

On the Way with **VoIP**

VOICE OVER INTERNET PROTOCOL IS STEADILY WORKING ITS WAY INTO ALL ASPECTS OF MILITARY OPERATIONS.

By **HARRISON DONNELLY**
MIT EDITOR

While the Pentagon ponders the possibility of moving the whole Department of Defense to Voice over Internet Protocol, VoIP technology is steadily working its way into all aspects of military operations and finding a host of converts to its

promise of lower-cost, network-based voice communications.

The shift to VoIP—which in truth represents a subset of the larger convergence of voice, video and data communications to IP-based networks—is taking place on a case-by-case basis

throughout DoD, with each of the services pushing initiatives. For example, the Navy has implemented VoIP on all of its active carriers, according to the Voice on Net coalition, which also estimates that DoD now has more than 130 VoIP networks worldwide.



VoIP communications also have played an unexpectedly important role in operations in Iraq and Afghanistan, and deployed personnel are using VoIP calls extensively to communicate with their families.

The central role in the transition, however, is being played by the Defense Information Systems Agency (DISA), which is working on the issue from several perspectives. Earlier this year, the agency asked industry for ideas about how to create an enterprise VoIP system that could provide a full range of voice related capabilities to more than 2.7 million DoD users.

In its solicitation, DISA identified a number of benefits that could accrue from a VoIP system, including avoiding duplication of costs, eliminating multiple networks, reducing base infrastructures, consolidating security operations and providing tighter integration with DISA enterprise collaboration and directory services.

At the same time, DISA is also including VoIP in its Unified Capabilities (UC) initiative, which it defines as the “seamless integration of voice, video and data applications services delivered ubiquitously across a secure and highly available IP infrastructure to provide increased mission effectiveness to the warfighter and business communities.”

A key element of DISA's efforts has been the development of the Assured Services-Session Initiation Protocol (AS-SIP), which adds military-oriented features to the SIP standard used to make VoIP calls, including multi-level precedence and preemption for establishing communication with resource priorities, ensuring system and network access and control, and providing precedence and preemption policies to assure connectivity for command and control.

The precedence and preemption features address what is one of the key issues in VoIP, which is the need for quality of service standards that, among other things, ensure that high-ranking officials' calls go through even when the network is congested with other traffic. While these precedence procedures have been developed to a fine point over the years for traditional phone traffic, they are not basically part of the IP world, and so need to be included in order to provide what can truly be a life-or-death capability in tactical situations.

The UC requirements document, which encompasses AS-SIP, must be adhered to by vendors wishing to be able to sell equipment to be connected to the Defense Switched Network by the military.

Another tension in moving to VoIP involves security. While the technology can offer some security benefits, it also poses a number of potential vulnerabilities and quandaries, especially in the form of tradeoffs between security and convenience and ease of use.

Nevertheless, observers say the momentum is building, and that VoIP, as part of a blended system of video and data, will become a standard form of military voice communications, both at the enterprise level and for tactical communications.

Jani Lyrintzis, vice president and general manager of Elektrobot, an electronics company whose offerings include tactical VoIP packages, summed up the outlook

DISA Looks at VoIP

Pentagon is aggressively pursuing an enterprise voice over IP strategy, says Network Services Director Moran.

(Editor's Note: Cindy Moran, director of the Network Services Directorate within Defense Information Systems Agency (DISA), recently responded to some questions about the current status of Voice over Internet Protocol (VoIP) programs. Following are her comments.)

Looking both within and outside of DISA, how would you describe the current role of VoIP and related technologies in military operations?

All of the Department of Defense strategic plans related to voice and video services include initiatives to migrate to IP in support of military operations. Different technologies will be used to transport the IP traffic, such as wireless, satellite, wired and line of sight, but IP is the future cornerstone for communications in DoD. When one looks at the history of voice technologies, the transition to IP has occurred at a much faster pace than any other transition.

Are there any statistics on overall use, or is it so decentralized that it is hard to get a complete picture?

Most of the funding for voice services in DoD is provided at the local level. This makes it difficult to determine the overall use. However, the department has been deploying IP-enabled Private Branch Exchanges and End Offices for the past five years, and large segments of DoD have already migrated to IP at the edge. DoD has approximately 2 million unclassified subscribers, and approximately 25 percent of those subscribers are currently using some form of IP for voice and video communications. Over the last two years DISA has deployed a network core of Wide Area Network (WAN) Soft Switches (SS) that allow VoIP to occur on an end-to-end basis. DISA envisions by 2017 that 80 percent of DoD voice and video traffic will be IP based on an end-to-end basis. In DoD, the migration started at the edge, but with DISA's deployment of WAN SS, it has aligned with industry.

DISA is in the process of developing and implementing the Unified Capabilities program, which includes VoIP. What is the current status of that?

DISA has been very successful with this program. In July 2011, DISA achieved full operational capability of the DISA

this way: "It's somewhere between trial use and limited operational use. It's not in full blown operational use, as far as we can tell, but it's well on its way. There's no question in my mind that at some point in the future, all the voice communication in the military will be VoIP-based, and that also applies to the global military market."

USER EVOLUTION

For all the advantages of VoIP, observers say acceptance by military users is still evolving. Although some are embracing the technology wholeheartedly, others appear reluctant for several reasons to migrate fully to it, according to Dinah Gueldenpfennig, vice president of planning and government program administration for REDCOM.

REDCOM offers the Slice 2100 system and the recently announced Slice IP Micro. The Slice 2100 is a converged network solution that also supports AS-SIP signaling requirements for local session controllers. The Slice IP Micro redefines tactical communications by integrating key IP multimedia subsystem elements and call management functionality into the size of a hardcover book. It represents a complete dual-stack IPv4/IPv6 VoIP solution, including AS-SIP signaling, in a single platform.

"We find the desire to maintain a level of compatibility with legacy equipment still strong within the tactical arena," Gueldenpfennig observed. "Ruggedized and reliable TDM-capable systems are not easily given up by the users in favor of a technology that requires multiple servers and is not so easily deployed in hostile environments."

Gueldenpfennig pointed to one military user, who said in effect, "Why should I have to change the equipment I'm using, which works well and doesn't have the same vulnerabilities as VoIP, just to meet new testing requirements? I cannot justify the cost."

While REDCOM has been developing to the UC requirements and tested against it for DoD UC Approved Products List (APL) certification by DISA, she explained, it also recognizes that not all users either want or have the funds to replace their existing equipment for a newer technology.

"Given that, and the knowledge that the move to VoIP is in full swing, we develop our products in such a way that the warfighters can expand their systems to connect the older and newer technologies, making them seamlessly interoperable, using TRANSip available in our switches. This gives you a softswitch and full media gateway in one unit. We can even connect a secure VoIP end instrument to a magneto crank phone all in one system," Gueldenpfennig said.

A key contributor to the spread of VoIP has been the development of AS-SIP, which ensures that all vendors follow the same standard and that whatever is deployed will work together. But as Gueldenpfennig noted, it also can pose challenges, in that AS-SIP, being VoIP-based, has some vulnerabilities.

"Security threats are numerous, and DISA is continuously tasked with having to counter them," she said.

backbone for VoIP. This included several of its industry-leading vendor partners successfully demonstrating their ability to meet DoD requirements. Those products are now being sold and deployed to the DoD community. Working with its industry partners, DISA has tried to leverage COTS solutions. All of the vendors support an integrated UC solution that provides voice, video and data. To provide multivendor interoperability, DISA uses industry standards as its cornerstone protocols, such as Session Initiation Protocol (SIP) and Extensible Messaging and Presence Protocol. In addition, DISA has worked with its vendors to ensure that the commercial solutions can be hardened to ensure that the identified threats are mitigated. DISA looks forward to continuing to work with its industry partners to embrace advances in UC technologies and integration to provide features like improved unified messaging, directory services, and mobility on wired and wireless platforms.

DISA earlier this year put out an RFI about moving to an Enterprise VoIP program. Why, and how will you use the information provided?

DoD is aggressively pursuing the deployment of an enterprise VoIP program and needs to understand how commercial VoIP technologies have evolved over time, and what capacity commercial industry currently has to provide those capabilities. We are using the information provided to help us identify an affordable way ahead in this sector, while providing a VoIP capability that meets military needs associated with efficiency and warfighter needs. The challenge that we continue to face is how to justify the upfront investments needed against the savings that follow as resources are redeployed away from the existing copper wire, circuit switched private branch exchange capability that provides the current DoD enterprise voice switching. The dual operations costs continue to be a challenge that must be addressed in a period of budget austerity.

How feasible is a shift to departmentwide use of VoIP, and what would be the benefits and potential risks?

DISA believes that it is feasible to migrate to VoIP for the majority of users. However, DISA also believes there will be a small subset of users who cannot migrate to VoIP for mission, technology or cost reasons. Industry has essentially stopped development on legacy Time Division Multiplexing (TDM) solutions, and TDM products will reach end-of-life within the next three to five years and will no longer be supported. However, DISA will continue to keep a reduced infrastructure to support its customers using legacy technologies. The main benefit from moving the department to VoIP and reducing the legacy infrastructure is the cost savings associated with the operations and maintenance (O&M) of that equipment. VoIP equipment has a smaller

footprint and O&M cost, which is in line with the IT efficiencies the department is trying to achieve. The largest risk of migrating completely to VoIP instead of legacy technologies is the single technology vulnerability. However, with the emergence of instant messaging, personal cell phone use, and other communication technologies, voice no longer is the only solution for communication for many users.

What role is the Assured Service SIP (AS SIP) playing in the military transition to VoIP?

AS SIP is primarily a specification to ensure different vendor implementations of SIP interoperate. Request for comment (RFC) 3261 and its associated RFCs allow for a lot of flexibility. Unfortunately, the flexibility also causes lack of interoperability between vendor SIP implementations. Commercially, the carriers place interworking devices between vendor solutions or limit the vendors in their network to a few and work out the issues internally. DoD uses open competition for products, and AS SIP allows those products to interoperate. In addition to interoperability, AS SIP also provides priority and preemption features that are not available in commercial products, in order to address the military unique needs where some command and control calls are more important than other calls.

However, the requirements in AS SIP related to priority and preemption are a small percentage compared to the requirements included for interoperability and information assurance. This leads to the last aspect of AS SIP. At the time that the AS SIP specification was written, commercial SIP signaling was mostly sent in the clear with no encryption, authentication or integrity. DoD could not accept the IA risk of using SIP in this manner and worked with our customers, the standards community and the vendors to secure the SIP signaling. This approach is now being used commercially to provide an interoperable secure approach. In summary, AS SIP provides interoperability, priority and preemption, and secure signaling for DoD voice and video communications.

What are some of the other VoIP-related initiatives underway at DISA and elsewhere?

Within DISA, Network Services is the lead organization for all voice related projects. DISA works with OSD and the services to ensure all voice related projects are synergistic through biannual UC conferences. NSA is pioneering secure sharing of information through their Suite B program, which we plan to leverage with wireless devices in our classified VoIP environment. Additionally, the executive agent for theater joint tactical networks continues testing UC products with a specific focus on how to use them in the tactical network while connecting back to the strategic backbone provided by DISA.

“This results in changes to the testing requirements, which means any vendor being tested for compliance had also better be able to prove that it has closed off any vulnerabilities. This is challenging, because these vulnerability mitigation changes can be required in a cycle that sometimes takes just weeks, and often occur during an APL testing cycle.”

To counter these vulnerabilities, global communication providers like Segovia, now Inmarsat Government – US, rely on extensive knowledge of government requirements and procedures to integrate COTS equipment with government certified encryption components and provide remote VOIP, as well as video and data reach-back communications solutions. This industry expertise makes it possible for military customers to reap the full benefits of VoIP, while being assured that operations are in compliance with the most rigid of security requirements and can be delivered across any technology platform via a secure network.

“Layering applications over an IP-based secure satellite and terrestrial network, with nearly 100 percent global broadband coverage, allows us to fully support the mission success of our customers, said Bill Raney, senior vice president of federal programs at Inmarsat Government – US. “In fact, within our network backbone, and extended to the customer edge, are quality of service levels that we implement to allow prioritization of time-sensitive IP traffic based on application requirements. That enables end-to-end service delivery across the LAN, WAN and satellite links, as well as secure, reliable point-to-point communications between anyone who has access to the Internet, cellular networks or to landline phones,” Raney continued.

The booming popularity of smartphones, with their mobile access to the Internet, has also expanded the ranks of potential VoIP users and uses. But security is a concern, as is true throughout the expanding universe of smartphone products. “Unfortunately, some deployments are occurring before the devices have been modified to fully encrypt the voice media stream and to have their vulnerabilities fully assessed and mitigated,” Gueldenpfennig said.

PRECEDENCE AND SECURITY

Another important company in the field is Ultra Electronics DNE Technologies, whose products include PacketAssure, an intelligent Layer 2 switching solution that guarantees that critical traffic will arrive on-time, regardless of network congestion. PacketAssure’s eight classes of service queues and network processors can police, mark, redirect or block packets before queuing, delivering assured LAN switching at line speed over Gigabit Ethernet links.

Such capabilities are critical in light of the differences between military phone systems as they have developed over the years and the world of IP, said William Berger, director of sales for Ultra DNE.

“I’m talking over a VoIP phone now,” Berger said in a recent interview. “If the lines were busy, either our call

would be degraded or blocked. But if I was a senior officer and needed to talk to the Pentagon, and had the right code, in a military network I could use priority and precedence. If I know I have enough bandwidth for five calls, I only allow five calls onto the network. I don't try to go with more bandwidth than I have. So I allocate how many calls to have, and I also have a prioritization scheme, so that if we're talking and someone more important comes on the line and they need to get access, and they get a busy signal, they can enter their code and the system will drop our call.

"Once you go to the IP world, it is great on cost savings and convergence, but you also then add some risks to the network, in that certain packets are more important than someone's email. The email will re-transmit, but if you're talking, there isn't the luxury of being able to re-transmit. So our call would be degraded if we were in congestion," Berger added.

"You have to make sure that you have absolute predictability," he continued. "Cell phones have made us a bit more accepting of dropped calls. If you had moved everyone to VoIP 15 years ago, you probably would have gotten more complaints. But because people have become accustomed to lower quality voice over cell phones, and to occasionally having dropped calls, then it's not as shocking as when it happens on your traditional desk phone. But in the military world, in a tactical situation or perhaps a key strategic meeting, that's not when you want to see your calls dropped."

Security represents another formidable challenge, Berger added. Unlike traditional phone systems, in which a particular number is essentially tied to a specific location, VoIP phones can be connected anywhere there is an Internet connection, and so do not have the protection of physical security

"I can plug in my VoIP handset or PC anywhere, so how do you know whom you're talking to? As a result, you have to get into authentication, public key infrastructure (PKI) and all of the other things that the military has in their environment. How do you get the keys or devices out to users? That's been the complex part. How do you make sure that it is the right person, and there is no one in the middle? So getting the right PKI keys out to users at the far end of a bandwidth-disadvantaged network is tough, especially when you are talking about every handset. A lot of that is automated, but you have to get it right," Berger said.

"It all comes down the security you want to have in your network versus convenience," he added. "If you don't know what a packet is, do you allow it through the network? The problem is that if you become too draconian, people can't call you. But if you make it too open, someone is now hacking your voice system."

Another company with a growing presence in this field is Quintron, which offers the DICES VoIP system. The White Sands Missile Range, N.M., this year selected DICES VoIP as its new voice system. ★

Contact Editor Harrison Donnelly at harrisond@kmiimagroup.com.
For more information related to this subject, search our archives at
www.MIT-kmi.com.