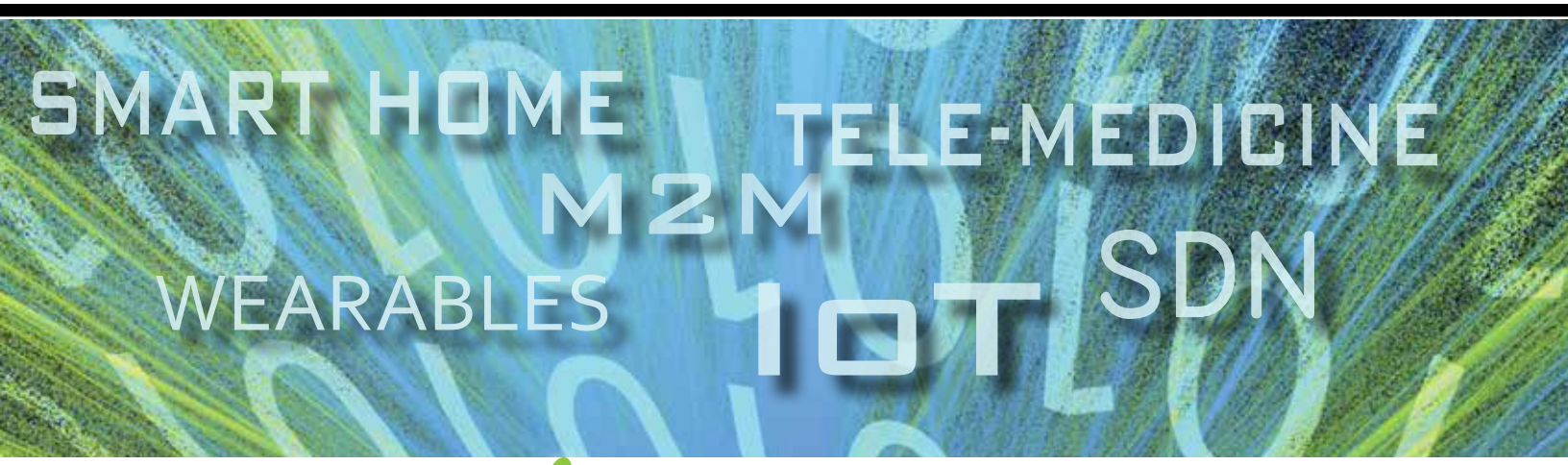
Skinny Wire

A Publication of WALKER AND ASSOCIATES INC

Volume IX, Issue 1 walkerfirst.com/skinny-wire Logistics Solutions for Telecom Professionals



Everything BROADBAND Everywhere

Supercharged Ethernet Services

Comprehensive Carrier Ethernet Solutions that Strike the Right Balance

Fujitsu Carrier Ethernet solutions combine our FLASHWAVE® 5300 Ethernet Access and Aggregation Devices with the FLASHWAVE 7120 packet optical platform and the NETSMART 1200 Management System. The result is a truly efficient, economical Ethernet growth path, balanced with seamless operation and management.

But that's not all. These solutions offer dramatically increased service velocity, together with carrier-grade reliability and performance. If you're planning to service high-value SLAs or 4G/LTE mobile backhaul, ask your Walker representative about supercharging your network with profitable Ethernet services using Fujitsu FLASHWAVE-based MEF-compliant Ethernet platforms.

FLASHWAVE 5300 SERIES

- GbE and 10 GbE interfaces
- MEF E-Line, E-LAN and E-Access services
- Class of service differentiation, shaping and policing
- Performance monitoring with ITU-T Y.1731
- Ethernet ring protection with ITU-T G.8032
- Link Aggregation with IEEE 802.3ad
- VLAN Push, Pop and translate
- Service and Link OAM and fault management
- Single or dual tag switching, S and C tag switching, QinQ

shaping tomorrow with you

FUJITSU

Fujitsu Network Communications • 2801 Telecom Parkway, Richardson, TX 75082 Tel: 888.362.7763 • us.fujitsu.com/telecom

In This Issue . . .

Feature Articles

Resource Articles

Walker News

Letters to the editor may be sent to SWEditor@walkerfirst.com

Skinny Wire is a bi-annual publication of Walker and Associates, Inc.
"Equal Opportunity/Affirmative Action Employer m/f/d/v"

Editor's Letter

Science fiction has always been a fascinating world where the technology to support gadgetry and ability required no explanation or sound logic. A writer can use terminology such as "flux capacitor" and suddenly the storyline is supported. Though prior generations of science fiction can sometimes read like ads for the next Consumer Electronics Show, a sound basis for today's technology driven devices clearly exists.

Our editorial theme for this issue is "Deploying the Everything Broadband, Broadband Everywhere Network." Indications are that we are just beginning to see the tip of the iceberg as it relates to the network impact brought on by the Internet of Things (IoT), Machine to Machine (M2M), connected vehicles, wearables, smart meters, smart homes, and more. Some are aptly describing it as the "Internet of Everything." Network operators face increasing demands on their infrastructure to manage the additional traffic, while considering ways to monetize services, seeking solutions that lower operating costs, and providing greater value to customers in efforts to curtail attrition.

Consider some of these recent headlines:

- Average household bandwidth requirements will increase 31% annually for the next 5 years according to a report from ACG commissioned by Ciena
- Carrier Wi-Fi equipment revenue will reach $8 billion by 2019, says ABI Research
- Manufacturing, utilities and transportation will be the top three verticals using Internet of Things devices in 2015, with 736 million connected devices in use next year, forecasts Gartner.
- IDC forecasts the IoT market to grow from $1.3 trillion in 2013 to $3.04 trillion in 2020, with a compound annual growth rate (CAGR) of 13 percent. By 2020, there will be 30 billion connected "things."
- Service providers will deploy more than 4 million public hotspots and 20 million homespots in 2015, according to a new report by Mobile Experts.

Equally compelling topics of policy, standards, the net neutrality debate, Title II ramifications, workforce readiness for the evolving ICT marketplace, and more are also covered in this issue. As stated in the bio for new contributor, TIA CEO Scott Belcher, the ICT industry is experiencing perhaps "the most dramatic change seen in decades." The carrier community is challenged to keep pace with new technologies, rising consumer expectations, and changes in policy. In a world with a growing number of connected devices that require greater bandwidth and broader coverage areas, Everything Broadband, Broadband Everywhere is indeed a relevant concept that has little, if anything, to do with science fiction.

Randy Turner

Editor, Skinny Wire
Director, Marketing Communications
Walker and Associates
336-731-5246
randy.turner@walkerfirst.com
SWEditor@walkerfirst.com

Everything Broadband, Broadband Everywhere

Cities, municipalities and metro areas are under pressure to maintain a competitive advantage in a new connected world in which knowledge workers manufacture digital applications and services; entrepreneurs collaborate over high-bandwidth networks and economic development stems from highly-connected ecosystems of people, things and services all connected ubiquitously. Some say it is a survival of the fittest ecosystem in the global competition for a share of the expected $9 trillion in annual GDP that will come from the Internet of Things.

By Timothy Downs
Vice President
Light Reading

Many are aware of what happened in 2012. It was then that Google announced it had selected Kansas City, Missouri as the site of its inaugural Google Fiber deployment, which promised gigabit speed connections to homes and businesses. Less known is the fact that Google was not the first to promise 1Gbps broadband connection to homes and businesses. EPB, the municipally-owned utility in Chattanooga, Tennessee has that distinction, launching in 2010.

Since Google's announcement, service providers of all types, including telcos, cable Multi-system Operators (MSOs), utility/municipalities, and even electric cooperatives have embraced the Gigabit movement. According to a February 2014 joint NTIA-FCC broadband data report, there were 99 Gigabit broadband networks operating in the U.S. Today the number of gigabit broadband networks is estimated to top 130. That same NTIA report found 232 networks offering 100 Mbps or faster (in the downstream). Washington State has the most Gigabit networks at 17 and only two states, Montana and West Virginia, have no Gigabit networks, according to the data.

Tier 1 carriers have responded aggressively: Comcast currently offers 2 Gbps service in Tennessee among other regions. AT&T has launched its GigaPower service in Austin, Atlanta and other service areas. Regional carriers like Comporium Communications of Rock Hill, South Carolina and Blue Valley Tele-Communications of Home, Kansas, both of whom are bringing Gigabit broadband to the heartland. Cable MSO Suddenlink and competitive carrier C-Spire are deploying gigabit speed networks in their service areas.

In May 2015, the State of Connecticut took steps to be the first "Gigabit State" with active interest from eleven private sector businesses, including two international investment banks, the state's largest telecommunications company, and the leading telecommunications industry group.

According to ADTRAN we are now entering phase three of Internet access, where we will once again see a 50x to 100x improvement in access speeds. Gigabit broadband, the next generation broadband, is enabling a new range of consumer and business applications that are redefining the broadband experience and energizing economic development in the communities where it is present.

For city and municipal government, economic development is foundational to the improved digital infrastructure. "It's the fiber that sets us apart. Our county has mountains, forests, fresh water lakes and a major river, but it's the fiber that sets us apart. Our new economic development plan will focus on attracting talented people who want to start businesses or work from their homes and still enjoy the outdoors." Jamie Wyrobek, Director, Pend Oreille County, Economic Development Council.

Gigabit Networks as Economic Development

According to the Wisconsin Economic Development Corporation (WEDC), access to high-speed Internet service has become a major factor among site selectors or corporations in deciding where to relocate or expand. In a 2008 ranking of top site selection criteria by Area Development Magazine, broadband ranked as the 21st most important consideration in such decisions. By 2013, broadband ranked fifth highest.

A study of 14 communities by the Analysis Group showed that, although gigabit broadband is in its infancy, the "communities with widely available gigabit broadband that we studied enjoyed over $1 billion in additional GDP when gigabit broadband became widely available, relative to communities where gigabit broadband was not widely available." *["Early Evidence Suggests Gigabit Broadband Drives GDP," David Sosa, Principal]* According to the study, Chattanooga attributed 1,000 new jobs, increased investment and a 'new population of computer programmers, entrepreneurs and investors' to gigabit broadband.

Jeff Smith, Co-Director of the New Economy Division for the Lansing Economic Area Partnership said, "Access to ultra-high speed broadband networks is increasingly becoming an invaluable asset for innovators, entrepreneurs and companies looking to compete globally utilizing the next generation of broadband enabled applications and software. Expanding such networks in our region is critical to the attraction of world-class talent and high tech businesses to the Greater Lansing region."

For Cities, Gigabit Broadband is the Ground Floor -- the Core Infrastructure

Ultra-high speed networks may be just be the prerequisite for city and municipal leadership to attract and retain residents and businesses. Wireless infrastructure designed for capacity and deployed to meet the exploding demand for mobile data is also an important consideration. The third consideration is a sensor-driven "Internet of Things" network that is designed to usher in an entirely new era of 'smart city' applications, automation and investment.

"The best of the new community ecosystems will be cities and towns that combine a university, an educated populace, a dynamic business community and the fastest broadband connections on earth. These will be the job factories of the future." -Thomas Friedman, Columnist, New York Times

A report by Freedman Consulting , LLC, *[Toward an Understanding of Best Practices in Community Wireless Networks]* in May 2015 and commissioned by the Ford Foundation found that community wireless networks have garnered renewed interest from municipalities across the country in recent years. City officials' motivations for developing networks are varied, from enabling mobile access to the Internet for city departments to boosting local business zones to helping bridge the digital divide.

The report cites Boston as an example of a wireless network that is being piloted in target areas with the explicit aim of addressing the digital divide. In Corpus Christi, a city-funded network began with the aim of enabling Automated Meter Reading and was subsequently augmented to include public access points. Oklahoma City's network covers 555 square miles, larger than the other networks examined in the report.

Cost, according to the Freeman Consulting Report, is the major catalyst behind new deployments of community wireless: "By today's standards, the wireless network equipment available in the early 2000s was very expensive. The least expensive pair of P2P radios cost between $1,200 and $2,000, depending on the power and antenna combination. The least expensive APs cost between $225 and $499, and CPE costs between $195 and $225."

Building and operating a fixed wireless broadband network in the early to mid-2000s, and as late as 2010, was a very expensive proposition and had a return on investment timeline of a minimum of five years. This timeline would increase if critical equipment malfunctioned or if the network administrator failed to capitalize the software expense separate from the network expense. This cost structure contributed at least in part to a decrease of wireless networks: of the over 4,000 WiSPs in existence in 2000, about half remain today.31

In a relatively short period of time, however, the cost of fixed wireless broadband networking equipment has dropped significantly while its performance has improved dramatically. As an example, a small fixed wireless broadband network might have two P2P radio pairs and six APs serving 120 customers.

Smart Cities with the Internet of Things

According to Verizon, today more than half of the world's population lives in urban areas; by 2050, that figure will be 70%. This trend is forcing local and federal governments to reconsider how they deliver effective services to citizens, control crime, protect aging infrastructures and keep core systems, such as power and traffic running smoothly. Leaders must look to the future, building more sustainable developments with limited resources.

Speaking at the PCIA Wireless Infrastructure conference in 2015, Chris Stark, Chief Business Development Officer of Nokia North America said, "A future of smart mega cities where traffic, resource use, emergency response latency and more are problems of the past. Existing networks have to become significantly more dense while technologies – WiFi, LTE, DAS, Small Cell – become significantly more interoperable. Once this happens, the end-user will see seemingly "infinite bandwidth seamlessly connected across all these different technologies."

Cities and Metro areas stand at the beginning of a new era of technology investment, deployment, operation and utilization. The business model is not solely focused on increased economic development. Cost savings, resource efficiency and automation are critical drivers of a renewed interest in sensor networks connecting city infrastructure and services.

Glasgow, Scotland, for example, has offered £24 million ($37 million) for technology which will make the city "smarter, safer and more sustainable." Applications developed or planned for the program include intelligent street lighting which will switch itself off to conserve energy when there's no one around, mapping energy use around the city to better understand demand, and mapping how people get around to maximize the use of bicycle and foot paths. Sensors attached to street lights and other outside urban furniture will measure footfall, noise levels and air pollution and this data will be used to prioritize delivery of other services.

The Internet of Things has the potential to fundamentally disrupt the way we live and work. It offers organizations the opportunity to transform how they operate: improving their customer experience, accelerating growth, and managing evolving risk. It's already transforming whole industries, from healthcare to retail. For city and municipal governments, the business case for a citywide Internet of Things solution is strong. Even a small reduction in accidents and crime, can reduce the burden on emergency healthcare, police and the courts. This can make a major impact on public sector finances and on a city's reputation as a safe place to live, work, invest, and visit.

The convergence of ultra-high speed 'gigabit networks' in city and metro areas, with dense wireless infrastructure designed for capacity and a sensor-driven "Internet of Things" architecture means that city and civic leaders are poised on the threshold of a new era in technology spending, development and disruption.

About the Author: Timothy Downs has been in the mobile, broadband and electronics industry for more than 15 years as an editor, publisher, conference director and consultant.

Net Neutrality Must Look Forward, Not Take Us Backwards

By Scott Belcher
Chief Executive Officer
Telecommunications Industry Association

Scott F. Belcher was named Chief Executive Officer of the Telecommunications Industry Association (TIA) in October 2014, following a seven-year tenure as President and CEO of the Intelligent Transportation Society of America (ITS America).

As the information and communications technology (ICT) industry experiences the most dramatic change seen in decades, Scott's leadership of TIA fosters adaptation and growth to meet its members' needs. He is responsible for managing TIA's overall operations and providing long-term strategic direction for the organization. Scott brings to TIA more than 25 years of public and private sector experience in Washington, DC.

Prior to becoming President and CEO of ITS America, Scott served as Executive Vice President and General Counsel at the National Academy of Public Administration in Washington, DC. Before his tenure at ITS America, Scott held senior management positions at a number of prominent trade associations, and worked in private practice at the law firm of Beveridge & Diamond, PC, and at the Environmental Protection Agency.

Scott holds a Juris Doctor from the University of Virginia, a Master of Public Policy from Georgetown University, and a Bachelor of Arts from the University of Redlands. Scott serves on the Boards of the Telecommunications Industry Association and the University of Redlands Alumni Association. He serves on the U.S. Department of Transportation Intelligent Transport Systems Program Advisory Committee and on the Advisory Boards of the University of Michigan Transportation Research Institute and the University of California Berkeley Transportation Sustainability Research Center.

Scott resides in Alexandria, VA and is married with two children.

Unlike almost any other advancement in modern history, the Internet has moved us forward – creating new businesses, new ways of communicating, new opportunities for curing illness, and so much more. Given all that, it's hard to understand why, when considering the best ways of ensuring an open Internet, government regulators have chosen to look backwards. Way backwards – all the way to 1934.

The Federal Communication Commission's (FCC) February decision on net neutrality applies "Title II" regulation to the Internet, using a law that was passed by Congress more than 80 years ago to regulate wired telephone service. With the popularity of the TV series Mad Men, it's certainly cool these days to be "retro." But when it comes to today's advanced, high tech economy, there's just nothing good about being retro.

We all understand that extraordinary problems sometimes require extraordinary government action. For this reason, it's worth looking at how the Internet has developed in recent years to understand what kind of regulatory action may be needed. A few facts:

- The private sector has been investing in broadband at a rate of $73 billion annually.
- Private sector broadband investment in U.S. is more than double that of Europe, where there is a burdensome regulatory environment ($562 per U.S. household in 2012, versus $244 per European household).
- Connections speeds have increased 250 percent since 2010 – jumping from 4.6 Mbps to 11.4 Mbps.

The reality is, with a "light-touch" regulatory approach in place, the Internet has thrived and driven tremendous gains for American consumers, businesses and our economy. Companies are investing at unprecedented levels to increase access, deliver faster speeds and meet the increasing demands of high-bandwidth video, music and more.

Of course, while it's clear that these regulations were working, we have to look for-

" . . . there is a real concern about whether investment will be able to keep up with demand."

ward to make sure they will continue to work. For this reason, we agree that some rules should be in place to keep the Internet open and available to all, and that no one receives second-rate service. And in fact, our companies reap significant benefits from a competitive marketplace where a variety of customers can reach consumers with all types of content.

To protect "neutrality," the government has tried a variety of regulations over the years – including pursuing a Title II approach many years ago. When that approach was abandoned, the impact was immediate and dramatic. Freed from an outdated regulatory system, private sector investment boomed, and tens of billions of dollars were spent to build new Internet infrastructure. In a single example, Verizon spent $23 billion to roll out FiOS, the company's fiber-optic communications network that now has millions of customers across the United States.

The U.S. needed this infrastructure as the Internet was becoming essential for both business and society. Now, that infrastructure is vital to meet the extreme and rapidly growing demands being placed on the network. According to the latest forecasts from Cisco, global data traffic will increase eight-fold over the next four years. In addition, all Internet traffic will double by 2018.

With Title II back in place, there is a real concern about whether investment will be able to keep up with demand. It's simple economics: companies will not continue heavily spending on infrastructure when the FCC can impose restrictions preventing them from earning a return; the risk with billion-dollars projects is just too high. And, while the FCC has said it will not use the full authority Title II gives them, the fact is, there is little to prevent future Commissioners from taking extreme action. Title II could easily be used to implement price controls, or to put in place other extraordinary and severely market-distorting measures.

It doesn't have to be this way, and we remain confident that Title II will be rejected. Our organization, and the high tech manufacturers that make up our membership, strongly support the principles of net neutrality – they are good for consumers and good for business. For this reason, TIA is actively working with Congress to pass sensible and effective net neutrality legislation that looks forward – to an even more robust Internet that serves consumers and that drives innovation, economic opportunity and growth.

About TIA
The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industry through standards development, policy initiatives, business opportunities, market intelligence and networking events. With support from hundreds of members, TIA enhances the business environment for companies involved in telecom, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications and the greening of technology. TIA is accredited by ANSI.

Learn more at http://www.tiaonline.org/.

TIA®
ADVANCING GLOBAL COMMUNICATIONS

Mark Walker Named as TIA Board Chair

Mark Walker, President of Walker and Associates, became Chair of the Board of Directors of the Telecommunications Industry Association (TIA) in January 2015 for a two-year term. He now leads a board that includes C-level executives representing a prestigious roster of technology companies, including Cisco, Dell, GM, Intel, Microsoft, LG, Panasonic and Qualcomm. Working with CEO Scott Belcher and other TIA executives, Mr. Walker is helping guide the organization in new directions. Mr. Belcher, who joined TIA in November 2014, said "As the ICT industry faces disruptive new technologies, quickly changing business models and a shifting regulatory landscape, we are very fortunate to have someone as experienced as Mark to lead our board. Mark is contributing his years of industry expertise and thoughtful guidance to TIA as we lead the industry during this time of significant change and opportunity."

Mark Walker has been President of Walker and Associates since 1998. He has a broad range of industry experience in manufacturing, sales, operations and customer support. He formerly served as President of Evergood Fabrication, a subsidiary of Walker, which was sold to Reltec/Marconi in 1998.

FCC Made All the Right Moves on Open Internet Decision

By Chip Pickering
CEO
COMPTEL

Chip Pickering became CEO of COMPTEL, the leading trade association advocating for competitive networks and competitive communications policy, in January 2014. Pickering was a six-term Congressman, representing Mississippi's Third District. During this time, he served on the House Energy & Commerce Committee, where he was vice chairman from 2002 to 2006 and a member of the Telecommunications Subcommittee. He also was co-chairman and founder of the Congressional Wireless Caucus and an assistant minority whip of the House. Previously, Chip worked for Sen. Trent Lott (R-Miss.) and served as a staff member on the Senate Commerce Committee, where he helped shape the Telecommunications Act of 1996. Because of his role in drafting the 1996 Act, he became well known as a Congressional leader on telecommunications issues. Most recently, Chip was a partner with Capitol Resources LLC, a public affairs and government relations firm, where he represented an array of telecom clients, including wireless, cable and competitive broadband providers, as well as non-profits and companies specializing in education, energy, technology and defense. There, he also played a vital role as one of the principal negotiators in developing a wireless industry agreement for interoperability in the 700 block.

About COMPTEL - Based in Washington, D.C., COMPTEL is the leading industry association advocating for competitive networks and competitive communications policy. COMPTEL members are entrepreneurial companies driving technological innovation and creating economic growth through competitive voice, video, and data offerings and the development and deployment of next-generation, IP-based networks and services. COMPTEL advances its members' interests through trade shows, networking, education, and policy advocacy before Congress, the Federal Communications Commission and the courts. COMPTEL works to ensure that competitive communications providers can continue to offer lower prices, better service, and greater innovation to consumers. For more information, visit www.comptel.org or follow us on Twitter @COMPTEL.

Since the Federal Communications Commission approved its Open Internet Order at its February Open Meeting on a party-line vote and released the full text on March 12, there has been a lot of Monday morning quarterbacking about how the decision will impact the market, including the businesses of Internet services providers.

Some pundits would have you believe that the Commission has overstepped its bounds, and arbitrarily made these decisions without any sort of precedent. But those claims couldn't be further from the truth.

In March, COMPTEL released a white paper that illustrated the long history of bipartisan support for a free and Open Internet. You can download the white paper from our website, but in summary, it explains how a Republican-led FCC originally established the principles that consumers should be able to access the lawful Internet content, applications and services of their choice. In 2005, the FCC, under Republican Chairman Kevin Martin, adopted and released the original Internet Policy Statement. At that time, the Commission expressed the belief that it could use its ancillary authority under Title I of the Communications Act to enforce the Internet Policy Statement and the principles articulated therein.

The Commission's Internet Policy Statement was supported by then President George W. Bush, who in 2006 issued a Statement of Administration Policy that expressed the Administration's belief that the FCC had sufficient authority to address potential abuses by Internet access service providers.

Comcast subsequently appealed the Commission's issuance of a decision finding that it had violated the Policy Statement when it interfered with BitTorrent traffic. The Court of Appeals vacated the decision on the grounds that Title I did not give the Commission authority to assert jurisdiction over network management practices. In response to that decision, the Commission adopted Open Internet rules that most ISPs supported using its Title I and Section 706 authority. Verizon's appeal of that Order resulted in the Court vacating the Commission's no-blocking and nondiscrimination rules in January 2014. Although the Court agreed with the Commission's assessment that the rules were necessary to protect consumers, it determined that the Commission's classification of broadband Internet service providers as information service providers exempted them from the common carrier obligations that the no-blocking and nondiscrimination rules imposed.

Because of the court rulings, today's Commission had no choice but to reclassify Internet access service as a Title II service, so that it has clear and explicit authority to prohibit abusive ISP practices such as blocking, discrimination, throttling and paid prioritization, and be able to quickly address consumer complaints and take enforcement action as necessary. At the same time, the Commission's decision to forbear from 27 provisions of the statute and more than 700 regulations that are not relevant to modern broadband services will ensure that broadband providers are not subject to onerous "utility style" regulation that the naysayers claim will burden providers and cause costs to rise. The Commission's Open Internet decision takes a prudent approach that both addresses the court-determined shortcomings of the previous Internet rules and continues to protect consumers' access to the Internet content, applications and services of their choice. A similar "Title II light" regulatory approach has been proven effective in the wireless market.

Many ISPs have stated that the decision will not impact their investment decisions, and many more small businesses and consumers that rely upon the Internet every day will benefit.

The Commission's decision is consistent with the comments it received from millions of consumers – regardless of political affiliation. In its Open Internet Order, the Commission made all the right moves to ensure that consumers, start-ups and companies of all sizes can continue to use the Internet to communicate, do business and innovate without fear of discrimination, blocking or having to pay exorbitant charges for specialized treatment. We do not believe these consumer protection measures will adversely impact investment, innovation or the growth of the Internet ecosystem.

Bringing Wireless Services to Large Venues

By John Spindler
Vice President, Product Management
TE Connectivity

The Environment
Large buildings and public venues need DAS technology because the large number of people in a space overwhelms the macro mobile network, leading to dropped calls, or data sessions an inability to connect, and service latency. Hundreds or thousands of visitors may be simultaneously calling, texting, browsing the web, or uploading or downloading video. Handling these communications successfully requires a high amount of mobile capacity over a large and complex service area.

A DAS consists of a main hub or head-end linked to a mobile operator's base station. The main hub transmits the mobile signal to remote amplifier units (RAUs) and antennas, which amplify the signal in specific areas of the venue. Because of traffic demands, large venues are often divided into sectors, in which a specific frequency band or operator's service is distributed. There needs to be at least one remote unit and antenna for each sector. (Figure 1.)

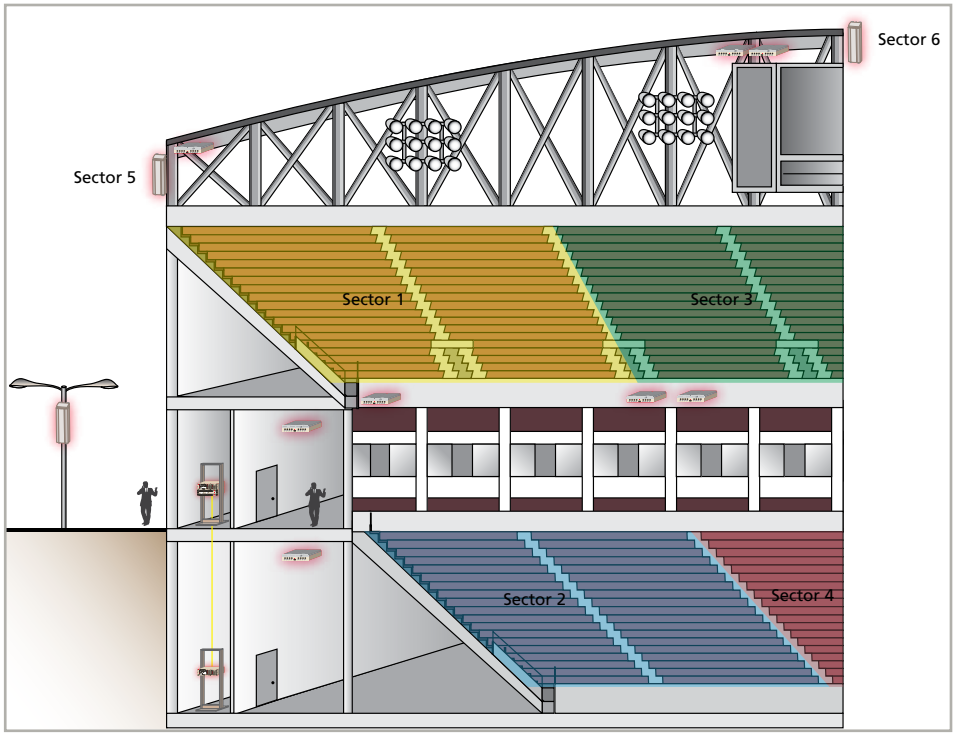


Figure 1: A stadium divided into six sectors per seating level.

Challenges
The main challenges in using DAS for large venue wireless service delivery are: cost, efficiency, and capacity.

Cost – Much of the cost of deploying a DAS in a large venue comes from the cost of installation, not from the cost of the DAS equipment. Traditional analog DAS systems require one fiber or fiber pair between each head-end and remote antenna. This one-to-one requirement in a venue that may need dozens of remote antennas means that a lot of fiber must be deployed. Use of existing fiber may not be possible as analog signals have low loss tolerance (typically 3 dB) or cannot overcome losses from splices and patching. In many stadiums, for example, it is not uncommon for such a system to require 192 fiber pairs. Pulling fiber, connectorizing fiber and splicing it in the field is extremely expensive, running as much as $250,000 USD for this part of the deployment alone.

Efficiency – A traditional analog DAS requires the use of a separate main hub for each base station and a large amount of space for RF combining solutions. Base station shelters at arenas and stadiums were not built to accommodate so much equipment, so they must be enlarged, leading to an extra expense and added time to the deployment. And all analog DAS RAUs need the fiber cabling "home run" connected to the main hub.

Capacity – An analog DAS requires an inordinate amount of traffic engineering before deployment because they require more fiber than a digital system. Digital DAS) supports wavelength optical multiplexing, allowing for less cable, a simple design and installation, and further reach of the DAS.

Solution
Specialty Fiber and DAS solutions mitigate the challenges of large venue deployment. DAS products that feature all-digital transport, enabling a single head-end to simulcast a signal to many remote antennas or radio heads and to deliver the same, high-capacity signal at each antenna are critical. In addition, you'll want head-ends that can aggregate the capacity from two or more base stations that are on-site, off-site or even at different locations, so the mobile operator can increase capacity by simply adding another base station (no additional head-ends, antennas, or radio heads required).

Finally, implementing fiber saving technologies such as coarse wave division multiplexing (CWDM) and dense wave division multiplexing (DWDM), will reduce the amount of fiber typically needed in large venues by 80 percent or more, saving significant costs.

John Spindler was named Vice President of Product Management for TE Connectivity's wireless business in December 2007 through the company's acquisition of LGC Wireless where he served as Vice President of Marketing. In his current role, Spindler is responsible for developing and managing an innovative wireless product portfolio for the company's Network Solutions Business Unit.

During his more than 20 years of industry experience, Spindler has held a variety of product management positions with companies such as Nortel Networks, GTE and InteCom. In these positions, he had responsibility for the areas of networking, network management, computer telephony integration and wireless technologies.

*Spindler received a Bachelors of Arts Degree from the University of California, Los Angeles (UCLA) and an MBA from the University of Southern California, Los An*geles.

Leave No Residential Customer Behind:

Delivering Gigabit Broadband to Multi-Dwelling Units

By Kevin Morgan
Director, Marketing Communications
ADTRAN

Multi-Dwelling Units (MDUs), structures with multiple living units per location, represent about 30 percent of the total US residential market for Fiber-to-the-Home (FTTH). Clearly, a service provider's success in deploying FTTH and enabling Gigabit service delivery in this residential market depends upon having an effective strategy to tackle MDU opportunities. Among the most important considerations in weighing this market are understanding unique stakeholder interests that exist in MDUs and bearing in mind the demands of each MDU property in determining the right technical solutions. Let's take a closer look at the dominant factors involved in these areas.

Understanding the Nature of MDUs

MDUs range from single-story buildings with two to four tenants to much more complex developments with hundreds of tenants. They primarily consist of either apartment units, typically rented, or condos, usually owned. This distinction is important since with tenant "turnover" higher for renters, a service provider is sure to have more chances over time to win or lose customers in the apartment MDU market.

Unlike the Single Family Unit (SFU) market, serving MDUs requires going beyond just knowing the building, to really understanding the interests of owners and tenants, both of whom have to understand the benefits of FTTH to reach a sales agreement.

The people that own MDU buildings tend not to be immediately sold on the benefits of FTTH. Instead, their primary interests lie with economic metrics such as rental rates, rental duration, occupancy levels and turnover. A service provider must address how FTTH translates into making those economic metrics improve for an MDU owner. For example, if there is local evidence that higher internet speeds translate into higher rental rates, this would be important data to share with residential building owners. Moreover, it is equally important to explain to owners how FTTH as a service offering will surpass cable and satellite over time. Such metrics can also be a major asset to the service provider when negotiating access to the building and space for equipment.

Once the benefits of FTTH have been conveyed to the building owners, providers would do well to educate the MDU resident community. Broadband community campaigns have grown in prevalence over recent years, hence it may be worthwhile to work in conjunction with such efforts to showcase the unique value of your solutions and service offerings for the local market.

Determining the Right Solutions for the Job

So you got the job, now what? Too often service providers have in their mind that certain designated equipment has to go with a particular structure or customer. The cardinal rule on FTTH deployment is that it's not about force fitting a set solution to a dwelling, rather it is about finding the right solution based on the needs of a particular project.

For example, working to have Optical Network Terminals (ONTs) fit a specific FTTH deployment should be a deliberative task. Low-density, low-story MDUs like duplexes tend to look more like single-family homes from a FTTH perspective. In such cases, if MDUs can be served with Single Family Unit (SFU) ONTs, then that is the best solution. Just as with SFUs, using an indoor SFU ONT with these types of MDUs carries benefits in cost, flexibility and ease of future improvements over most traditional outdoor ONTs.

Taking the indoor ONT value proposition one step further, micro ONTs may present the ideal solution for the job. These devices, some of which are small

enough to fit in the palm of your hand, offer a wealth of advantages for MDU applications. Micro ONTs can be left at a residence, so when tenants change there's no need for a truck roll to retrieve equipment. In addition to simplifying and streamlining installation procedures and offering better security, these ONTs are also independent of the wireless router. This increases the life of the ONT and raises return on investment (ROI) because the ONT does not have to be replaced as Wi-Fi standards evolve.

As we get into larger, more complex MDUs, such as high-rises, the density of tenants increases considerably. The ability to serve these types of MDU units with FTTH raises the likelihood of more centralized solutions like Fiber Ethernet, Wi-Fi and GPON. These three technologies represent varying levels of service and capital commitment.

Let's take for example a combination solution leveraging optical Ethernet and Wi-Fi—it has bandwidth superiority over using in-home copper wiring solutions, but is more capital intensive. It requires a fiber-fed active device placed inside the MDU (typically in the basement or equipment room) and CAT-5 wiring to all common areas and/or each unit. In the case of wiring out only to wireless Access Points, the service provider can provide ubiquitous Internet service (over Wi-Fi) throughout the building. Simplicity of use and the ability to easily acquire customers (tenants and visitors) offer additional benefit with this solution.

Key Takeaways

There are all kinds of MDUs in the US market: duplexes, apartment complexes, high rises, etc. They may need to be served differently but they all remain "residential" buildings and the services required (i.e., voice, video and data) are essentially the same. As such, service providers may do well to gravitate towards a smaller, yet more versatile portfolio of ONTs or Customer Premises Equipment (CPE) devices for most deployments, since more versions of ONTs or CPE means more maintenance and support costs.

Remember that MDU owners are focused on providing tenants with reliable, solidly performing communications services regardless of the technology used. Owners are motivated mostly by occupancy and will entertain improvements at their building(s) that can generate tenant satisfaction and growth in rent. Service providers must translate the benefits of FTTH into how it can improve the bottom line for MDU owners and their tenants. MDU FTTH projects truly can be win-win for all involved, but it requires the service provider forging a real partnership with building owners and residents throughout the endeavor.

Kevin Morgan currently serves as the 2015 Board of Directors Chairman for the FTTH Council Americas. He was first elected to the Board in 2010 and is past Chair of the Government Affairs committee and Marketing committee for the FTTH Council. He is the Director of Marketing Communications at ADTRAN and has spent his career gaining experience in advanced communications technology, fiber optic systems, and business product marketing. He joined ADTRAN after working in the Science & Technology department for several years at BellSouth.

Kevin holds an Electrical Engineering degree from Auburn University and an MBA from the University of Alabama.

The Need for Gigabit

Gigabit networks are still in their infancy. Many question the need for Gigabit speeds, when we have not fully utilized the bandwidth available today. But others have embraced the vision for Gigabit services, and are using it as a force for change within the communities they serve. Gigabit services connect the citizens of a community and enable growth and prosperity. Areas that were once desolate or dying have found new life through the emergence of Gigabit services. These ultra high-speed broadband networks are also serving as a catalyst for the future, bringing new jobs, new innovation and new beginnings.

Drivers for Gigabit Communities
1. Education
2. Business and Job Growth
3. Improved HealthCare
4. Civic Life
5. Connected Homes
6. Municipal Services

Research is already heralding the impact Gigabit networks can have on a community. David Sandel of Sandel & Associates developed a model for measuring the economic impact of a Gigabit network. His initial study focused on a small area in the creative center of St. Louis and showed a significant impact of a Gigabit network. His initial study focused on a small area in the creative center of St. Louis and showed a significant impact:

- 1,000 high-tech jobs paid at industry standard
- 972 additional jobs across a number of industries, including real estate, employment services, food service and drinking establishments, hospitals/ health care providers, telecommunications and wholesale trade
- $132,590,000 in wages and benefits
- $172,227,000 in additional economic benefits

In summary, this study estimated a total annual economic output in excess of $265 million derived from an initial investment of less than $3 million. To read the full report, go to http://bit.ly/1dhtAfH.

WALKER AND ASSOCIATES INC

BROCADE

BREAK THE STATUS QUO:

THINK BIG. START NOW.

In a world that relies on the steady flow of critical information, you can't afford a network that holds you back.

See how Brocade data center networks give you the power to accelerate innovation, modernize your business, and tap into a new world of opportunities.

Start your journey to the New IP today.

www.brocade.com
#NewIP

Realizing the Benefits Promised by NFV

By Prayson Pate
Chief Technology Officer
Overture Networks

I am passionate about helping the telecom industry go virtual. I believe network functions virtualization (NFV) is the key to profitability and at Overture we are making NFV real and profitable for communication service providers (CSPs) and mobile operators. Businesses and consumers are demanding a lot from the providers of the data, communications and media services that help us work well, live large and play hard. The telecom and mobile industries are suffering from escalating operational costs while scrambling to scale for the mad crush of on-demand services and to support new paradigms like Internet of Things.

There is no question that Network Functions Virtualization (NFV) is the key to future profitability for communication service providers (CSPs). As I've talked with our customers and others at industry events, I've sensed a general consensus on the anticipated benefits of virtualizing service delivery.

New On-demand Service Capabilities
At the heart of NFV is the concept of replacing single-function proprietary appliances with standard servers running software-based Virtualized Network Functions (VNFs.) VNFs can be designed to take advantage of horizontal scalability to support services that expand or contract with demand.

By decoupling hardware and software and making use of cloud technologies, NFV enables cost-effective, highly scalable on-demand services.

Flexible Deployment Models
Separating the hardware and software has some advantages in itself. The bigger advantage comes when you use proper software design to build the VNFs, and advanced orchestration techniques to place VNFs where they make the most sense. Doing so allows the operator to construct valuable new services with the VNFs placed at different locations based on constraints such as utilization, bandwidth, latency and security.

For example, a firewall VNF might need to reside at the customer site to ensure privacy on the uplink, but a VPN VNF could be hosted in a metro datacenter. Flexibility like this maximizes the ability of service providers to meet the needs of their customers.

New Revenue-Generating Service Opportunities
Virtualization enables cost-effective acquisition of new and growing revenue streams as CSPs respond automatically and immediately to an end-customer's opt-in for services.

How? By doing the following:

- Leverage advanced orchestration and network control techniques to dynamically construct services.
- Use big-data analytics to measure and assure SLAs.
- Take advantage of modern and open APIs to connect the virtual services to existing OSS/BSS systems.
- Update customer portals to present these new services to customers on a self-serve basis.

Making NFV Real
From my conversations I've come to understand there is no "one-size-fits-all" approach. Every CSP we know has taken a unique approach. Each is leveraging different parts of the Overture NFV offering with additional virtualized offerings from other industry players.

And THAT, to me, is the real benefit of NFV. It allows CSPs to pick and choose best-of-breed components to create an overall solution that works best for them.

The good news is that you can deploy NFV and optimize profitability today! The right set of VNFs, coupled with open orchestration, analytics and control solutions turns the promise of NFV into real value.

2015: The year SDN and NFV go mainstream

By Steve Alexander
Network World

According to Infonetics Research's "2014 SDN Strategies: North American Enterprise" survey, which estimates that 87% of U.S. businesses intend to have SDN live in their data centers by 2016. From that perspective, SDN is well on its way.

These deployments have kept the hype somewhat subdued, but this is the most transformative technology we have developed in decades, and 10 years down the line – maybe even sooner – SDN will simply be known as "networking." In 2015, the technology will begin the journey down that path with the first deployments of SDN in telco networks across the globe. This will be a huge step and could push SDN toward achieving critical mass; we expect to even see SDN deployed on global submarine networks to enable more dynamic services than anything available in the past.

We will also begin to see NFV become a technology du jour. There were NFV whispers in 2014, but 2015 promises to put the discussion on the map in the same way SDN was during the past 12 months. Once people see the tangible results of what software can do for a network, it's only a matter of time before people begin to see the benefits of replacing hardware functions with virtualized equivalents. Infonetics research backs up these predictions in its "Carrier SDN and NFV Hardware and Software Market Size and Forecast" report, which predicts that the NFV and SDN markets will reach $11 billion globally in 2018. Along with the major telcos announcing SDN deployments, we'll also see initial NFV deployments in high-touch enterprises.

Reprinted from Network World. Read the full article at http://www.networkworld.com/article/2858736/sdn/2015-the-year-sdn-and-nfv-go-mainstream.html

Service Assured Networking for Power Utilities

RAD offers energy utility customers field-proven Service Assured Networking solutions over SONET/SDH and packet switched networks for the operational needs of their transmission and distribution (T&D) grids.

These include:

- Substation multiservice connectivity and migration with Traffic Duplication
- Distance and differential Teleprotection
- IEC 61850-3 secure substation communications
- Operational core network using carrier-grade Ethernet
- Distribution automation and smart metering backhaul
- Integrated security and firewall tools

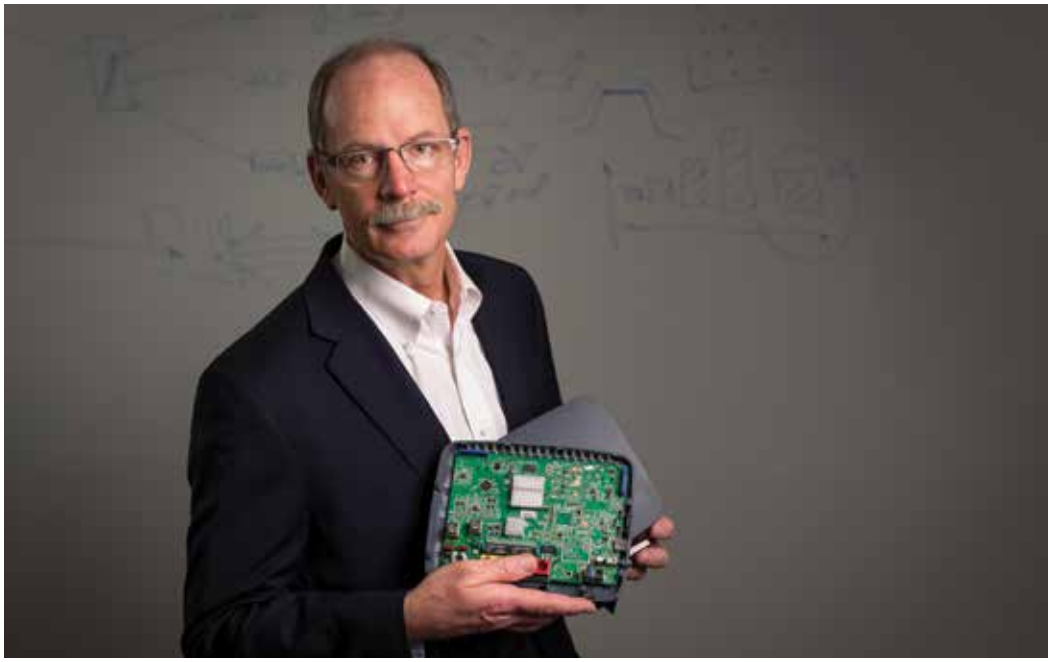
Visit RAD in Booth #401 at APPA's 2015 Public Power Expo in Minneapolis (June 8-9)

RAD

Contact RAD today at: (800) 444-7234 | Market@radusa.com | www.radusa.com

Re-thinking the Retry; Four Steps to Superior WiFi

Tim Bennington-Davis
VP of Engineering
SmartRG



We have all become dependent upon WiFi in homes and businesses, and have experienced the frustration when WiFi "doesn't work" in the middle of a video chat session, downloading a video, or making a purchase over the Internet. Want to know why? Retries.

The WiFi protocol is pretty straightforward. Every device, whether an Access Point (AP) or client (STA), must share time on the air. Only one device can be send a packet or packets at any point in time, and every transmission requires an acknowledgement (ACK) back from the receiver. Transmissions are randomized to give all devices an equal chance, and all transmitters must listen for clear air before transmitting. The devices communicating must get enough airtime to keep up with the needs of the application, such as a video stream.

Faster modulation rates can shorten the amount of time it takes to move data, but only if the transmissions are successful. If a transmission isn't acknowledged by the receiver, the data must be resent. In 802.11 protocol, this is known as a retry. It is the retransmission of a packet for which there is no acknowledgement received. Retries are inherently undesirable, because they waste airtime. Wasted airtime is undesirable because we tend to have many devices in our homes that need to move data, each needing airtime.

However, faster modulation rates also carry a risk. The higher the modulation rate, the better the signal/noise ratio must be. Given that our homes are inherently noisy with many sources of interference from all our devices and neighbors, often the higher modulation rates simply don't work. This causes the transmitting devices to have to "hunt" for the right modulation rate that enables successful reception. This is known as rate adaptation, and uses retries (airtime) while hunting for a modulation rate that will work. Because a transmitter has no indication as to why a receiver fails to hear the transmission, the transmitter has to assume that the reason for the failure is that the receiver has or encountered interference. The transmitter is at a fixed power level, so the only option is to issue a retry at a lower modulation rate, which amounts to sending exactly the same information out again more slowly, which takes even more airtime than the original transmission. This process is repeated with successively slower modulation rates until the transmitter finally gets an acknowledgement back.

If this were just one packet of information, the application might not be impacted by this delay. Applications streaming video or voice are constantly adding a "backlog" of frames that also need to be transmitted. While the retry process is resolving logjam of frames builds up, and applications begin responding again only after this logjam has been cleared. This causes the periodic "freezing" of video and audio we often see, and lasts until the system has been able to catch up.

As might be expected, if devices are positioned near to the Gateway or Access Point, these problems are minimal. When distances increase, so does the wasted airtime. The traditional approach to this problem is to think that just choosing Access Points with more transmit power will help. However, it is important to remember that the communication must be bidirectional, it only works if the device and Access Point are equally loud, and equally clear in their communication. This is practically impossible to achieve, given that many of the devices are being held in our hands, up against our heads, or in our laps.

So, the key to best performance is to think in terms of efficient communication, especially where there are many devices and data-hungry applications. Situations that cause retries and rate adaptation need to be minimized, preserving airtime for what really matters – successful transmission of data.

- Work to maximize the probability of success that each transmitted packet will reach its intended destination. Keep distances short.
- Minimize the number of devices per Access Point that are big consumers of airtime. Put multiple Access Points to work in your environment, on non-overlapping channels, so that all devices have a high probability of a short reach and little contention for airtime.
- Turn the power down on Access Points to make a smaller service area. The devices that connect at the "fringe" edge of the service area will be the devices which suffer the highest number of communication problems (retries), and will create congestion on the air for all concerned.
- Consider upgrading your legacy devices to newer technology. The slower devices consume much more airtime per transmission.

A single access point in a large house with many data-hungry devices is sure to create disappointing results for the end user. Look at things from the point of view of efficient communication, and make WiFi work well for you.

Delivering Dedicated Fiber Ethernet Performance at DSL Prices

By Bill Beesley
Principal Solutions Architect
Fujitsu Network Communications, Inc.

In North America, data services at symmetrical rates of over 100 Mbps have traditionally only been available to large enterprise customers because of the high costs of fiber construction and enterprise data equipment. Small-to-medium enterprise customers have been relegated to lower performance cable modem or DSL technologies that have proven unable to deliver high symmetrical bandwidth economically.

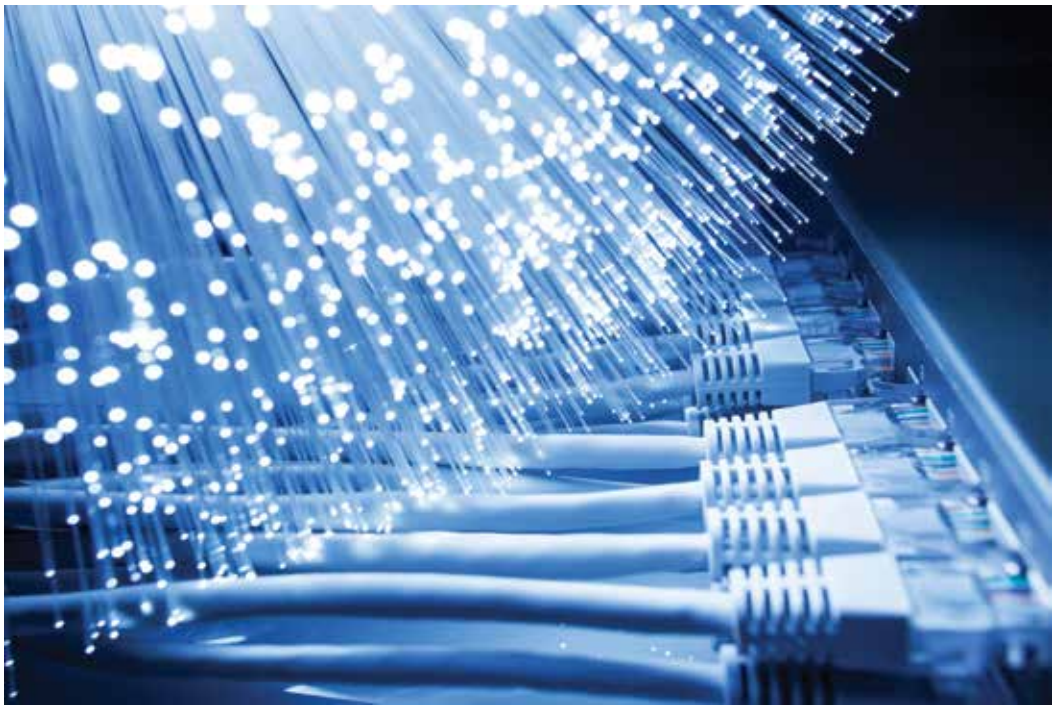
Passive Optical Networking

As small-to-medium enterprise customers adopt bandwidth-intensive applications such as cloud services, demand for dedicated fiber Ethernet performance at a DSL or cable modem price point is increasing rapidly. This, in turn, demands technologies that can allow service providers to serve this profitable market. Existing dedicated enterprise Ethernet solutions, while capable of meeting the technology requirements, are too expensive for the small-to-medium business customer. Passive Optical Networking (PON) offers promising possibilities in terms of both service quality and price point, and is thus emerging as an appealing option because of its use of low-cost equipment to deliver symmetrical gigabit speeds, its support for multiple service offerings, and its immunity to radio frequency impairments that can disrupt customer quality of experience and inflate operational costs.

EPON or GPON?

Operators have two valid PON technology choices to serve this market: EPON and GPON. GPON is currently in wide deployment by providers delivering Fiber-to-the Home (FTTH) services in North America, but because of the increasing strategic importance of active Ethernet, it is likely to be superseded by EPON, which is a superior technology investment for delivering residential and small-to-medium enterprise Ethernet services. This means EPON is the technology of choice for delivering large-enterprise quality Ethernet services to small or medium enterprises and residential customers at a price they are willing to pay.

Originally, GPON had a technical market advantage in that its transmission convergence layer natively accommodated not only encapsulation of native Ethernet frames, but also of ATM cells and TDM services. This capability made it an ideal choice for carriers wishing to deliver simultaneous voice and data services. As telephony services have migrated from traditional TDM to IP, the original technical advantage GPON held over EPON has lost most of its relevance.



The Economic and Technical Merits of EPON and GPON

The costs of the optical distribution equipment (fiber type, splitters, connectors, and so on) are similar for both GPON and EPON. The primary technical and, therefore, cost variation between the two standards is to be found in the Optical Line Terminal (OLT) and the Optical Network Unit (ONU). The majority of GPON products available on the market are FPGA-based, while EPON products predominantly utilize lower-cost ASICs. High demand for EPON in Asia, where tens of millions of units have been deployed to-date, has allowed manufacturers to amortize the initial ASIC investment while continuing to lower the cost of the components as demand, and therefore volume, grew. The economies of scale at higher volumes for ASIC manufacturers suggests that it is unlikely the price of GPON products will decline as EPON chipsets have done thus far (and will continue to do as demand increases).

The optical modules for GPON are also more expensive than EPON due to the faster on-off laser modulation and the multiple laser power leveling required by the ITU-T standard. Additionally, the 2.4 Gbps rate used by many GPON manufacturers is non-standard to the optical industry which limits the volume of demand necessary to drive down manufacturing costs for those devices. It is very doubtful that the cost of GPON equipment can ever be as low as that for EPON in the long term.

EPON has a distinct technical advantage

in a network where services are defined as Ethernet or IP over Ethernet, in that Ethernet frames are carried natively on the passive optical network. GPON requires additional layers of encapsulation to carry the same traffic. In GPON, Ethernet data and TDM frames must pass through two encapsulation stages for transport on the PON. While this worked well where the need to carry native TDM and ATM traffic was required, in an all-Ethernet network the encapsulation needed for GPON adds unnecessary complexity and serves no real benefit in transporting pure Ethernet frames.

Additionally, GPON is architected specifically to support point-to-point connections and thus, where Ethernet bridging or LAN/VLAN support is required, overlay equipment is needed. Conversely, delivery of MEF-defined services is among the standard capabilities of EPON systems. Because EPON is built upon the IEEE 802.3 Ethernet standards, it inherits the standard Ethernet Management Information Base (MIB), which is well supported by the OSS systems already deployed to manage carrier networks.

EPON's Total Cost of Ownership Advantage

In the late 1990s when ATM and SONET dominated carrier transport networks, few would have envisioned the position that Carrier Ethernet holds today. In the 40 years since its introduction, Ethernet has become the primary transport technology due to its flexibility, simplicity, and the economies of scale that have naturally driven down its cost. These same technical capabilities and market dynamics will continue to give EPON a total cost of ownership advantage over GPON.

Clearly, EPON is quickly gaining both technical and economic advantages that will further encourage operators to choose it over GPON. Just as Ethernet transport has eclipsed SONET and ATM and consequently declined in cost, the manufacturing costs of EPON will continue to decline as this technology gains momentum in North America. Ultimately, products that provide better features and lower costs dominate in the marketplace and EPON is clearly well positioned to become the dominant last-mile fiber delivery mechanism.

Walker and Associates Awarded NASA Enterprise-Wide Procurement Contracts

By Randy Turner
Director, Marketing Communications
Walker and Associates

Walker and Associates, Inc. has been awarded multiple contracts under the NASA Solutions for Enterprise-Wide Procurement (SEWP) V. More than 233 proposals were received for SEWP V. Walker and Associates received status in the Group C contracts, which provide server support and multi-functional devices through small business set asides, and in Group D, which provides networking/security/video and conference tools for full and open competition.

All the awards are for firm-fixed-price, indefinite-delivery/indefinite-quantity contracts. Each contract will have an effective ordering period of 10 years, consisting of a five-year base period from Nov. 1 to Oct. 31, 2019, and one five-year option to extend the period of performance through Oct. 31, 2024.

Walker's CEO, Chrystie Brown, states "Walker and Associates is excited to be a part of the NASA SEWP program. The DOD and other government agencies will now have easy access to our broad product selection and carrier grade distribution services. SEWP V will just be an expansion of what we already do reliably well."

The principal purpose of the SEWP V contracts is to provide state-of-the-art information technology and computer technologies, high-end scientific and engineering processing capabilities, network equipment and peripherals. These Government-Wide Acquisition Contracts are available for ordering by all NASA centers, all federal agencies and their contractors. NASA's Goddard Space Flight Center, Greenbelt, Maryland procures and manages the SEWP V effort.

More information about the SEWP V program are available at: https://www.sewp.nasa.gov/sewpv/. SEWP V officially opens for business beginning May 1, 2015.

For information about NASA and agency programs, visit: http://www.nasa.gov.

Managing the Physical Layer

Pat Thompson
Director, Global Product Management
TE Connectivity

Markley One Summer Street is New England's largest and longest operating mission critical and multitenant data center. The operator recently provided its customers with improved redundancy and reliability from its more than 80 domestic and international network providers using an innovative cross connect frame and physical layer management from TE Connectivity.

The Challenge

One Summer Street houses more than 200 clients, including industry leading financial, healthcare, academic, government, entertainment, and science and technology firms. The One Summer Street data center features superior redundancy with service entry at both ends of the facility, and Markley Group's robust data center has never experienced a primary power outage throughout its more than a decade of operation.

"I'm all for adding redundancy wherever possible, and I felt that we could improve it within our own facility between the carriers and the customers by adding yet another level of redundancy to our existing fourth-floor cross connect room," said William (Bill) McLean, director of telecom operations for Markley Group. "Cross connects are what enable us to hand off access from the carriers to our customers—the carrier cable is terminated there and then extended to our customers' suites."

Markley Group decided to add redundancy by adding an additional managed fiber cross connect room to the fifth floor of their 920,000 square-foot data center. With eight points of entry into the centralized Boston location and the ability to provide customers with cost-effective cloud services, unlimited bandwidth, low latency and direct connection to any carrier or enterprise, Markley Group needed an all-inclusive system.

The Solution

Markley Group chose to provide improved redundancy, reliability and diversity throughout the building utilizing cutting-edge optical cabling from TE's Cross Connect Frame (Q-Frame) system, complete with Quareo physical layer management. Specifically designed for fiber intensive data centers, the four Q-Frames selected for the new cross connect room each hold 3,072 strands of fiber, while providing several key fiber management features.

The Q-Frame installed at One Summer Street houses TE's Q4000 managed network chassis and blades, which supports TE's Quareo Physical Layer Management Solution. The Quareo-enabled fiber jumpers, record real-time data from embedded microchips at the time of installation. This information is then utilized by TE's Quareo Infrastructure Configuration Manager (ICM) software to explore, discover and map all connections and automatically record any changes to the connections as they happen. With this system, Markley Group can view, manage and audit all of the fiber connections within the frame and beyond. This information provides them with unprecedented security and business continuation by making every interruption, intrusion or outage instantaneously visible via graphic display and reporting tools.

Quareo physical layer management reduced time-to-service for new clients and those adding circuits. Because the network technicians can now see which ports are activated and open, they no longer need to spend 2-3 days deploying technicians to validate network data. Today, there is real-time visibility to activate circuits quickly, minimize human errors with cross-connects and records are automatically updated.

"I really like the physical layer management capabilities that we have with the new cross connect room and the ability to track port-to-port connections," says McLean. "If a jumper gets unplugged, we'll know immediately. The enhanced record keeping will help us to continue to maintain availability and reduce our meantime to repair because we can find ports extremely quick."

Pat Thompson is director of global product management for TE Connectivity, responsible for physical layer management solutions. In this role, Mr. Thompson is responsible for indentifying, developing and introducing new solutions that address the customers need to grow and operate their networks in a faster and more cost effective manner.

Pat has more than 20 years of experience in the telecom industry, he has held a variety of Mechanical Engineering, Design Engineering, Systems Engineering, Product Management and Business Development positions and has worked with service providers around the world to design, engineer, and manage fiber optic networks. Mr. Thompson holds a Bachelor of Science degree in Mechanical Engineering from the University of Minnesota.

COMPLETELY COVERED

Quareo Physical Layer Management

Know, in real time, when and where connectivity changes take place in the network.

KNOW YOUR NETWORK

Visibility

REDUCE SLA PENALTIES BY **UP TO 80%**

Optimization

IMPROVE UTILIZATION OF ASSETS BY **90%**

Efficiency

REDUCE SERVICE TURN-UP TIME BY **UP TO 50%**

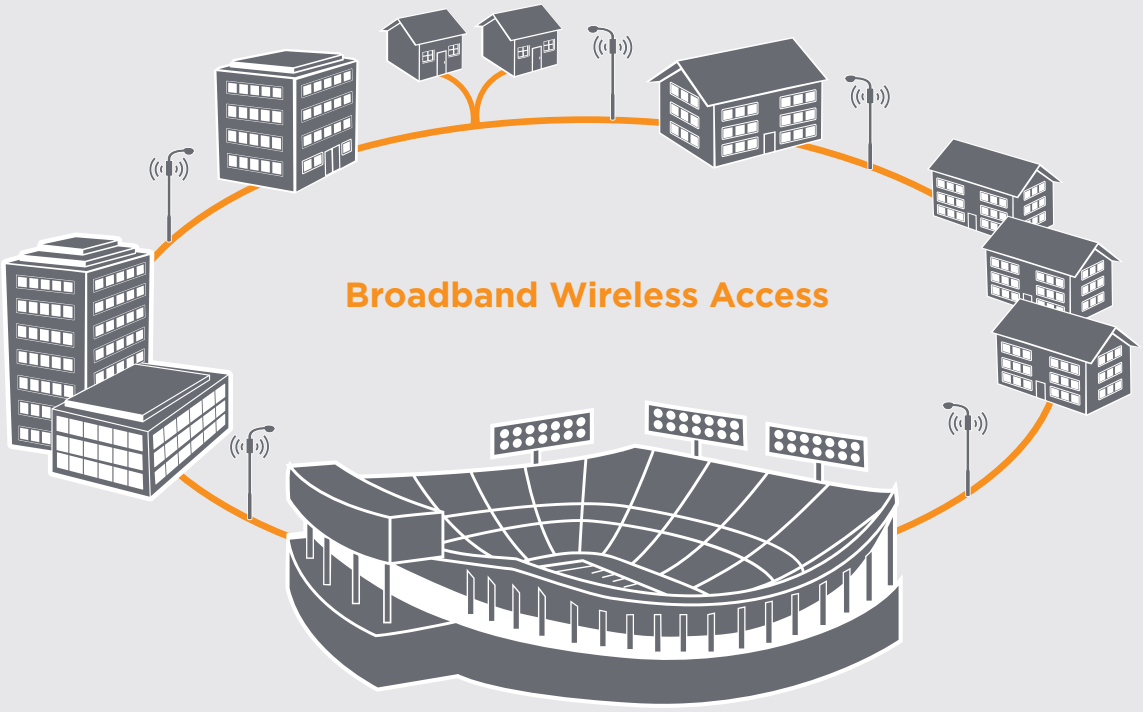
TE Connectivity is revolutionizing the way networks are maintained and controlled. With Quareo, network administrators now have instant visibility to unauthorized physical intrusion, activity awareness control, and automatic documentation changes. All of this while reducing troubleshooting time and expense by up to 68%.

See how implementing a Quareo system can save you time and money at te.com/quareo

COMPLETE COVERAGE

End-to-End Digital DAS Solutions

FlexWave products support multiple technologies and multiple frequency bands, addressing coverage and capacity needs for wireless networks.



A leader in digital DAS (Distributed Antenna Systems), TE is helping revolutionize the way people communicate through high performance and scalable wireless networking. FlexWave Prism and Spectrum offer mobile operators flexible solutions for extending macro network coverage for 2G, 3G, and 4G services more cost-effectively than ever before.
See how our Digital DAS Solutions can increase your coverage and capacity at te.com/DAS

NEWMAR®

Powering the Network℠

AC-DC
Voltage/Power Range:
120/240 VAC Input 12, 24, 48, or 110 VDC Output 150 Watts - 14 kW
Components: Rectifiers, Battery Chargers, Power Modules, Power Supplies, Power Management, Rack Mount, Wall Mount, Desktop
Systems: Hot Swap Rectifiers Shelves with Distribution and Monitoring
Power Plants: Rack Mount Systems with Batteries

DC-DC
Voltage/Power Range:
12, 24, 48, 72, 110 VDC Input 12, 24, 48 VDC Output
Configurations:
Isolated/Non-Isolated, Step-Up, Step-Down, Stabilizers, Battery Charger, Rack Mount, Mobile, Wall Mount, Desktop

DC-AC
Voltage/Power Range:
12, 24, or 48 VDC Input 120/240 VAC
Output 1000 - 5000 Watts
Configurations: Rack Mount, Wall Mount, Mobile

DC Power Distribution
Voltage/Power Range:
12, 24, or 48 VDC Input 200 - 900 Amp VDC Output
Configurations: Rack Mount

DC UPS
Voltage/Power Range
12,24 VDC Input / Output 5-20 amps
Configurations: Mobile Mount

Battery Chargers
Voltage/Power Range
120/240 VAC Input, 12,24,110 VDC Output
Configurations: Wall Mount, Mobile Mount

Monitoring/Control
Remote and Local Monitoring; DC Voltage, AC Voltage, Alarms, Batteries, Security, Cameras
Remote Control of DC and AC Equipment


Hot Swap Rectifiers


Power Modules


Power Plants


Power Management


DC-DC Converters

Inverter-Chargers


Inverters


DC Distribution Panels


Battery Chargers

DC UPS

Site Monitor & Control

For more information, contact your Walker and Associates representative or visit walkerfirst.com

Secure High-Speed Connectivity
Protecting Critical Data in Motion without Compromise

By Dr. Michael Ritter
VP. Technical Marketing & Analyst Relations
ADVA Optical Networking

Enterprises of all sizes have been adopting cloud-based applications, in which company data constantly interacts with customers, partners and suppliers and where the cloud architecture takes on an important role. The cloud has proven its ability to offer flexibility, scalability, ease of use and lower costs. As a result, more and more data is flowing outside of traditional enterprise networks. But as cloud computing technology grows in popularity, IT professionals are increasingly worried about the data security threats that could jeopardize their company's future.

Cybercrime and espionage are on the rise and set to intensify. IT decision makers are therefore not only concerned about protecting data inside their own corporate walls. They also look for solutions to protect their data when transported between their own locations and those of their business partners.

Fiber-optic networks have long been considered to be the fastest and most secure method of moving information for just about every industry. Verticals including finance, telecommunications and healthcare as well as government sectors interconnect their critical data appliances with fiber-optic networks. As data theft and hacking technologies have become less expensive and easier to obtain and use, fiber-optic networks have become increasingly vulnerable. Cybercrime continues to be on the rise and all industries fall victim to it. Industry research reports conducted by organizations such as the Ponemon Institute underline that corporate and commercial espionage is real and must be considered in the security plans for every organization. Focusing on internal network security alone is not sufficient as information traveling between sites can be intercepted without a great degree of difficulty.

With security concerns increasing, most companies are focusing on preventative measures within the walls of their data centers. Encryption is the most effective way to increase the level of security and safeguard external network connections against unauthorized access and usage of internal assets. While algorithmic data encryption is a straightforward and well-understood process, network-wide introduction of cryptography poses new challenges on enterprises and service providers.

Network infrastructure providing scalable connectivity between locations and points of presence is at the heart of every communication network. Securing data in motion by encryption at the connectivity network layer ensures superior network performance, simplifies network operations and reduces the overall cost of data protection. Data encryption at the lowest network layer also protects data at all layers in the network stack, as everything must flow through the connectivity layer before going anywhere. ADVA Optical Networking offers field-proven and widely deployed network solutions for secure optical and Ethernet connectivity services. The ADVA ConnectGuard™ security portfolio is designed for maximum security and highest transmission performance.

Cybersecurity and UTC

UTC UTILITIES TELECOM COUNCIL

UTC believes that cybersecurity is the 21st century reliability challenge. To help our members address this challenge, we are implementing a comprehensive holistic strategy that provides practical tools and information about handling cybersecurity challenges in a utilities telecommunication environment.

UTC Cybersecurity design includes three elements:

Policies and Standards
UTC helps create effective and practical cybersecurity policy environment globally. UTC is actively engaged in educating legislators and regulators on cybersecurity-related aspects of utilities telecommunications environment. UTC participates in a number of leading cybersecurity standards bodies to ensure that there are useful and usable cybersecurity standards that can help manage cybersecurity risks in practical ways. UTC focuses on reducing duplication and facilitating harmonization of standards to help our members streamline their cybersecurity policy and standards implementation.

Education and Awareness
UTC's facilitates cybersecurity awareness and information sharing among the critical infrastructure industry and with the policy makers. UTC helps share cybersecurity best practices and solutions to common problems and identifies cybersecurity educational and certification opportunities to help our members stay current in the field. We also work to facilitate collaborative dialog among utilities, vendors and regulators to share best practices.

Practical Tools
UTC is developing and identifying practical tools that can help reduce cybersecurity risks to critical infrastructure. We work with a variety of partners across critical infrastructure industries, government agencies, standards bodies, and other industry associations to identify, tailor, or develop specific practical solutions to help our members manage cybersecurity risks.
(source; UTC.org)

Data Privacy for Mobile Backhaul

Pete Moyer
Principal Solutions Architect
Brocade

In a recent Wall Street Journal article, it is said that security is at the top of minds for most CIOs these days. The article stated that Piper Jaffray surveyed over 100 CIOs and found that 75% plan to increase security spending in 2015, up from 59% last year.
[Reference: http://blogs.wsj.com/cio/2015/01/07/piper-jaffray-security-again-the-top-cio-spending-priority/]

This survey result shouldn't really surprise too many people in the networking industry. But what does this mean for mobile providers; particularly the Tier 2 & 3 mobile backhaul providers, in terms of network security? This article will take a look at the requirements, challenges and use cases for security services in this market.

The LTE network architecture project began with 3GPP in 2004 to enhance the UMTS architecture and optimize the radio air interface and access architecture. What is commonly referred to as "LTE" today is actually standardized as the Evolved Packet System (EPS), consisting of two distinct architectures – the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) addressing the radio aspects, and the Evolved Packet Core (EPC) addressing the non-radio aspects. Together, the E-UTRAN and EPC provide the network system that enables mobile devices, or User Equipment (UE), to access various network operator and non-operator services, including voice, video, and general Internet services. Here is a simple diagram showing this architecture.

Included in the 3GPP standards is a clearly defined security architecture. This is documented in the 3GPP Technical Specification 33.102. This includes IP network security and network element security. Embedding security into the overall mobile network architecture is critically important; as this network is based on IP technologies for both the network control plane and user data plane traffic. In contrast, the previous 2G systems did not have IP-based security mechanisms embedded into the core of the network as the 2G system was not based on IP standards. The 3G/4G adoption of packet switching and IP technologies requires that the open and accessible protocols associated with IP be specifically addressed in the security architecture. The security specifications create a defense-in-depth strategy, as security is enforced at multiple points and layers in the overall 3GPP architecture. It is well understood that security cannot be a bolt-on afterthought; it must be embedded into the system from inception. Security services that are required include authentication, confidentiality, and integrity.

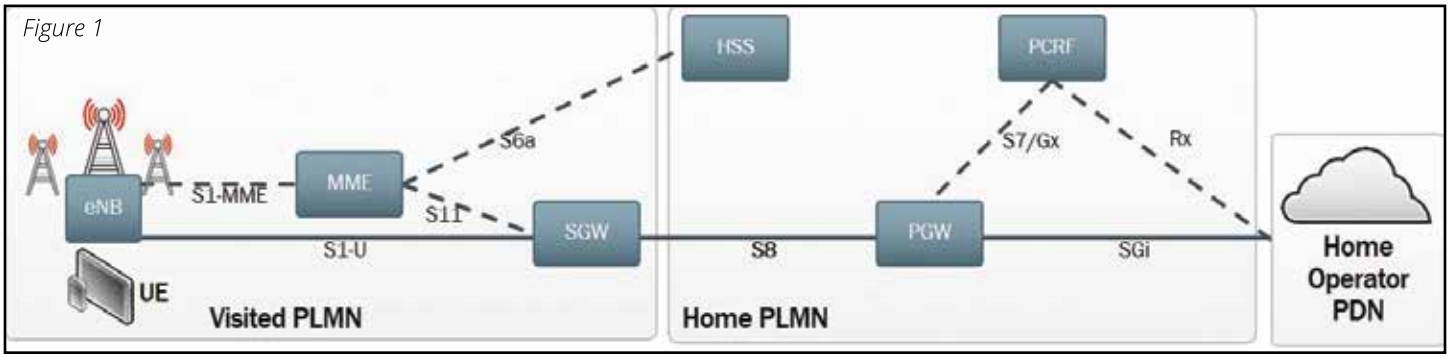
he 3GPP 33.102 security specification defines five functional areas for securing the mobile network: Network Access, Network Domain, User Domain, Application Domain, and also includes the visibility and configuration of security. This article will focus on Network Domain Security (NDS), specified in 3GPP 33.210, which defines the features needed for securing the communications between EPC nodes, including the backhaul links. The NDS is clearly focusing on the security aspects of the IP network layer.

The NDS specification introduces "security domains" to the 3GPP EPS. While a single mobile provider manages its own domain from an administrative perspective, the mobile provider often divides its network into multiple security domains. These security domains typically align to the operational domains that mobile providers use; with specific security for devices, backhaul networks, EPC, services and applications, and OSS/BSS. In this way, security and defense-in-depth can be provided within each security domain which allows greater control and easier manageability. The question then becomes: How does the provider secure the communications between the security domains? The NDS specifically requires a Security Gateway (SEG) node on each side of the security domain to concentrate and protect all traffic entering or leaving each security domain.

That is a somewhat simple use case for security services. A more interesting use case involves LTE subscriber roaming and true inter-domain communications between mobile providers.

As depicted in Figure 2, below, home routed roaming architecture diagram, the roaming subscriber is attached to a visited Public Land Mobile Network (PLMN) but requires authentication, policy, and PDN/IP services from its home PLMN. The inter-domain connectivity between the Serving Gateway (SGW) and the Packet Data Network Gateway (PGW) becomes a critical interface for encryption services. This S8 interface provides the inter-PLMN reference point for the user data plane traffic. The traffic on this connection should be encrypted since the S8 is an external interface and this encryption capability must perform at a high level of performance, so as not to negatively impact real-time applications and the associated user experience. There are additional challenges in terms of scale and ease of deployment for providing this aggregated data plane encryption; including the additional cost for providing this type of inter-domain security.

Figure 1



This inter-domain use case for encryption services in the mobile EPC is very similar to the enterprise and service provider use case for encryption services on Inter-DC connections. Most of these Inter-DC connections are now being encrypted due to the high degree of sensitivity of the traffic that is transported between data-centers. This Inter-DC traffic is typically a mixture of customer user data traffic and internal enterprise application traffic. Both of these traffic types benefit from encryption services if they can be provided at the required scale and performance levels, while meeting an acceptable price point.

While the direct inter-PLMN use case may require encryption services on the S8 external interface, a more interesting mobility roaming scenario is when a GPRS Roaming Exchange (GRX) is involved. The GRX network connects many Mobile Network Operators (MNO) together and provides a hub inter-connection service for the aggregation of roaming subscribers. In this use case, the roaming subscribers' data traffic does not traverse a dedicated inter-PLMN link as in the use case from the previous blog. Another example of an exchange service between MNOs is the IP Exchange (IPX); which is a multi-service, enhanced IP exchange service that provides inter-domain connectivity for not only the MNOs but also for Fixed Network Operators. [It is an interesting side note that the IPX provides a similar service for connecting mobile networks together as the Internet Exchange Point (IXP) does for connecting ISPs together.] The widespread use of these roaming exchanges raises yet another question: How does the security posture change when the roaming exchanges are in the middle, as compared to the direct inter-PLMN connections?

When comparing this IPX-based interconnection to the simpler direct inter-PLMN use case, the addition of the IPX cloud in the middle poses some interesting security questions. The Stream Control Transmission Protocol (SCTP) [IETF RFC 4960] based Diameter Base Protocol [IETF RFC 6733] for control plane traffic and the GPRS Tunneling Protocol for user data plane traffic must both be secured through the external IPX network. In the Diameter traffic scenario depicted above, each MNO network aggregates its traffic into a Diameter Edge Agent (DEA) to support scalability, resilience and maintainability. The DEA is the only point of contact for traffic entering and exiting the operator's network. If the assumption is that the external interface from the DEA to the IPX is not trusted, then security policies and enforcement mechanisms should be applied here.

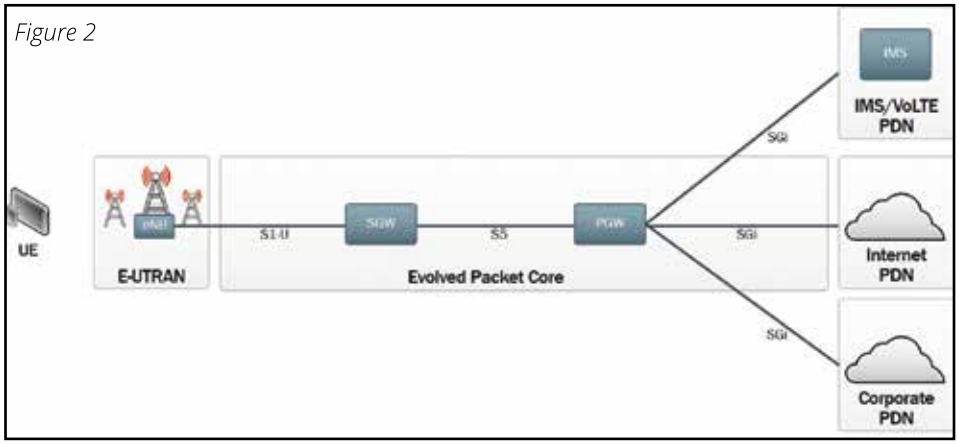
So, what does the IP network domain security specification [3GPP Technical Specification 33.102] actually require for encryption services? The 3GPP security architecture specifically calls out IPsec [IETF RFC 4301] for providing IP level security in the EPS. IPsec provides a wide set of security services; such as, data integrity, data origin authentication, anti-replay protection, and confidentiality. The NDS specifically requires IPsec with Encapsulating Security Payload (ESP) in tunnel mode, where the entire original IP packet is encapsulated with a new packet header added. The Internet Key Exchange (IKE) v2 protocol [IETF RFC 5996] is required to set up the security associations between the nodes in the EPS.

In addition to the inter-domain communications that may require IPsec encryption services, the internal mobile backhaul links also require integrity and confidentiality protection. The NDS specifies that all traffic in the mobile network requires security services; including control / management and user data plane traffic. There is one exception to this rule; that is, when the network interfaces for user data plane traffic are within the same domain and are trusted (e.g. physically protected), then IPsec is not mandatory. However, 'not mandatory' should not be mistaken for 'not beneficial'. Encryption is always beneficial; the question is one of "What are the trade-offs for providing encryption services in the mobile EPC network when they are not outright required"?

Tier 2 & 3 mobile backhaul providers could offer encryption as part of their backhaul service to the Tier 1 carriers. This could possibly be a differentiator from the competing Tier 2 & 3 mobile backhaul providers.

One additional EPC interface, the SGi, would also benefit from the encryption services that IPsec provides. This is the external interface that connects the mobile EPC to the Internet and other external domains and this interface should not be considered a trusted interface. It is shown in Figure 2, below.

Figure 2



So, there are several use cases and EPC interfaces that would greatly benefit from the encryption services that IPsec provides. A few of these have been discussed in this article. In addition to IPsec, MACsec is another possible encryption services that could be deployed in mobile backhaul networks. MACsec operates at Ethernet Layer-2 while IPsec operates at IP Layer-3. They are not mutually exclusive technologies; however, enabling both of them on the same links would not be a common deployment scenario.

WALKER AND ASSOCIATES INC

ciena | Diamond Partner

Avert Network Threats Before They Happen.

Cyber attacks can happen anywhere—as attacks become more sophisticated, the unguarded parts for your network are most vulnerable. Do you have a complete active defense shield for your critical network infrastructure?

The transport network is often overlooked as a vulnerability. Not anymore. Walker and Ciena are introducing strategies to protect transport infrastructure on multiple fronts.

In addition to preventive measures, learn about active reactions and mitigations by reading our white paper: "Cyber Strategies for the Protection of Transport Infrastructure."

DOWNLOAD THE WHITE PAPER AT:

www.TransportThreats.com

Learn the Top Defense Strategies from Ciena & Walker

Our approach to protecting all levels of network architecture includes:

- Monitor ports that are intentionally unused to detect unauthorized activity
- Comparing log data to baseline data to detect anomalous behavior
- Extend encryption to protect management, control and data planes

SIP Has Evolved, Making Unified Communications Easily Accessible to All

-SIP offers a platform that easily integrates all UC technologies onto one easy-to-manage solution

By: Phil Bowers
Global Marketing Communications Manager
Grandstream Networks, Inc.

If you ask most non-engineers what they know about SIP, their answer will probably involve the terms "VoIP" and "internet telephony." Launched in the early 2000s, SIP has primarily been seen as a voice transmission protocol (VoIP), though it has always had the ability to do so much more than just voice. SIP – and SIP hardware – has evolved to integrate all sorts of communication technologies and applications in addition to voice. Where separate networks (sometimes proprietary) and complicated installations used to be needed for every communication technology, from video conferencing to voice calls to video surveillance, SIP offers one simple platform that easily converges all of these communications into one easy-to-manage solution. For these purposes, "SIP" might as well stand for "simple integration process." Thanks to the evolvement of SIP, unified communications have never been as accessible, as easy to use or as easy to install.

Let's take a look at a detailed example of this integration in Figure 1. You can deploy a SIP network that allows employees to make and receive video conferences while allowing in-office or remote employees to call in using voice or video

Figure 1: SIP Unified Communication Network

phones, and workers can make video calls to employees or clients using the same extension without any configuration. You can fully customize a voice network to route calls in a variety of ways to the appropriate contact. Easily add video surveillance protection using the same network infrastructure already in place and allow those cameras to proactively send out alerts when security events occur. You can integrate a door access solution into the same network, where door access cameras make SIP voice/video calls to registered phones when a guest appears and allows the door to be opened directly from the phone. Use the existing SIP network to create an intercom system – either through the SIP cameras and their audio inputs/outputs or built-in speaker/microphone – or through the SIP telephony system. Through use of analog telephone adapters and/or IP video encoders, you can even integrate existing analog phones or cameras that you may already have.

Who does this integration benefit, you ask? Everyone. End-user customers receive a state-of-the-art unified communications platform that is fully future proof and allows them to communicate and keep in touch like never before. Installers and integrators are able to offer their customers more communication options than ever before, which are all easily and efficiently installed and can be managed remotely. This simply expands the value of any resellers' business. Finally, distributors and service providers are able to expand their offerings to include more in-demand technology that their customers can quickly and easily take advantage.

In case you could not tell, SIP has evolved.

Walker Awarded Americas Telco Partner of the Year by Juniper Networks

Randy Turner
Director, Marketing Communications
Walker and Associates

Walker and Associates announced that it has received the Americas Telco Partner of the Year Award from Juniper Networks, the industry lead in network innovation. Walker and Associates was recognized at IDEAS/Connected 2015 by Juniper executives for outstanding overall performance and its ongoing commitment to providing market-differentiating, value-added services and resources to the service provider market.

"Walker has a successful record in the telecommunications market and this award is further validation of their commitment to Juniper and our mutual customers. We look forward to continued growth by jointly solving challenging customer problems," said Jonathan Belcher, vice president, Americas Partner Sales, Juniper Networks.

"Walker and Associates is pleased to receive this award, which recognizes significant collaboration and teamwork between Juniper Networks and Walker on behalf of our customers," stated Lisa Smiley, Marketing vice president at Walker. "Through our strategic alliance with Juniper, we offer robust technical solutions that match emerging growth areas in the all IP network, including virtualization."

ASSURED NETWORKING
A Critical Foundation for Today's Networks

By Renee Reinke
Sr. Advisor Industry Marketing
Ciena Corporation

As evidenced by the increasing number of media reports about massive cybersecurity breaches at corporations—from Anthem to Sony, Target, eBay, and others—information security is now a boardroom issue.

The steady stream of bad news underscores the difficulties inherent in protecting organizational information and maintaining data privacy. Cybercrime, 'hacktivism,' and advanced persistent attacks continually threaten enterprise networks. Preventing attacks by keeping bad guys out using traditional techniques such as firewalls and intrusion detection systems are no longer enough.

Today, more than ever, networks play a critical role in creating a more stable, safe, and resilient enterprise infrastructure. Three essential technology elements are key to protecting critical infrastructure: availability, encryption, and authentication.

For many large enterprises, sudden or unexpected downtime is considered more than inconvenient, as network disruptions can wreak havoc on 'business as usual,' resulting in revenue losses and damaging customer loyalty. Packet-optical network technologies function at the lowest levels of the OSI stack, Layers 0-2.5, and can be architected to deliver a very high degree of resiliency. Networks based on Ciena's 6500 Packet Optical Platform leverage various protection, restoration, and control plane technologies to deliver up to six-9s (99.9999%) availability, meeting the requirements of today's enterprise networks.

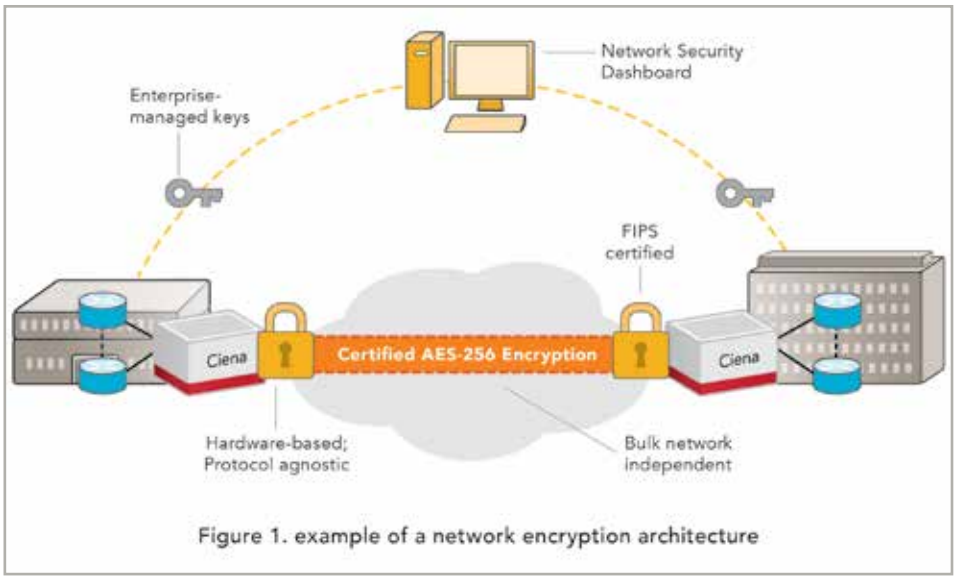
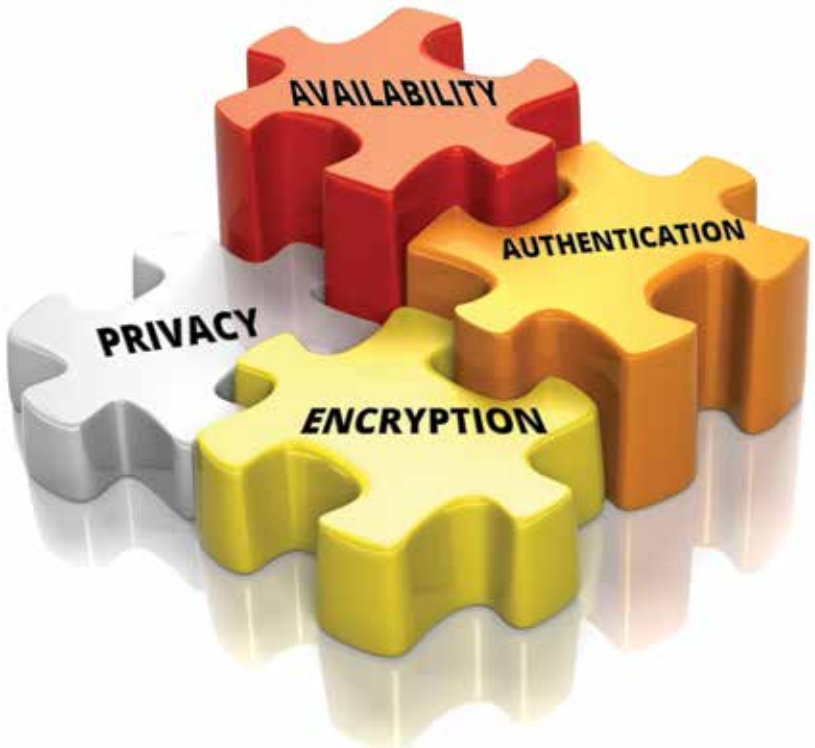


Figure 1. example of a network encryption architecture

According to a 2014 Ponemon Institute research study, the average cost of a data breach rose 15 percent over the previous year, reaching $3.5M . Breaches are practically inevitable, but data can still be protected in flight by utilizing FIPS-certified encryption solutions. Network-level encryption solutions like Ciena's 6500 4x10G encryption card delivers wire-speed throughput with a low-latency AES-256 encryption solution that supports a variety of communication protocols, helping enterprises better protect personal or confidential information and ensure full compliance with legal and federal privacy and security mandates. See Figure one.



Finally, organizations must be able to authenticate network elements in their network to ensure only authorized devices are present and that they can only be managed by appropriate personnel. Integrating within existing enterprise PKI infrastructures, Ciena's 6500 solution simplifies this task.

Information security requires the protection of network infrastructure and the in-flight data transiting the network. Network availability and resiliency ensure the performance of the network. Encryption and authentication ensure data privacy is maintained across the network in spite of cyber breaches of in-flight data. Ciena's 6500 is well-positioned to support enterprises as they strive to shore up network availability and information security on daily operations.

Attacks, Regulations Drive Utility Focus on Cybersecurity

By Dave Thomas
Business Development Director
RAD

The alarming increase in cyber attacks on critical infrastructure poses new risk management challenges for utilities. At the same time, the need to comply with the North American Electric Reliability Corporation's (NERC's) latest Critical Infrastructure Protection (CIP) requirements is focusing utilities' concentration on the problem, at the risk of significant fines for non-compliance.

The latest detailed reports from the Department of Homeland Security note that some 40 percent of cyber attacks on U.S. targets were aimed at energy sector companies. This poses major risk-management issues for utilities, among the most challenging of which is the need to improve security in remote substations.

By definition, remote substations are often difficult to access, making timely and effective response difficult for even the most qualified cybersecurity and SCADA network experts. This drives the need for solutions that can be monitored, managed, and reconfigured as needed from a central site.

NERC data shows that the top areas for violation are Systems Security Management and Electronic Security Perimeter. Systems Security Management focuses on port control and access, patch management, malicious code detection and prevention, incident log capabilities, and access controls; Electronic Security Perimeters are aimed at managing electronic access by guarding against compromise that could lead to misoperation or instability. Additionally, provisions have to be included to insure protection against internal breaches whether accidental or intentional.

To address these two areas in particular requires a solution that provides resilient cybersecurity controls for remote substations in compliance with the NERC CIP standards.

An optimal solution, for example, would function as a comprehensive SCADA security appliance, with security and efficiency advantages, such as the ability to dynamically reconfigure each SCADA device within a remote substation. This would include IPsec VPN tunnels, separate access controls, whitelisting, and remote collection of logs.

A dynamic cyber risk management approach, likely to become the norm, puts a premium on the capability to adjust controls to new threats, requiring security managers to invest in highly adaptable security solutions. NERC CIP 5, the latest series of standards, aligns with that approach.

An ideal NERC CIP 5-compliant solution should include a SCADA-aware firewall, dynamic configuration for detecting and deep analysis of various SCADA protocols, anomaly detections for traffic spikes, failover communication redundancy, and automatic detection of "normal" baselines.

Of course, introducing new security measures to remote locations adds to the strain on already overburdened utility IT staffs. In an increasingly hostile cyber landscape, security managers need solutions configured with a hardened security baseline for resilience, as well as ease of configuration modification and change management to increase efficiencies.

Dave Thomas is Business Development Director for RAD, provider of security and migration solutions for power utilities.

MHEC Contract Award

Ciena available from Walker and Associates, Inc.

Colleges, universities, K-12 districts and schools in 41 states can use national distributor Walker and Associates, Inc. for less, thanks to an agreement with the Midwestern Higher Education Compact (MHEC) for Ciena wavelength divisional multiplexing products.

Colleges and universities have seen the increased growth in communications on their campuses simply because everyone is connected in some fashion through their electronic devices, Many campuses underestimate these fiber optic needs and multiplexing has been proven to be a more cost effective solution.

One of four regional higher education compacts in the United States, MHEC serves approximately 1,000 public and private nonprofit institutions – more than 4 million students. The agreement also extends to the Southern Regional Education Board and the Western Interstate Commission for Higher Education – 41 states in total.

Walker and Associates is an authorized telecommunications distributor for Ciena's wavelength division multiplexing equipment and software. Ciena's Packet-Optical Platform converges three comprehensive networking layers into a single platform to provide customizable services from the access edge, along the backbone core, and across regional networks. The contract also features value added services such as custom cable assemblies, kitting, material management, integration, and installation.

The competitively awarded contract establishes ceiling pricing for wavelength division multiplexing equipment, software, and related services.

Questions:
John Lackey
Sr. Sales Executive
P: 800.840.2259
D: 336.731.5474
F: 336.731.1647
john.lackey@walkerfirst.com
Contract: MHEC-02262015

Why Leaders Fail

By Mark Sanborn, CSP, CPAE
President
Sanborn and Associates, Inc.

Headlines regularly inform us of the public downfall of leaders from almost every area of endeavor--business, politics, religion, and sports. One day they're on top of the heap, the next, the heap's on top of them.

Of course, we think that such catastrophic failure could never happen to us. We've worked hard to achieve our well-deserved positions of leadership--and we won't give them up for anything! The bad news is: the distance between beloved leader and despised failure is shorter than we think.

Ken Maupin, a practicing psychotherapist and colleague, has built his practice on working with high-performance personalities, including leaders in business, religion, and sports. Ken and I have often discussed why leaders fail. Our discussions have led to the following "warning signs" of impending failure.

Warning Sign #1: A Shift in Focus

This shift can occur in several ways. Often, leaders simply lose sight of what's important. The laser-like focus that catapulted them to the top disappears, and they become distracted by the trappings of leadership, such as wealth and notoriety.

Leaders are usually distinguished by their ability to "think big." But when their focus shifts, they suddenly start thinking small. They micromanage, they get caught up in details better left to others, they become consumed with the trivial and unimportant. And to make matters worse, this tendency can be exacerbated by an inclination toward perfectionism.

A more subtle leadership derailer is an obsession with "doing" rather than "becoming." The good work of leadership is usually a result of who the leader is. What the leader does then flows naturally from inner vision and character. It is possible for a leader to become too action oriented and, in the process, lose touch with the more important development of self.

What is your primary focus right now? If you can't write it on the back of your business card, then it's a sure bet that your leadership is suffering from a lack of clarity. Take the time necessary to get your focus back on what's important.

Further, would you describe your thinking as expansive or contractive? Of course, you always should be willing to do whatever it takes to get the job done, but try never to take on what others can do as well as you. In short, make sure that your focus is on leading rather than doing.

Warning Sign #2: Poor Communication

A lack of focus and its resulting disorientation typically lead to poor communication. Followers can't possibly understand a leader's intent when the leader him- or herself isn't sure what it is! And when leaders are unclear about their own purpose, they often hide their confusion and uncertainty in ambiguous communication.

Sometimes, leaders fall into the clairvoyance trap. In other words, they begin to believe that truly committed followers automatically sense their goals and know what they want without being told. Misunderstanding is seen by such managers as a lack of effort (or commitment) on the listener's part, rather than their own communication negligence.

"Say what you mean, and mean what you say" is timeless advice, but it must be preceded by knowing what you mean! An underlying clarity of purpose is the starting point for all effective communication. It's only when you're absolutely clear about what you want to convey that the hard work of communicating pays dividends.

Warning Sign #3: Risk Aversion

Third, leaders at risk often begin to be driven by a fear of failure rather than the desire to succeed. Past successes create pressure for leaders: "Will I be able to sustain outstanding performance?" "What will I do for an encore?" In fact, the longer a leader is successful, the higher his or her perceived cost of failure.

When driven by the fear of failure, leaders are unable to take reasonable risks. They want to do only the tried and proven; attempts at innovation--typically a key to their initial success--diminish and eventually disappear.

Which is more important to you: the attempt or the outcome? Are you still taking reasonable risks? Prudent leadership never takes reckless chances that risk the destruction of what has been achieved, but neither is it paralyzed by fear. Often the dance of leadership is two steps forward, one step back.

Warning Sign #4: Ethics Slip

A leader's credibility is the result of two aspects: what he or she does (competency) and who he or she is (character). A discrepancy between these two aspects creates an integrity problem.

The highest principle of leadership is integrity. When integrity ceases to be a leader's top priority, when a compromise of ethics is rationalized away as necessary for the "greater good," when achieving results becomes more important than the means to their achievement--that is the

moment when a leader steps onto the slippery slop of failure.

Often such leaders see their followers as pawns, a mere means to an end, thus confusing manipulation with leadership. These leaders lose empathy. They cease to be people "perceivers" and become people "pleasers," using popularity to ease the guilt of lapsed integrity.

It is imperative to your leadership that you constantly subject your life and work to the highest scrutiny. Are there areas of conflict between what you believe and how you behave? Has compromise crept into your operational tool kit? One way to find out is to ask the people you depend on if they ever feel used or taken for granted.

Warning Sign #5: Poor Self Management

Tragically, if a leader doesn't take care of him- or herself, no one else will. Unless a leader is blessed to be surrounded by more-sensitive-than-normal followers, nobody will pick up on the signs of fatigue and stress. Leaders are often perceived to be superhuman, running on unlimited energy.

While leadership is invigorating, it is also tiring. Leaders who fail to take care of their physical, psychological, emotional, and spiritual needs are headed for disaster. Think of having a gauge for each of these four areas of your life--and check them often! When a gauge reaches the "empty" point, make time for refreshment and replenishment. Clear your schedule and take care of yourself--it's absolutely vital to your leadership that you continue to grow and develop, a task that can be accomplished only when your tanks are full.

Warning Sign #6: Lost Love

The last warning sign of impending disaster that leaders need to heed is a move away from their first love and dream. Paradoxically, the hard work of leadership should be fulfilling and even fun. But when leaders lose sight of the dream that compelled them to accept the responsibility of leadership, they can find themselves working for causes that mean little to them. They must stick to what they love, what motivated them at the first, to maintain the fulfillment of leadership.

To make sure that you stay on the track of following your first love, frequently ask yourself these three questions: Why did I initially assume leadership? Have those reasons changed? Do I still want to lead?

Heed the Signs

The warning signs in life--from stop lights to prescription labels--are there for our good. They protect us from disaster, and we would be foolish to ignore them. As you consider the six warning signs of leadership failure, don't be afraid to take an honest look at youself. If any of the warnings ring true, take action today! The good news is: by paying attention to these signs and heeding their warnings, you can avoid disaster and sustain the kind of leadership that is healthy and fulfilling both for yourself and your followers.

Mark Sanborn is an acclaimed speaker, bestselling author and president of Sanborn And Associates Inc, an idea studio for leadership development. For more information about Mark's work and related resources, visit www.marksanborn.com. For information about booking Mark, please contact Helen Broder at 703-757-1204.

REDEFINING BROADBAND

Delivering Tomorrow's Services Today

The demand for Gigabit broadband services is growing at an unprecedented rate. ADTRAN broadband solutions enable service providers to reinvent their networks with proven solutions that are optimized for premium services delivery, rapid deployment and network optimization. Our solutions offer ultra-low cost of ownership and enable carriers to maximize their addressable market.

To learn more, visit ***adtran.com/ultrabroadband***

ADTRAN®

Using virtualization to Reduce the Business Risks of Launching New Services

By: David Noguer Bau
Senior Manager Service Provider Marketing
Juniper Networks

Launching a new service by the telecommunication industry is not an easy task: it requires a lot of research and planning in order to make sure the huge investment is safe. Profits come from taking business risks, but in front of a huge investment, corporations prefer to take calculated risks. The dependency of telecom services to heavy network investments, limits the amount of innovation they bring in the portfolio, specifically when compared with the Over-the-top OTT providers.

Those Telecom Providers looking to reduce their investment risk while continuing to innovate in new services, should introduce the following technologies in their processes:

- Virtualization in x86 compute platforms to reduce the dependency on dedicated infrastructure
- Build a common platform for innovation
- Automated network analysis and optimization
- Automate the service provisioning with NFV MANO
- DevOps to accelerate the development of new services
- Transforming the Service Provider Organization

The new culture helps Service Providers to innovate faster over a common platform and reduce the upfront costs in launching a new service.

Where do we start?
A good place to start experimenting using the new techniques for service-creation is in areas of real potential revenue growth with high uncertainty.

Many service providers see the potential of the ICT services market for enterprises. The traditional approach requires sophisticated CPEs but the scope of services is too limited, expensive and inflexible. With infrastructure virtualization, carriers could build a modular platform with lots of options to the market. A customer can personalize services through a self-service portal with 'instant' activation.

After working with some customers, we have identified some key advantages:

- Building an Open platform reduces the vendor lock-in risks.
- Each new service will be based in VM instances with no hardware dependencies.
- Rapid time-to-market with simplified integration.
- The fixed cost of launching a new service is limited to the integration to the platform. Variable costs include compute, bandwidth usage and each individual software license.
- Working on a common platform and variable costs model, allow service providers to maintain a large number of services portfolio with lower penetration ratios.
- Service providers can fast-fail non profitable services with limited loss and use the learning to plan future services.

It is true that the price/performance ratio for some services is better in physical infrastructure than virtual. Virtualization mitigates the risk by allowing carriers to experiment with new services, and if they are successful in the market, they can be transferred to a more scalable physical infrastructure.

In the Spotlight

By Randy Turner
Director, Marketing Communications
Walker and Associates

Tal Strolicht recently joined Walker and Associates as Regional Account Manager for the BlueSteel Territory, covering TN, OH, MI, IN and KY. Over his career he has taken on a variety of roles in sales, engineering, marketing, strategic planning and product management, working for some of the leading companies in the telecommunications industry including ADTRAN, Nortel, Lucent, Symmetricom, and Calix.

"I look forward to working closely with my customers to add value and help in network design options. I am very excited to join the team of experienced professionals at Walker," stated Strolicht. He can be reached by phone at 615-427-8280, or by email at tal.strolicht@walkerfirst.com.

Trevor Reynolds recently joined Walker and Associates as Regional Account Manager for the Northwest territory, covering Alaska, Washington, Idaho, Oregon, and Wyoming.

Over the past 14 years Reynolds hasworked with Alcatel-Lucent as a Systems Engineer. His background and areas of expertise include microwave, optical, IP, LTE, cell site backhaul and a number of other technical disciplines.

Trevor states "I am honored to join the team of experienced professionals at Walker. Earlier in my career I was one of Walker's customers while working for a CLEC. Walker has a great reputation for combining best of breed technologies with best practices to provide solutions that give customers a maximum return on their investment."

He can be reached by phone at 509-990-3661 or by email at trevor.reynolds@walkerfirst.com.

Craig T. Feigh joined Walker and Associates as Regional Account Manager for the Heartland Territory, covering CenturyLink, Sprint, Charter Communications, and Zayo. I also cover all accounts in the states of Arkansas, Kansas, Missouri, and Oklahoma.

He has been in the telecom industry for over 30 years and was fortunate to work for such great companies as Tellabs, Cerent/Cisco, Redback, and Fujitsu. Hisbackground and areas of expertise are in optical transport, access data, broadband wireless, and taking great care of customers.

Feigh stated "I am very excited to join the team of experienced professionals at Walker and Associates. As a Value Added Distributor, we offer everything from product selection and advice to stocking, inventory management, engineering support, as well as many EF&I Services.

He can be contacted by phone at 913-908-9082, or by email at craig.feigh@walkerfirst.com.

Micheaux Simmons has joined Walker's Engineering/Tech Service department as the SmartRG OEM Development Manager. His responsibilities include network design and engineering, presales support, configuration management, product market support, branding and more. Micheaux most recently worked as an installer/technician for residential gateways at AT&T. He and his family recently relocated to Winston-Salem, NC. Micheaux can be reached at 336.731.5362, or by email at micheaux.simmons@walkerfirst.com

Reggy Jones has joined Walker and Associates, effective May 1. Reggy has over 10 years of specific SEWP sales account experience with SEWP III and IV and a total of 22 years in Federal Sales and Procurement. He has worked for both small and large companies supporting Federal government purchases. Prior companies include PC-Mall-G, Northrop Grumman IT, and Government Micro Resources (GMR). He has a degree in Business Administration and Finance.

Reggy's background includes enterprise equipment sales, such as HP, Dell, Cisco, Apple, Microsoft, Adobe, VMWare, Oracle/Sun, Synmantec, APC and Xerox. Walker looks forward to adding his experience and professionalism to its current Federal group.

Reggie can be reached at 336-731-5239, or by email at reggie.jones@walkerfirst.com.

Annette Bittner has been promoted to the position of OEM Development Manager with Walker, moving from her role as Inside Sales Executive. Her experience in sales spans nearly a decade, and includes work with strategic carrier accounts in the northeast US. She is a past recipient of the Inside Salesperson of the Year Award, in addition to having received several sales performance awards from Walker manufacturer partners.

Her new role involves building and maintaining relationships with targeted manufacturers, forecasting sales, running marketing campaigns for those manufacturers, contract and pricing negotiations, assisting with resolving customer issues, and more. Her manufacturer accounts include Tellabs, Telco Systems, Overture Networks, Coriant America, Polycom, Mitel, Grandstream, Digium, and ZyXEL.

Annette can be reached at 336-731-5378, or by email at annette.bittner@walkerfirst.com.

Trey Hall has been promoted to Vice President of Marketing and Technology at Walker and Associates. Trey joined Walker in late 2013 as the Director of West Region Sales for Walker where he successfully led a sales team responsible for growing market share throughtout western North America.

Trey has worked in the telecommunications industry for over 16 years, previously working at Fujitsu Network Communications where he served in various roles including channel sales, business management, and operations management. Trey holds an MBA from the University of Texas Dallas and an Industrial Engineering BS from Texas A&M University.

Trey can be reached at 336-731-5275, or by email at trey.hall@walkerfirst.com.

Grandstream

Innovative IP Voice & Video

Innovative Unified Communication Solutions

GXP1610

GXP2140

GXP2160

broadsoft

UCM6102 IP PBX

Metaswitch Networks

GXV3240

HT702 ATA

GXV3275

All Grandstream products are available at:

WALKER AND ASSOCIATES INC

www.grandstream.com

sales_northamerica@grandstream.com

As the Internet of Things Becomes Reality, SDN and NFV Become Essential

By Dr. Michael Ritter
VP. Technical Marketing & Analyst Relations
ADVA Optical Networking

The Internet of Things (IoT) has evolved to be more than a vision. It is being built today. Cisco predicts that 50 billion devices could be connected to the IoT by 2020. When you consider the 8 billion phones already in existence as well as the rapid adoption of wearables such as activity wristbands and smart watches, it appears that this forecast could well become reality.

The IoT's value proposition seems straightforward and the stakeholders are known. The debate about what it means to our communication and control networks has yet to start. It is common sense that our networks have to evolve to be able to collect, analyze and share data in real-time between appliances that traditionally have lacked IP connectivity.

So what will really happen when things, homes and cities become smart? The Internet of Things Council predicts that the result will probably be a tsunami of what at first looks like very small changes. 50 billion devices will generate a staggering amount of data and data without analytics is fairly useless. Our networks are crucial when it comes to enabling real-time analysis of sensor data. And they'll need to become much more agile to enable hyper-scale distributed processing at affordable cost.

It's easy to imagine that today's networks are unprepared for it. They are skeptical, even hostile when it comes to connecting new devices. Their focus is on proof-of-compliance involving devices, the user and many other parameters that make it difficult for endpoints to add themselves and communicate with service, data analytics and control instances hosted somewhere in the cloud. What the IoT needs are networks that welcome endpoints. In the future, successful networks will even compete for connections. New methods to monetize the relationship between endpoints and the network need to be developed and designed to supports migration and evolution in order to enable applications beyond the imagination of today.

SDN and NFV are core technologies on this evolutionary path. Defining functions in software and decoupling them from hardware means that architectures can be more easily tweaked as IoT requirements evolve. The implementation of SDN and NFV technology will radically improve service agility, operational efficiencies and innovation capabilities. This will create a foundation that can meet the challenges and requirements imposed by the IoT.

"New methods to monetize the relationship between endpoints and the network need to be developed and designed to supports migration and evolution in order to enable applications beyond the imagination of today."

And SDN and NFV can be instrumental in other ways too. The IoT will be reality soon but we'll need to be wary about putting our trust in each and every thing. Hyper-connectivity will threaten us in an entirely new way, creating the need for more secure network architectures and services. Things cannot be secured. There are far too many devices with an incredible variety of operating systems and hardware configurations. The best hope for preserving end-user privacy, for ensuring data integrity and for protecting devices against intrusions and corruption is adopting SDN and NFV in our networks.

As the IoT gathers speed, software-defined SDN and NFV approaches will become integral. Through them we will achieve the agility and security needed to support billions of connected devices and services and only then will the vision become reality.

As an active member of multiple state, regional and national industry associations, Walker and Associates is strategically engaged with organizations supporting telecommunications markets. We demonstrate our commitment through event sponsorships, exhibiting at conferences and expos, and directory advertising.

Look for us at the events listed here, and refer to the Upcoming Events section of our website, www.walkerfirst.com, for additional details.

We look forward to seeing you at these events!

JUNE	
* TIA Future of the Network 2015	Dallas, TX
TTA Annual Meeting	Franklin, TN
* NYSTA Annual Conference	Clayton, NY
OTA 120th Annual Convention	Columbus, OH
OTA-WITA Joint Annual Meeting	Gleneden Beach, OR
ITA Annual Convention - Illinois	French Lick, IN
TAM Annual Convention	Rockport, ME
* Tri-State Meeting	Charleston, SC
JULY	
* PTA's 113th Annual Convention	Hershey, PA
CTA Summer Convention and Showcase	Breckenridge, CO
AUGUST	
Tri-State Telecommunications Conf.	Jackson Hole, WY
TTA Convention & Product Showcase	San Antonio, TX
ACTA Cable Show	Orange Beach, AL
NCEC/NCAEC Technology Conference	North Myrtle Beach, SC
TechNet Augusta	Augusta, GA
SEPTEMBER	
* OSP Expo	Denver, CO
* UTC Regions 1 & 2 Meeting	Galloway, NJ
ITA Vendors' Showcase	East Peoria, IL
Northeast Telecommunications Showcase (NETS)	Binghamton, NY
OTA CO-IT Seminar	Florence, OR
Great Lakes Technology Showcase	Cleveland, OH

* - Indicates Walker and Associates is an event sponsor

Proud Member of:

TIA ADVANCING GLOBAL COMMUNICATIONS

UTC UTILITIES TELECOM COUNCIL

comptel MEMBER

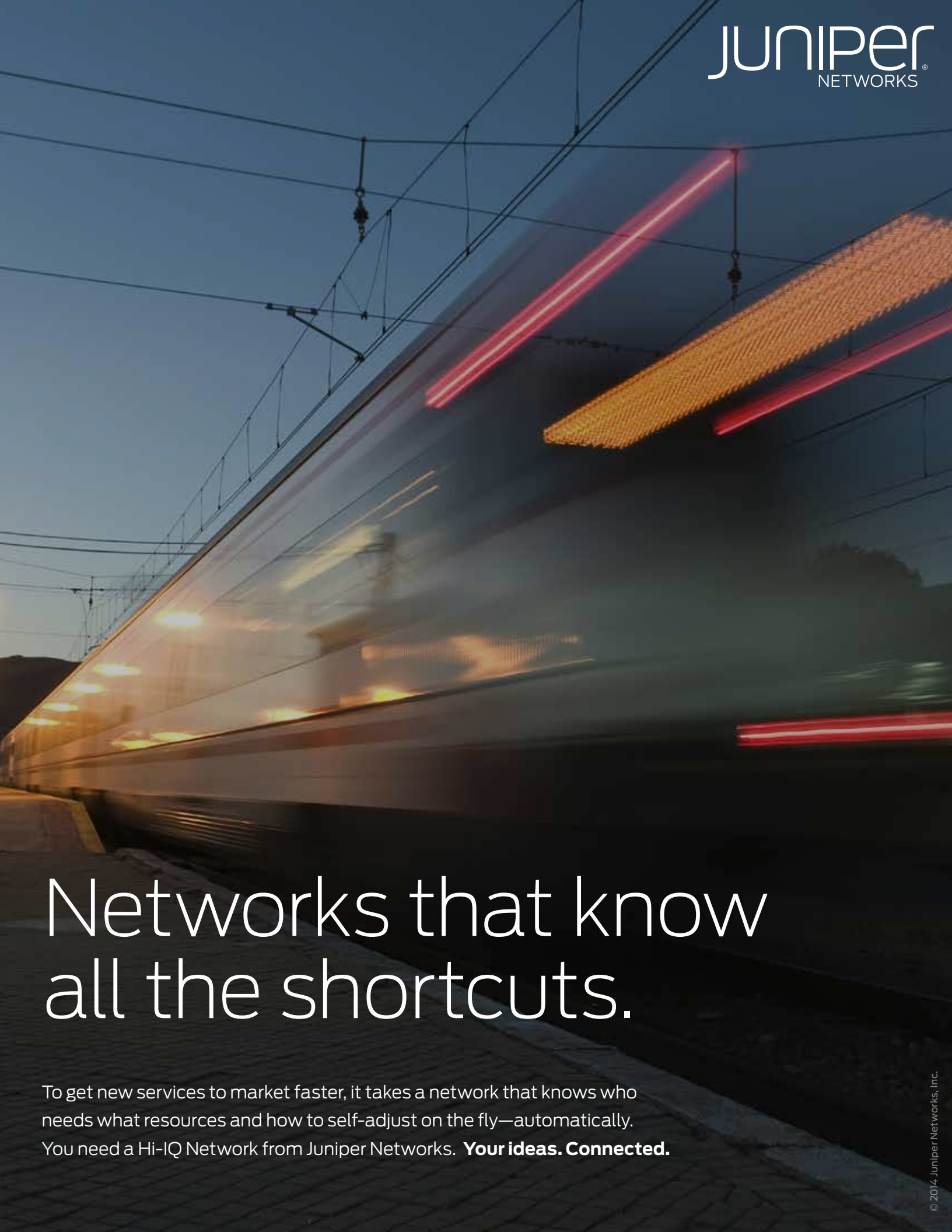
NTCA THE RURAL BROADBAND ASSOCIATION

CCA The Competitive Carriers Association

AFCEA

SCTE Society of Cable Telecommunications Engineers

INDATEL


JUNIPER
NETWORKS
Networks that know all the shortcuts.
To get new services to market faster, it takes a network that knows who needs what resources and how to self-adjust on the fly—automatically. You need a Hi-IQ Network from Juniper Networks. **Your ideas. Connected.**
© 2014 Juniper Networks, Inc.

SMART/RG®
forward thinking

Give your subscribers **the WiFi they want**

with the industry's most advanced, fully managed, xDSL, Gigabit Ethernet and DOCSIS Gateways. Extend your broadband service even deeper in the home with SmartRG's lineup of manageable PLC-based extenders and repeaters. See more at smartrg.com.

Contact your Walker and Associates account manager to start your trial today.

WALKER AND ASSOCIATES INC

7129 OLD HWY 52 N, WELCOME, NC 27374, 1-800-WALKER1, WALKERFIRST.COM