View from the Top: VoIP comes of age

August 4 2005

Voice over Internet Protocol has emerged as an increasingly popular alternative to traditional phone connections for its ability to transport voice communications over data networks like the Internet.

Users are adopting VoIP services in record numbers, attracted to its relatively low cost and the ability to make unlimited calls anywhere in the United States and Canada for a flat monthly rate, and other international calls at modest incremental fees.

As telecommunications and cable service providers continue to launch an increasing array of VoIP offerings to enterprise and residential markets, potential users need to educate themselves on the technology, its benefits and current limitations.

In a traditional telephone system, a phone number is part of a circuit-switched network that links callers via wires and routing computers. VoIP services work by transforming voice signals into data packets that are able to travel over IP-based networks before they are converted back to voice signals when they reach their recipient.

With VoIP, a caller's number is linked to an IP address. Voice signals are broken up into data packets and travel from one computer to another, across the Internet, until they reach the intended recipient's IP address. At this point, voice packets are reconciled into a complete signal, enabling users to hear and speak to each other exactly as they would using a traditional telephony service. Or, at least, that is the goal.

VoIP already has transformed the communications landscape, and many industry watchers predict it likely will completely replace telephone services as we know them in the United States and abroad. However, mainstream and widespread adoption will depend on how well the industry addresses performance and security issues, including enabling reliable connections to 9-1-1 services, deterring Internet hackers and ensuring quality of service.

The industry has made significant strides, but there is more work to be done.

One current challenge associated with VoIP is both a physical and information-technology security issue. During emergency situations, connecting to 9-1-1 dispatchers in a timely manner can be the difference between life and death. Because VoIP calls are associated with IP addresses, rather than a phone number linked to a physical location, not all VoIP services allow 9-1-1 emergency dispatchers to locate callers automatically.

The implications of this issue are clear with respect to residential services, but imagine the impact a failed 9-1-1 connection could have for enterprises in terms of both employee safety and corporate liability.

In an effort to improve the effectiveness and reliability of 9-1-1 services, the Federal Communications Commission ruled in May that certain VoIP providers must supply 9-1-1 emergency calling capabilities to their customers as a mandatory feature of service. With government-backed mandates on the table, it now seems assured that users will soon experience the same dependability from Internet-based voice communication that they have come to expect from conventional phone services.

Information security concerns have touched all areas of IT recently, and

VoIP is no exception. The nature of VoIP, ruled by the laws of data communications, opens the potential for security breaches on a par with those that impact any IP-based service. To address the need for secure, predictable and efficient VoIP services, security must be pervasive and proactively built into the network, not just an afterthought hastily developed in response to a security breach.

For example, there is the potential for hackers to break into VoIP servers, compromising data. In VoIP, private branch exchanges are replaced by server-based IP PBXs. These call-management boxes, used for both serving VoIP services and for logging call information, are susceptible to virus attacks and hackers. Server break-ins could result in the loss of sensitive data.

Another example of a VoIP security threat is a concept known as spam over Internet Telephony or SPIT. Much in the same way that SPAM afflicts e-mail in-boxes, a VoIP spammer or "spitter" can copy one phone call and send it to many other users, mirroring the process of carboning an e-mail to create spam. The potential exists for an individual to make unwanted calls to hundreds or thousands of users simultaneously and anonymously.

Perhaps the most basic challenge that VoIP must overcome is also the most complicated. The data networks over which VoIP services must traverse were never designed to carry voice. The migration from circuit-switched networks to VoIP brings a new set of quality challenges that can manifest in packet impairment and ultimately result in poor call quality. Measurement and monitoring of performance and QoS parameters have assumed critical importance. Service providers must commit to delivering toll-call quality without impacting other critical data applications and provide a highly reliable infrastructure that can survive partial outages.

VoIP has accelerated competition among service providers looking to increase time-to-market for new services and ultimately boost revenue. For residential and enterprise users alike, service reliability will have a dramatic impact on the adoption rates and providers' ultimate success. Enterprises in particular are demanding enhanced management of QoS levels and new ways they can measure, understand and negotiate service levels with their providers.

VoIP is gaining major momentum, but service providers must meet the high standards both residential and enterprise customers have come to expect from traditional telephone services. Providing customers tangible evidence of the health and performance of IT services will be key to winning their confidence and loyalty. In the end, the goal is clear, consistent, good-quality conversation.