generated by IoT devices. Not only will data centers have to increase in size in an effort to hold the massive amounts of data, but the methodology of data centers will also have to change to object-based storage to meet the analytics requirements of IoT.

A major hurdle will be determining who will analyze the data generated in the classroom environment. Will each department hire their own data analytics expert, or will there be a rise of a new data analytics department in academic IT? This also creates the problem of whether or not the employee handling data analytics is an expert of that particular field. If not, how will they know what data is worthwhile? These and other questions must be answered before successful implementation of IoT analytics takes place.

How Are We Doing?

To try to get a sense of how academia was fielding these issues, we surveyed other colleges and universities in Indiana. The survey was sent to CIO-level professionals for all higher-education organizations in the state of Indiana. We plan to go national with this survey, but the state of Indiana acts as a baseline. The survey was returned in early April, and we compiled the results in early May.

The survey had multiple sections. The first was baseline information to gauge knowledge and interest in IoT. This gave us an understanding of how these CIO-level professionals perceive IoT and of their concerns regarding the issues of IoT. We then surveyed their current and future plans in dealing with the incoming wave of IoT at their particular organization. And we created a time series design about IoT. From this, we determined that IoT has substantially grown in popularity just within the last three years.

For the first section of our survey, Baseline Knowledge, we created a scale from 1 to 10 and averaged the answers from all of the individuals surveyed. This section included questions to determine how an individual CIO-level professional feels about IoT and how it will evolve in the near future. An interesting trend we found is that while many individuals are concerned with security within IoT, they do not think that IoT as a whole is relevant to their department. We feel this is potentially dangerous, because many departments do not think it is their job to research and implement IoT for an organization. It is important for a high-level discussion to take place about IoT and to start putting into action thoughts and plans regarding how to deal with this rising phenomenon.

Hackers Coming in through the Toaster

We must take precautions not to underestimate the impact of IoT traffic on communication servers, and security requires an update in many cases. In the summer of 2016, hackers embedded malware in toasters and other appliances, IoT devices including CCTV video cameras and digital video recorders, causing them to launch coordinated, simultaneous message transmissions that resulted in a 24-hour shutdown of backbone Internet servers on the East Coast of the United States.

No one knows (or those who do are not saying) exactly what type of botnet was established and activated or by whom, although the evidence seems to point to Russian state actors employing Mirai malware. The IoT includes many things one typically would not consider as networkable computers, such as automobiles, major household appliances (e.g., refrigerators), DVRs, webcams, smart TVs, printers, control systems (e.g., HVAC) and security systems that not only are IP addressable but also can initiate alerts and alarms to servers supporting centralized diagnostic tools and other network management tools—there are even intelligent IP addressable light bulbs. I suspect there soon will be intelligent IP addressable toasters, irons, coffee makers, etc. These things are not well secured, if at all. It would be a relatively simple matter for a hacker to gain access to the relevant IP address blocks and default or hard-coded passwords, plant malware and create a botnet that could be activated in its entirety at a given time to launch a DDOS attack and overwhelm Internet routers. That means lights out!

Transition to IPv6

The next section of our survey dealt with IP addressing within their organization. The transition to IPv6 has been a growing concern over the years because of the depletion of IPv4 address space. With IoT coming and the possibility of 50+ billion devices that need to be connected, will this finally be the end of IPv4? We have seen some devices that require an IP address and others that use Bluetooth to communicate with your smartphone. But even if a small portion of those 50 billion devices require an IP address, IPv4-only networks will run into trouble.

Most of the colleges we surveyed felt that they are ready for the transition to IPv6. The core infrastructure is there, and they just need to flip the switch. However, there are still small applications out there that need to be updated. In the past, when the Internet was young, most people on college campuses only needed one IP address for their computer. Today, however, that number continues to increase and is now up to an average three or four per student. With devices such as smartphones, gaming devices, wearables, and tablets, college campuses are dealing with many more IP addresses than in the past. With IoT sensors and actuators, there will be an increased demand for IP addresses.

Regarding IP addressing, a large majority of those surveyed believe they will need more IP addresses as a result of students introducing more IoT devices onto the network. While they know that IoT is coming and that it will impact their university, they believe it is still years away. The individuals surveyed think that IoT will not have a major impact on their organization for three, four, or even five or more years.

Based on our research, we think the impact on campus will come much sooner than when our survey respondents expect. Talks about IoT need to start happening now in order to be ahead of the curve. That way, when students begin buying and bringing IoT devices, they will not be opening security holes that can compromise data. As we all know, students expect to have their devices work perfectly with the network with minimal setup.

Results of our survey show that not much formal discussion about IoT is taking place on campus. We asked a range of questions covering many areas that were used to gauge how IoT is being discussed and implemented throughout colleges and universities. Many institutions are just beginning to think about IoT and trying to answer the questions of when and how much IoT will affect their operations. Looking ahead a few years, colleges

▶

and universities are planning to start more formal talks and carry out strategic implementation in an effort to tackle IoT.

Time Series Design

We decided to perform a time series analysis for IoT occurrences. A time series is a sequence of measurements of the same variable collected over time. It allows us to observe the dramatic increase in awareness of IoT and research.

The number of scholarly articles that focus on IoT continues to grow. We chose a couple of the large educational publications and analyzed how often the term "Internet of Things" appeared in scholarly articles or white papers. Just three years ago, there were very few. Now, there are almost two dozen in just one year. People want to know what is new in the market and how the technology is maturing and progressing. Because of this, there has been a dramatic increase in Google searches over the year. People are talking about IoT everywhere, and consumers are showing interest in the products. IoT has been all over the news in recent months and years. More and more, companies are spending time and research to develop IoT products. This both helps company operations and meets consumer needs, which ultimately results in increased sales.

Conclusion

In its current state, IoT has introduced more questions than answers. Two of those questions are, "What devices do I need?" and "How do I get those devices to collect the data that I want?" In addition, there are many administrative questions that will be presented with the implementation of IoT. Here are three of the most common questions we found:

- What changes to our school's policies need to be made, especially concerning best effort?
- How do we handle charging for the additional services we will need for IoT to function on the network?
- Who will handle the data analytics and collection that comprises a large part of the demand of IoT?

While these and other hurdles are currently standing in the way of IoT, it is only a matter of time before IoT is implemented everywhere, changing not only industry but academia as well.

Ron Kovac, PhD, a former ACUTA president, is director/professor at Ball State University. Contributing to this article were BSU graduate assistants Ryan Patterson and Dominic McClung.

•

How to Choose Good Passwords

The following information was taken from information published by the Department of Homeland Security on their official website: https://www.us-cert.gov/ncas/tips/ST04-002. The site provides considerable information about hacking, how to prevent it, and how to mitigate if it happens.

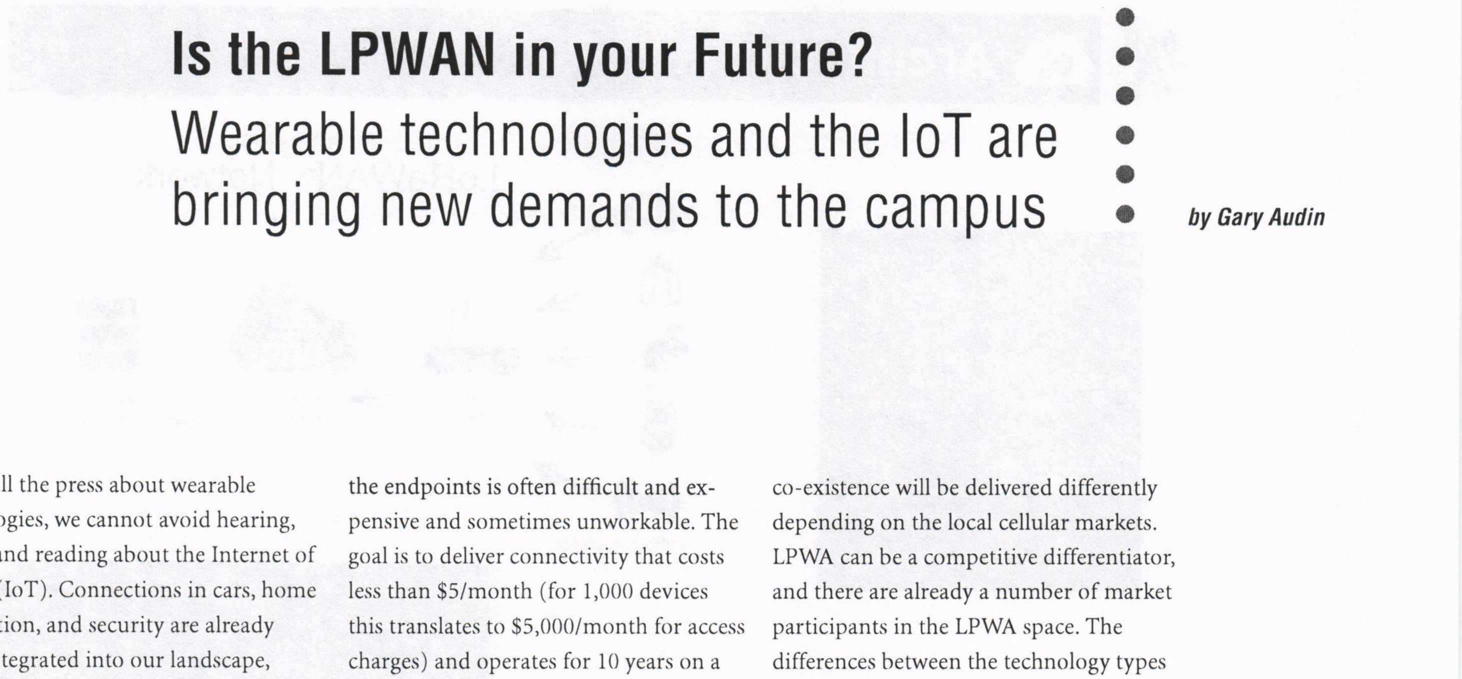
Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to crack them. Consider a four-digit PIN. Is yours a combination of the month, day, or year of your birthday? Or your address or phone number? Think about how easy it is to find someone's birthday or similar information. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to dictionary attacks, which attempt to guess passwords based on common words or phrases.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IlTpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Changing the same example used above to "Il!2pBb." creates a password very different from any dictionary word.

Longer passwords are more secure than shorter ones because there are more characters to guess, so consider using passphrases when you can. For example, "Passwd 4 miemale!" would be a strong password because it has many characters and includes lowercase and capital letters, numbers, and special characters. You may need to try different variations of a passphrase—some applications limit the length of passwords, and some do not accept spaces. Avoid common phrases, famous quotations, and song lyrics.

Don't assume that once you've developed a strong password you should use it for every system or program. If attackers do guess it, they would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts:

- Use different passwords on different systems and accounts.
- Don't use passwords that are based on personal information that can be easily accessed or guessed.
- Use a combination of capital and lowercase letters, numbers, and special characters.
- Don't use words that can be found in any dictionary of any language.
- Develop mnemonics such as passphrases for remembering complex passwords.
- Consider using a password manager program to keep track of your passwords.



Is the LPWAN in your Future?

Wearable technologies and the IoT are bringing new demands to the campus

by Gary Audin

With all the press about wearable technologies, we cannot avoid hearing, seeing, and reading about the Internet of Things (IoT). Connections in cars, home automation, and security are already being integrated into our landscape, and exponential growth is part of every forecast.

IoT is entering the education market as well, with IoT devices that will soon be supporting building maintenance, building operations, energy management, and security. We will also see IoT endpoints in agricultural settings (such as measuring the environment and use of resources) and even discover IoT devices in vehicles, lawn mowers, tractors, and construction equipment. Higher ed institutions must add to their agendas consideration of IoT devices, their network connections, and their cost.

IoT Device Characteristics

The institution needs to focus on IoT devices in the mobile-to-mobile (M2M) space that are low cost, consume very little power, and are powered by batteries that do not need recharging or replacement for years.

IoT devices may be separate or embedded in other devices such as a vehicle or building HVAC machinery. The number of addressable devices—which could be in the thousands—will likely have wide geographic distribution.

Budgeting will be a significant challenge because IoT can require a large number of endpoints, and wiring up all the endpoints is often difficult and expensive and sometimes unworkable. The goal is to deliver connectivity that costs less than $5/month (for 1,000 devices this translates to $5,000/month for access charges) and operates for 10 years on a single AA battery.

The network architecture for wireless IoT devices should:

- Support long-range communications
- Operate with low power and long battery life
- Manage a large number of endpoints
- Support both low and high latency (delay) applications
- Deal with radio interference
- Deliver secure communications
- Operate with one way and bi-directional communications
- Allow a range of applications, many of which have yet to be discovered

Introducing Low Power Wide Area Technologies

How does Wikipedia define LPWA? "Low-Power Wide-Area Network (LPWAN) or Low-Power Network (LPN) is a type of wireless telecommunication network designed to allow long-range communications at a low bit rate among things (connected objects), such as sensors operated on a battery. The solution to these issues may lie with a new form of cell service called Low Power Wide Area (LPWA) technologies."

LPWA providers need to co-exist with the cellular mobile network and other short-range technologies. This co-existence will be delivered differently depending on the local cellular markets. LPWA can be a competitive differentiator, and there are already a number of market participants in the LPWA space. The differences between the technology types include the radio spectrum used (licensed versus license-exempt) and the network provider's local market strategies.

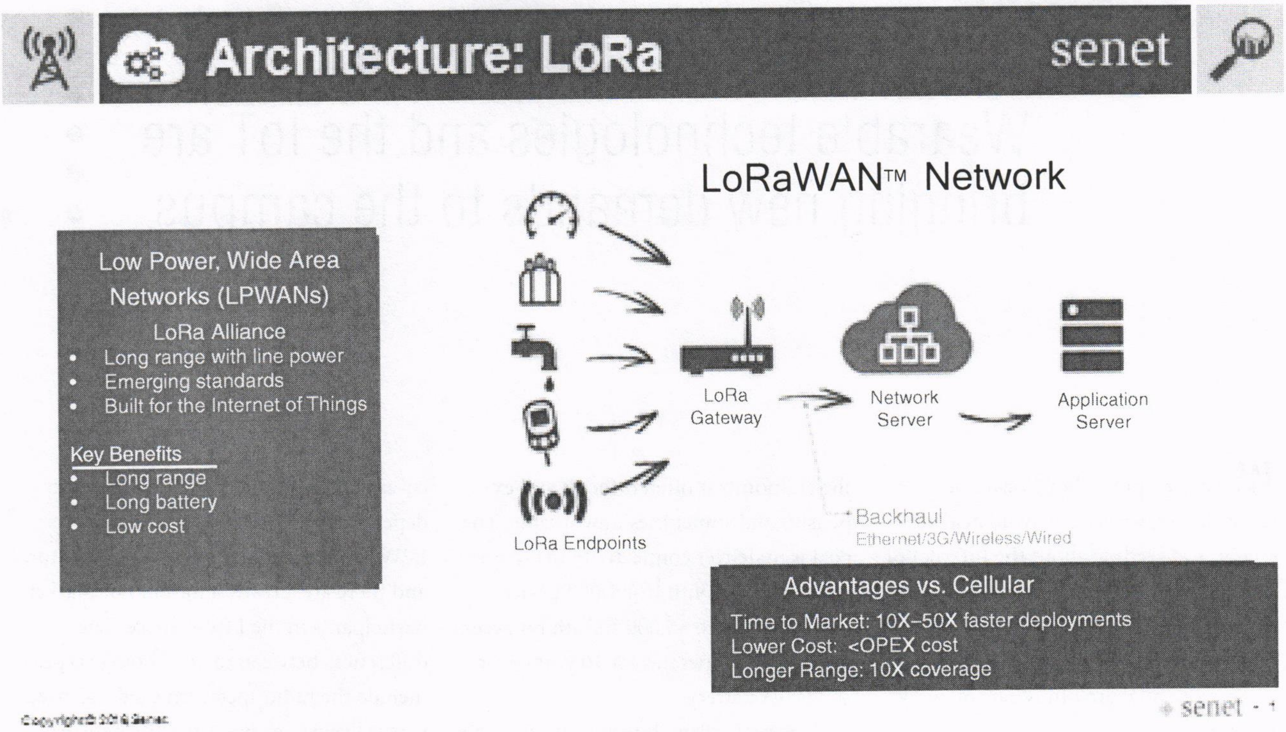
The LoRa® Alliance

According to their website, the LoRa Alliance™ is "an open, non-profit association of members who believe that the Internet of Things era is now! Our members are collaborating and sharing experience to drive the success of the LoRa protocol, LoRaWAN™, as the open global standard for secure, carrier-grade IoT LPWA connectivity. With a certification program to guarantee interoperability and the technical flexibility to address the multiple IoT applications—be they static or mobile, we believe that LoRaWAN can give all THINGS a global voice."

The LoRa® Alliance's mission is to produce a global standard for LPWA that enables and stimulates IoT, machine-to-machine (M2M), industrial, and consumer applications. To drive the worldwide adoption of LoRaWAN, members share knowledge and experience to guarantee interoperability among operators and IoT endpoints.

LoRaWAN targets IoT devices such as secure bidirectional communication, mobility, and localization services. The

▸



Low Power, Wide Area Networks (LPWANs)

LoRa Alliance

- Long range with line power
- Emerging standards
- Built for the Internet of Things

Key Benefits

- Long range
- Long battery
- Low cost

Advantages vs. Cellular

Time to Market: 10X–50X faster deployments
Lower Cost: <OPEX cost
Longer Range: 10X coverage

Copyright© 2016 Senet

standard provides interoperability among IoT devices without requiring complex local installations.

LoRaWAN network architecture is usually configured in a star-of-stars (cluster) topology in which gateways support a transparent bridge relaying messages between IoT devices and a network server. Gateways are connected to the network server through IP connections. IoT devices use a single-hop wireless communication to one or more gateways. IoT device communication is expected to be bi-directional. Multicast operation supports operation software upgrades or other mass distribution transmissions to reduce the communication time, thereby conserving cellular network time. *See "A technical overview of LoRa® and LoRaWAN™" https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf for more information.*

Are All LPWA Implementations the Same?

No, there are two competing open-standards-based technologies, which are LoRa and proprietary, and more vertically integrated solutions like Sigfox and Ingenu. These two provide only uni-directional communication to a limited number of applications.

A LoRa-based network offers bidirectional communication, mobile device support, adaptive data-rate support, and strong security features for a rich and diverse ecosystem of IoT applications for a variety of markets.

Are there interoperability issues?
Interoperability is not an issue if you use a LoRa solution. There will be interop issues if someone uses the other LPWAN networks that are proprietary.

Interoperability is a key part of the LoRa Alliance mission that offers a certification program to guarantee interoperability. The LoRaWAN™ certification program provides assurance to end customers that their application-specific end devices will operate on any LoRaWAN network. The program includes a vigorous suite of interop testing designed to confirm that the end device meets the functional requirements of the Lo rotocol specification.

If you consider LoRa certified services, you will have a wider range of endpoints available for IoT application.

These three blogs and a podcast provide more background on IoT and LPWA:

- LPWA Live for IoT at http://www.nojitter.com/post/240171930/lpwa-live-for-iot
- IoT at the Network Edge at http://www.nojitter.com/post/240172079/iot-at-the-network-edge
- Are You New to IoT? at http://www.nojitter.com/post/240170952/are-you-new-to-iot.
- A podcast is available as well, "LPWA for IoT Connections" at https://telecom-reseller.com/2016/07/13/lpwa-for-iot-connections/.

Gary Audin is a consultant with many years of IT and telecom technology experience. He writes on technology topics such as this at nojitter.com. Reach him at delphi-inc@att.net.

•

Ingredient for Wireless Success: DAS

When Wi-Fi isn't quite enough, add DAS to the mixture

by Scott Gregory

College students are the most demanding mobile-technology consumers on the planet. Whether downloading videos from Netflix, uploading photos to social media, or sending the latest assignment to a professor, most students have little idea what technology supports their mobile lifestyles—and they don't care. They just want it to work.

College students, staff, faculty, and visitors bring their own devices to campuses and expect ubiquitous access, anywhere and all the time. To meet expectations, colleges and universities are being forced to spend millions of dollars to provide campuswide coverage and deliver unlimited bandwidth at little or no additional cost to the student. According to Earl Lum, president of EJL Wireless Research, "Many IT staff are looking for a unicorn solution: a free network with unlimited capacity and bandwidth for consumers who don't want to pay anything."

Campuses have invested in Wi-Fi and fiber rings to address many of the communications needs of their staff and students. Using a Wi-Fi access point, students can Skype, Viber, WhatsApp, and make calls using voice over Wi-Fi. On some campuses, the combination of Wi-Fi and the macro cellular network meets the need for communication on campuses, but relying on this approach alone can lead to significant gaps.

According to Lum, for one campus, the wake-up call for change came from a mother who tried to call her freshman daughter for days, and finally contacted the chancellor's office to ask, "Is my child safe and how can I reach her?" She learned that the service provider's network didn't penetrate into her daughter's dormitory, so calls didn't get through.

The 9-1-1 emergency system falls into another communications gap. The wireless carriers are mandated to deliver location data along with every outgoing 9-1-1 call so that emergency first responders and services can locate callers within minutes. No similar service or technology exists for Wi-Fi or voice over Wi-Fi, and carrier Wi-Fi calling is still in early stages of deployment. With heightened concerns about public safety on campus, the lack of outgoing 9-1-1 location services from dorms or classrooms poses unacceptable risks of liability.

A third gap will be more obvious in the near future. Tens of millions of square feet of new buildings are being constructed on campuses nationwide, many of them LEED certified. The new building materials allow virtually no mobile signal to penetrate inside the building from the service provider's antennas outdoors. So mobile devices won't connect to the service provider networks in those buildings either, turning them into cellular dead zones, and amplifying risk in an emergency.

According to Donny Jackson, editor of *Urgent Communications:* "In these energy-efficient buildings, the idea that radio signals from an outdoor tower consistently will be able to penetrate inside a building to provide indoor coverage—particularly coverage that does not drain battery life from a device—no longer is realistic. Instead, a more reliable approach is to design coverage inside a structure" with in-building networks.

Balancing Wi-Fi Traffic

Another complicating factor is the increasing load on Wi-Fi networks. Suppose that a large university has 5,000 to 10,000 users relying on Wi-Fi that addresses gaps in the macro cellular service. As more mobile users adopt voice over Wi-Fi, demand on the campus Wi-Fi network rises, prompting network upgrades. Already many campuses are experiencing heightened demand from data traffic alone.

Many IT staff are looking for a unicorn solution: a free network with unlimited capacity and bandwidth for consumers who don't want to pay anything.

Wi-Fi does not possess the bandwidth and throughput of wired networks. Campus IT departments must move access point (AP) locations, or add additional APs, to deliver services as capacity requirements continually change and increase. Physically shifting and deploying new infrastructure adds to costs.

Rather than doubling down on Wi-Fi, some campuses are balancing their investments by using private spectrum from cellular carriers, delivered via DAS (distributed antenna systems), to address growth in voice and data traffic, while preserving their public spectrum. By combining

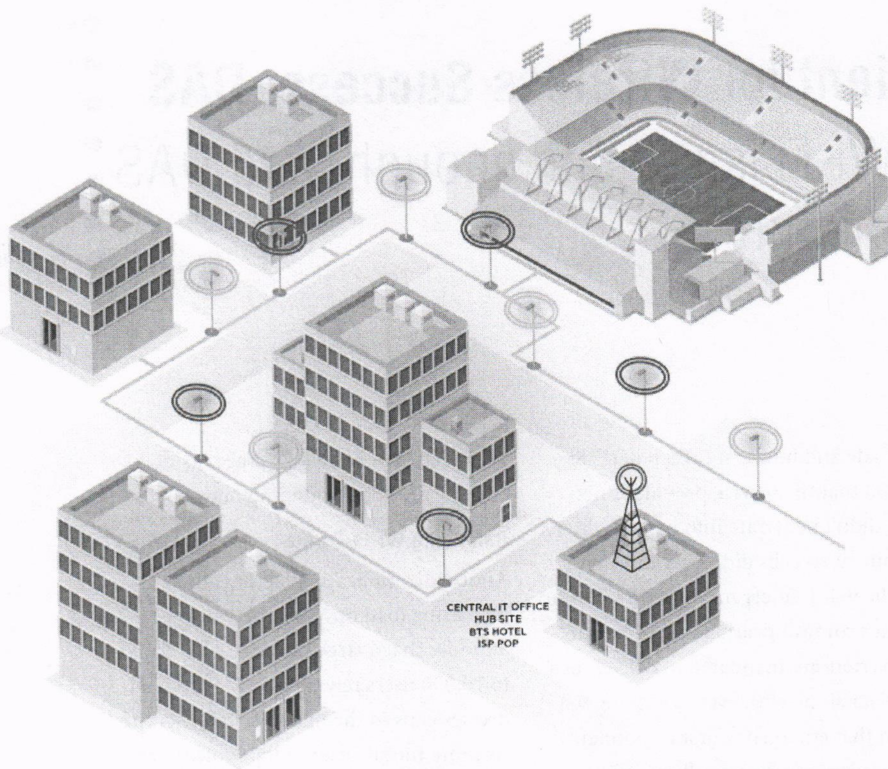


Figure 1. Example of Outdoor Campus DAS Solution. The connected university requires wireless solutions that keep students, faculty, administrators, operations personnel, visitors, and first responders connected.

licensed and unlicensed spectrum, campuses can offload traffic to the most cost-effective network as demands inevitably increase.

So what is DAS?

Imagine that the macro cellular network has been shrunk down so that it can be deployed in buildings or across a college campus. Mobile-service providers connect to a centralized head end that connects, in turn, to the campus network. Remote antennas on the campus network radiate RF signals to smartphones on campus, like sprinklers from a hose. The DAS network extends and strengthens the service provider's signal in places where it is weak, lacks capacity, or suffers from RF interference.

DAS equipment can "densify" the edge of the carrier's network by addressing both coverage and capacity. Coverage issues crop up when the radio signal can't penetrate to a location. For instance, RF signals can have difficulty penetrating through a second or third wall into a building's center. LEED- certified buildings use materials that block RF signals, specifically the glazing used for windows.

As LTE and VoLTE become more prevalent, capacity will have a bigger impact. Lack of capacity is to blame when you see five-bar coverage on your smartphone, but it lacks the bandwidth to load a webpage. Capacity issues can crop up in large, crowded stadiums where thousands of people are uploading photos to the web at the same time, for instance.

DAS equipment can support multiple technologies (3G/4G), frequency bands, and multiple carriers, providing the comprehensive coverage most campuses require. They integrate easily with existing fiber ring networks and can be flexibly deployed where needed.

Gigabit Ethernet fiber multiplexing solutions will increasingly be deployed to address fiber exhaustion. Data throughput and speed are typically constrained by the point-to-point fiber- optic links that connect campus buildings. Fiber multiplexing solutions use wavelength divisional technologies to channelize fiber strands—increasing the capacity of existing fiber deployments without the need to install or lease costly new fiber strands. As an example, a single strand of fiber can deliver multiple wavelength channels each running symmetrically at 1Gbps up and down stream. This represents significant CAPEX and OPEX savings.

Fiber infrastructure is physically smaller and lighter than copper, and is easily installed by technicians. Most importantly, fiber delivers almost unlimited room for future bandwidth expansion.

The connected university requires wireless solutions that keep students, faculty, administrators, operations personnel, visitors and first responders connected.

Controlling the Last Wireless Mile on Campus

With DAS, campuses can maintain control over the last mile of their wireless networks, just as they already control their PBX, LAN, WAN, and WiFi networks. Think of your campus as a population center with growing demands that need to be met over time. Because DAS relies on a centralized head end, campuses can spread capacity over their fiber network gradually as demand grows, rather than negotiating with carriers for network build-outs or small cell deployments.

On the 8,709-acre Duke University campus, more than 200 buildings are connected to the DAS network. The university owns and controls this vital asset. Carriers paid a pro rata share of the network build-out, with a seven-year, self-renewing commitment to network refreshes as the technology evolves.

Bob Johnson, Duke's senior director of communications infrastructure and global strategies, evaluated various approaches before deciding to maintain control over the DAS network. He persuaded carriers to join the university-owned model by running the numbers. "We've got 45,000 people working on campus or attending Duke. We said to the carriers, 'If you are not in on the DAS network, you'll miss out on four to eight years of a Duke demographic, and you'll lose those subscribers." AT&T, Sprint, and Verizon partnered with Duke, with the initial investment for the in-building wireless network costing approximately $1.00-$1.50 per square foot. The carriers are paying for usage either by sectors or by frequencies.

In Duke's hub-and-spoke model, a fiber ring connects the buildings, with carriers connecting to the network at a single head-end location. SOLiD's DAS equipment brings signal into the buildings, supporting voice and data traffic. The entire system is designed to scale as demand increases over time.

Johnson chose to invest in both Wi-Fi and DAS networks. He says, "You need both technologies today. With DAS, when fans leave Duke's stadium after a home game, they can continue the fan experience all the way home." For more details on Bob's decision-making process, see this video: http://www.solid.com/bold-ideas/the-middleprise.html

Looking Ahead

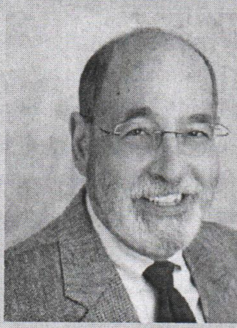
The problems facing higher-education campuses will grow if they continue to struggle with disparate networks they don't control and unlicensed frequencies they cannot maximize or that do not have a clear ROI. The urgent need to provide clear communication for public safety and the exponential growth in demand for capacity means that technology solutions will need to be consolidated offerings that provide unfettered access for students, employees, safety personnel, and the general public.

Scott Gregory is director of marketing at SOLID. Reach him at scott.gregory@solid.com.

•

Snapshot

DIDs for ELINs?



Geoff Tritsch
Vantage Technology Consulting Group

Additional DIDs (direct inward dial) for emergency line identification numbers (ELINs) are not so much for callback as they are for location. The PSAP's ANI/ALI databases are static (or at least they cannot be updated in real time) so you need to have a specific phone number associated with each emergency response location (ERL). Most E911 centers are only able to look up location information based on a 10-digit phone number (automatic number identification or ANI). That ANI is associated in the database with a response location (ALI) such as "2nd floor Administration Building" with a street address. In the past, a caller's DID provided both the callback number and the location information as moves were not dynamic and telecom would update the ANI/ALI database daily or as needed.

When doing E911 with a VoIP system, the additional DIDs act as static ELINs associated with a specific ERL in order to provide the required static phone number for the PSAP's ANI/ALI database. The number of additional DIDs required depends on the level of granularity you have selected for 911 location services (one per building, one per floor, one per TR, I per port, ...). If the PSAP needs to call the caller back, they call back on the DID associated with that ERL (the one that shows up on their screen). Part of the purpose of the 911 software from providers like West 911, RedSky, and others is to cache the caller's actual DID and temporarily associate the caller's actual DID with the DID associated with the specific ERL.

To the best of my knowledge, the "unique key" mentioned sometimes for use in place of ELINs presently only applies when you are using a VoIP Positioning Center (VPC). A VPC is a national subscription (read: recurring cost) service that acts as a 911 intermediary and routes calls to the appropriate PSAP. VPCs are especially useful if you have lots of remote workings scattered across multiple calling areas.

Unlike traditional PS-ALI (Private Switch Automatic Location Identification), the VPC solution is not limited to the use of 10-digit ELINs to identify the location of the caller. VPCs can also use a variety of other unique identifiers (MAC, IP, extension) in their national ALI database (different from the regional ALI databases used by the PSAPs) to determine the location of the call. The limiting factor can still be the PSAPs and their ability to use the newer National Emergency Number Association (NENA) data exchange formats. Newer versions of the NENA data exchange formats and Next Generation 911 (NG-911) are intended to bring the data exchange process in line with current technology—but not all PSAPs are on-board as yet.

You can reach Geoff at geoffrey.tritsch@vantagetcg.com.

•

Hot Issues in Communications Technology Law

TCPA, Kari's Law, E911, FCC, FTC and more

by Martha Buyer

It was my privilege to speak at this Fall's ACUTA seminar in Denver. As a result of those presentations and ensuing conversation, what follows will outline some of the hot issues in communications technology law, particularly over the past few months. The topics presented here are not exhaustive—many others are not included. But these areas are relevant, based on both my work experience and events of the recent past.

It's not exactly a disclaimer, but I think that it's important to acknowledge the underlying issues that affect academic communications that are, perhaps, different from those presented in traditional enterprise communications environments. Issues associated with academic freedom and the maintenance of academic integrity combined with scholarship must underlie every discussion about communications technology and the laws that are evolving on almost a daily basis in an academic environment.

The Telecommunications Consumer Protection Act (TCPA) was originally enacted in 1971 when, I suspect, too many federal legislators had their dinners interrupted by telemarketers.

TCPA

The Telecommunications Consumer Protection Act (TCPA) was originally enacted in 1971 when, I suspect, too many federal legislators had their dinners interrupted by telemarketers. The law has evolved to take into account a number of technological innovations, particularly with respect to mobile devices. The TCPA has clear (well, sort of) guidance, particularly with respect to texting and calls made to mobile phones where it is assumed that the owner of the device pays to receive messages. Without going into the long and somewhat twisted history of TCPA, it's important to recognize a couple of relatively recent twists that affect those entities that make outbound calls—particularly those that are made by auto dialers or which do not involve human intervention. Read: robocalls.

Not so long ago, entities could make such calls to consumers claiming that they had an "existing business relationship" with call recipients. This exception applied to numbers that were on the FTC's Do-Not-Call list that were either traditional landlines or mobile devices. However, such exceptions have not existed for the past two years.

The most recent batch of regulatory guidance directly relevant to robocalls made to mobile devices in academic environments allows calls made for three specific reasons, and with specific limitations, to mobile devices. The first is for emergency purposes, the second is with the prior consent of the called party (an individual's mere listing of a number as a contact number is not, in and of itself, such permission), and the third is to collect debts either owed to or secured by the federal government (Note: According to a 2015 study by the Department of the Treasury, the government has $1.3 TRILLION of non-tax receivables, of which $162.1 billion is delinquent.)

Notably, calls made for emergency purposes must really be for emergency medical or safety reasons. No other content is considered tolerable. For example, "there's a fire in West Andrews" (my first dorm) would be acceptable. "There's a fire in West Andrews and the medical clinic is giving flu shots this week" would be a violation. For more information on specifics related to the TCPA, please contact me or your TCPA-compliance staff.

Texting as a Business Practice

It would be my hope that most people understand that texting as a business practice is a bad idea. Period. Always. While it is certainly a convenient communications vehicle, the fact is that the risks associated with texting far outweigh the benefits. For example, potential violations of HIPPA and OSHA requirements, among others, make texting a platform to be avoided in a business context. There's just too much that can go wrong when a message is sent to an unintended recipient.

Kari's Law Update

Kari's Law, named after murder victim Kari Rene Hunt, passed the U.S. House of Representatives in May 2016. The bill essentially forbids the blocking of calls made to 9-1-1, even when a 9, or some other digit, is required for a caller to reach an outside line. While the law awaits a Senate vote, it is currently existing law in Maryland, Pennsylvania, Suffolk County in New York, Tennessee, and Texas, with other states currently contemplating their own versions. (Be advised that state or regional Kari's Laws may vary slightly). The text of the federal law reads as follows:

> (Sec. 2)This bill amends the Communications Act of 1934 to prohibit businesses from manufacturing or

importing for use in the United States, or selling or leasing in the United States, a multi-line telephone system unless it is pre-configured to allow users to directly initiate a call to 9-1-1 (without dialing any additional digit, code, prefix, or post-fix, including any trunk-access code such as the digit "9") from any station equipped with dialing facilities.

Businesses are prohibited from installing, managing, or operating multi-line telephone systems without such a direct 9-1-1 call configuration.

Businesses installing, managing, or operating such systems for use in the United States must configure the systems to provide a notification to a central location at the facility where the system is installed, or to another person or organization regardless of location, if the system is able to be so configured without an improvement to the hardware or software.

Is a university campus a business for purposes of the law? That fight has yet to be fought, but it wouldn't take a great attorney to make the argument that a campus is a business and that compliance with the letter and spirit of the law is "reasonable," the ultimate word in legal parlance!

Security/Privacy

In its regularly scheduled monthly meeting at the end of October 2016, the FCC approved new privacy rules for providers of broadband Internet access service. The new rules were made necessary when broadband service was reclassified as common carrier service in the 2015 Open Internet Order, and thus moved from the realm of the Federal Trade Commission to the Federal Communications Commission. But the new rules, whose final version has not yet been fully released, are also a major step toward aligning the FCC's rules with those of the FTC and some of the states.

The complete final rules have yet to be fully released, and once they are released, providers will have six months from the date of publication in the Federal Register to comply. But there are some important changes that end-users of broadband Internet-access services should be aware

Drones and the Law

They're not quite everywhere, but they are lots more drones around than there used to be. Primarily in the interest of public safety, drone operation is now regulated to an extent that hasn't been seen before. A couple of interesting factoids since new rules became effective in August of this year:

- States and municipalities are prohibited from imposing limits on where drones may be operated or requiring operators to complete certain training. Local laws that address privacy, land use, and local law enforcement are NOT preempted by federal rules.
- The FAA defines an "unmanned aircraft system" or UAS as "an unmanned aircraft that is capable of sustained flight in the atmosphere, flown within visual line of site of the person operating the aircraft, and flown only for hobby or recreational purposes."
- As of December, 2015, all UAS devices must be registered with the FAA. This includes both recreational and commercial-use drones weighing between 0.5 and 55 lbs. Registration information is available at https://register-myuas.faa.gov/. Registrants must be U.S. citizens, and at least 13 years old. The cost for registration is $5.00 for 3 years.
- Commercial drone operators no longer require a pilot's license, although all operators must pass a knowledge-based exam and obtain a drone-specific operator's certificate with a small UAS rating.
- Operators MUST MAINTAIN VISUAL LINE OF SITE with the drone at all times.
- Drones may only be operated only during daylight hours, must stay below 400 feet, and must travel no faster than 100 mph.

of before the new rules take effect. Very briefly, there are a number of areas of interest. Space limits the depth in which these issues can be presented, but each is important in its own right.

The first is that broadband providers must disclose, in clear and obvious terms, the nature of the information that is being collected, as well as general information about the types of entities with whom the information will be shared. Notifications by providers to consumers on changes in terms must be provided immediately (either when the subscriber initially signs up or when the provider changes its policy). Such terms must also be available on the provider's website at all times.

Secondly, there must be formal and clearly defined "opt-in" and "opt-out" provisions not only to notify consumers of what information is being collected, but to identify the types of data for which permission is implied, and does not require explicit permission. Special information, which will require the explicit "opt-in" includes geo-location, children's information, health information, web browsing, app usage history, and most importantly message content.

One other new twist is that the broadband rules will apply to voice services (read: call detail) as well. Call detail records will be included in the special information category. The sharing of any of this information clearly, and unequivocally, requires the customer's consent. The flip side of this is that there is a small amount of information to which the consumer cannot "opt-out" of providing. Most of this relates to information necessary to generate bills, although aggregated information, where personal identifiers have been removed with the purpose of general trending information, may also be shared without consumer-provided consent.

In addition, broadband providers will be required to take "reasonable measures" to protect consumer data from either disclosure or unauthorized use. What's "reasonable" is for a court to decide, but the FCC will be monitoring provider practices, and it's likely that there will be some additional clarification provided in the next Notice of Proposed Rulemaking that the FCC makes on these issues early next year.

Notices to consumers when data breaches occur will also take a more consistent form (and may be completely standardized) that more closely aligns with current standards used by the FTC along with the states. Further, obligations to notify federal law enforcement (FBI, Secret Service) in the event of a breach have also been codified.

More clarification on the finer points of the FCC's action will be available once the complete rules are published in the Federal Register. For the time being, consumers and providers should be satisfied that they know, at a minimum, the direction that rules are evolving.

TDM Migration to IP

Over the summer, the FCC took major steps to lighten the process as incumbent carriers continue their slow but steady migration away from TDM (time division multiplexing) services. At the prompting of carrier advocate USTelecom (in the form of a petition for a declaratory ruling), the FCC agreed that the designation of incumbent local exchange carriers (ILECs) as dominant “when providing interstate mass market and enterprise switched access services” be abandoned since, for all practical purposes in most parts of the country, such providers are no longer dominant. Bang.

This takes a giant step forward in leveling the playing field between the embedded incumbents and other IP-based service providers who are offering similar services without some of the regulatory burdens imposed on the ILECs when they were, in fact, dominant.

Secondly, the FCC created a new and simplified process for evaluating and approving requests from legacy voice providers to transition away from TDM to IP-based services provided that such replacement services provide, according to the FCC, “adequate replacement for a legacy voice service.” This is particularly critical when considering issues related to not only 911 access and general interoperability, but also to services offered in remote and rural areas, with particular attention to tribal lands.

In practical terms, this action means that a provider can—at least legally, if not practically—transition a network from TDM to IP-based in 30 days if the entity seeking such permission can pass a voluntary three-point test. The word “voluntary” is critical. Carriers who cannot—or choose not to—meet the terms of the test can still go through the process “the old-fashioned way,” but the timing for approval will be considerably longer. The three-point test requires:

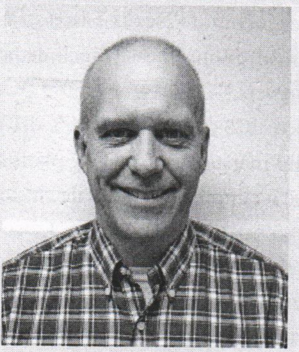
1. Proof that network performance, reliability, and coverage will be substantially unchanged;
2. Proof that access to 911, cyber security, and access for people with disabilities meets current rules and standards; and
3. Proof that the IP-based network will provide compatibility with a defined list of legacy services that remain popular with consumers and small businesses, including home security systems, medical monitoring devices, credit card readers, and fax machines. This requirement is scheduled to fade into the sunset in 2025.

From point 1 above, the potential for litigation over what the word “substantially” means is significant as IP providers struggle to work out some of the technological kinks that exist between legacy equipment and IP services (consider, as an example, fax machines). The same litigation opportunity exists when considering the definition of “current rules and standards.”

The issues associated with the third point are obvious, but not insurmountable. By recognizing the challenges posed by the transition, the FCC clearly recognized and acknowledged not only the technological challenges, but the need to educate consumers on what these modifications may mean to end-users, not necessarily those who are technologically sophisticated or supported.

Martha Buyer is an attorney whose practice is a certified New York Woman-Owned business, primarily focused on telecommunications law. She is also a frequent contributor to No Jitter. Martha can be reached at martha@marthabuyer.com.

Snapshot



David Lutes
Marymount University

We have just deployed Cisco Sourcefire appliance along with Lancope StealthWatch. Everything is up and running but we are still tweaking and integrating everything with our existing Cisco ISE. We also brought on Entrust and are in the process of integrating it with our ERP system for all faculty/staff to access through 2-factor. And we bought into KnowBe4, but I’ve not deployed that yet.

This year was the year of security for our campus since the past two plus years have been nothing but adding capacity through switch, WI-FI, VoIP, and faster throughput on our backbone and cloud connections. I needed order and a simplified way to manage the security aspect of all that we’ve done, and so far I think I might have got what I wanted.

Cisco UCS for HPC

New research computing solutions for higher performance computing increase agility, control, and affordability

Renee Patton & Tae Hwang

If you're using either the public cloud or traditional bare metal for research computing, consider Cisco's innovative use of technology for higher performance computing (HPC) workloads to improve efficiency and performance without compromising on quality.

Traditional HPC clusters are generally difficult to build, use, and manage. These same clusters also present compounding challenges as they grow—in terms of operational staffing costs as well as diminishing returns due to complexity, poor utilization, and administrative overhead.

Also, expanding the cluster's infrastructure (compute, network, or storage components) often creates interoperability issues that can result in degradation of both performance and stability as well as software vendor support issues.

Numerous factors—costs, performance, data sovereignty, security, compliance, risk, intellectual property, integration with on-premises resources—have to be weighed and balanced; and in some instances, HPC workloads may not be a good fit for public-cloud approaches.

The main driver of cloud adoption is an increase in accessibility, agility, and availability of IT resources to users within the organization. The applicability of cloud computing to science and data analytics is clearly indicated by the increased use of public-cloud providers such as AWS, Azure, and Google Compute in this area. However, due to numerous factors—cost, performance, data sovereignty, security, compliance, risk, intellectual property, and integration with on-premises resources, HPC workloads are rarely a good fit for public-cloud consumption.

Giving researchers easier access to compute and storage resources helps them make discoveries, and share breakthroughs, faster. For instance, at Wake Forest University in Winston-Salem, North Carolina, research findings are driven by the capabilities of an intelligent HPC system. For the instructors and researchers who use the cluster, the priority is always a more powerful computer, which in turn tackles more difficult problems.

Often, the cost to transfer and store data in public clouds is not considered and can be substantial (on average a 30 percent premium on top of compute resource costs), and these costs pull dollars away from research programs. Furthermore, certain workloads require bare metal performance, which is typically either not available in a public-cloud platform or is cost prohibitive.

Alternatively, a properly designed, deployed, and managed private cloud can provide the agility of public cloud but with the flexibility and performance characteristics of on-premises HPC infrastructure at a significantly lower cost.

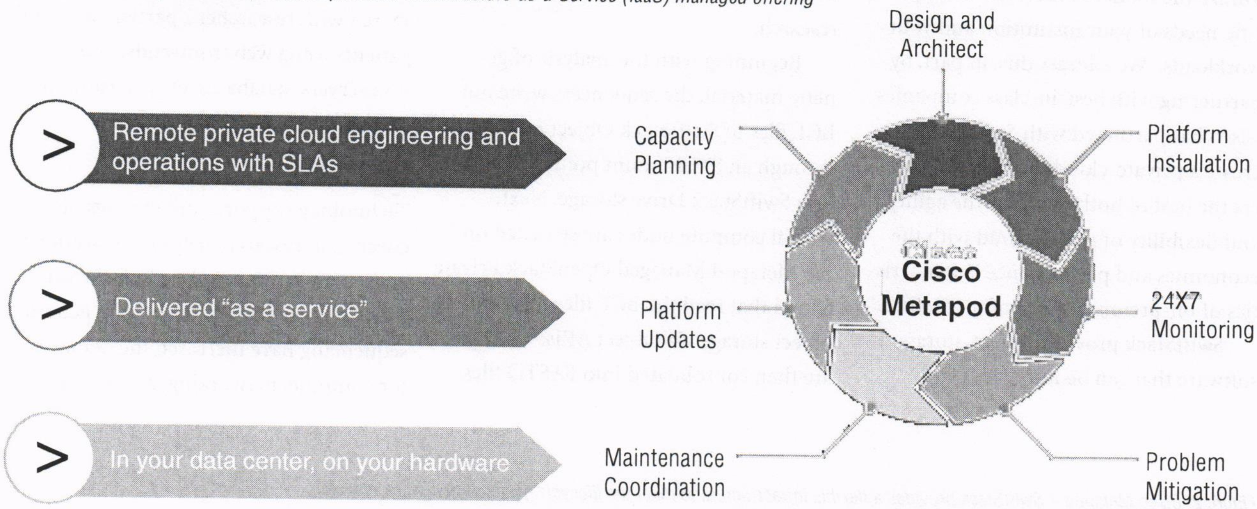
Cisco and the Cloud

Cisco's research computing vision is based on three pillars: Unified Computing, Unified Fabric, and Unified Network Services. Aside from providing carrier-grade performance, availability and stability, what makes Cisco private-cloud architecture unique is our ability to collect all cloud elements into a single, converged platform. This greatly reduces complexity, lowers cost, and eases administrative overhead.

Cisco's Unified Computing System (UCS) server is at the heart of our research computing strategy. UCS includes blade servers with a fabric-integrated chassis and chassis extenders, or rackmount servers and a set of multiprotocol switches (the Nexus line) that connect servers and storage. Both Cisco offerings are designed to couple software virtualization and cloud tools (such as VMware's vSphere and vCloud) and create virtualization-friendly data centers that are then connected to become cloud data centers. Cisco's UCS blade strategy integrates all data center and network components into a Cisco-created cloud, and the rackmount Nexus-based strategy allows institutions to easily include non-Cisco servers.

Cisco UCS creates a network-driven, centrally-managed computing platform. Because it simplifies large-scale cluster deployment and configuration, Cisco UCS helps researchers and their teams shorten deployment, reduce maintenance time, and realize a lower total cost of ownership. And, Cisco UCS makes it much easier to expand clusters and refresh equipment as research initiatives require. Whether customers choose to build private cloud or bare metal HPC, or install a combination, Cisco UCS simplifies the deployment and operation of the research computing.

Figure 1. Cisco Metapod is an OpenStack-powered Infrastructure-as-a-Service (IaaS) managed offering



HPC at Wake Forest

At Wake Forest University, the use of a high performance computing cluster started out as a need in the physics department, not the IT department. Knowing its applicability and importance to all STEM areas of study, the university centrally backed and funded the cluster, making it an IT department offering. As cluster use expanded, the system's architect needed help managing the cluster's growth and increasing complexity, which is where Cisco UCS came in.

For Wake Forest University and others, Cisco UCS also reduces the cost of staff, infrastructure, power, space, and cooling with a versatile platform that converges compute, network, and storage into a unified platform with a single management interface. Before using Cisco UCS, Wake Forest was limited in terms of networking—its prior systems were connected via 1G Ethernet cluster wide, with faster infiniband restricted within a few chassis. Cisco UCS enabled up to 20G connectivity throughout the entire infrastructure, giving the university a significant advantage, allowing researchers to push more jobs out more quickly and to obtain more resources without limitation. Holistically, this means that the cluster is highly available to researchers, and the infrastructure is more flexible.

In addition to providing a common interface to a converged infrastructure, Cisco UCS also provides a single programmatic API for software-defined compute, network, and storage provided by OpenStack to decrease administrative burden on staff and to increase operational efficiency and response to users. Further, Cisco UCS provides a wide range of options, including a dense form factor, which can reduce the number of components and amount of data center space needed for efficient cloud computing.

Wake Forest University's use of HPC and Cisco UCS has helped the university move beyond studying physics calculations within the cluster; now, research has expanded to biology, chemistry, computer science, math, biomedical-engineering, romance languages, and the school of business.

Metapod and SwiftStack

Another option for HPC workloads is Cisco Metapod, an OpenStack-powered Infrastructure-as-a-Service (IaaS) managed offering that delivers a reliable and programmable infrastructure for research. This production-ready, on-premises solution is deployed, managed, and remotely operated 24x7x365 on your behalf by Cisco engineers and provides a public cloud experience, but in your own data center or colocation facility of your choice. (See Figure 1.)

Administrators receive the visibility and control of the infrastructure that they require, while researchers gain the agility and self-service access that they desire. Either third-party hardware or Cisco validated UCS designs can be used, and the turnkey cloud is deployed within 14 days or less. Once deployed, a dedicated team of Cisco engineers provide continuous monitoring and management of the platform, both hardware and software, including continuous updates and upgrades. This enables researchers to reap the benefits of the feature velocity in the open source OpenStack development community without burdening administrators with new skill or staff acquisition. Multi-tenancy, elasticity/auto-scaling, and multi-discipline workloads increases both infrastructure utilization and value. All of this is covered by a 99.99%, financially backed, uptime service level agreement. In short, Cisco de-risks and de-costs the path to private cloud adoption.

In addition, Cisco understands that an important part of the private-cloud value proposition is the ability to cus- ▸

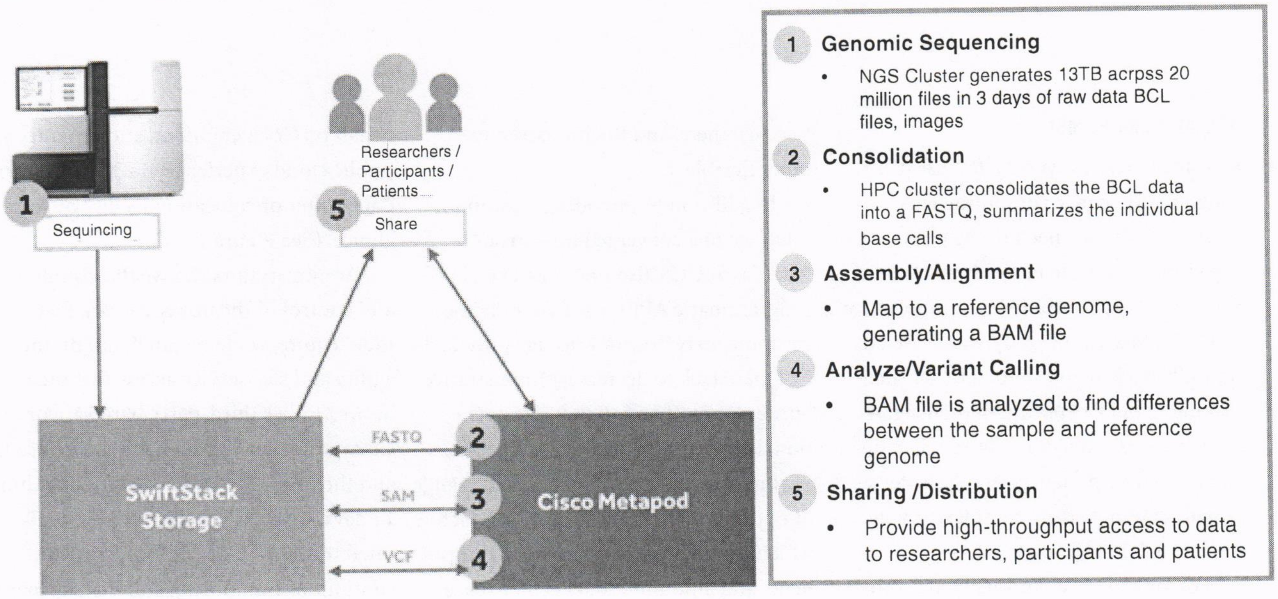
tomize the model to meet the very specific needs of your institution and your workloads. We address this, in part, by partnering with best-in-class companies. Cisco has partnered with SwiftStack to create a private-cloud solution that delivers the best of both worlds—the agility and flexibility of public cloud with the economics and performance characteristics of on-premises HPC infrastructure.

SwiftStack provides object-storage software that can be integrated with Metapod and runs on Cisco UCS hardware in your own data center. The solution delivers an Amazon S3-like object-storage service on-premises to complement the Metapod private-cloud offering. Built on OpenStack Swift, SwiftStack provides the proven scale of public cloud with management made for enterprises.

One research application for Metapod + SwiftStack is within genomics. Genomics is a complex operation encompassing a sequence of steps, each with demanding requirements. Cisco Metapod + SwiftStack provides a flexible infrastructure to meet the lifecycle needs of genomics research.

Beginning with the analysis of genetic material, the sequencers write out BCL files to SwiftStack Object Storage through an SMB mount point provided by a SwiftStack Drive storage. Next, virtual compute nodes are spawned on the Metapod Managed OpenStack Private Cloud that read the BCL files from the object storage via Object APIs. These files are then consolidated into FASTQ files that summarize the individual base calls and their associated quality scores. (See Figure 2.)

Figure 2. Cisco Metapod + SwiftStack provides a flexible infrastructure to meet the lifecycle needs of genomics research.



1 Genomic Sequencing

- NGS Cluster generates 13TB acrpss 20 million files in 3 days of raw data BCL files, images

2 Consolidation

- HPC cluster consolidates the BCL data into a FASTQ, summarizes the individual base calls

3 Assembly/Alignment

- Map to a reference genome, generating a BAM file

4 Analyze/Variant Calling

- BAM file is analyzed to find differences between the sample and reference genome

5 Sharing /Distribution

- Provide high-throughput access to data to researchers, participants and patients

In parallel, more virtual compute nodes read the indexes of the FASTQ files created in the previous step to align with a reference genome. SAM files are then created with aligned sequence data and metadata that can be compressed into binary BAM files. Finally, the BAM file is analyzed for differences in the sequenced genome, and a reference genome and the variants are written out to a VCF file. All of the data produced in these steps can be stored long-term in the SwiftStack cluster for further analysis. This data can then be shared with researchers, participants, and patients using web front-ends, application servers, databases, etc., all running on the Metapod infrastructure.

Final Thoughts

Technology supports and elevates discoveries in research, helping institutions and organizations evolve clinical treatments. In particular, advances in genomic sequencing have increased the demand for compute, networking, and storage. As a result, HPC is undergoing the same evolution to cloud-native technologies as the rest of enterprise IT.

When evaluating approaches to HPC, consider alternatives that will enable you to take advantage of new, cutting-edge technologies that save time and money—and deliver superior results.

Renee Patton, US Pubic Sector Director of Education at Cisco, and Tae Hwang is US Public Sector Technical Solutions Architect. Reach Renee at rpatton@cisco and Tae at tahwang@cisco.com.

•

Institutional Excellence Award

California State University Fullerton's Shared Cloud Services

The Information Technology Department at CSUF (CSUF) implemented cloud solutions that are shared by multiple institutions to achieve the goals of the California State University system's Synergy project. The Synergy project was enacted in 2010 by the CSU system in order to reduce administrative costs by joining together to find ways that things can be done more effectively and efficiently. Through the shared cloud services, CSUF has been able to successfully create partnerships with other campuses, improve services, implement cutting-edge technologies, and reduce costs, which has, in turn, benefitted the students, the CSU system, and the State of California.

Collaboration Underway

The shared services are:

1. CSUF hosting disaster recovery infrastructure for San Francisco State University
2. CSUF hosting the production environment for the CSU Chancellor's Office
3. Learning Management Solution (LMS) – CSUF and CSU Los Angeles
4. Campus Business Intelligence (BI) solutions using CSUF's Campus BI baseline model – CSU Los Angeles, CSU Dominguez Hills and CSU San Bernardino.
5. Telephone Services – CSUF and CSU Dominguez Hills (CSUDH)
6. Virtual Computing Lab (VCL) – CSUF and University of California, Irvine

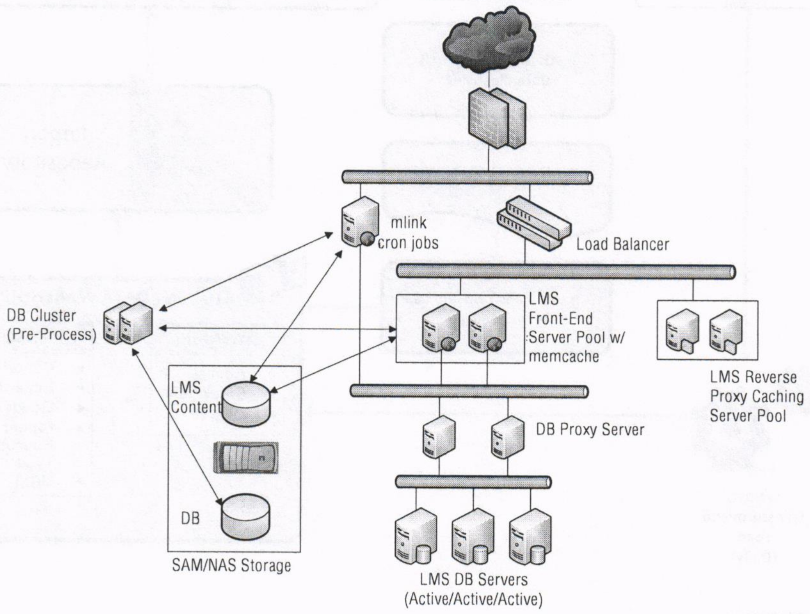
University leadership has stated its intent to reduce IT expenditures and consolidate IT services. IT synergy efforts guided by the CIOs have, comparatively, made the most progress among ongoing initiatives. CSUF embraced the synergy project and collaborated with multiple campuses.

CSUF's collaborations with other campuses began prior to the Chancellor's Office's initiation of the Synergy project. For example, CSUF and San Francisco State University host each other's disaster recovery infrastructure. In 2010, the CSU Chancellor's Office decided to close their data center. CSUF collaborated with the CSU Chancellor's Office to host their production environment at our campus' main data center.

In 2011, CSUF implemented a new learning management system (LMS). CSUF had been using an industry-leading learning management system for several years. The high cost of the LMS system and the operational instability led the campus to look into alternative systems. After considering various LMS solutions, an open-source system was introduced to the campus. LMS can be a major expense for an institution, especially when implementing a robust, versatile LMS that can support many courses for a large-sized institution like ours. The new LMS features dashboards, learner tracking, and multimedia support. This open-source LMS also gives faculty the ability to create mobile-friendly online courses and integrates with third-party add-ons. This conversion resulted in significant savings on product-license and support-maintenance contracts.

CSU Los Angeles is one of the 23 CSU campuses located about 30 miles northwest of the CSU campus. Through collaborative discussion between the CIOs of both campuses, an agreement was reached to host the CSU Los Angeles

Figure 1. System Architecture Diagram of the Learning Management System (LMS)



LMS on the CSUF infrastructure. CSU Los Angeles is a quarter system while CSUF is a semester system. The difference in schedules had its set of challenges and benefits. To minimize disruptions to either of the campuses, the IT teams worked collaboratively and developed operational support procedures including an annual maintenance plan. The IT teams of both campuses meet regularly to discuss operational issues and discuss continuous improvement needs for faculty and students. (See Figure 1 on page 29.)

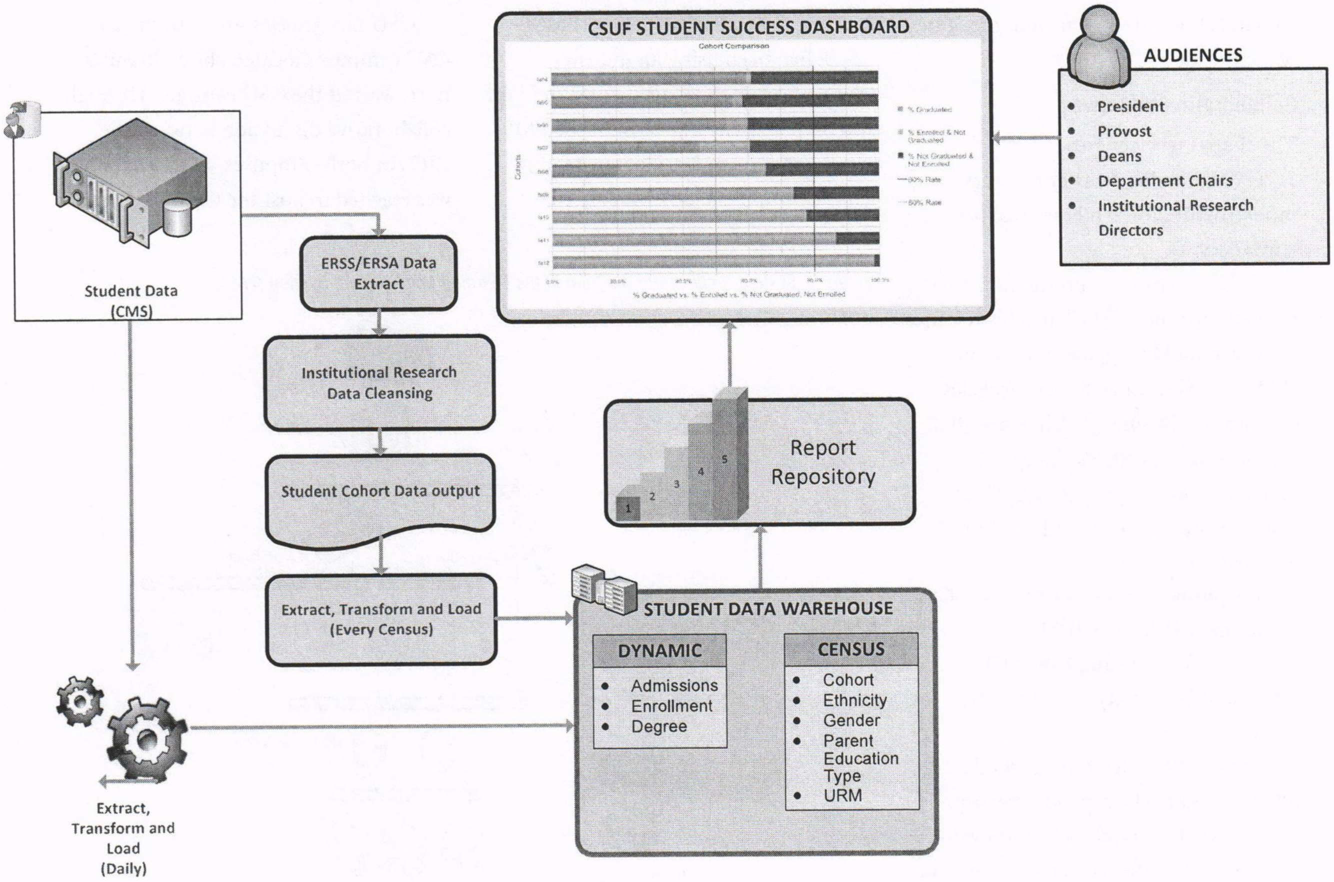
The Business Intelligence Solution

Another CSUF collaboration is our campus business intelligence (BI) solution. CSUF's strategic plan is centered on student success. In support of this, we developed a student-success dashboard that tracks and compares the performance of first-time freshmen and transfer students. This information is broken down by gender, ethnic-race, parents' education, underrepresented status, college at entry, latest college, and prior institutions. It also lets users focus on information for a particular subgroup of students that can be helpful in intervention. Of course, this information is refreshed daily and limited to specific users based on the security settings of the application.

The IT department (IT) and the Institutional Research department (IR) worked together to create the student success dashboard. The dashboard was built using an enterprise business intelligence system using the waterfall software development life-cycle model. IR created the product requirements that included the aggregate performance indicators, the charts and tables for the dashboard, and the high-level query, dashboard design, and implementation. IR also performed data validation and testing. IT created the underlying data warehouse and the extract, transform, and load processes. Employees can access the dashboard via their portal where there is a single sign-on process for authentication.

The demonstrated benefit of this BI solution attracted many CSU campuses to use it. CSU Los Angeles, CSU San Bernardino, and CSUDH utilize this shared infrastructure to deliver various dashboards to their campus constituents. The Campus Business Intelligence project has been very successful, and all three campuses are live with their Campus Solutions reports, including Fullerton's Student Success Dashboards. Typical deployment using Fullerton's BI solution model takes about four months and includes standing up the infrastructure, data validation, dashboards and reports

Figure 2. System Architecture Diagram for Business Intelligence (BI) System


CSUF STUDENT SUCCESS DASHBOARD
Cohort Comparison
Cohorts
% Graduated
% Enrolled & Not Graduated
% Not Graduated & Not Enrolled
0.0%
20.0%
40.0%
60.0%
80.0%
100.0%
% Graduated vs. % Enrolled vs. % Not Graduated, Not Enrolled
AUDIENCES
President
Provost
Deans
Department Chairs
Institutional Research Directors
Student Data (CMS)
ERSS/ERSA Data Extract
Institutional Research Data Cleansing
Student Cohort Data output
Extract, Transform and Load (Every Census)
Report Repository
1
2
3
4
5
STUDENT DATA WAREHOUSE
DYNAMIC
Admissions
Enrollment
Degree
CENSUS
Cohort
Ethnicity
Gender
Parent Education Type
URM
Extract, Transform and Load (Daily)

development, and deployment. (See Figure 2 on page 30.)

From PBX to VoIP

At the beginning of yet another shared service collaboration, CSUF needed to upgrade its legacy PBX to a VoIP system in 2012. The VoIP PBX was installed in March 2012 in parallel with the TDM PBX to avoid service interruption to end users. While most phones were converted to IP phones without any issue, many analog lines—including campus emergency phones, modems, and alarm lines—required gateways that can convert analog signals to digital and vice versa. After migrating all 6,000 end user phones to the VoIP PBX, the next phase of the project was to install SIP trunks to the PSTN. In November 2014, SIP trunks were installed and substantial cost savings were realized. The monthly cost of telephone services was reduced by about 40 percent.

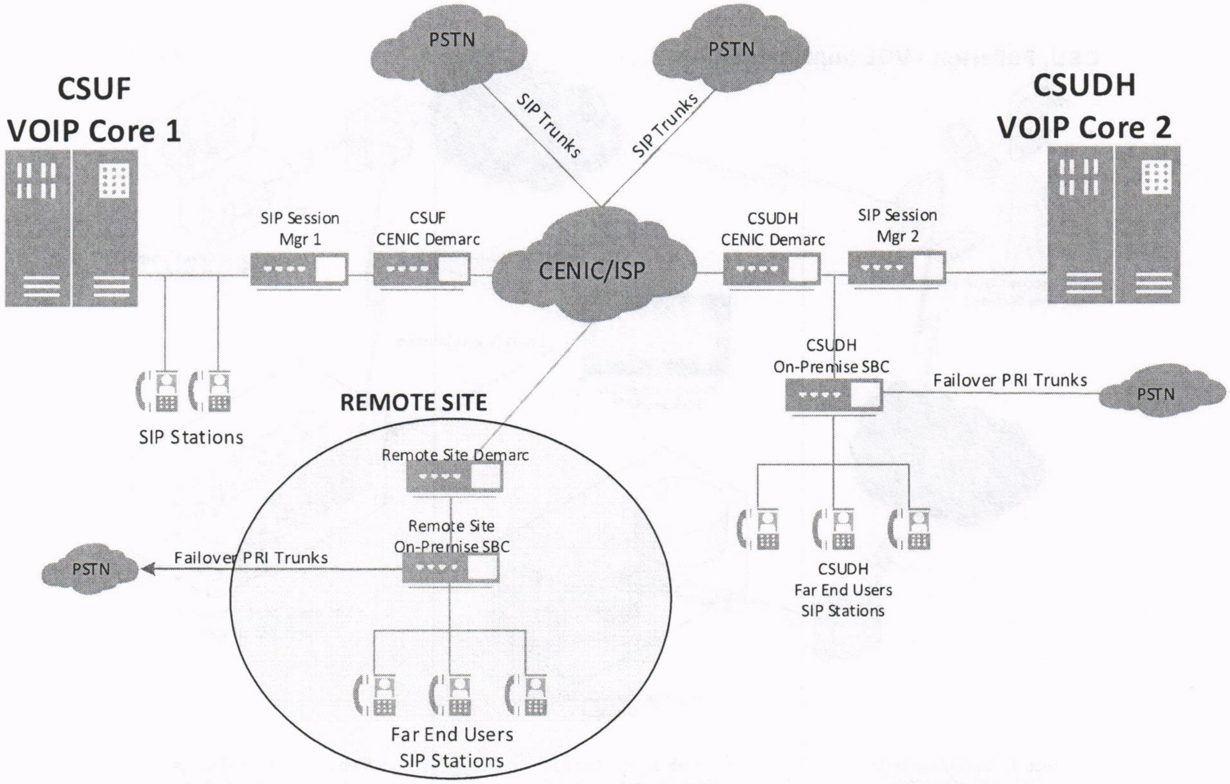
CSUDH is one of the 23 CSU campuses that is located about 25 miles west of the CSUF campus. CSUDH has been using the same legacy TDM PBX as the one CSUF had decommissioned. The campus issued an RFP for telecommunications services and explored various vendor proposals, including some cloud offerings. After several months of exploration, CSUF considered hosting their services on our career-grade VoIP PBX. To ensure proper infrastructure readiness, we upgraded the PBX system to the latest software version and upgraded each component to a fully redundant configuration. For better geographical diversity, we installed the redundant core of the PBX at the CSUDH data center.

The system is designed to operate in survivability mode, which offers local phone services—including 911 in the event of wide area network disruptions. Telephone system upgrades are always challenging due to the need to avoid disruption of service for an extended period of time. The co-existence of the legacy TDM and the new VoIP PBX was needed during the migration of the project to avoid significant service disruption. To help reduce cost, the CSUDH new telephone services rode on the existing CSUF contract with the PBX vendor and the telecom carrier.

A successful implementation of a complex project requires tremendous collaboration among project team members across both campuses. The telecommunication, network, and project management teams of both campuses worked collaboratively to complete this complex project. A memorandum of understanding (MOU) was developed outlining the financial responsibilities of each campus. This collaborative project was approved by the presidents of both campuses.

▸

Figure 3. System Architecture Diagram of Shared Telephone Services



This project helped reduce the total cost of ownership and improved the availability of telephone services for both campuses. The implementation budget for CSUDH was less than $900,000. The implementation cost includes 2200 desk phones, perpetual licenses, PBX and infrastructure upgrades. (See Figure 3 on page 31.)

Virtual Computing Lab

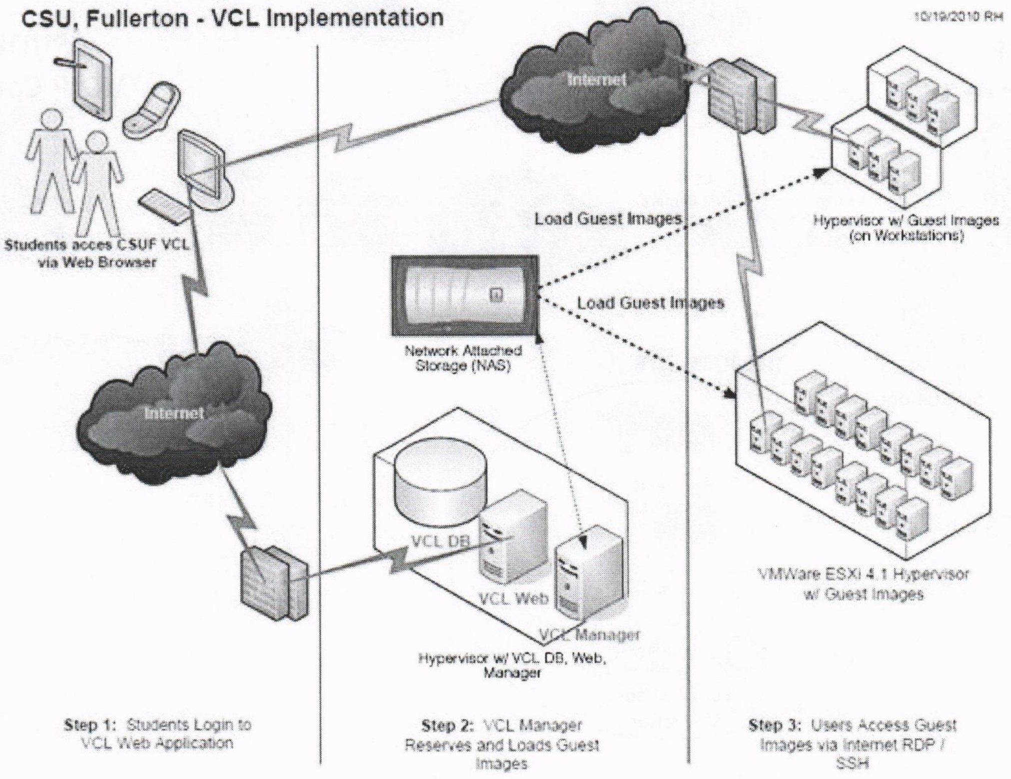
Lastly, but surely not the end of CSUF's shared services collaborations, is the Virtual Computing Lab. Computer labs, that are always in-demand but never have enough monitors, seem to be the mainstay of 21st century higher learning, but will soon become invisible. The development of the virtual computing lab (VCL) started in 2004 as a joint venture of the College of Engineering (COE) and the Office of Information Technology (OIT) of North Carolina State University to efficiently use hardware investments and to provide remote access to a wide range of advanced compute requirements by NCSU students, faculty, and researchers.

In November 2008, NCSU donated the VCL source code to the Apache Software Foundation (ASF) as part of on-going efforts to expand the VCL community and to foster open-source development. NCSU continues to be heavily involved in the development of VCL through the open-source community at ASF.

Many higher-education institutions followed NCSU's path and implemented virtual computing lab environments. CSUF recognized this trend and quickly implemented VCL. CSUF is among the leading institutions who have begun reaping the benefits of the VCL to accommodate the growing demand for computer labs. At CSUF, students, faculty, and staff can access university-licensed computer applications via the Internet. VCL allows them to work on a lab computer from home or any location with a high-speed Internet connection. Virtual Computer Lab service is available free of charge to all CSUF students. Using their campus login and password, students are able to log in to http://www.fullerton.edu/vcl to gain access to a wide range of software that is normally only available for use in our public-access computer labs located on campus. This service will allow all CSUF students access to any of the licensed software that they need to use in order to complete their assignments—24 hours a day, 7 days a week.

University of California, Irvine, a neighboring institution in Orange County, approached CSUF's IT team to pilot test the VCL. After several technical and administrative discussions, a memorandum of understanding (MOU) was

Figure 4. System Architecture Diagram for Virtualized Computing Lab (VCL):


CSU, Fullerton - VCL Implementation
10/19/2010 RH
Internet
Students acces CSUF VCL via Web Browser
Internet
Load Guest Images
Load Guest Images
Network Attached Storage (NAS)
VCL DB
VCL Web
VCL Manager
Hypervisor w/ VCL DB, Web, Manager
Hypervisor w/ Guest Images (on Workstations)
VMWare ESXi 4.1 Hypervisor w/ Guest Images
Step 1: Students Login to VCL Web Application
Step 2: VCL Manager Reserves and Loads Guest Images
Step 3: Users Access Guest Images via Internet RDP / SSH

developed to host 50 concurrent VCL instances for UC Irvine starting July 1, 2014. The CSUF team built the backend system and created the initial images. The UC Irvine team is now set up with the administrative privileges to manage the application. Image creation and security administration of the images is being managed by the UC Irvine team. The CSUF team is responsible for the backend administration only. In September 2015 CSU Irvine requested and received additional 50 instances. (See Figure 4 on page 32.)

CSUF hosts these applications in robust, redundant, and scalable private-cloud infrastructure. System performances are regularly monitored with a clear escalation procedure in place to manage outages and incidents. CSUF has implemented an IT Service Management framework that emphasizes continuous improvements.

Stakeholders meetings are held on a regular schedule with service owners, business managers, and the technical teams to discuss operational issues and future enhancements. An annual maintenance plan is in place to minimize maintenance downtime requirements. Most planned and unplanned system maintenances are performed without service interruptions by leveraging the redundancy and failover capabilities of the private-cloud infrastructure. Capacity increases are usually accommodated through vertical and horizontal expansion of system resources.

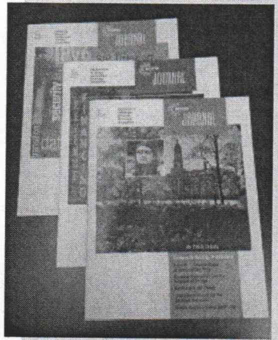
The cost of building infrastructure to host these applications can be significant. With the shared services, significant cost savings have been realized by all participating institutions. There is a base cost for infrastructure even when hosting a small resource footprint application. It is abundantly clear that incremental cost of a leveraged infrastructure is much less than multiple silo implementations.

Final Thought

Overall, users of these shared services are satisfied with the performance and availability of these applications. Participating institutions have either increased the capacity of existing applications or have used additional shared services. We get inquiries from multiple institutions to utilize these shared services. CSUF looks forward to collaborating with many institutions to reduce cost of operations and improve reliability and availability by building a leveraged, highly robust and redundant cloud infrastructure.

The contact for this project is Berhanu Tadesse, associate vice president for Information Technology/Infrastructure Services. Reach him at btadesse@fullerton.edu.

The ACUTA Journal Wants Your Story!



Be a part of ACUTA history...

Write for the Journal!

For 20 years (that's 80 issues now), the *ACUTA Journal* has brought you the insights and experiences of campuses from coast to coast about every imaginable topic of relevance to higher ed technology.

We consistently hear that campus case studies are the most useful articles of all. You like to know what others are doing—what has worked and not worked—to help you make important decisions.

Has your campus implemented a new procedure or a new strategy?

Have you discovered a shortcut that might benefit others?

Is there an application or program that resolved some really tough issue for you?

The next few issues of the *Journal* will consider some very interesting topics:

- **Winter: 2020: Vision of the Future**
- **Spring/Summer: Providing Telephony on Today's Terms**
- **Fall: The Business Side of the IT/Telecom Office**
- **Winter: Student Services: Meeting Needs and Expectations**

You are cordially invited to share your own campus story with other members via the *ACUTA Journal*. If you don't have time to write it, just **contact editor Pat Scott at pscott@acuta.org,** and she will connect you with someone who will work with you to get this done.

It's an opportunity for excellent visibility and recognition for your school, your department, and yourself.

Thank you for reading the **ACUTA** *Journal!*

We hope you found our digital format convenient and enjoyable and the content interesting and useful. We welcome your comments at any time. To share a story with our audience, please contact Pat Scott, ACUTA Communications Director, at 859-721-1659 or pscott@acuta.org.

Coming issues of our *Journal* will focus on the following topics:

Winter: 2020: Vision of the Future
Spring/Summer: Providing Telephony on Today's Terms
Fall: The Business Side of IT/Telecom
Winter: Student Services: Meeting Needs and Expectations

Tell __your__ story in the next ACUTA *Journal!*

Pat Scott, Editor • pscott@acuta.org