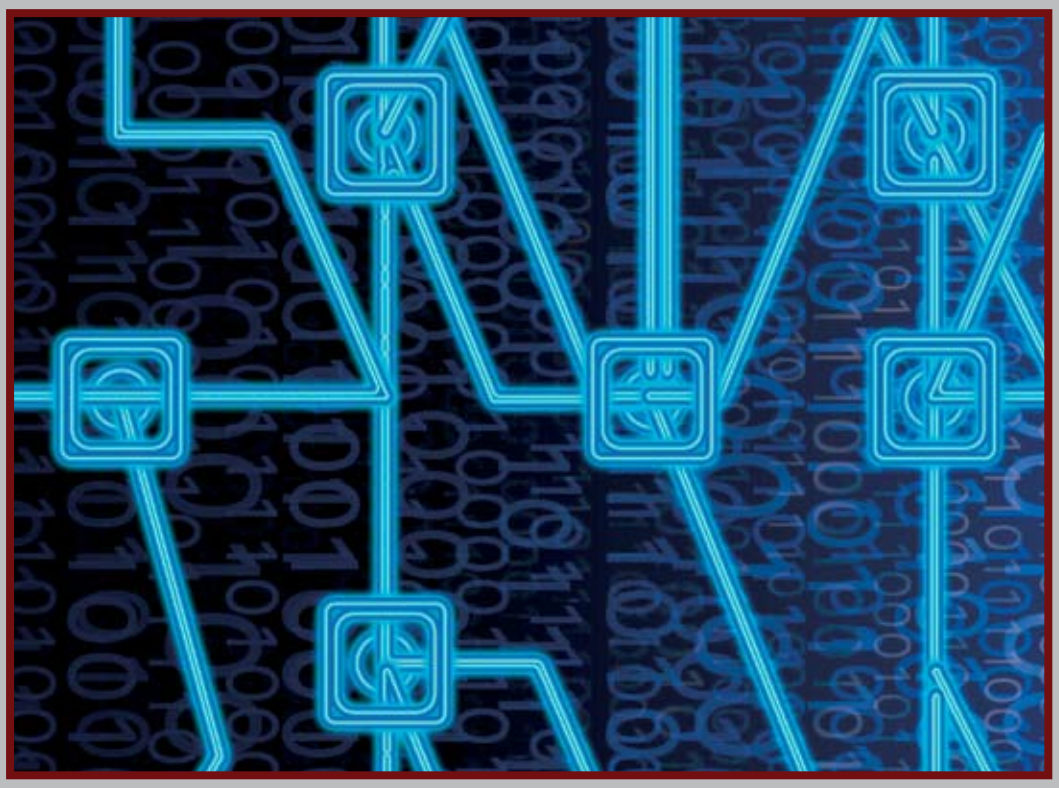
Homeland Defense
JOURNAL

IT SECURITY

SPECIAL REPORT

New IP Telephony Solutions for the Government Enterprise

The Opportunities and Challenges of Migrating to VoIP



By Marc Robins

Table of Contents

VoIP and IP Telephony Defined 2
Primary Advantages 2
Cost Savings 2
Management and Administration Efficiencies 3
A Wealth of Options — The Different Flavors of VoIP 3
New Communications Systems 3
New End-Point Devices 3
New Hosted VoIP Services 6
Nine Steps to Ensuring a Secure Migration to VoIP 4
The Challenges of Migrating to VoIP 6
Network Assurance and Quality of Service 6
Achieving Optimal Security 7
Interoperability Concerns 9
Higher Than Expected Startup Costs 9
Providing 911 Emergency Services (E911) 10
Ensuring Priority Services 10
The Importance of Testing to Ensure Optimal IP Telephony Quality of Service 8
Powerful IP Telephony Applications: A New Prescription for Increased Productivity and Efficiency 10
Remote Office/Telecommuting Solutions 11
Web and Speech-Enabled Unified Communications 11
Presence-Powered Collaboration 11
Voice and Video Conferencing 12
Wi-Fi Telephony 12
IP Contact Center Solutions 12
Looking Ahead 13
About the Author 13
Customer Case Study 15
Product Profiles 20
Vendor Listing 21

A revolution is under way in communications technology today, and the upside for government enterprises is worth celebrating. A full-scale migration from circuit-switched networks, systems and services to those based on packet-based Internet Protocol, or IP, communications is in full swing. According to Gary Amato, chief of the Technology and Programs Division, National Communications System in the Department of Homeland Security (DHS), "IP is overtaking the circuit world and turning it upside down. We're in the midst of radical change; the mountain that represents IP is no longer far off in the hazy distance but rather, we're standing right on it now. Everything has an IP flavor to it these days, and it's impossible to ignore." Rick Kuhn, a computer scientist at the National Institute of Standards and Technology (NIST), agrees, "We think there's strong movement toward VoIP, with a great deal of government agency interest."

Indeed, the convergence of voice, video and data occurring on communications networks today — and the IP-enabling of communications and computing equipment designed to connect to these networks — is creating a host of new opportunities and challenges for government enterprises and agencies of all sizes and types looking for more choice, more value and powerful new communications capabilities and applications.

VoIP and IP Telephony Defined

Voice over IP (VoIP) is a set of software, hardware and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network or across the Internet. IP telephony, broadly described, is a collection of new communications technologies, products and services that encompasses the convergence of voice, video and data on these IP-based communications networks. VoIP is generally considered a subset of IP telephony.

The technology behind it all has been steadily evolving over about a decade. In VoIP's early days, PC-to-PC Internet calling software let people talk over the Internet through their dial-up connections. Over time, sophisticated systems called gateways were developed that, in essence, serve as bridges between the traditional public switched telephone network (PSTN) and the Internet (or some other IP network), allowing communications to cross over from one to the other.

VoIP technology has been adopted by practically all of the major telecom carriers and service providers in their network cores. Most major service providers, including AT&T and Sprint, have been offering VoIP as an option with their respective virtual private network (VPN) services for several years, providing service-level guarantees for voice quality. VoIP technology has also spawned a whole new breed of service provider called an ITSP, or Internet Telephony Service Provider, such as upstart broadband-based Vonage, whose business models leverage the global Internet to offer cut-rate long distance service. VoIP is also the enabling technology behind the cable companies' aggressive plans to turn themselves into phone companies.

Primary Advantages

The rationale behind this growing migration from circuit-switched communications technology to IP telephony is based on a number of factors, most importantly cost savings, management and administration benefits, and the availability of new features and applications that promise to boost staff efficiency and productivity. (For a review of some of these leading new applications see the "Powerful IP Telephony Applications" section.)

– Cost Savings

One of VoIP's primary drivers, plain and simple, is that it saves money. Service providers employ it to reap dramatic improvement in network capacity — meaning they can carry more calls over the same "pipes." And by using VoIP technology on site, government enterprises can enjoy a converged network architecture that serves as a single network for the transmission of voice, data and video — eliminating the need for multiple networks, terminations and devices. "Just like in the public enterprise space, the technology is very cost-effective in terms of infrastructure," says Sandra Wheeler, director of End-User Secure Products, General Dynamics C4 Systems. "Many government enterprises currently have two separate networks — a voice network and data network. VoIP brings them together to become a single infrastructure that provides services."

In addition, by sending voice as data over existing WANs and VPNs that connect branch offices and other

remote locations to a central headquarters, agencies get to bypass the public telephone network to dramatically cut phone costs between these locations. Savings of 70 percent to 90 percent for international calls are not uncommon, while agencies can enjoy a 20 to 30 percent reduction in costs for domestic long distance. However, there is a limit to the cost savings derived from a bypass strategy.

– Management and Administration Efficiencies

VoIP solutions also deliver a number of advantages associated with the management and administration of equipment and services. Browser-based administration portals allow managers and administrators to gain a unified view of the network as well as manage individual users, setting profiles, classes of service and enabling/disabling various features through a point-and-click graphical user interface.

More importantly, moves, adds and changes (MACs) on a system — usually the bane of telecom managers because they need to physically change cabinet wiring and go through a number of tedious programming changes with legacy, circuit-switched systems — is greatly simplified with VoIP. Because new VoIP phones and other end-point devices can be automatically authenticated and registered by the network, moving a phone "extension" from one location to another is simply a matter of plugging the phone into a different network jack.

A Wealth of Options — The Different Flavors of VoIP

New VoIP systems consist of an array of new technology, including traditional telephone handsets, conferencing units, mobile units and software-based phones (softphones). In addition to end-user equipment, VoIP systems also include a variety of other components, including call processors/call managers, gateways, routers, firewalls and a variety of special protocols. In this section, we'll review some of this technology.

– New Communications Systems

At the same time service providers were taking the first steps to migrate their circuit-switched network infrastructure to IP, the leading telephone systems vendors, including Avaya, Siemens, Mitel Networks and Nortel Networks, recognized that their futures were also tied to the adoption of IP-based communications technology. Even datacom giant Cisco Systems saw the IP telephony opportunity, and today it is the leading supplier of "pure" IP-based phone systems geared for new "greenfield" installations and for customers looking to completely replace their existing legacy equipment.

After several years of continuous evolution and improvement, these vendors now have on hand new families of customer premises equipment (CPE) phone systems called IP-PBXs that are based completely on an IP-centric architecture. They can also support the more than 500 features common to most traditional systems (hold, transfer, conferencing, page, etc.) and deliver dramatic benefits to government enterprises that embrace the technology for their communications infrastructure.

By all accounts, the IP-PBX represents the next generation of CPE-based communications system technology, and will eventually displace all of the traditional PBXs in use. According to research house Instat/MDR, 2004 was the year when IP phone shipments first exceeded that of traditional PBX phone sets.

– New End-Point Devices

The most important thing, to most government users of communications systems, is the phone on their desk. The phone is, after all, the device that allows the user to access system features and applications and communicate with agency personnel, as well as the public at large.

Today's new IP-PBXs offer users a choice of new and ingenious communications devices that leverage the full suite of applications, communications mediums and features available on these systems. Top on the list are new IP phones designed to connect to converged communications networks — usually by the use of an Ethernet cable. These phones come in a variety of different models ranging from no-frills units that perform basic functions to Web-browser enabled models that feature large, color touch screens, speakerphones and a second Ethernet jack that can be used for plugging in a laptop or other network device. Other features include power over Ethernet capabilities, an infrared port for PDA and PC application integration and a multitude of buttons to access features and functions.

Nine Steps to Ensuring a Secure Migration to VoIP

The Computer Security Division of the Information Technology Laboratory at the National Institute of Standards and Technology has published an excellent report on VoIP-related security issues entitled "Special Publication 800-58: Security Considerations for Voice Over IP Systems." This report, authored by D. Richard Kuhn, Thomas J. Walsh and Steffen Friesand, is available at http://csrc.nist.gov/publications/nistpubs/index.html.

Because of the growing trend of the integration of voice and data in a single, converged network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. This report includes a number of extremely valuable recommendations and guidelines that government managers should consider carefully before installing and deploying new VoIP equipment. Some of these guidelines are included below (please note they have been edited for space considerations, and that interested readers should refer to the publication for the full recommendations.)

1. **Develop the appropriate network architecture.** Recommendations include the separation of voice and data on logically different networks if feasible; disallow SIP, H.323 and other VoIP protocols at the voice gateway from the data network; use strong authentication and access control on the voice gateway system, as with any other critical network component; deploy a mechanism to allow VoIP traffic through firewalls, which can include application level gateways (ALGs) for VoIP protocols and Session Border Controllers; employ IPsec or Secure Shell (SSH) for all remote management and auditing access, and if practical, avoid using remote management at all and have IP-PBX access from a physically secure system; and if performance is a problem, use encryption at the router or other gateway, not the individual IP phones or appliances, to provide for IPsec tunneling.

2. **Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations and continuity of essential operations when deploying VoIP systems.** An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology and security controls and policies must be updated. Therefore, agencies should carefully consider such issues as their level of knowledge and training in the technology; the maturity and quality of their security practices, controls, policies and architectures; and their understanding of the associated security risks.

3. **Special consideration should be given to E911 emergency services communications, because E911 automatic location service is not available with VoIP in some cases.** Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the trade-off is that this flexibility severely complicates the provision of E911 service, which normally provides the caller's location to the 911-dispatch office. Although most VoIP vendors have workable solutions for E911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E911 issues in planning for VoIP deployment.

4. **Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.** Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis. Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical securities measures, including barriers, locks, access control systems and guards, are the

first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks, such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking, this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. **Evaluate costs for additional power backup systems that may be required to ensure continued operation during power outages.** A careful assessment must be conducted to ensure that sufficient backup power is available for the office VoIP switch, as well as each desktop instrument. Costs may include electrical power to maintain UPS battery charge, periodic maintenance costs for backup power generation systems and cost of UPS battery replacement. If emergency/backup power is required for more than a few hours, electrical generators will be required. Costs for these include fuel, fuel storage facilities and cost of fuel disposal at end of storage life.

6. **VoIP-ready firewalls and other appropriate protection mechanisms should be employed.** Agencies must enable, use and routinely test the security features that are included in VoIP systems. Because of the inherent vulnerabilities when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. Additional measures, in particular firewalls designed for VoIP protocols, are an essential component of a secure VoIP system.

7. **Softphone systems, which implement VoIP using an ordinary PC with a headset and special softphone software, should not be used where security or privacy are a concern.** Worms, viruses and other malicious software are extraordinarily common on PCs connected to the Internet and very difficult to defend against. Well-known vulnerabilities in Web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised Web site. Malicious software attached to e-mail messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of softphones for most applications.

8. **If mobile, wireless units are to be integrated with the VoIP system, use products implementing Wi-Fi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).** The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WPA, a snapshot of the ongoing 802.11i standard, offers significant improvements in security and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access or other active probing attacks.

9. **Carefully review statutory requirements regarding privacy and record retention with competent legal advisers.** You should be aware that laws and rulings governing interception or monitoring of VoIP lines and retention of call records may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisers.

Because security is generally recognized to be the primary concern of government implementers of VoIP systems (see "The Challenges of Migrating to VoIP" section), General Dynamics has developed their new Sectéra VoIP phone, which provides the latest technology for securing Voice over IP networks. "With voice and data markets coming together, we see the need for the ability to provide a secure voice over IP product with a commercial look and feel, and a 'clear' mode for commercial use," says Wheeler of General Dynamics C4 Systems. "In this way, the Sectéra can be used both for non-classified and classified communications scenarios."

The Sectéra uses SCIP/FNBDT signaling and commercial open standards and is planned for certification to protect information classified Top Secret and

below, including Sensitive But Unclassified (SBU). The Sectéra phone is available with multiple key sets to support U.S. government-sponsored interoperability (e.g., NATO and coalition), is built to provide seamless communications with legacy phones and encryption systems and is software programmable with extensive memory to easily accommodate future upgrades and functionality.

Another new type of communications tool offered by most of the IP-PBX vendors is software programs, called softphones, which are designed to run on standard PCs, laptops and even hand-held computers like a Pocket PC. Softphones emulate the features and functions of an IP phone and present a graphical user interface to system features and functions, providing "point and click" functionality, such as autodialing numbers from Microsoft Outlook contact lists or personnel directories, and add great value in terms of making esoteric communications features more intuitive.

For government employees who are required to work remotely — in the field or while at home — they can be virtually connected to agencies' communications systems, providing access to the full suite of system features and functions, whenever and wherever they need them.

There are however, a host of security issues related to the use of softphones that in many cases can curtail their use in Top Secret and SBU situations (see "The Challenges of Migrating to VoIP" section).

– New Hosted VoIP Services

Hosted, or outsourced, VoIP services, also referred to as hosted IP-PBX and IP Centrex, enable a government institution to subscribe to next-generation communications services rather than requiring the purchase of costly new equipment, thus saving on capital expenditures and ongoing maintenance and operations.

Beyond offering lower costs, hosted services also provide customers with new communications functions and features, and because the service provider is tasked with keeping up with technology upgrades, a bit of insurance is offered from the risk of CPE equipment becoming obsolete. This fact is not insignificant, as VoIP technology is fast evolving and has not fully matured in many respects.

In addition, many service providers offering hosted services are providing them over an existing managed network infrastructure, providing a fairly high degree of quality of service and security. For non-sensitive communications, such as certain types of contact with the public, this type of VoIP implementation might be preferable to deploying an in-house system.

The Challenges of Migrating to VoIP

As the speed of VoIP implementation increases, there are a number of new issues that are vital for government managers to review prior to deployment in their agencies and institutions. New challenges exist in determining how to implement the technology properly, including how to provide for optimal performance and essential security measures.

– Network Assurance and Quality of Service

VoIP communications between two or more individuals is performed in real-time on the network, meaning that the demands that this type of communication places on network performance is far and above what is required for general data tasks, such as e-mail and file transfers. Slight delays, or latency, in the transmission of packet data from one end of the network to the other, while hardly noticeable with e-mail or file downloads, can introduce unacceptable quality issues with voice communication and in some cases render effective communication impossible. And if video communication is required on the same network, this will add additional Quality of Service (QoS) requirements. Other QoS impairments can result from packet loss, jitter (variable latency levels over time) and echo.

"We're going to be spending a lot of time getting decent QoS with VoIP, because the circuit side has such good reliability and availability," says Gary Amato. "So just to get back to square one, we're doing a lot of work." Indeed, QoS is fundamental to the operation of a VoIP network that meets users' expectations. A number of considerations must be made in testing and evaluating network infrastructure and performance before the implementation of VoIP equipment is done, such as ensuring the network has adequate bandwidth and minimal latency and packet loss (see "Testing to Ensure Quality of Service" sidebar for more on QoS issues regarding VoIP deployment).

Furthermore, the implementation of various security measures can themselves cause a marked deterioration

in QoS. Data security is based on the deployment of a number of security devices and applications to protect and observe networks such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), VPNs, authentication services, anti-virus software and gateways. Paradoxically, because VoIP is highly sensitive to delay, packet loss and jitter, many of these data security measures are inadequate and must be specialized for VoIP. For example, current firewall/NAT devices can delay or block call setups, encryption engines can introduce additional jitter and in-line IDS/IPS devices can add delay to inspected packets.

– Achieving Optimal Security

Not surprisingly, security is usually the primary concern that government managers voice when it comes to the deployment of VoIP and IP telephony solutions. As mentioned above, the opportunities that VoIP introduces to a government enterprise come at a price in terms of added complexity in securing voice and data. "Because VoIP systems are connected to the data network and share many of the same hardware and software components, there are more ways to attack a VoIP system then there are with a TDM-based system," says Rick Kuhn, computer scientist at NIST. "Encryption is easier to accomplish, although it adds more overhead to the VoIP communication, impacting performance and call quality."

In short, VoIP equipment has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. VoIP infrastructures include a wide range of components and applications that allow for new forms and types of security attacks. According to Amato, "IP creates new vulnerabilities and new threats, in part because it provides easy access and it's everywhere." Administrators may mistakenly assume that because digitized voice travels in packets, they can simply plug VoIP-related components into their already-secured networks and remain secure. Another challenge of using data security devices for VoIP security is that there is a lack of coordination between security devices making it ineffective in protecting VoIP services from sophisticated, system-level attacks and internal threats.

Indeed, there are a number of potential threats to be aware of, including eavesdropping and malicious replay, and a number of new threats such as toll fraud, service theft, voice spam (SPIT) and identity theft. According to Bahaa Moukadam, vice president of IP Telephony Performance Analysis at Spirent Communications, based in Calabasas, Calif., "Security with VoIP has multiple dimensions. Beyond eavesdropping and hacker scenarios are situations where during a conference call people can insert themselves in the middle of a conference session and pretend to be one of the people in the discussion. This can happen even in one-to-one conversations. In addition, some people in a caller ID environment can take over a different number and pretend to be somebody else calling in — something that can happen quite a bit in cellular communications. Other tricks include rerouting of calls to prevent them from being completed."

Other security issues involve the use of certain types of VoIP hardware and software products. Softphone use, for example, can pose a major security risk. According to Kuhn, "A major concern with security is softphones running on standard PCs and laptops. Since the PCs might be shared for Web browsing and e-mail, there are lot of vulnerabilities as a result. In addition, this greatly increases the risk to the communications network if you're operating a PC for other things besides voice communications, which is usually the case."

New technologies such as VoIP over Wi-Fi, Wi-Max and IMS create another area of security concerns. Presently, VoIP wireless networks do not provide strong encryption and authentication, and they are much more accessible to potential attackers. While wireline networks require physical access to the wires, wireless technology allows remote attackers to tap into the VoIP networks without any physical access to the network.

Current PSTN voice services provide high voice quality and very high reliability (99.999 percent), while carrying critical services such as E911, providing federal agencies with the ability for lawful intercept and ensuring a very high level of security. Clearly, all of these issues have to be addressed before VoIP services are deployed on a massive scale for government use, but security is surely the most critical area that has the potential of delaying and disrupting VoIP deployment.

With the accelerating deployment of VoIP or IP telephony comes the increasing need to find ways to effectively secure VoIP as well as the PSTN. (Refer to the sidebar "Nine Steps for Ensuring a Secure Migration to VoIP" for specific NIST VoIP security-related recom-

The Importance of Testing to Ensure Optimal IP Telephony Quality of Service

As the spread of IP telephony and converged networks into the government enterprise opens the door to dramatic networking efficiencies and costs savings, as well as an array of new enhanced applications and services, the growth of converged networks is also bringing with it a unique set of challenges. According to Bahaa Moukadam, vice president, IP Telephony Performance Analysis, Spirent Communications, "For government agencies — and especially those that interface externally with the public — it's critical as they transition over to VoIP to make sure that all the public-facing services work effectively. They need to make sure they have all the features and capabilities to make the experience as good or better than what was previously available."

Indeed, new converged networks will need to serve double duty when they begin to support real-time voice (and possibly triple duty with new video applications), whether an agency is converting to a pure IP solution or making due with a mix of legacy phone equipment and an IP telephony gateway. The new demands placed on these networks can quickly overwhelm them if proper planning and testing isn't conducted prior to deployment.

If personnel tasked with network management fail to ensure that the network and equipment are up to the new tasks at hand, more and more deployments will start running the risk of experiencing an array of quality of service (QoS) issues. These QoS issues can result in an unacceptable degradation of voice and video traffic quality, including packet loss, excessive latency levels, jitter, clipping and excessive levels of echo. Indeed, an untested IP telephony deployment is simply asking for trouble, as these QoS issues can seriously affect the quality of communications at minimum and lead to complete network failure in the worst case scenario.

According to Moukadam, testing shouldn't only be used to determine the quality of service of the network infrastructure. "Testing the Quality of Experience, or QoE, is also very important. What this means is that it's necessary but not sufficient to just test the infrastructure of a network — it's also important to differentiate between QoS and the actual voice quality. Testing has to be taken to the next level, and voice quality must be tested by sending actual audio files across the network, with specific measurements taken to see how they come out on the other end. The bottom line is that there really isn't a linear correlation between QoS and voice quality in general. An average of 1 percent of packet loss spread out over a call's duration might mean that you won't notice any degradation in quality, but if that 1 percent is all concentrated in 3 seconds out of 10 minutes of a call's duration, you'd be pretty irritated!"

Essential Pre-Deployment Considerations

In order to get the most out the new IP telephony equipment on the market and to avoid the risk of communications disruption and network failure, there are a number of essential considerations one must make before choosing and deploying a new IP telephony solution.

1. **Get a Good Handle on Network Performance.** What is the network currently capable of? What loads and traffic types can be placed on it before performance is impacted?
2. **Understand the Level of Interoperability.** Are data and voice equipment interoperable with each other, as well as any legacy equipment kept in the mix?
3. **Determine the Impact of Security Equipment.** Firewalls and other network security equipment, while essential, can seriously affect the quality of voice and video traffic by introducing additional jitter and latency, and in some cases make effective communications impossible.
4. **Determine the Impact of Software Upgrades and New Hardware.** When making changes within the network, what is the impact these changes will have on network performance?
5. **Assess Real-World Performance vs. Vendor Representations.** Many vendors make claims such as "guaranteed interoperability" with Product Type A or guarantees regarding load capacity or scalability. But what happens when products are deployed in the real world?
6. **Right Size the Equipment Investment.** What is the amount of equipment and the scalability you will require? Having a certain amount of foresight

is a requirement as you begin the process of migration.

Testing Solutions From Spirent Communications

Comprehensive lab testing, or at the very least pre-deployment testing, is increasingly viewed as the most reliable way to ensure a converged network will operate successfully in its new configuration. A number of companies, including Spirent Communications, offer innovative testing solutions to address this increasingly important market requirement.

Spirent's recently introduced Abacus 5000 IP Telephony Migration Test System combines IP telephony and PSTN testing in a single platform. This solution offers real-time call statistics and protocol analyzers for identifying all types of quality of service issues. The system works by generating real voice streams and simulating enterprise traffic loads for an accurate analysis of voice quality impact. It also offers the ability to test interoperability of a number of devices and switching schemes, including analog, TDM and VoIP traffic. The call generation feature supports a number of popular IP telephony protocols, including SIP, H.323, Megaco/H.248, MGCP and RTP.

On the service front, Spirent has started to offer a new integrated IP Telephony Assessment Service for institutions that recognize the need to perform network testing, but don't want to incur the additional cost of purchasing a testing system. The Spirent IP Telephony Assessment Service is designed to provide analysis of both IP and PSTN networks in separate and converged configurations. First, a complete assessment is conducted of an organization's requirements in terms of desired applications and scalability, as well as the type of network and services being implemented. Then a customized network analysis follows, which includes voice quality assessment and connectivity analysis based on location. A summary report is then provided that features detailed call quality statistics and charts, as well as problem identification for additional testing. Follow up testing can address specific QoS problems like latency and jitter.

mendations.)

– Interoperability Concerns

Another issue that requires careful review is that of interoperability between the various components and devices that comprise a VoIP implementation. General Dynamics' Wheeler says, "One of the biggest challenges is to gain interoperability while conforming to all the technology standards. And for government operations, interoperability is two-fold — it involves the ability to interoperate with equipment on the commercial side as well as on the government side.

"Interoperability on the government side of the equation is very far ahead — the specifications related to the security protocols are standards that all Type 1 products meet, and interoperability is really not an issue."

Indeed, in the commercial space "convergence" is a relative term, and the IP telephony industry is still experiencing growing pains. There are multiple IP telephony standards and protocols, which are still changing and expanding on a regular basis, and it is important to understand that Vendor A's media gateway may not work with Vendor B's SIP proxy server.

The extent to which a government manager should familiarize himself with industry developments depends on the types of solutions he is implementing, as well as the level of interoperability promised by the vendors selling him their equipment. Is he purchasing a full-service IP-PBX that is guaranteed to work with his existing trunk lines, ACD and handsets? Or maybe he's making a slow conversion and is planning to install a media gateway and some H.323 handsets to start.

Whatever route is being planned, it's essential to ensure that data and voice equipment are interoperable with each other, as well as any legacy equipment an agency may be keeping in the mix. For more information on IP telephony standards, visit the International Telecommunications Union (ITU, http://www.itu.int) and the Internet Engineering Task Force (IETF, http://www.ietf.org).

– Higher Than Expected Startup Costs

Despite the operational cost savings that VoIP can deliver in the long run, it's important to realize that the initial installation of equipment can be more complex and expensive than first expected. As mentioned above, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard or expect

to make relatively frequent changes as the VoIP field develops.

– Providing 911 Emergency Services (E911)

Yet another area that requires careful review is the requirement to be able to provide E911 service on the communications system. Because of the inherent differences in the architecture of VoIP technology compared and circuit-switched systems, the type of emergency services currently being offered via VoIP are not the same as traditional 911 services. This is currently an issue that has instigated Federal Communications Commission action that requires VoIP service providers to conform to new regulations governing the provision of emergency services. (For more information regarding FCC regulations, go to http://www.fcc.gov.)

Rather than relying on automatic number identification, caller ID, to help pinpoint the exact location of an emergency call, VoIP service dictates that 911 must first be activated through a registration process that involves telling the service provider the physical location of the line. After that, the 911 calls go to a general access line at a Public Safety Answering Point (PSAP).

This is different from the 911 Emergency Response Center, where traditional 911 calls go, and also requires that the caller must state the nature of the emergency, including location and telephone number, as PSAP personnel will not have this information on hand. Other drawbacks are that power and broadband service outages will prevent 911 calls from being made, and if you travel with your VoIP adapter or IP phone to another location, you must update your account with the new address information.

– Ensuring Priority Services

Another important issue regarding the migration to VoIP is the ability to have vital priority services — including those that are critical to national security — carry over from the traditional, circuit-switched world.

One of the areas Gary Amato and the National Communications System (NCS) division in the Department of Homeland Security are responsible for is tapping into the vast commercial telecom infrastructure in the event of a man-made or natural emergency. By leveraging industrial and commercial resources, the NCS is responsible for protecting the telecom infrastructure, as well as managing the interdependencies among the 13 critical national infrastructures, such as transportation, energy and water.

One such vital service that NCS/DHS has responsibility for is government emergency telecom service (GETS). GETS is an emergency service built on top of the commercial wireline infrastructure, and can be invoked when a person enters a special code on a phone's keypad for priority call completions.

According to Bahaa Moukadam, "GETS gives certain government callers priority in cases of oversubscription or overcapacity situations on public telephone networks. In the event of certain emergencies, such as an earthquake or terror attack, the phone network can come to a standstill. With GETS, even in situations where a network is overloaded by 800 percent, calls can go through."

For Amato, a major challenge is determining how to ensure that services such as GETS carry over to the IP domain. "One of my big challenges is guaranteeing that critical government employees, such as first responders, get priority service in VoIP the way they are used to getting it with the traditional phone network. This includes things like alternative routing, queuing and exemptions from restrictive controls. With VoIP there's no SS7 to leverage, so we need to work with SIP and other new emerging standards. It's an order of magnitude harder in the new environment, just in the way the IP network works."

Powerful IP Telephony Applications: A New Prescription for Increased Productivity and Efficiency

Today, a number of factors are finally in place to propel the adoption rate of VoIP and IP telephony products and services to new heights. While plain "Voice" over IP has received much of the attention lately, it's really just the tip of the iceberg in terms of what's possible. IP telephony also enables the delivery of a host of unique, productivity-enhancing devices, applications and features that are simply not possible in the circuit-switched world.

It turns out that when IP-based communications extend all the way from the network to some IP-enabled end-point devices, like an IP phone, some truly amazing applications emerge. Today's IP telephony

products and services leverage the IP infrastructure to provide entirely new ways to build relationships among all of our devices, to add new intelligence and to create more efficient and powerful ways to communicate.

For example, innovative services are emerging that allow the public to combine Web access with telephone features through a single PC or terminal, enabling a government agency contact center representative to discuss various procedures with a citizen using the agency's Web site. Other applications offer the ability to support video conferencing using the same Web access.

Such applications and more are providing the means for all government institutions to attain new communications capabilities. According to Bahaa Moukadam, "VoIP is leveling the field for agencies not involved in national security, enabling them to gain access to leading edge collaboration and communications applications that before were only available to the chosen few."

– Remote Office/Telecommuting Solutions

One of the main differences of VoIP and circuit-switched communications is that with VoIP a call is not associated with a physical telephone line, but rather with an IP address that is virtually associated with a phone number. The device that carries the IP address, such as an IP phone connected to the IP network, is the termination point, not the end of a physical copper wire. Hence, the whole concept of a telephone line with VoIP is outdated.

This intrinsic difference creates what is commonly referred to as the "nomadic" communications feature of VoIP, meaning that an IP phone can be moved to different points of connection on an IP network (either a LAN or WAN) and retain its specific network profile or ID. In this way, IP phones can allow remote workers to tie into agency communications resources while offsite in a branch office, at home, in a hotel room or even overseas.

For example, a government employee who needs to work from home can simply plug his IP phone into his home's broadband connection and all calls to his office extension will ring on the remote phone. To the caller, it appears as if the employee is working in the office. As many IP phones also include built-in firewalls, these devices can also provide security for data and voice communications.

– Web and Speech-Enabled Unified Communications

Government workers today can be overwhelmed with the sheer number of messages they receive. E-mails, voice messages, faxes — each oftentimes residing on a separate system that requires its own login method and uses a separate menu and command structure. Unified communications applications act like a single message store that combines e-mails, faxes and voice messages under a unified, intuitive interface.

A good example of such an application is the Avaya Unified Communication Center — an integrated solution suite that delivers wireless, Web and speech-enabled access to applications including messaging, communications and collaboration tools. From phones, cellular phones, PCs or wireless hand-held devices, government employees can easily manage e-mail, voice mail and fax messages, in addition to accessing agency-specific communications applications, such as calling, conferencing, directories, desktop calendar and task functions.

– Presence-Powered Collaboration

Today's leading-edge collaborative computing solutions allow geographically dispersed users to fully interact and share applications and documents as if they were in the same conference room. Collaborative computing applications are supported by many of the IP-PBXs on the market today and offer an extremely rich and highly cost-effective communications experience.

The HiPath OpenScape middleware solution, from the Enterprise Networks division of Siemens Information and Communication Networks, is on the leading edge of this application space. OpenScape provides users with consolidated access to all communication resources, including voice features and services, e-mail and instant messaging (IM). HiPath OpenScape takes collaborative computing to the next level, offering intelligent, real-time access to people, calendars and files through three new capabilities: presence-based communication, multi-resource collaboration and an architecture based on open-industry standards.

Today, instant messaging has become as common

a communications tool as e-mail. Users have grown accustomed to using buddy lists and checking the availability or presence of key contacts before starting a communication. HiPath OpenScape brings the buddy list concept to the entire spectrum of government enterprise communications, making it possible to extend presence awareness to the desk phone, the cell phone, e-mail, IM and other media. Users can click to identify which resources they want others to use at different times or in different circumstances, and the buddy list identifies the allowable choices for those looking to make contact.

– Voice and Video Conferencing

Voice conferencing is a standard feature of all telephone systems, but it is also one of the most frustrating to use: Just think how many times you or a coworker has had to reach for the telephone user manual or ask the person next to you for help before launching a conference call.

Today's new solutions take the guesswork out of setting up conferences. Through the use of software controls running on a PC, launching a conference call can now be accomplished by dragging and dropping names from a contact list into a conference application window on the screen. The system does the rest. Users can benefit from the ability to hold private sidebar conversations, make other phone calls or add new people to the call without putting the conference on hold. It's all done while continuing to listen to the conference call in the background and is managed through an interface on an IP phone, networked PC or wireless PDA.

A converged IP communications infrastructure is also ideal for video conferencing; because the video runs on the same IP infrastructure as voice and data, there are no additional networking costs. With a number of solutions, setting up a videoconference is as easy as making a telephone call. In fact, you simply telephone anyone equipped with the same solution, then invoke an instant video conferencing via the PC screen. You can handle a video call just like a voice call, placing it on hold, transferring and conferencing in additional participants.

– Wi-Fi Telephony

With a profusion of new wireless LAN or Wi-Fi network hotspots cropping up everywhere, momentum is building for the various applications that take advantage of the bandwidth and "anywhere, anytime" wireless connectivity that Wi-Fi delivers. While wireless e-mail and Web access are still the big market drivers, there is another application that is also on the top of the application list: voice communications.

"As Wi-Fi proliferates, Wi-Fi telephony — a new technology that gets rid of the physical access requirements to get into the communications network — will follow. There's a bit of a trade-off on security, but mobility is a growing, critical requirement," says DHS's Amato.

As long as enough security can be provided, Wi-Fi telephony can extend the reach of the IP telephony communications infrastructure to give government employees uninterrupted access to their voice communications, regardless of where they are in the office.

A number of companies, such as Ayava, Cisco and wireless solutions providers like Symbol Technologies and Spectralink, have entered the market with Wi-Fi telephony solutions that include the availability of mobile Wi-Fi-enabled handsets. Avaya supports Wi-Fi-telephony with its IP softphone for Pocket PC, is currently partnering with Spectralink for handsets and is working with new partner Motorola, which has developed a dual-mode Wi-Fi and GSM mobile phone. Avaya envisions providing customers with the ability to be on the public mobile network, walk into an agency building and be picked up by a Wi-Fi network, and then seamlessly be able to transfer the call from one network to the other without any interruption.

– IP Contact Center Solutions

IP contact center solutions enable a host of new IP-based communications features and can support a geographically dispersed contact center workforce. Even home-based agents can be supported and managed in the same manner as if they were working out of a centralized location. This way, government institutions can take advantage of greater flexibility in managing call loads and the routing of calls to agents with specific skill sets. Many IP-PBXs support optional IP contact center capabilities and a number of service providers are offering solutions on a hosted basis.

Over the last couple of years, there has been a huge public experience improvement driven by the use of the World Wide Web as a primary communications medium. For many citizens, using the Web has become the preferred method of making contact with the

government. Today, it is commonplace to see people renewing drivers' licenses and registrations, filing their tax forms and even paying taxes online.

Indeed, one of the most exciting new features associated with IP contact centers are the "click-to-talk" Web-based applications that allow a Web surfer to initiate a live voice call while on the same Internet connection.

According to Bahaa Moukadam, "Web telephony applications like click-to-talk can help government agencies meet their mandates of serving the public more effectively, given the budgets they have. With such applications, they can expand their capabilities and improve the services they can offer their constituents. Specific benefits can include reduced wait times, the ability to provide more relevant information, all the while being able to serve more people with fewer staff."

Looking Ahead

It's clear that with the right implementation, government institutions can significantly boost staff productivity and gain an impressive return on investment on their IP telephony purchases. Easy savings can come from reduced networking costs, free or reduced long distance charges, the elimination of expensive audio and video conferencing, lower real estate costs, lower travel costs and other operational efficiencies. But perhaps the greatest added value of IP telephony is its use as a strategic and even tactical communications tool.

According to General Dynamics' Wheeler, "We see specific applications that we are developing take advantage of VoIP technology in a tactical environment. We're at the beginning of a long evolution of going to a truly multimedia communications experience."

Indeed, once a comfort level has been reached with the technology in terms of providing basic voice communications services, the same technology is ready and waiting to be tasked for more innovative purposes.

About the Author

Marc Robins is an internationally known authority in the field of IP telephony and emerging new IP communications technologies, with more than 25 years experience in the communications industry as a reporter and analyst, conference producer and publisher, and marketing executive and consultant.

From 1998 to 2003, Robins served as vice president of publications and trade shows and group editorial director at TMC, publisher of the trade magazine Internet Telephony, and producer of the Internet Telephony Conference & EXPO trade shows, for which he also served as chief architect and conference co-chairman.

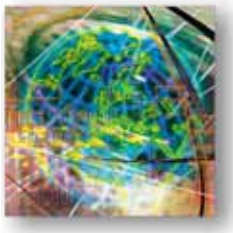
Today, Robins runs an IP communications technology consultancy and marketing firm and has recently launched a new publishing company focused on providing definitive sources of information for prospective buyers of IP communications technology. For more information about Robins Consulting Group services, call 718-548-7245 or e-mail info@robinsconsult.com.

SPIRENT
Federal Systems

Accelerate Your IP Telephony Rollout

Expertise, Resources, & Test Solutions. Make it happen. Call (714) 692-6565 www.spirentfederal.com/voice

TESTED with SPIRENT



Customer Case Study
Quintum Technologies

"Our customers are building their businesses based on our products. With Spirent Global Services and Abacus, we can make sure that they're getting a stable product with which they'll be fully satisfied."

–Leon Kravets, Test Engineer, Quintum Technologies

Highlights

Company

Quintum Technologies

Industry/market

Network equipment for VoIP technologies.

Key business issues

- Ensure stability and reliability of VoIP MultiPath switches and session border controllers
- Test systems to capacity in order to validate performance in real-world environments
- Ensure that new features and software upgrades work properly before release to customers
- Test for multiple protocols, including those used outside the United States

Results

- Abacus VoIP testing solution provides the capacity and stability to ensure performance under real-world loads
- The Abacus solution allows Quintum not only to replicate current customer environments but also easily expand its capabilities in the future by adding new cards
- Spirent's professional services team worked closely with Quintum to configure and debug tests, custom engineer special features, and analyze results, helping Quintum automate the testing process, decrease testing times and maximize its investment
- Abacus ensures that new features work before deployment, improving quality and customer satisfaction
- Multiprotocol support enables Quintum to verify interoperability and performance for markets around the globe.

VoIP manufacturer ensures product quality, customer satisfaction with Abacus and Spirent Global Services

Today, one of the hottest areas in networking is Voice over IP (VoIP). For businesses, VoIP promises lower call costs, integrated voice and data applications and simplified network operations; for service providers, it offers a significant new source of revenue. In countries where VoIP is much less expensive and more widely available than traditional telephone services, demand for the technology is increasing rapidly.

For vendors racing to get a toehold in this highly competitive market, the key issue is delivering the quality of service (QoS) and reliability that customers expect while providing interoperability with existing systems. A company's reputation—and survival—rests on the quality of its products. With its Tenor line of MultiPath switches, New Jersey-based Quintum Technologies addresses these challenges. However, like all equipment manufacturers and service providers in this market, Quintum needed a test platform to verify features, capacity and performance of its systems before they reach customer networks.

To ensure that its VoIP products will provide the dependability its customers demand, Quintum tests them with the Abacus IP telephony test platform from Spirent Communications. By emulating the demands of real-world environments, Abacus systems validate the performance, functionality and interoperability of Quintum's Tenor switches before deployment, ensuring that they will provide the quality that Quintum customers expect. Combined with customer engineering tailored for Quintum's specific testing needs, Abacus's ease-of-use features also shorten QA and testing cycles, helping Quintum get to market faster and save costs.

"Our customers are building their businesses based on our products. With Spirent and its Abacus IP Telephony Migration Test System, we can make sure that they're getting a stable product with which they'll be fully satisfied," said Leon Kravets, Quintum Technologies.

Spirent's Global Services team works closely with Quintum to shorten testing times and help the company get the most out of its Spirent equipment.

Increasing testing capacity

Headquartered in Eatontown, New Jersey, Quintum specializes in VoIP technologies that bring the reliability and voice clarity of public telephone networks to Internet telephony. Its Tenor VoIP MultiPath switch product lines are designed to

Spirent Communications
26750 Agoura Road
Calabasas, CA
91302 USA
E-mail: productinfo
@spirentcom.com

Sales Contacts:
North America
+1 800-927-2660
Europe, Middle East, Africa
+33-1-6137-2250
Asia Pacific
+852-2511-3822
E-mail:salesasia
@spirentcom.com
All Other Regions
+1 818-676-2683

www.spirentcom.com

help enterprises and service providers of all sizes achieve a risk-free migration to a converged network.

For example, Quintum's Tenor Carrier MultiPath Switch (CMS) supports intelligent call routing, VoIP and tandem circuit switching, H.323 or SIP protocols, and QoS—all in one solution—with support for up to 960 VoIP channels or 32 T1/E1/PRI spans per chassis. The Tenor Call Relay Session Border Controller allows end-to-end VoIP communications across multiple IP networks, with support for up to 720 simultaneous VoIP calls.

To validate the performance of these two products before deploying them in customer networks, Quintum's Test Group in Schaumburg, Illinois, needed a testing solution with the capacity, scalability and stability to emulate most demanding real-world environments. The group had discovered that its existing testing solution simply didn't provide the capacity it needed to fully test its systems.

"The test solution with which we started couldn't even support 16 spans of calls," Kravets says. "We had to use two different units: one with 8 T1s, one with 8 E1s."

Quintum quickly saw that Spirent's Abacus, a high-capacity, single-chassis VoIP testing solution, provided the capacity the vendor needed—and then some. The Abacus system can generate and switch more than 20 million calls per hour. It can handle more than 10,000 TDM and more than 32,000 VoIP calls; and support up to 448 T1 or 320 E1 circuits.

"The high capacity of the Abacus lets us replicate a variety of customer environments in our lab with a single test system—instead of several," says Kravets.

Spirent's Abacus family of products offers functional and performance testing for all voice testing and IP telephony needs, including call generation, performance, conformance, functional, and quality of service (QoS) testing, protocol monitoring and impairment emulation. Abacus can test a complete range of possible configurations, from terminal devices to carrier-grade softswitches and media gateways and from POTS to VoIP, VoATM, VoCable and VoDSL.

Scalability for future needs

Quintum selected an Abacus system configured with four PCM Circuit Generator (PCG) subsystems, one IP Circuit Generator (ICG) subsystem and two Virtual Resource Generator (VRG) subsystems. The PCG subsystem provides 28 full-duplex T1 circuits or 20 full-duplex E1 circuits. When performing call generation, the PCG subsystem executes a call sequence (script) for each channel. When performing switching, it routes a call from one channel to another channel on the Abacus system based on the number dialed by the system under test.

"The four PCG subsystems in our Abacus system simulates up to 112 full-duplex T1 circuits or 80 full-duplex E1 lines," says Kravets. "Our previous test system didn't have a quarter of that capacity."

The ICG subsystem provides four 10/100 Ethernet ports for generating and terminating VoIP signaling and traffic, with H.323, SIP, MEGCP, and Megaco signaling. When performing call generation, the ICG Subsystem acts as multiple IP telephones or gateways generating the call signaling and delivering the signaling and/or traffic to a system under test at the rate of 512 simultaneous calls per subsystem. The VRG subsystem provides resources for generating fax, modem, voice traffic and CODECs in the Abacus test system, with support for both VoIP and mobile voice CODECs.

"One of the main reasons that we chose Abacus is its scalability," says Kravets. "The system not only suits our needs for the present, allowing us to accurately replicate our customer environments, but also allows us to expand its capabilities in the future simply by adding new cards."

Another reason that Quintum chose Abacus was for its scalability, which gives Quintum room to grow as its testing needs increase. Each Abacus chassis can house up to 16 CG or RG subsystems on a common midplane, and provides hot-swappable functionality of any card.

Professional services decreases testing times

Once Quintum had selected Spirent and Abacus, Spirent professional services staff worked hand-in-hand with Quintum's testing team to ensure that the vendor got the most out of its Abacus system. Spirent provided expert test methodology development, rapid customer engineering, test automation, training and support.

Leveraging their deep industry knowledge and experience, Spirent helped Quintum configure the Abacus system as well as third-party equipment for its testing environment, and develop testing procedures and metrics. This helps Quintum shorten its testing cycles substantially

"We also used online conferences to walk through the Abacus application together and check the configuration in real-time," says Spirent's Anthony Nguyen. "I was able to see and control his Abacus GUI and make changes right then, rather than having him relay the information over the phone."

Spirent also increased Quintum's test functionality by custom engineering several features requested by Quintum. For example, Spirent engineers created an "event analyzer" that allows the Abacus to capture problems as they occur and save them to an events window, highlighting where the error occurred.

Another new feature added at Quintum's request was the ability to easily divide channels into multiple sets, with each set having a different group of phone numbers. This greatly speeds up

test configuration and modifications, decreasing testing times.

On an ongoing basis, Spirent engineers help Quintum debug tests, interpret and analyze test results, and ensure that Quintum gets needed hardware or software patches quickly—often within a day or two. According to Kravets, Quintum has found this level of support invaluable to its testing process, helping the company maximize its investment and decrease time to market.

"Spirent engineers work hand in hand with us to customize the application for our needs," Kravets says. "They have been available around the clock. They don't just work until it's time to go home—they work to resolution. I can only say good things about Spirent support. They do an outstanding job."

Ensuring product performance, customer satisfaction

To ensure that Quintum's Tenor products can reliably route calls between the PSTN, PBX systems and IP network, the company needed to stress the switches' ability to function correctly under real-world loads. This assures that users will experience the same level of functionality, voice quality and performance on a live network. Abacus allows Quintum to create telephone traffic, route calls, verify connectivity, determine capacity and measure criteria such as interruptions, delay, QoS, jitter and packet loss. Abacus also lets Quintum mix call generation and switch functions on a single system. Repeatable results, even with multiple interfaces, ensure that Quintum products are ready for the customer networks.

In addition, Abacus automates he entire testing process by offering pre-configured test environments with realistic call patterns, and gives Quintum the flexibility to set up desired call loads and distribution patterns—thus shortening QA and testing cycles. Unlike other test solutions, Abacus provides real-time measurements on all channels simultaneously.

"Abacus gives Quintum the ability to do the testing they needed without having to write every single step of every single state," says Vince Boggia, Spirent Communications IP Telephony Regional Manager. "They can now set up environments where groups of channels call other groups of channels and perform different types of quality path confirmation."

Another key use of the Abacus system in Quintum's test environment is for regression testing. According to Kravets, when Quintum implements new features and software upgrades in its products, Abacus helps ensure that these features are working properly before release to customers.

"By using Abacus to test our Tenor Carrier MultiPath Switch and Tenor Call Relay Session Border Controller, our products have become much more stable, which is exactly what our customers are looking for," says Kravets. "As a result, customers have been very happy with our products. This increased end user satisfaction is a definite benefit of using Abacus."

Multiprotocol support

Another reason that Quintum chose Spirent was the extensive protocol support provided by the Abacus solution. Abacus allows Quintum to develop and decode ISDN PRA, T1 CAS, E1 CAS, GR-303, V5, SS7, SIP, MGCP, H.248/Megaco and H.323 protocols with built-in protocol analyzers. These protocol analysis and conformance testing capabilities help Quintum verify interoperability between legacy and new converged networks. In addition, Abacus' protocol development tool allows Quintum to modify protocol parameters to its specific needs.

For Quintum, this flexible protocol support was especially important, as the company has extensive sales outside the United States, especially in Asia. In particular, Spirent engineers worked closely with Quintum to implement support for the MFR1.5 protocol used in Russia, so that Quintum can ensure that its products work in Russian telecommunications environments.

"The Abacus supports all of the major protocols that we do, including those used in emerging markets like China and Russia," says Kravets. "Because we can use the same system to test many different protocols, we save time, energy and costs."

Ease of use, outstanding support

The Abacus system's ease of use was another benefit for Quintum. Besides eliminating the need for multiple systems (and multiple training sessions), Abacus features a user-friendly, intuitive GUI that runs under the Windows operating system, and easy-to-use scripting tools. Set up is fast, with a step-by-step configuration process.

"It only took us 20 to 30 minutes to get up and running," says Kravets. "The Abacus GUI is essentially self-explanatory."

Results from Abacus tests are automatically gathered and presented in customizable tables and graphs. Quintum can program the Abacus system to generate reports by specific times or events.

"These reporting features are very important to us," says Kravets. "Every time we run a test cycle, the system generates a report that verifies results for future test cycles. That's very helpful to have."

He continues, "My experience with Spirent Communications has been outstanding. I can only say good things about Spirent's customer support. Everyone I've worked with has responded to me in a very timely manner and has been extremely knowledgeable. They work with us until our issues are resolved."

SPIRENT Communications

Spirent Communications
26750 Agoura Road
Calabasas, CA
91302 USA
E-mail: productinfo
@spirentcom.com

Sales Contacts:
North America
+1 800-927-2660
Europe, Middle East, Africa
+33-1-6137-2250
Asia Pacific
+852-2511-3822
E-mail:salesasia
@spirentcom.com
All Other Regions
+1 818-676-2683

www.spirentcom.com

SPIRENT Communications

Analyze | Assure | Accelerate™

P/N 79-000168 Rev.A 0905

It's time for STU to retire.

Meet your new Security Guard.

- Cost-Effective Desktop End-to-End Security
- Type 1 FNBDT Interoperable
- High Quality Voice

The New Integrated IP Phone Solution for Your Secure Voice Needs

- Office and Tactical Environments
- Multiple Security Levels
- Easy to Use

www.gdc4s.com/sectera
(800) 972-0068 / sectera-info@gdc4s.com

GENERAL DYNAMICS
C4 Systems

This product is currently under development. Accepting orders January 2006.

PRODUCT PROFILES

Spirent Federal Systems

Spirent Federal Systems provides value-added equipment and services, and ongoing customer support for Spirent Communications products to government customers and their contractors within North America.

Spirent Communications believes testing determines the best migration path when transitioning from legacy networks to IP. The Office of Management and Budget (OMB) mandated move to IPv6 increases this need for testing.

Spirent enables service providers and equipment manufacturers to test the migration from legacy to converged networks — including the triple play of voice, video and data — and maintain the networks once deployed.

We begin with VoIP conformance, functional, and performance testing in R&D and QA labs. As products move from the lab onto live networks, our tools then ensure a network's viability throughout deployment and production stages.

Spirent tests scalability, performance, interoperability, and voice quality prior to deployment. Our advanced VoIP performance testing capabilities eliminate the need for multiple test tools, resulting in reduced costs.

Spirent also provides operations with expert analysis of hard-to-diagnose IP issues. With IP diagnostic appliances deployed in the network, Spirent quickly troubleshoots complex IP problems and restores QoS expectations, including those surrounding VoIP and video.

http://www.spirentfederal.com
Jim Jordan at jim.jordan@spirentfederal.com
or 949-673-3265

General Dynamics C4 Systems

General Dynamics C4 Systems is a leading integrator of secure communication and information systems and technology. With more than 10,000 employees worldwide, the company specializes in command and control, communications networking, space systems, computing and information assurance for defense, government and select commercial customers in the United States and abroad. The company has more than 35 years experience in designing, developing and producing Type 1 information security equipment for the National Security Agency (NSA), Department of Defense (DoD) and other federal agencies.

We provide secure communications from network to desktop to individual. The Sectéra VoIP Phone provides the latest technology for securing Voice over IP networks. Using SCIP/FNBDT signaling and commercial open standards, the VoIP Phone is planned for Certification to protect information classified Top Secret and below including Sensitive But Unclassified (SBU) and is available with multiple key-sets to support U.S. government sponsored interoperability (e.g., NATO and coalition). Built to provide seamless communications with legacy phones and encryption systems, the secure VoIP phone is software programmable with extensive memory to easily accommodate future upgrades and functionality.

www.gdc4s.com/sectera
480-441-4300
Sectera-info@gdc4s.com

Avaya

Avaya enables enterprises and government agencies to achieve superior results by designing, building and managing their communications networks. More than 1 million businesses worldwide, including 90 percent of the FORTUNE 500® and a majority of government agencies rely on Avaya solutions and services to enhance value, improve productivity and gain competitive advantage.

Focused on enterprises large to small and government agencies, Avaya is a leader in secure and reliable IP telephony systems, communications software applications and full life-cycle services. Driving the convergence of voice and data communications with applications — distinguished by comprehensive worldwide services — Avaya helps agencies leverage existing and new networks to unlock value and enhance performance.

www.avaya.com/gov
1-800-492-6769

VENDOR LISTING

Spirent Federal Systems

22345 La Palma Ave., Ste. 105
Yorba Linda, CA 92887
Jim Jordan
jim.jordan@spirentfederal.com
949-673-3265
http://www.spirentfederal.com

Spirent Federal Systems markets and sells Spirent Communications products to government agencies and government contractors.

General Dynamics C4 Systems

8220 E. Roosevelt St.
Scottsdale, AZ 85257
Sectera-info@gdc4s.com
Phone: 480-441-4300
Fax: 480-441-2515
www.gdc4s.com/sectera

General Dynamics C4 Systems is a leading integrator of secure communication and information systems and technology.

Avaya

4250 North Fairfax Drive
Arlington, VA 22203
1-800-492-6769
www.avaya.com/gov

Avaya is a leader in secure and reliable IP telephony systems, communications software applications and full life-cycle services.

L-3 Communication Systems-East

1 Federal St.
Camden, NJ 08103
Keir Tomasso
keir.tomasso@L-3com.com
856-338-5995
www.L-3com.com/IA

L-3 Communication Systems-East provides Type I secure communication and encryption devices supporting legacy and next-generation requirements.

Network Equipment Technologies

NET Federal
21660 Ridgetop Circle, #100
Dulles, VA 20166
George Holmes
George_holmes@net.com
703-948-1828
www.net.com

Network Equipment Technologies is a major supplier of multi-service access and broadband aggregation platforms and IP telephony gateways.