Pipeline
It's in here.

Tracking the Elusive "IP Application"

By Edward J. Finegold, Editor-in-Chief

The IP applications wave is like the next blockbuster movie hit – it sounds cool, everyone is talking about it, but no one knows any details. Most of the time, if you ask someone around the telco business what the hot new IP services actually will be, the response is something like, "well, email, web hosting, VoIP and video." For the record – these are not the great new IP applications to which we look forward, but rather network functions already in use. The service provider's burden lies in deepening its expertise in IP applications and giving customers superior alternatives to what they already use. To serve enterprise customers this means deepening expertise in security, identity management, storage, hosted applications, content management and capabilities that take advantage of presence and mobility.

Application Outsourcing Grows Fast

IDC research estimates that the combined market for application services and web hosting will grow from approximately $7 billion to $14 billion within the next four years. The firm predicts the greatest growth will come from network- or web-resident applications, a $666 million market today that could see 500 percent growth by 2008. There are no secrets behind these numbers. Enterprises' IT expenses are skyrocketing as they take on more devices and applications and have to secure and manage them all. Most of what these enterprises have pulled in-house involves repeatable functions that are necessary for running their business, but aren't their competitive secret sauce.

What Did I Do With That Number?

People who use email and make phone calls often struggle with what can be called "information housekeeping." People have multiple address books, contact databases, email inboxes, and voice mail accounts. The number of these accounts is increasing as people use more mobile email and messaging services and have more devices and applications that can store contact data. To help with the mess, and also help increase their career networking, many users are turning to web-based services like Plaxo and LinkedIn that automatically manage and update their business and personal contacts. This is basic stuff, but the kind of capability people use every day.

Enterprises have security concerns regarding these web-based services because they are outside of the corporation's control. Further, even some users equate the impersonal emails these services generate with spam. Telcos can provide secure versions of these services as part of a total offering and help overcome information security concerns.

Email and messaging unification is a slightly bigger challenge, but is perhaps the next step given the number of email and messaging users the increasing number of email and messaging capable devices in the workplace. These are all practical ideas that attend to users' every day needs and provide secure alternatives to public, Internet-based providers.

No Spam. No Phishing

Of the most notorious of IP expense hogs are Spam and Phishing. These two Internet devils, spawned by hacker anarchists and hucksters, cost enterprises and their employees hundreds of millions per year, both as a result of the scams they perpetrate and the expense to combat them.

Spam, as all email users know, is unsolicited junk email that not only wastes disk space, but can carry viruses and worms. It also encourages users to visit places on the Internet employers and IT staff would rather they avoided. Phishing is a slightly more devious scam. Spammers pose as legitimate financial institutions and bombard corporations with email, with the intent to fool users into surrendering credit card information.

Like most other IT functions, commercial software exists to combat these common problems, but this is yet another growing expense corporations inherit with their basic IT infrastructure. If an enterprise can contract for an email solution with a carrier, it makes sense for it to pay a premium for a spam and phishing-free experience, courtesy of the service provider. Rather than throwing money at the problem and failing to solve it, enterprises should be able to count on their communications partners to clean their email before it's delivered.

Master of Your Domain Names

Domain names can be a petty pain. Most businesses, large and small, own multiple domains and corporations can own hundreds or thousands of them. Domain name licenses expire over time, of course, and some domain names go in and out of service. Though it's a smaller item, a basic service that automates management of domain names, their status, their expiration dates and who has permission to administer them would provide a common staple in the IP environment. Any enterprise might want to see this as part of an overall offering, as opposed to the alternative of paying someone to manage a system that in turn manages domain names.

Business Applications

One the major reasons enterprises are clamoring for services like MPLS networking is that they want flexible – but QoS manageable – bandwidth to support their applications. Most corporations use any combination of SAP, Peoplesoft, Siebel, Microsoft Exchange, Salesforce.com and a range of other common business systems that provide the basis for their every day operations. Applications are being used increasingly by large and small

companies for things like automating international trade functions, managing supply chain logistics, and tracking real-time inventory.

Of the biggest hurdles for enterprises to move from in-house applications to an outsourced model is whether it would have to change the applications it uses, or try to re-make all of it's customizations on a new version of its application. Part of the carrier's service would have to include not just the application, but the customer's migration to it. These applications services do not exist in a vacuum. They will be used side by side with services like voice, messaging and email. They will also drive traffic because they generate support calls, sales, and customer service follow-ups.

Storage Area Networks (SANs)
Data is to enterprise IT managers what nuclear waste is to a power plant – there's too much of it and not enough places to hide it. Massive storage arrays and data warehouses were once thrown at the problem, but solutions have become more sophisticated. SANs are gaining intelligence and the cost of SAN devices has dropped significantly as the quality has improved – as is generally the case with maturing technologies. SANs are being complemented with data and document management applications that incorporate automated workflows. They can make rules-based decisions about where to store documents, where and when to back-up data, how to identify and delete redundant data, and how to optimize storage capacity.

In a reliably connected broadband world, where the SAN physically resides is not an issue, as long as it is secure. SAN is a natural for an outsourced IP service on its own. Enterprises use SANs for everything from internal administrative and insurance data to materials for sales personnel, contracts for leased equipment, manuals for office equipment and software, and telecom agreements. SANs can also provide a data backbone for other applications, and can help enable mobility and presence capabilities. An outsourced SAN can provide all of the same functionality, but none of the hardware, maintenance or system management expenses.

You Must Comply
A major benefit that a well managed SAN can provide is a foundation for what's called strong "information stewardship." Information stewardship a something corporations must undertake to insure they comply with Sarbanes-Oxley, HIPAA, the Graham-Leach-Bliley Act and other mandates. It means insuring complete, accurate, secure data that is stored appropriately, backed up and ready for auditing. AMR research estimates that corporations will spend roughly $5.5 billion in 2004 to comply with Sarbanes-Oxley requirements alone.

Enterprise managers say they do not have the people, time or resources to manage the sheer volume of data management, processing and auditing involved in compliance. Not surprisingly, a host of software tools designed to manage data and automate compliance reporting have surfaced in the IT world. 46 percent of the 500 IT executives *Network*

World and Research Concepts recently surveyed said they will upgrade or purchase new applications this year for regulatory compliance. This is, once again, a common service that is highly repeatable and adds massive value to any data storage, hosting or management service.

Presence and Mobility

Playing further on the SAN theme, network-accessible data enables both presence and mobility in IP. In a simple example, a person connected to a WiFi hotspot, working on a document accessed from a SAN, communicating with a colleague via instant messenger (IM) is expressing both mobility and presence. The mobility comes in being able to access "home" services – i.e. the SAN – from any IP connection, regardless of geography. Presence is represented in IM, where the user "appears" to others on the network when he or she is "present."

Mobility and presence are critical capabilities because people are on the move and need to be able to communicate and remain highly productive wherever they go. People that work for large corporations are mobile, not just the jetsetters, but those that go from meeting to meeting or room to room. Hospitals, for example, are an extreme case where people work in a confined space, but never stay in one place for very long. Though this opens the door to many service opportunities, the first and most obvious is instant messaging.

Instant Messaging

Radicati Group estimates that 85 percent of all companies worldwide use instant messaging in some form. The research firm says that as many as 125 million people use unsecured IM services from AOL, Yahoo and others – up from 100 million just nine months ago. Corporate employees often use these services for anytime, anywhere communication with colleagues. But IM presents security vulnerabilities and can be a gateway for hackers to break into corporate networks and steal information or identity.

Corporations want and need IM, but it needs to be the kind of bullet proof, secure service for which they'd typically turn to a telco. AOL is trying to step into that role now, competing with WebEx, and is rolling out a business service that includes AOL Instant Messenger (AIM), online meeting functions and voice conferencing. AOL estimates that 15 million of its 36 million AIM users access the service for work purposes. Both IBM with Lotus Notes and Microsoft have also added secure IM infrastructure to their corporate offerings in response to business demand.

Collaboration

Presence and mobility will take users beyond IM as broadband IP connections become more easily accessible. One example of this is found today in collaboration tools that give colleagues working on projects their own virtual workspace. This space is used to share files and comes with functions like whiteboarding, chat, application sharing, voice conferencing and web presenting. These capabilities are familiar to those in software

development and project management, but they have now entered the mainstream. Early adopters are taking this one step further and rolling out video portals that deliver education, training, corporate news and even work-related entertainment all over IP.

In an ideal sense, people will move from meeting to meeting, office to office, and city to city and always have complete access to resources, information and voice calls. Mobility and presence are inherent to VoIP – in certain architectures – so that users should be able to tap into an IP connection anywhere and have calls routed to that location. Combined with collaboration tools, the foundation is set for an enterprise workforce that is enabled for mobility and not constrained by it – and enterprises consider that an advantage.

Security Management

With people moving around, and in and out of network environments with a range of devices, security risks skyrocket. Corporations are already struggling to manage things like anti-hacker, anti-virus and anti-user-who-ignores-all-rules security, plus basic management of accounts, policies, permissions and corporate protocols. The cost, as with all other IT areas, is escalating along with the volume of events, the types of vulnerabilities and number of things that require security.

IM alone opens networks to viruses and worms, identity theft, firewall tunneling, data security problems where users may communicate trade secrets over unsecured channels, and "spim" – instant messaging spam that already makes up 5 to 7 percent of IM traffic, according to *Network World (June 28, 2004).* These are primarily network and policy security issues – in other words, users are accessing unsecured network services. If prevented from using public services, but given access to secure alternatives, users can be sated and these problems largely avoided.

Security vulnerabilities are also created by desktop PCs, laptops, and devices that move between public and corporate network environments. Too often users fail to adhere to security protocols – like updating their Windows software – and create holes for hackers, worms or viruses. Corporations are spending money for management systems that automate patch updates, and intelligent security measures that quarantine vulnerable systems when they try to access network resources. They are also looking to software to provide vulnerability scanning on an ongoing basis; most companies only scan a few times a year, if at all. These capabilities are repeatable, commonly needed, and commercially available – prime candidates for valuable IP services enterprises need.

Identity Management

Another significant challenge IP presents for enterprises is in managing and protecting user identities. With more information that is network accessible, be it corporate, or personal and financial in nature, the greater the risk of fraud. Identity theft is already an escalating social problem, and it is perhaps easier in the electronic world. The law is still

catching up with electronic identity theft though, so there is plenty of room for fraudsters to invent scams for which they can avoid prosecution. While Dr.Evil is not likely to take over GE's email infrastructure any time soon, some companies do fear corporate saboteurs stealing an executive's identity and sending damaging emails in his name to major customers – surprisingly, there's no real law against this as of yet.

Identity management is critical, however, in business environments where people work with multiple suppliers' systems, or multiple web interfaces in general. Single sign-on across partner domains, for example, is a key productivity feature on which networked applications rely. This kind of capability can't be shot down, so it must be secured against identity theft. Corporations are just beginning to turn to technologies like biometrics, thumb prints, and various automated password reset and encryption features to insure users are who they claim to be. These technologies are critical but often inaccessible to a range of businesses for financial or expertise reasons, and thus another area where service providers can provide a staple support service while offloading cost and complexity for their best customers.

In the end, this is what IP applications are all about – taking away the growing complexity and management burden associated with communications and recognizing that IT is part of it all. Enterprises are already spending billions on basic IT infrastructure that is, in function, common to them all. There is a clear economy of scale to be created here, and one that ASPs are trying their best to accommodate. In the end, however, it's the telcos that have the experience with scale, reliability and security to deliver what enterprises need in their core operations. What telcos have lacked thus far is direction and a realistic set of examples to follow from their advisors and suppliers.