ENG Q3 06

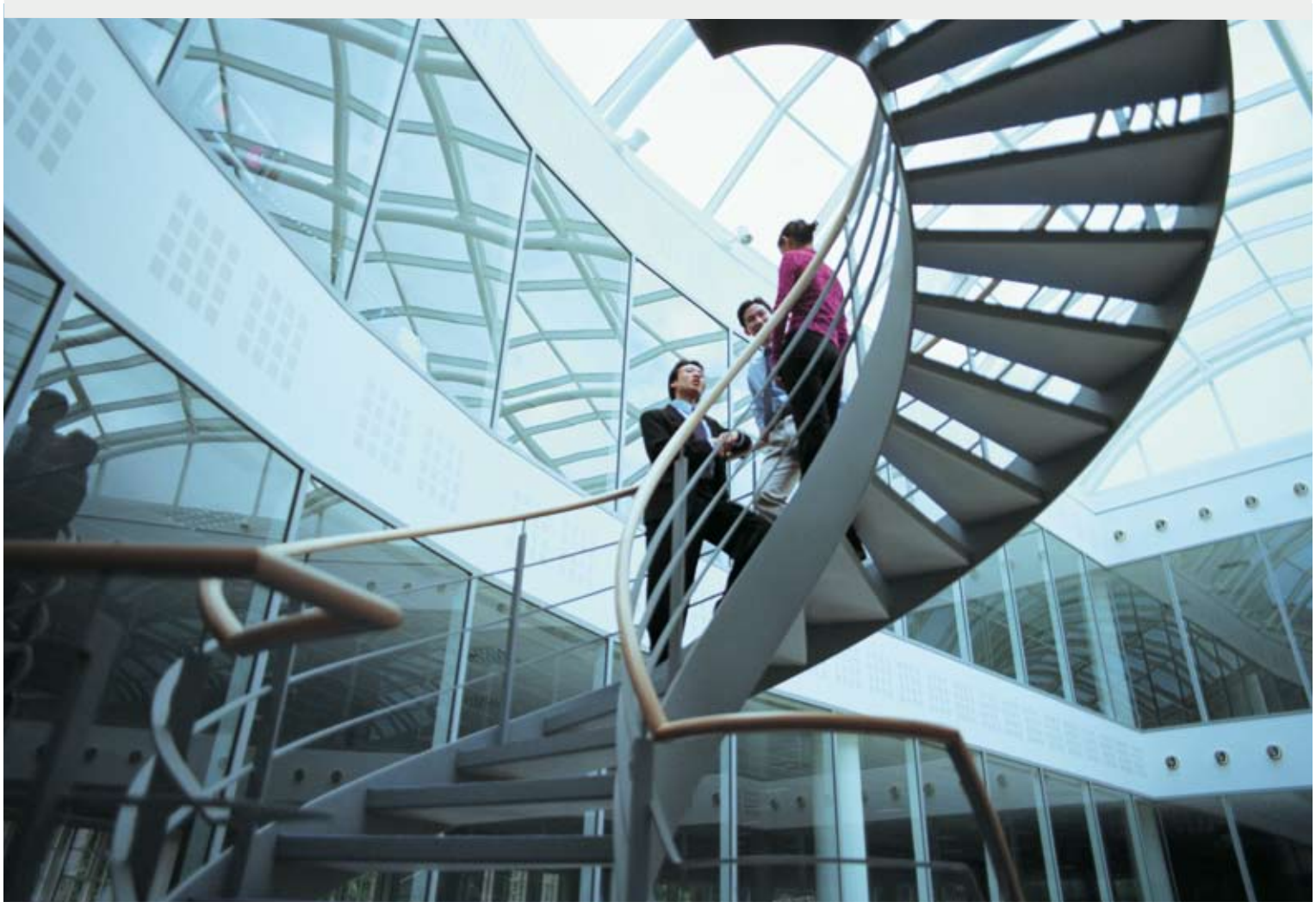
Lucent Technologies
Bell Labs Innovations

LUX

[lux *latin :* light]

Lucent Technologies Customer Magazine

Solutions for the Public Sector



Patricia Russo

Chairman and CEO
Lucent Technologies

Dear Customers,

What makes our industry so exciting to me personally is that communication is a critical part of life. As such, advancements in communications can have a positive impact on virtually every industry, market or sector. Some of the most tangible and rewarding solutions we offer are those designed to help the public sector stay connected to its various constituencies.

Lucent and Bell Labs have a long history of providing solutions in this area. From installing the first telephones in the U.S. Capitol early in the 20th century to the technical support we provided to first responders in the wake of Sept. 11 to helping England's Lancaster University deploy a high-speed network that connects more than 1,000 educational institutions, we have more than a century's worth of experience designing, engineering and implementing secure, reliable, world-changing communications systems for universities, health care agencies, governments and other civil organizations around the world.

We continue to build on that legacy today by leveraging our unrivaled expertise in network integration and security, as well as our leadership in next-generation technologies. One example is our work with the European Commission on a comprehensive analysis of Europe's electronic communications infrastructure, including its Internet and mobile networks. Another is our work as Visa's Qualified Data Security Company (QDSC) in the United States. In this role, Lucent is helping Visa protect the identity, assets and personal information of its cardholders and merchants. (See article on page 18.)

In this issue of LUX, you will learn more about the work Lucent and Bell Labs are doing in such areas as network security, mobile responder communications, hosted VoIP and multivendor network integration. You also will find an article about how Lucent is partnering with a leading physical security company to provide fully integrated physical and network security solutions to help secure public places, including airports, hotels and universities.

I hope you find the issue informative and enjoyable. We look forward to continuing to serve people everywhere by providing reliable, secure communications for the public sector for yet another century – and beyond.

Sincerely,

Patricia Russo

CONTENTS

Targeting the Public Sector

On a daily basis, public-sector IT administrators confront communications and technology challenges that match and often exceed those faced by private sector enterprise. From health care to education, civil-government service provision to the machinations of governance itself, the technologies employed by the state must serve huge numbers of users across myriad geographic borders, potentially spanning decades' worth of legacy hardware, infrastructure, applications and client systems.

But with public expectations on a perpetually rising curve and budgets tighter than ever, governments are now actively seeking strategies, technologies and products that streamline costs and provide both greater access to services, as well as improved integration and flexibility of systems.

This clearly represents a huge opportunity for product and service providers, but the big issue facing firms that want to target government is identifying the best alignment between technology and business/policy requirements. As a result, every new technology development and service forged for this sector must be modelled after a careful mapping of government-specific functionalities required to support vertical-specific business-process blueprints.

Prevalent trends

While there are clearly local and historical factors shaping demand in specific markets, short to medium term we can point to four major technologies and/or trends that are likely to form government sector IT/communications procurement imperatives worldwide:

- Voice over IP – In the U.S., the government is already one of the largest spenders on voice over IP (VoIP) technologies. Spending on IP PBX equipment is high, primarily due to the overall size and scope of the government and efforts to improve communications between distributed offices. This is a trend that's likely to ramp up worldwide, although it's set to be a slow-burn evolution rather than a revolution. Few government agencies are likely to move with any particular urgency while there are still adequate legacy systems in place. In the meantime, there remain serious concerns over the ability of VoIP systems to handle large call volumes and the costs associated with interconnecting individual buildings and data centers.

- Assessment of IPv6 and eventual migration strategies – Another slow burner, but with an intermittent edge of urgency whenever security issues are thrust to the fore. The problem with implementing this enhanced Internet Protocol is that the benefits are decidedly long-term, with initial deployments possibly implying at least as many challenges as advantages. The payoffs - which include easier administration, tighter security and an enhanced addressing scheme - mean that government agencies worldwide can't ignore the inevitable, although few outside the defense community are hustling to be first out of the gate. However, one of the few happens to be the European Union, which regards the new protocol as a key enabler for a new generation of e-government services. To this end, it has brokered cooperative deals between leading global research and education networks with a view to establishing the world's first all-IPv6 research network. The upshot of this is that researchers living and working in different countries have access to state-of-the-art networking services in order to pursue their research.

- Long-term data storage and access – This is a huge issue for every government agency. Legislation coupled with day-to-day social and state information requirements mean that ever larger amounts of data must be stored, networked, shared and accessible for ever longer periods.

- Cross-agency system consolidation – The demand for joined up and more efficient government means that state agencies are expected to become increasingly interconnected with regard to data exchange and flow. This means that government data systems must become more consolidated and this in turn requires increased communications bandwidth to handle the escalation of inter-agency traffic. Long term, it seems likely this trend will lead to the development of strategies involving regional data centers that will take on the roles now played by multiple local systems. This will trigger an investment in network equipment.

Key sectors

Health

While it's usually the potential of mobile data services in health care that grabs the headlines, it is often the rather more prosaic matter of data storage, security, access and integration that tops the list of most hospital and health care administrators. This said, there have been numerous trials and a growing volume of live deployments that have started to demonstrate the value of mobility services to this sector.

Administrators are increasingly acknowledging the potential of wireless services to improve and speed up patient care, cut down errors, improve records management and decision-making in emergencies. With close to 50 percent of physicians employing either a laptop or PDA in many developed markets, the ability to access x-rays, patient history and diagnosis anywhere on a hospital site can save time and money as well as lives. In addition to improved data access, wireless technology is also demonstrating its value in the care and diagnostic process – for example, in the medical supervision of intensive care patients in transit between hospitals.

It is important to note that, quite apart from the practical advantages of such systems, the integration of information and communications technologies (ICT) into an institution like a hospital or school brings about cultural changes to both the institution itself and its workforce.

Firstly, ICT systems inevitably lead to a greater democratization of data – i.e. more information can be accessed by more people, paving the way for informed decision-making across the organization and fostering better teamwork. Secondly, and perhaps even more significantly, such systems also enable the incorporation of knowledge bases deep into the fabric of institutional business. This means knowledge is no longer segregated from frontline activity in "The Library" or in "Patient Files" but can be more effectively integrated into the actual work process.

For example, using access points and triangulation, relevant information can be found by the appropriately provisioned device and patient data automatically downloaded to a doctor's PDA as he or she approaches the patient's bed.

Health is also one of the key areas in which states and institutions are employing ICT resources to inform stakeholders and influence public policy. For example, with health services around the world buckling under escalating demand, there is a growing trend for reducing general practitioner and health center visits by improving the volume and quality of publicly available information related to health.

Education

Like the health sector, technology procurement in education is today heavily focused on the security of networks and data, with a growing emphasis on the need for universities and educational centers to ensure secure and flexible access between as well as within institutions. Once again, this is also about delivering the communications bandwidth that enables the circulation of huge volumes of information.

A recent example of the kind of system driving global research and collaboration is the new high-speed network being developed by China and Europe. Co-funded by the European Union, China and European National Research and Education Networks, the €4.15 million ORIENT (Oriental Research Infrastructure to European NeTworks) project is being developed to foster cooperation between 45 million researchers and students across Europe and China.

With network launch in late 2006, ORIENT will connect Europe's GÉANT 2 - the world's most advanced international research and education network - to the Chinese research networks CERNET and CSTNET. According to EU Information Society and Media Commissioner Viviane Reding, 'Access to applications such as telemedicine, digital libraries and e-learning will help the general public, as well as the research community, to build academic and cultural links between Europe and China and an open exchange of opinions and expertise between Chinese and European researchers.'

On the one hand, governments are coming to recognize the value of ICT investment as a means of maintaining competitiveness in aggressive global markets. At the same time, major projects like ORIENT bring together the world's best minds to tackle global challenges like climate change and sustainable development – issues that demand the cumulative impact of multinational collaboration and expertise.

In a local context, modernizing educational information and communications systems on a university campus

Bell Labs Looks Ahead:

Certain customers require security and processing power that exceeds the capabilities of classical computing. Quantum computing has the potential to make a huge leap forward in making communications highly secure as well as managing enormous databases with sophisticated search algorithms. Bell Labs' science, mathematics, MEMS, nanotechnology fabrication, electronics and systems expertise are enabling scaleable quantum computers, a quantum Internet for secure communications and quantum simulation of complex physical systems.

often demands the consolidation of diverse applications into single systems – for example, the integration of student recruitment and registration, classroom and course management, alumni interactions and so on. Again mirroring developments in health care, like the hospital the school or university also lends itself to the mobility proposition – facilitating remote access to schedules, tutors and peers, as well as course and research content.

Defense

Defense is clearly an important focus for product and service providers, not least because its systems have so often led the way by forming the evolution of IT and communications systems elsewhere in government - especially in the context of security. For example, it's already clear that the defense sector will play a significant role driving IPv6 deployments – the move is already mandated in the U.S. and under serious consideration by much of the rest of the defense community worldwide.

The demand for improved functionality with regard to issues like battlefield data sharing and for collaboration between intelligence agencies means security will always be writ large in any defense agenda. This in turn implies a fair measure of customization in terms of product delivery. However, increasing budget pressures are also resulting in a perceptible shift towards commercial off-the-shelf systems whenever possible and even the accession of some hosted services, formerly avoided by government buyers because of potential security risks.

Empowerment and inclusion

Finally, a growing preoccupation of many governments worldwide is the role IT and communications technologies can play in driving and advancing social inclusion. This can start, for example, with the ability to file applications and make payments online, order and check the status of personal documents like passports, birth certificates and license applications, as well as check on the backgrounds and voting records of elected officials.

Fast growing economies like India are embracing ICT e-government solutions as the only way for state institutions to keep pace with change. A recent government report identified eight sectors of central government where online and/or mobility solutions have the potential to save money, empower citizens and speed development - income tax returns, passport & immigration, company registrations, insurance, national citizen database, central excise, pension and banking.

Mobile operators are pitching to governments on the ground that mobile devices are now seen as a 'trusted tool' – they are already employed to pay for video clips, ringtones and cinema tickets, why not extend that use to include local community charges, road tolls, congestion and parking charges, public transport charges or even on-the-spot fines? The SIM technology has long been in place, it's just a matter of bringing local government back-office systems up to date.

Many commentators also believe there are strong arguments for further extending the ambit of e-government to include affordable network access, library, health and social services access, along with online interactions with mentors and educators.

All of this clearly adds up to improved democratization of services and promises to greatly boost social inclusion and further the role of technology as a tool of individual empowerment.

The Next Big Steps

In February 2006, Larstan Publishing unveiled the latest publication in its Black Book series – The Black Book on Government Security. This work features articles on a variety of topics, including a chapter on the need for evolution of government security standards, by S. Rao Vasireddy, Member of Technical Staff, Bell Labs, Lucent Technologies. The following is an excerpt from Rao's chapter, "Standards: The Next Big Steps."

Government security standards are continually evolving. Standards, of course, are the "Holy Grail" of any government IT systems, but achieving comprehensive, end-to-end security is no simple matter. That's especially true in the realm of Next-Generation Network (NGN) security, where a cohesive security architecture is needed to deploy end-to-end network solutions. Here's a closer look at the constantly changing nature of this nettlesome problem and practical ways to address it.

A CIO (Chief Information Officer) of a government agency must consider various standards and guidelines and then apply the relevant aspects needed to secure the agency's IT network. Today there is a myriad of government standards and guidelines in the area of information security. These standards provide specific security recommendations for numerous systems, applications and processes. However, they do not provide a unified and comprehensive security architecture framework that is necessary to plan, design and implement end-to-end network security. If a CIO in a government agency follows various standards, will it be sufficient to ensure comprehensive network security? What else is needed to ensure secure planning, design and maintenance of networks?

What's needed is an architecture framework that leverages the strengths of existing standards. To be practical, any new security standards framework should be consistent with the evolving nature of security, and it must address the emerging paradigm shift caused by the convergence of networks and applications. It also needs to complement existing standards and illustrate how to analyze and implement security more efficiently.

Quality of security: A new paradigm

Current security frameworks and standards lack an approach to analyze quality of security. Any new security framework should help in the end-to-end planning, design and maintenance of the security of Next-Generation Networks while helping to establish a methodology to determine quality of security. For example, if very strong encryption is required, can the application tolerate the accompanying delays in processing? If the answer is yes, what are the other metrics required to assess quality of security?

The quality of security is a new paradigm that is not well addressed in today's security standards. Many of the current security frameworks combine more granular security metrics into availability, integrity and confidentially. This view needs to be expanded to develop the necessary additional security metrics. When these metrics are expanded and incorporated into a comprehensive security framework, a quality of security definition similar to the network QoS (Quality of Service) measures of throughput and propagation delay will be achievable. When the list of security metrics is expanded, it becomes apparent that current network security measurement concepts are not adequate. For example, almost everyone understands availability. A hacker on a data network can launch a Denial of Service attack on a specific VoIP end device or phone, without impacting the network's ability to process the call. The network or the end-user will not know the status of the end device until they attempt to use it. This is a deviation from the traditional phone service where dial-tone interruptions can be easily detected. To comprehensively characterize how the hacker from a data network impacts end-to-end VoIP service availability, one needs to know the security interactions of management, control and user traffic and their impact on networks, services and applications.

Even the well understood "availability" measure is a function of multiple other security metrics, which impact different types of network traffic differently. The security architecture frameworks need to evolve, to ensure that gaps in the current planning and design can be easily identified and the relevant, existing technical standards are leveraged to establish and maintain end-to-end "quality" of security.

Supporting the paradigm shift

ITU-T X.805 (ISO 18028-2) provides a security architecture framework to dissect the end-to-end security planning, implementation and maintenance into easily manageable segments. (See also LUX Q106 "Securing the world's communications".)

Black Book on Government Security Giveaway

To find out more on the Black Book on Government Security and how you can win a free copy, visit www.lucent.com/lux.

Figure 1 shows the multiple security planes, security layers and security dimensions and their interactions with threats and vulnerabilities. The eight security dimensions, together with their interaction and impact on the model shown in figure 1 can be used to develop the parameters for quality of security.

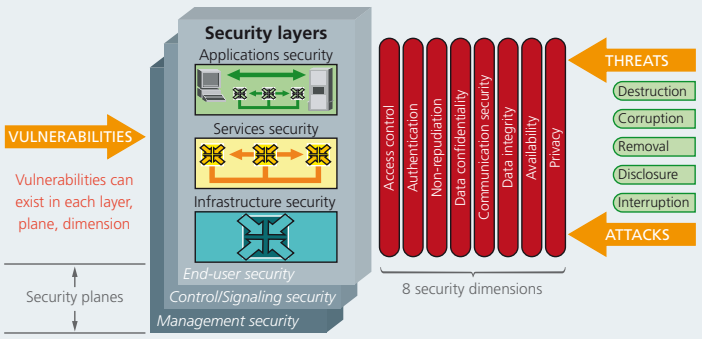


Figure 1: Security Architecture for Systems Providing End-to-End Communications - ITU-T X.805 (ISO 18028-2)

How can the new framework help?

Security discussions have usually been conducted within certain types of security boundary definitions. These boundaries have traditionally been confined to pre-defined network and system interfaces. This is not the case anymore with the advent of converged data, voice and multimedia applications supported by the wireless and NGN networks.

The X.805 security architecture framework shown in figure 1 takes into account end-to-end security of multiple aspects of user, signaling and management traffic across network infrastructure, services and applications. This framework is well suited to characterize and design security for legacy as well as NGN applications with time variant and elastic security perimeters as it breaks down the security into its atomic concepts.

NGN applications and wireless networks are increasingly used in the government IT environment. The ITU-T X.805 (ISO 18028-2) security standard should be used as a guiding framework to select appropriate security standards to ensure comprehensive coverage for design and implementation.

Example

Take the case of Wi-Fi (Wireless Fidelity) networks in government agencies. There are many security recommendations for Wi-Fi, such as NIST 800-48. This standard can be used along with other established guidelines for firewalls, IP network security and other recommendations on monitoring and auditing networks. However, even with all these standards together, a network engineer can't be certain that end-to-end security has been achieved for all different phases of the life cycle from design and planning to implementation maintenance. A framework such as X.805 will be invaluable in developing such a view, since it can be used to verify if the design and implementation have taken into consideration the more granular security dimensions in multiple security layers and security planes for the eight security dimensions. When an agency is designing a new network or deploying a new technology such as Wi-Fi, they can utilize the X.805 framework to analyze security aspects of solutions provided by their vendors.


© Jeff Schmaltz, MODIS Rapid Response Team, NASA/GSFC

Public Safety Networks

» Mobile Responder Communications Networks Critical to Integrated Public Safety

Sometimes the most simple idea becomes the most complicated to implement. Before we placed under a microscope the response and cooperation of all level of government on some high-profile disasters the general public around the world believed that our ability to communicate in a crisis would not be hampered. We have spent the last few years examining not only what went wrong, but more productively trying to decide what is the best road forward for public safety networks.

Due to the massive size of the consumer wireless market, substantial research dollars are pouring into finding new, creative ways to appeal to the growing masses. As a result, there have been significant technological advances and innovations in commercial wireless technologies that offer significant benefits to first responders: video streaming, multimedia messaging, high-speed data access and other applications made possible with today's so-called 3rd Generation, or "3G", commercial wireless technologies.

By embracing commercial wireless technologies, public safety agencies can take advantage of the significant technological advances that have been and will continue to be made in commercial wireless technologies. In doing so, public safety agencies can begin to use capabilities that aren't technologically or economically feasible in today's public safety wireless networks. Application of commercially available wireless technology to public safety networks will set these networks up to achieve what today would be considered impossible – robust, interoperable, multimedia information networks capable of seamlessly handling the multi-level relief and rescue efforts that are facing our world today.

Improving Public Safety Technologies

Differences in market forces and requirements as well as spectrum policy and other factors have driven today's public safety Land Mobile Radio (LMR) and commercial wireless technologies along disparate evolutionary paths.

Non-interoperable, feature-poor wireless communication is a serious issue plaguing public safety agencies. In many instances, agencies lack the technology necessary to perform their mission-critical duties. Furthermore, public safety wireless systems are based on technology dominated by a very small vendor community. Because of this small vendor community and relatively closed market, innovation and competition is limited, forcing the Public Safety community to accept out-dated capabilities at a high price.

Today, public safety systems worldwide are based on narrowband, circuit-switched digital voice technologies with limited support of low-speed data services. In contrast, commercial wireless networks are now transitioning to spectrally efficient, broadband, packet-switched interfaces that will support a wide variety of real-time multimedia applications.

A Public Safety wireless solution based on commercial 3G wireless technologies can offer standards-based, secure, interoperable voice and high-speed data communications to Public Safety users in a cost effective manner. Originally developed for the public cellular spectrum bands, these technologies can be re-banded to provide dedicated wireless communications capacity for public safety agencies, an approach which allows public safety organizations to leverage the large investment in research and development. Extensions to the technology, both within the standard and in support of the standard, will allow this commercial technology to meet the unique needs of the Public Safety community.

Use of commercially available technologies can provide a number of benefits to first responders including lower cost devices, increased data rates and a multitude of new services including multimedia, messaging, location, high-speed data services and video. Leveraging the R&D (Research and Development) investment made to meet the needs of the commercial market to support a relatively small base of the public safety users will greatly accelerate the introduction of new capabilities at lower cost for this important set of users.

One answer to this challenge would be the creation of a public safety communications solution that bridges the commercial wireless and LMR infrastructure. This system could use a common IP-based core to provide local, regional and national service. Lucent has designated this a Mobile Responder Communication Network (MRCN). A MRCN can do two critical things: 1) accelerate the rate at which public safety users can benefit from commercial wireless technology and 2) preserve the legacy investment in public safety LMR technologies.

Creating Mobile Responder Communications Networks for Public Safety

Traditionally public safety networks have been built, owned and operated by individual agencies – fire departments, law enforcement, emergency medical services - as completely separate networks, and at either the federal, state or local levels. While these networks are designed to support mission-critical voice services within their respective areas, they were originally not designed to interoperate with each other or to support new features such as wireless data services.

Recent domestic and global events have shown the impact and limitations of this "closed" system. But migrating to an MRCN model would allow convergence of real-time IP-based multimedia thus delivering all services over a unified public safety communications infrastructure. By its open nature, MRCN can enable interoperable responses to large-scale catastrophes while providing enhanced coverage and reduced costs.

MRCNs may also be created and jointly managed through cooperation among national, regional and local public safety agencies by providing access to all stakeholders. MRCNs do not necessarily need to be funded, built and owned by public safety agencies; they could be owned and managed by third parties (i.e. commercial cellular providers) with the objective of providing services to a multitude of public safety agencies. "Virtual" MRCNs thus may operate in existing or new commercial or public safety LMR infrastructure environments.

For services such as user-to-user voice and high-data-rate access, commercial wireless access is superior to LMR access from both a technological and a cost standpoint. However there are instances where public safety application requirements are more stringent. One area where this is the case is push-to-talk (PTT) voice communications. Because of these factors the preferred architecture for MRCN is one that supports multiple wireless access technology. This approach allows public safety agencies to continue using their existing LMR spectrum allocations, network infrastructure and terminals while selecting the technology (LMR or access via commercial wireless technologies) that best meets their need for new services and deployments.

A dual approach allows public safety networks to both preserve their legacy LMR access networks, to take advantage of interoperable IP-based multimedia services available to commercial users. This approach also provides the ability to offer new specifically tailored services to public safety. Commercial wireless also offers several other benefits for public safety users including better interoperability, reduced costs, and an array of continuously evolving open standards that take advantage of the latest technological innovations. With this communications model, based on a standard platform, far-greater cross-functional communications are possible, ensuring close communication links between local, regional and national and international agencies. Ultimately, the better public safety networks communicate, the better they can work together to navigate the challenges that modern life delivers.

Public Safety in Action: Building the Advanced First Responder Network in Iraq

In 2004, Lucent was awarded a contract by the United States Department of Defense to help rebuild, restore and modernize communications systems in Iraq, a nation of more than 20 million citizens. Iraq was hampered by its inadequate communications infrastructure as it struggled to support its security, intelligence operations and its new government.

Prior to the project, Iraq was a country where only two to three percent of its citizens had their own phone. Perhaps even more troubling was the fact that the nation had no central or regional emergency facilities that could receive and dispatch information. For example, if an Iraqi citizen needed to call for medical help, there was no central dispatching system capable of handling their call.

Working as a prime contractor with the Coalition Provisional Authority (CPA), Lucent helped rebuild, restore and modernize the communications infrastructure in Iraq. In addition, under the leadership of Lucent Worldwide Services, Lucent also managed a cross-functional team of other technology leaders including DynCorp/CSC, Lockheed Martin, Booz Allen Hamilton, AT&T Government Solutions, and CH2M HILL.

The Lucent-built and operated Advanced First Responder Network (AFRN) was delivered on schedule even though it was constructed under some of the harshest physical and security conditions. The work included design, construction, reconstruction, renovation, restoration, implementation and systems integration with existing systems and equipment, as well as operation and maintenance support.

Lucent has also worked closely with Iraqi citizens to train them to manage and operate the network.

The Lucent-built AFRN was used during the first Iraqi elections in January of 2005 to ensure safe voting conditions for Iraqi citizens and then again in December 2005 for the second elections. The AFRN will serve as a core communications backbone as the country around it continues to build a safer, stronger nation.

Pandemic Business Continuity Planning

» Protecting the Global Workforce and Global Economy From a Bird Flu Pandemic

Dr. Jim Kennedy, Lucent's Business Continuity Practice Lead and Distinguished Member of Consulting Staff, Lucent Worldwide Services, examines the operational importance of Business Continuity, including preparing for economic disruptions in the event of a bird flu pandemic

The news headlines seem grim – and the experts across the globe have issued a warning and call to action for governments, corporations and other private industries to work together before it's too late. A new strain of the influenza virus – commonly called "bird flu" – has the potential to cause millions of illnesses worldwide. And the threat of a pandemic also jeopardizes the health of the world's economies as well.

While seasonal influenza (or "flu") continues to baffle health and human services experts, a new strain inflecting birds in Asia has shown that it can affect human beings especially in Southeastern Asia countries. According to a report issued by the United States Homeland Security Council, entitled *National Strategy for Pandemic Influenza*, the statistics are frightening. To date, millions of birds worldwide have died or have been destroyed because of the illness. The virus, which is now being transmitted to humans in a few circumstances, has infected many people in several countries.

The last three flu pandemics in 1918, 1957 and 1968 killed millions of people worldwide. The first priority of global governments is, of course, the health and well-being of their citizens. But global business leaders are also concerned about the disease and the potential economic devastation it may cause. In fact, the bird flu is viewed as a greater global threat than terrorist attacks in 2006, according to a study released in February at the World Economic Forum.

The science and medical community predict that one or more pandemics will hit the globe in this century. The potential for a pandemic outbreak is even greater today because people can jump on a plane and be in another country in less than a day. So why are we so worried? Global economies experience and recover from disasters all the time. For instance, the U.S. economy and infrastructure bounced back from devastating natural disasters like Hurricane Katrina and Rita last year. The difference is the deadly "bird flu" virus could last as long as eight months before the outbreak could be contained. And what will the implications be on the state of worldwide businesses?

The Possible Effects of a Pandemic

Global health organizations are working to prepare for a possible pandemic outbreak. For instance, the U.S. Homeland Security Council has developed a paper called the *National Strategy for Pandemic Influenza*, which provides a guide for helping the U.S. population prepare and respond to an influenza pandemic. However, private industry and government organizations also have a responsibility to prepare their employees and operations before a pandemic crisis hits.

The Centers for Disease Control (CDC) and other global health and human services agencies, including the World Health Organization, that are charged with protecting us from all sorts of nasty diseases and infections have made a sobering prediction. Experts believe businesses across the globe can expect that 25 to 50 percent of the world's industrial workforce could be adversely affected if a pandemic breaks out. This in turn would have a tremendous financial and operational impact on the world's business, with potential financial losses in excess of 300 to 500 billion U.S. dollars.

Global health organizations in many nations, and private corporations, including Lucent Technologies, are building contingency plans – from policies on absenteeism, worker's compensation, and public transportation, to restrictions on travel.

How Should Businesses Prepare for a Pandemic?

More importantly, what do business contingency planners need to do to prepare businesses for this impending crisis?

A prolonged reduction in the workforce due to the impacts of the pandemic will require that businesses prioritize their essential business functions and for a period of time prepare to suspend other non-essential business functions. As business continuity planners, we need to perform Business Impact Analyses to determine which functions are essential and need to continue on no matter what is faced, and those that can be temporarily suspended in light of this unique type of event.

Here are some guidelines from business contingency experts that businesses should examine before a pandemic outbreak happens:

- *Planning and development* – How do you get ready for a pandemic before it's too late?
- *Monitoring* – Developing plans and policies for monitoring the crisis
- *Pre-pandemic preparation* – Knowing what to do if a pandemic hits
- *Pandemic* – What to do once people are exposed to the bird flu?
- *Post-pandemic* – What to do after the pandemic winds down?

Contingency experts also recommend that businesses implement flexible telecommuting policies that will help reduce the number of employees that need to travel to and from work and potentially limit them to coming into close contact with other people and thus the virus itself. In essence, a strong telecommuting policy covering all operating units needs to be established and the technical infrastructure needs to be implemented to provide for the increased activity.

Cross training of critical jobs needs to be undertaken. Documentation of critical functions listing title, roles and responsibilities, necessary training and skills and process flows and descriptions, and staffing levels will need to be developed if not already in place. These will act as training aids for those who will be required to fill in for ill and absent co-workers.

Companies will need to establish additional supply and delivery chain alternatives. There will undoubtedly be widespread impacts on the shipping and receiving of necessary goods and services to sustain business. Getting consultants, service personnel, and sales people to clients will be affected by travel restrictions placed by governmental authorities. Some companies in the services sector have already begun to put together "service packs" which allow client personnel to perform simpler equipment repairs on their own equipment, and consultants will need to be able to perform interviews and other work via video or web conferencing. Current business continuity plans will need to be reviewed to ensure that all response and recovery teams have adequate alternative team leads and members in case any are unavailable due to the flu.

Businesses also need to ensure that third-party suppliers are also prepared for the special circumstances brought about by the pandemic, and have their own necessary contingencies in place. Business unit leaders or continuity planners should verify that those contingency plans can be identified and communicated by the supplier so that they (the contingency planners) can validate their existence. Companies also need to prepare policies to ensure that employees who are ill will remain home thus reducing the possibility of adverse impact by further spreading the virus throughout the company.

Lastly, organizations need to work closely with public health officials to determine how to properly protect the public good while still remaining open to provide goods and services to their clients.

Take Action Beforehand and on Your Own Terms

Experiences and lessons learned from disasters such as Hurricane Katrina, the Asian tsunami and the Severe Acute Respiratory Syndrome (SARS) epidemic of 2003 can help contingency planning experts properly plan for other disasters including a potential pandemic caused by bird flu.

Planning ahead appropriately and responding rapidly to any given crisis should not be an afterthought by any business in operation today.

Dr. Jim Kennedy is Business Continuity Practice Lead and Distinguished Member of Consulting Staff of Lucent Worldwide Services. Dr. Kennedy has over 25 years' experience in the business continuity and disaster recovery fields and holds numerous certifications in network engineering, security and business continuity. He has developed more than 30 recovery plans, planned or participated in more than 100 BC/DR plan tests, has helped to coordinate three actual recovery operations, and has co-authored two books on Security and Business Continuity.

Lancaster University Delivers High-Speed Broadband for Education Sector

Lucent Sales Business Partner Imtech Telecom integrates best-of-breed regional network using market-leading equipment from Lucent and Juniper Networks

Overview

Lancaster University is one of the North-West of England's leading higher education institutions, internationally recognized for the quality of its teaching and research. However, the University has recently taken on an entirely new role, as Internet Service Provider for hundreds of education establishments. With the help of specialist systems integrator Imtech Telecom, and leading technology vendors Juniper Networks and Lucent (who enjoy a very fruitful global partnership, collaborating on some of the world's largest production networks), Lancaster University is providing a high-speed, high-capacity network that is benefiting schools, universities, colleges, libraries, museums and adult learning centers across the region.

Broadband everywhere?

Recognizing the real potential of high-speed Internet access to revolutionize the education sector, the British Government has pledged that all schools should have broadband connectivity by 2006. To aid the initiative, about $90 million was made available to the Regional Broadband Consortia (RBC), specifically set up to procure Internet services and broadband infrastructure for LEAs (local education authorities) and schools.

However, broadband in every school presents a big challenge for some of Britain's most rural areas, particularly Lancashire and Cumbria. Combined, the two counties have over 1,000 primary schools, 114 secondary schools and 20 further education centers, the majority of which are situated in small, remote communities. Schools either can't afford the high cost of broadband access from commercial telecommunications providers, or are simply beyond the reach of these networks.

The Cumbria and Lancashire Education Online (CLEO) Regional Broadband Consortium was established in 2000 by Lancaster University and the County Councils of Lancashire and Cumbria to step up to this challenge. CLEO set out to provide a sustainable, low-cost, high-capacity broadband network that would benefit not only schools, but also other learning institutions across the region, such as universities, colleges, libraries, museums and adult education centers.

"Our first priority was to deliver a network that offered schools reliable, high-speed Internet access at a price they could afford. However, to make this project work, we had to ensure that the network would be self-funding once the government's RBC investment ended in 2006. We needed to create our own broadband infrastructure that we could operate independently of public telecoms carriers," said Professor Barry Forde, Lancaster University's Head of Technical Services in ISS (Information Systems Services) and the chief architect of the new network infrastructure.

CLEO turned to specialist network systems integrator Imtech Telecom to transform the University's network design into a scalable, best-of-breed network infrastructure. The solution included Lucent's Stinger® Access Concentrator DSLAMs (Digital Subscriber Line Access Multiplexers) for local-loop unbundling, and Juniper Networks M-series routing platforms for the hub and aggregation points, plus Juniper's ERX platforms for broadband aggregation.

High-speed education

Working with its County Council partners, Lancaster University has delivered what is currently the largest 'last-mile' regional broadband infrastructure, connecting over 1,000 education establishments.

As well as providing high-speed Internet access across the region, the CLEO network has also allowed teachers and lecturers to offer a much richer learning experience. For example, using video and audio clips as part of their classroom teaching; holding lessons via video conference to reach pupils in other schools and colleges; or streaming lectures to students in locations off campus. The innovative strategy of providing a common network infrastructure to disparate communities is also benefiting small businesses in the region, which are now able to utilize the spare capacity of the CLEO network at a competitive market rate.

This remarkable achievement was recently recognized at the Queen's Anniversary Prizes in November 2005, when CLEO was awarded the 'Prize for Connecting the Last Mile: the largest Regional Rural Broadband Network for Education in Europe'.

Securing Public Places

» From the Front Door to the Furthest Depths of the Network

In recent years there has been a heightened focus on security of public places, including airports, hotels, power plants, government buildings and the like. The larger the facility and the more access points there are, the more complex the task of keeping it secure becomes. The very nature of security ranges from the task of providing commercial-grade physical locking mechanisms, to modern biometric access technologies such as fingerprint, retinal and face recognition.

In addition to the mounting challenges associated with securing physical infrastructure and operations, there is the additional modern challenge of hardening our communications and data networks against intrusion and malicious disruptions. And as physical security relies increasingly on networks to manage electronic security and access controls, the necessity of securing these systems takes on even more importance.

To better tie together this complicated fabric of security, Lucent Technologies has joined with ASSA ABLOY Asia Pacific, a division within ASSA ABLOY, the world's leading manufacturer and supplier of locking solutions, to create a breakthrough relationship for delivering end-to-end security solutions. The two companies are applying what they do best to create and market fully integrated *physical and network security* solutions targeted at governments, large corporations, airports, hotels and universities, with an initial market focus in the Asia-Pacific region.

ASSA ABLOY works to meet tough end-user demands for safety, security and user friendliness. The Swedish-based company has some 30,000 global employees and annual sales of about EUR 3 billion.

As a part of this innovative joint-marketing approach, Lucent and ASSA ABLOY Asia Pacific will offer a complete package of security solutions and services, seamlessly linking state-of-the art electronic physical security within highly secured network environments.

The Lucent-ASSA ABLOY solution combines physical security solutions offered by ASSA ABLOY – including identification technology, automatic doors and electric door-locking systems – with the network integration and security services offered by Lucent and its Bell Labs R&D expertise. Lucent is combining its communications technology solutions, including home networking, power solutions and broadband Wi-Fi, with its security services, such as network security assessments, and intrusion detection capabilities via Lucent's Security Network Operations Centers.

The resulting combination of ASSA ABLOY and Lucent's expertise is an unrivaled, end-to-end security design and deployment solution that can protect and secure physical structures and network infrastructures alike.

Some examples of the ASSA ABLOY-Lucent Security Solution include:

- Securing a large Asian airport construction project and various renovation and upgrade projects for other airports in Asia. This includes managed security services as well as maintenance for Lucent's networking equipment and ASSA ABLOY's physical security equipment alike.
- Work with a large ocean front hotel resort complex that is seeking secure Wi-Fi deployment for both building access and guest services. The system includes an online check-in system and unified guest card, enabling customers to access their room and other hotel amenities, as well as charge goods and services. This single-card approach could also be used to provide the hotel with additional surveillance capabilities to ensure overall guest security and alert hotel management about irregular behavior.
- Home networking for a high-end apartment complex that integrates room-by-room security. This includes an outdoor environment with closed-caption television and card readers to be able to simultaneously monitor the kids at the playground and be instantly alerted when a visitor arrives in the garage.

The rule of thumb in the security industry is that facilities are only as secure as their weakest link. The combination of two security powerhouses, who understand how the many layers of security must fit together, creates a totally unique offer in the marketplace by taking best-of-breed security expertise to the next level.

Lucent's Base Station Router – A Game Changer

There is an overall market trend towards convergence – delivering blended broadband IP services to any device over any network. Today's networks, largely through the emergence of IMS (IP Multimedia Subsystem), are addressing the move to IP (Internet Protocol) at an application and services level. While 3G mobile networks are becoming more widely available, there is still a need for further innovation to deliver the vision of ubiquitous personalized services to any device on the mobile network.

Lucent Technologies' Base Station Router (BSR) delivers Bell Labs innovation to 3G networks as it realizes the potential not only to reduce complexity and save cost, but also to offer fundamental improvements in the architecture of mobile networks that will enable true personalized broadband multimedia services to be deployed over converged networks.

How the BSR Works

The BSR, an innovation that began as a Bell Labs research project, integrates key elements of 3G mobile networks into a single network element, thus "flattening" what is typically a more complex architecture. With the BSR, there are no wireless access specific controllers in the core of the network – just access-agnostic IP routers and service nodes. All the "access-technology specific" control that makes the mobile network function, happens at the access point, or edge, in the BSR. It functionally converges network elements and combines signaling and transport into a single IP connection. This means a BSR – and therefore a mobile network – can be deployed anywhere an IP connection exists, placing the BSR in deployment scenarios that are difficult or impossible for traditional network elements.

Benefits of BSR

The BSR integrates the base station, radio network controller and mobile data IP gateway (e.g. PDSN/SGSN/GGSN) functions into a single network element. In fact, some models, like the compact BSR used for disaster recovery efforts, have a small footprint. By combining several technologies into one chassis, the task of upgrading the equipment is reduced substantially.

Simplifying network elements also helps reduce backhaul costs, which is a big selling point for service providers. It also enables highly scalable and economical upgrade of 3G networks to support high-speed data services.

The BSR also addresses several current application needs in the telecommunications market:

- **Faster network deployment** – Fewer network elements means faster network deployment and set-up time. The BSR can be quickly deployed for a public safety network or used to enhance commercial mobile network coverage in buildings.

Bell Labs Innovation:

The BSR integrates key elements of third-generation (3G) mobile networks into a single network element, thus "flattening" what is typically a more complex architecture. It functionally converges network elements and combines signaling and transport into a single IP connection, which means a BSR – and therefore a mobile network – can be deployed anywhere an IP connection exists.

- **Broadband** – The increasing consumer demand for communications services, which includes not only voice service but also data and multimedia services, is fast outstripping the current supply of bandwidth. The BSR is an ideal way of increasing bandwidth, because it enables the economical deployment of micro or pico cells. Therefore, the network can be more precisely engineered to accommodate user data traffic, resulting in significantly higher data throughput to each user for each service.

- **Reducing Latency** – Collapsing network elements has a positive impact on lowering signal delay, which means quality of service improves, enabling carriers to deliver real-time services such as VoIP, video telephony and mobile gaming together with high-bandwidth content-oriented services like multicasting, IPTV, and mobile video streaming.

- **Ubiquity** – As consumers begin to expect seamless mobile communications services at any spot in the world, the business economics of licensed cellular telephony becomes an issue. Deploying large base stations in patterns sufficient to provide coverage that meets customer expectations is complicated and expensive. The BSR allows the network to go anywhere IP is available – including in tunnels, underground facilities, inside buildings, on airplanes, or in environments without wireline infrastructure but mobile IP access such as disaster areas.

- **Personalization** – The effect of deploying mini or pico cell networks based on the BSR is that the network can accurately pinpoint exactly where each user is – allowing the delivery of highly personalized context- and location-sensitive services.

- **Flexibility** – As networks evolve from delivering point-to-point services to managing multi-point session-based communications, network elements will need a new level of intelligence and flexibility to configure themselves dynamically in real time. Because of Bell Labs' advanced algorithms and IP's natural dynamic optimization capability, the BSR is an ideal platform upon which to base a flexible network.

In addition, the BSR will enable operators to fill in coverage gaps more quickly and at lower cost as well as introduce new mobile broadband and IP services and expand into new markets, all while offering the benefits of seamless access to the broader 3G network.

BSR in the Future – and Beyond

The BSR is the first product based on Lucent's plans for a new streamlined Internet Protocol (IP)-based mobile network architecture. And it's just the beginning of this kind of revolution – a building block to simplifying and streamlining the large and complex mobile network architecture. In fact, Bell Labs already has begun to apply machine learning to the edges of a flat network architecture. The approaches to future telecom networks that are currently being researched are directed towards delivering communications networks (wireless and wireline) that deploy and manage themselves, optimizing constantly to benefit both end user and operator.

Hosted Services

» Lucent Technologies Helps Sprint Deliver More Services to Enterprise Customers

Since its emergence on the telecommunications scene, Voice over Internet Protocol (VoIP) has gained popularity with end users worldwide. With benefits like cost effectiveness, flexibility, and enhanced features and capabilities, the growth and user demand for VoIP is easy to understand.

As demand for VoIP and other next-generation services and applications increases, the pressure on operators to offer such technologies also grows. To remain competitive, many global service providers and enterprises – including universities, government agencies and hospitals – are looking to evolve to a VoIP platform. However, for these organizations, the high cost of migration and maintenance may overshadow the positive aspects. To avoid these expenses, many organizations are choosing the hosted route. One service provider that recently took the hosted road is Sprint, which recently launched its IP Voice Connect service, an enterprise solution enabled by Lucent Technologies.

The lure of the hosted model is simple: companies can provide their end users with the new technologies and applications they demand, without the effort and high cost of migrating their network. In addition, the service provider and/or enterprise is not burdened by the expense and hassle of network maintenance. Plus, hosting allows the operator to get to the market much more quickly with new services, enabling them to be more competitive and innovative.

Hosted VoIP in Action

As a hypothetical employee of one of Sprint's university customers, Jane Smith reaps the benefits of IP Voice Connect. Jane uses her mobile phone much of the day to stay in touch with colleagues and co-workers. However, while she's on the go, she misses her office phone system, based on VoIP technology, which allows her to customize features to suit her needs. Now, with Sprint's IP Voice Connect service, Jane's mobile phone acts just like her office phone – providing Jane with the office phone capabilities she wants, with the flexibility of a mobile phone that she needs. And the added benefits of features like a single voicemail box and simultaneous ringing of her office and mobile phones allow her to be more productive than ever while away from her desk.

For Sprint's enterprise customers, like Jane's university, IP Voice Connect means high-speed data, local, long-distance and mobile voice services in one bundle over an Internet Protocol (IP) network. This is a more efficient, effective and inexpensive alternative for businesses that have in the past used up to four different operators – and paid four different bills – for these separate services.

More importantly, enterprise users like Jane can now remain productive in or outside the office thanks to features like one voicemail system for desktop and wireless phones, simultaneous ringing to multiple phones and unified messaging, which is the technology that allowed Jane to check her various messages through one device. In the long run, these help improve productivity and customer satisfaction – and even deliver increased revenue – for their organizations.

Behind Sprint's new service is Lucent's Hosted VoIP Solution for Enterprises and its Global Network Operations Centers (GNOCs). By leveraging the capabilities of the GNOCs – which operate, manage, monitor and analyze all aspects of the IP Voice Connect service – Lucent is able to provide Sprint with a very innovative and competitive solution. As a result, Sprint can offer their enterprise customers more features and the simplicity of one bundled package of services, rather than four.

A Market on the Rise – Hosted Services

It seems in coming years, more and more organizations will follow in Sprint's footsteps, and take advantage of the hosted services model. In fact, Infonetics, a leading market research firm, forecasts that the U.S. Hosted Business VoIP market will grow to an $8.1 billion opportunity by 2009.

What's driving this growth? In a recent report, IDC analyst William Stofega offered an answer. "As carriers look to reduce cost and quickly deploy new revenue-generating services, deploying a hosted service has become an increasingly attractive option when considering time to market and risk reduction," Stofega said.

For these organizations, like Sprint, Lucent's hosted environment offers the opportunity to easily add these revenue-generating applications – which GNOC experts can simply install and host through the existing platform that operates IP Voice Connect – to further differentiate Sprint from its competition. That means Lucent's hosted applications, including Hosted IP PBX with Mobile Extensions and Hosted Messaging solutions, can be quickly deployed to IP Voice Connect customers with little additional capital investment from the customer or Sprint. These applications can then be leveraged to offer enterprise end users features like mobile four-digit dialing, speech dialing, speech messaging, Web messaging, location-based services and ring-back tone service.

While the IP Voice Connect solution was nearing its March 3 launch date, Lucent's GNOC experts handled the operational and technical details, enabling Sprint to concentrate on launching, marketing and selling the service. With the service now operational, Sprint can address the challenges facing enterprises today, like dispersed workforces and multiple forms of access, without being concerned with service maintenance.

Thanks to IP Voice Connect, Sprint's enterprise customers reap the benefits of VoIP, like reduced long-distance expenses, simplified network management and more productive employees, who can work effectively anytime, anywhere. And thanks to Lucent's hosted service, Sprint can focus on what's really important to them – satisfying their customers.

Lucent's Hosted Services and Applications

Lucent's Hosted Solution Suite includes the Hosted IP PBX service, Hosted Messaging and Hosted MiLife™ mobile application service. These offerings are hosted from one of Lucent's four GNOCs and leverage the carrier's existing network. The offerings' key capabilities include:

Hosted IP PBX: A completely outsourced network-based IP PBX that delivers advanced IP PBX functionality supporting SIP-based calls and connections. This includes extending standard office PBX features, such as four-digit dialing, to mobile phone users.

Hosted Messaging: Provides advanced services such as web messaging, fax receipt, and text-to-speech reading of e-mail messages. The Hosted Messaging solution, which leverages Lucent's AnyPath® Messaging System, also includes an array of advanced voicemail and unified messaging capabilities.

Hosted MiLife™: Lucent's Hosted MiLife™ Solutions include a wide range of outsourced applications, such as iLocator for location-based services, SurePay® for pre- and post-paid charging, and MiRingBack for ring-back tone service. Lucent also can support a variety of additional hosted solutions based on the MiLife suite – a comprehensive set of service delivery platforms and software-based, plug-and-play applications – targeted to the Mobile Virtual Network Operator (MVNO), enterprise, and consumer markets.

VISA Relies on Lucent

» Protecting Personal Information Millions of Times – Every Second of Every Day

The public sector is increasingly deluged with security threats. However, a major growing concern for both businesses and consumers is attacks that focus on the access and misuse of personal information. Companies need to take the right steps today to protect the information of their customers. This process isn't as simple as installing a one-time security 'quick fix', it must include ongoing and constant vigilance every day, each week and year after year.

Identity theft and the theft of personal information is a growing threat for consumers around the world. Credit card fraud poses a real problem for the Payment Card Industry. The losses are estimated to be close to $1bn a year and this without even taking into account the loss of reputation to both the credit card companies and the businesses. Reports from the Financial Services Authority (FSA UK) state that e-commerce growth is seriously affected by the perception of risk by consumers.

This is equally as scary for the Internet community as it is for traditional bricks-and-mortar, telephone and mail-order businesses. It goes almost without saying that credit card companies, such as Visa, are putting in place new protections and more stringent requirements for their merchants to help to insure consumer safety and confidence.

Getting Serious about Data Protection

In June of 2001, Visa launched a security program called the Cardholder Information Security Program (CISP). The program aims to protect Visa cardholder data –wherever it resides–, ensuring that members, merchants, and service providers maintain the highest information security standards.

This program was taken one step further in December 2004, when Visa and MasterCard announced a worldwide standard for consumer data protection, called the Payment Card Industry Data Security Standard (DSS). The PCI DSS has since been adopted by other card brands under their respective programs while Visa U.S.A. maintained CISP as their program's name.

For instance, Visa merchants and service providers need to ensure PCI compliance and validation in accordance with CISP. This is taken extremely seriously by Visa, which has imposed severe penalties for non-compliance including prohibition of network participation and hefty fines of up to $500,000 per incident.

As a matter of principle, these rules apply to any kind of merchant accepting credit card payments, from a local supermarket to the driver and vehicle licensing authorities to an Internet Service Provider. Merchants that conduct more than 6,000,000 transactions a year or have suffered a breach that resulted in account data compromise must have yearly on-site security assessments conducted by a qualified third-party security assessor, also called a Qualified Data Security Company (QDSC). The same is required of all service providers that are directly connected to VisaNet and payment gateways and those that store, process, or transmit over 1,000,000 transactions a year. Merchants and service providers falling outside of these criteria are required to submit a self-assessment questionnaire for validation.

Even the self-assessment can be a tricky proposition, with many companies preferring to get advice from an outside consultant in order to ensure proper compliance.

Assuring Compliance by Using a Trusted Security Advisor

Lucent Technologies has recently been accepted by Visa as a QDSC in the United States and is hoping to become a QDSC in Asia, Latin America and Europe. For companies, QDSCs can offer two kinds of services. These are:

- Third-party, independent compliance assessment against the PCI Data Security Standard that includes a report presented to Visa.
- Independently advise on complying with the PCI requirements; pre-audit report and recommendations for smaller and mid-sized companies that choose to conduct their audits on their own.

With its extensive security knowledge as well as global breadth and depth, Lucent has joined an elite group of skilled companies that are providing this service.

Bottom Line: No One Can Afford A Breach

Security breaches, especially those involving personal data theft, are costly to both credit card companies, merchants and consumers. As our culture rapidly moves towards a cashless society, the importance of security becomes paramount. Consumers must feel absolutely certain that they can freely use credit cards anyplace and for anything they wish to purchase. If that trust is put in jeopardy there could be a backlash against electronic payment in general. By putting stringent security measures in place, merchants and service providers are actively controlling their destiny and creating a security process that any enterprise can model.

John Giere
Chief Marketing Officer
Lucent Technologies

Dear Customers,

When Hurricane Katrina battered the U.S. Gulf Coast last year, it left behind an extensively damaged telecommunications network that severely hindered the efforts of police, fire and rescue personnel. As a result, satellite phone traffic spiked to a reported 3,000 percent of usual levels. Similarly, in the wake of the Asian tsunami in December of 2004, weakened cell phone signals and unreliable land lines led to Short Message Service (SMS) becoming one of the most valuable communications tools of the tragedy's recovery efforts.

Natural disasters provide just one example of the importance of ubiquitous and secure communications. From health care to education to the fight against terrorism, communications plays a critical role in a government's ability to ensure the health and safety of its residents.

Just as in any business, we understand that governments struggle with the need to reduce costs while also ensuring the continuity of government services and improved effectiveness. Our IMS (IP Multimedia Subsystem) solution, supported by Bell Labs' unique Service Enhancement Layer, reduces network cost and complexity while increasing service flexibility. The result: improved network management and reliability, increased return on investment, and the ability to roll out advanced new voice, video and data services – including Voice over IP (VoIP) – over a single platform. Ultimately, IMS can revolutionize the effectiveness of communications during times of urgent need.

Government agencies around the world are recognizing the value of VoIP, and similar IP telephony tools, in economically connecting thousands of users, call centers and critical resources.

At Lucent, we understand that government business must function seamlessly 24 hours a day, 365 days a year. And we know that network failure and security breaches are simply never an option. With the benefits of communications survivability, advanced connectivity services and network reliability, we believe that it is no longer a matter of *if* IMS will catch on in the government space, but rather a matter of *how soon*.

For more information on IMS and Lucent's convergence solutions, contact your local customer representative or visit www.lucent.com/gov/next_gen_nets.html

We hope you enjoyed this edition of LUX. As always, your feedback on our format, suggestions for future topics and opinions about our individual stories are more than welcomed.

Warm regards,

John Giere
Chief Marketing Officer

IMPRINT

Published by:
Lucent Technologies
600 Mountain Ave.
Murray Hill, NJ 07974
USA

Editor-in-Chief:
Dirk Kolassa, e-mail: kolassa@lucent.com

Published on a quarterly basis

Edition: 3Q FY 2006

www.lucent.com/lux

LUX FEEDBACK FORM

I would like to receive LUX regularly in future.

First Name

Last Name

Company

Address

City

State/Province

ZIP/Postal Code

Country

E-Mail

Tel.

Please indicate your preferences:

◯ I would like to receive LUX electronically.

◯ I would like to receive LUX in print.

◯ I would like to cancel my LUX subscription.

I would like to have a Lucent representative contact me.

Topic

Tel.

» Please fax your feedback to:
+49 228 243 1198
or fill out the form at
www.lucent.com/lux

NAR

Lucent Technologies
Corporate Headquarters
600 Mountain Ave.
Murray Hill, NJ 07974
USA
Tel. +1 908 582 8500
www.lucent.com

Lucent Technologies
1380 Rodick Road
Markham, Ontario L3R 4G5
Canada
Tel. +1 905 943 5000
www.lucent.ca

EMEA

Lucent Technologies NS UK Ltd.
Nations House
103 Wigmore Street
London W1U 1QS
United Kingdom
Tel. +44 207 318 1030
www.lucent.co.uk

Lucent Technologies Belgium
Alfons Gossetlaan 54
1702 Groot-Bijgaarden
Belgium
Tel. +32 2 467 89 10
www.lucent.be

Lucent Technologies España, S.A.
Avenida De Bruselas, 8
28108 Alcobendas (Madrid)
Spain
Tel. +34 91 7148400
www.lucent.es

Lucent Technologies
Network Systems GmbH
Brühler Straße 9
53119 Bonn
Germany
Tel. +49 228 2430
www.lucent.de

Lucent Technologies
France S.A.
16 Avenue Descartes
Le Plessis Robinson
Cedex 92352
France
Tel. +33 141 28 7000
www.lucent.fr

Lucent Technologies Italy
Via Tucidide 56 Torre 1
20134 Milan
Italy
Tel. +39 02 75290.1
www.lucent.it

Lucent Technologies
Nederland B.V.
Larenseweg 50
Postbus 1168
1200 BD Hilversum
The Netherlands
Tel. +31 35 687 3111
www.lucent.nl

Lucent Technologies
Poland Sp. z o.o. - Sp. jawna
Ul. Senatorska 27
Warsaw
Poland
Tel. +48 22 692 3600
www.lucent.com.pl

Lucent Technologies
Abu Dhabi, UAE
P. O. Box 44770
CERT Technology Park
Muroor Road
United Arab Emirates (UAE)
Tel. +971 2 407 9400
www.lucent.com.sa

Lucent Technologies Egypt
124 Othman bin Affan Street
Heliopolis
Egypt
Tel. +20 2 648 0400
www.lucent.com.sa

Lucent Technologies Saudi Arabia
Building 35
King Abdulaziz Complex for Telecom
Mursalat, Riyadh, Saudi Arabia
P. O. Box 4945, Riyadh 11412
Saudi Arabia
Tel. +966 1 263 8300
www.lucent.com.sa

CALA

Lucent Technologies
Rua Thomas Nilsen Jr. 150
Parque Imperador
Campinas, SP - CEP 13097-105
Brazil
Tel. + 55 19 3707 7000
www.lucent.com.br

Lucent Technologies
América Latina y el Caribe
2400 SW 145 Ave.
Miramar, FL 33027
USA
Tel. +1 954 885 3100
www.lucent.com

APAC

Lucent Technologies
29/F, Shell Tower
Times Square
1 Matheson Street
Causeway Bay
Hong Kong
Tel. +852 2506 8000

Lucent Technologies Taiwan
Telecommunications Co., Ltd.
13F., No.8, Hsin-yi Road, Section 5
Taipei, 110
Taiwan
Tel. +886 2 8789 8388

Lucent Centre
68-72 Waterloo Road
North Ryde, Sydney NSW, 2113
Australia
Tel. +61 2 9491 6500

Lucent Technologies (S) Pte Ltd
750D Chai Chee Road
#06-06 Lobby 2
Technopark @ Chai Chee
Singapore, 469004
Tel. +65 6240 8000

Lucent Technologies Hindustan Pvt. Ltd
Prime Corporate Park, 4th Floor,
Sahar Road, Andheri (East),
Mumbai - 400099
India
Tel. +91 22 56798700

Lucent Technologies
No.25 Mori Building 1-4-30
Roppongi, Minato-Ku
Tokyo, 106-8508
Japan
Tel. +81 3 5561 3600
www.lucent.com/jp/

Lucent Technologies World Services Inc.
Block B, Unit 1, Hassanin Complex,
Simpang 42, Jln Maura,
Kpg Pancha Delima BB4513
Brunei Darussalam
Tel. +673 2 342 300

Lucent Technologies Korea
4,6-7 fl. Shinyoung Bldg. #68-5,
Chungdam 1-Dong, Kangnam-Ku
Seoul 135-953
South Korea
Tel. +82 2 767 4000
www.lucent.com/kr

朗讯科技（中国）有限公司
北京东城区东长安街1号
东方广场东方经贸城
东二办公楼21层
邮政编码: 100738
中国北京
电话: +86-10-65288688
网址: www.lucent.com.cn

Lucent Technologies Philippines
19-20/F The Enterprise Center
6766 Ayala Avenue
Makati City, 1226
Philippines
Tel. +63 2 884 8888

Lucent Technologies Thailand
5th Floor, Abdulrahim Place
990 Rama IV Rd, Silom, Bangrak
Bangkok, 10500
Thailand
Tel. +66 2 638 5000

Lucent Technologies Malaysia
Level 58, Tower 2
Petronas Twin Towers
Kuala Lumpur City Centre
50088 Kuala Lumpur
Malaysia
Tel. +603 2168 6600

Lucent Technologies Vietnam Co., Ltd
Unit 6, Level 15, Tower B
Vincom City Tower
191 Ba Trieu Street
Le Dai Hanh Commune
Hai Ba Trung District
Hanoi
Vietnam
Tel. +84 4222 5368