

COMMERCIAL ADVISORY COMMITTEE

D-Mystifying VoIP

BY ALAN R. SHARK

Most people never realize the multiple paths a phone call can take. A digital cell phone takes our analog voice and converts it to a digitized signal. The signal travels wirelessly to a nearby tower and from there it may be connected to a network through a series of microwave signals or underground cables. That same call may well go from wireless to wired in the form of high-speed or fiber-optic cables. It will be switched dozens of times without losing a word or letter and may indeed be carried at some point by a satellite or Internet connection. This all happens in microseconds, and—in the end—the digitized signal is placed back into analog mode so we can hear it.

Today, voice over Internet protocol

(VoIP) is becoming increasingly popular. This is evidenced by the aggressive market penetration of companies providing such services (e.g., Vonage, Skype). Even traditional phone companies are entering this new and highly competitive arena.

Essentially, VoIP means voice transmitted over a digital network. But keep in mind that just because a phone is digital, as most are today, it's not automatically a VoIP device. The Internet protocol (or simply IP) is what makes VoIP unique. IP provides a popular, standardized way to communicate over an internal network to almost any location using the Internet as its main path. Not too long ago, the Internet protocol was being used only through the Internet. Today, information

using IP can travel over almost any network, making IP the standard of choice.

VoIP is packet-switched, which means that the signal travels to and fro with a unique ID and can travel and be rerouted many times without loss of quality. Remember the plain old telephone service (commonly referred to as POTS) relied on a circuit-switched network, which by comparison has many feature and functionality limitations.

IP is a robust, dynamic protocol that offers users amazing applications. For example, someone in a remote office connected to the Internet can receive and send calls as if they were in the home office. A communications manager can assign numbers and or extensions to

COMMERCIAL ADVISORY COMMITTEE CONTRIBUTION

Emerging Technology: The Watchword Is Adaptability BY KRISTEN SMATHERS & DONALD COOVER

Technology keeps changing and advancing in ways once never imagined. With these advances comes the need for adaptation to ensure that technology is appropriately deployed and used. With respect to communication networks, Internet protocol has been used for quite some time, primarily for data services. More recently, IP has been adapted to support voice calling, or VoIP.

VoIP is one of the newest technologies affecting public safety organizations and operations. As VoIP has become a cost-effective way of communicating and making telephone calls, many businesses and governments have adopted this technology to reduce costs. They are replacing older traditional networks and communication equipment while still providing reliable services for employees.

The newest VoIP trend involves wireless networks. The first implementations of this type of service use 802.x, or WiFi, networks and are known as VoWiFi. VoWiFi is designed to work mainly with PDAs and laptop computers, but is quickly being adapted to the commercial market through the manufacture of WiFi handsets and dual-mode mobile telephones. In 2004, worldwide revenue from dual-mode handsets reached \$6.7 million while the total revenue from all WiFi VoIP handsets reached \$54.7 million. Already, VoWiFi has been adopted in many regional metropolitan areas where deployment of WiFi hotspots is prevalent.

Companies and hospitals are using VoWiFi to enhance in-building communication with their workers while adding mobility. This presents new issues for public safety organizations, such as figuring out

how to call back a VoWiFi handset that roams off the WiFi network. Getting proper caller location information can also be impeded if the call is not properly routed to provide the MSAG data. These challenges will continue to grow as the technology is further adopted by the general public.

Many issues need to be dealt with to ensure reliability with both VoIP and VoWiFi. System latencies can reach 400–600 milliseconds, resulting in poor voice quality and delay on the data being sent. A poor network design will add additional packet delay. Although you may be talking, it takes the receiver extra time to completely receive and “hear” what you said. Voice traffic must be properly prioritized to ensure there are no slowdowns or lags as a result of other data traffic being handled by the network.

Other issues that must be dealt with are security and roaming access. One of the cost-saving advantages of IP is the ability to send information, both voice and data, over a common network that may or may not be privately owned and operated by the agency. *The drawback:* Without proper measures being implemented, an unauthorized hacker can extract information being sent or even reconstruct a conversation. Passwords, firewalls, virtual private networks, tunneling and other standard security options offer some levels of protection. However, a network used for public safety, police and fire rescue must be properly secured to ensure no unauthorized access to information or calls being transmitted.

Roaming access is also very important. Public safety agencies

employees wherever they are located in the building or in another part of the country.

Field employees can conduct regular telephone conversations with their laptop computers using what is referred to as a “soft phone,” which is all software except for the headset. This raises some interesting challenges regarding E9-1-1 obligations, local governments’ ability to regulate and tax, and quality-of-service options.

Public Safety Communications will take some of the mystery out of VoIP in the next several issues, tackling the following topics:

- VoIP as a replacement internal phone system and network: understanding the pros and cons;
- VoIP & E9-1-1: What's the problem?! Why VoIP phones are causing havoc in E9-1-1 centers. *Plus:* Identifying the fixes and when they'll be available;

need the ability to control which users are permitted on the network as well as the ability to maintain reliable and secure communications while users roam onto other networks.

As more agencies move to an IP-centric platform, manufacturers are providing multi-mode, multi-band communication devices. IP networks that support voice, data and video will require agencies to focus attention and resources on ensuring these systems are designed, deployed and maintained to keep pace with the user requirements and technology. These increased capabilities will strain poorly designed and deployed networks and could put sensitive information at risk.

~KRISTEN SMATHERS is a member of APCO's Commercial Advisory Committee. Donald Coover is vice president of V-COMM, a leading provider of integrated network engineering and support services for telecommunications. For more information, visit www.vcomm-eng.com.

- VoIP goes wireless: advantages and disadvantages;
- How secure is VoIP?

~ALAN R. SHARK is the executive director of Public Technology Institute (PTI) (www.pti.org).

TOOLS

VoIP Recording Challenges in a Hybrid Environment

BY DON GILLIS

When most people in public safety circles think about VoIP, they immediately focus on incoming 9-1-1 calls. But VoIP is also entering the public safety arena another way—through the back door.

The rapid emergence of VoIP in commercial enterprises is due to the convenience and cost-effectiveness of having a single network for both voice and data. The benefits of a single network are self-evident from an operation and maintenance perspective. So, with VoIP voice quality improving, it's no wonder public safety and government agencies are moving this way when they upgrade their systems.

Many PSAPs have IT staffs that are already overburdened with managing multiple networks, mission critical communications technology and the demands of making the entire system reliable and easy to use for the front-line team. So it's likely VoIP will be implemented in stages, as older hardware is gradually replaced. *The bottom line:* If your public safety agency is not already using VoIP, it will in the near future.

The dilemma is that many departments require calls to be continually or selectively recorded. Sub-optimal approaches to the integration of VoIP into existing systems include the use of multiple recorders, as well as software-only or analog phone taps that are costly to install and maintain and may be a point of failure. What is needed is a simple, practical voice recorder solution that meets both current and future requirements.

Every PSAP faces a few realities. First is funding. Although some new PSAPs have

the opportunity to start with a blank slate when designing their communications and data network, the overwhelming number must fit technical upgrades into existing buildings and networks. As funding becomes available, segments of the network are upgraded; things don't happen lock step.

Second, technology and networks continue to evolve. In many ways, VoIP is still in its early stages of adoption, and the technology will continue to improve and migrate from one department to another. So IT departments are trying to hit moving targets. Given the need for PSAPs to record mission-critical analog radio communications, incoming 9-1-1 calls on their digital PBX and now VoIP communications in the back office, the challenge is how to accommodate these technologies into the current infrastructure.

Third, users demand quick, easy, comprehensive and reliable access to communications for the support of front-line personnel and for use in incident reconstruction, training, etc. Professionals also need simple-to-use, intuitive user interfaces, allowing them to respond quickly and be self-sufficient. Trying to pull information from various sources creates challenges for IT administration and end users.

Fourth, IT departments are already overloaded, so maintenance and support of multiple products and vendors are undesirable. Additionally physical space in IT rooms is very limited.

Fifth, there is no standard network configuration. Collecting communications traffic and associated data, integrating pertinent information for easy database searches and knowing where to tap the network in the right places are all keys to success. The trouble is finding a vendor that acts like a partner, is knowledgeable and can solve the unique requirements of the application.

The challenges are clear. But the good news is that a solution exists.

VoIP communications are currently recorded two ways. Some vendors use a separate box dedicated to VoIP communications, but this approach has its drawbacks: two recorders must be installed,