WIRELESS

Voice Over WLAN: The Current State

Paul B. Robinson, PhD and David H. Yedwab

All the key standards will be in place by the end of next year. The market is ready to take off.

In our globalized world, workers travel near and far to perform their business tasks. They roam from office to office within the enterprise, or they hop on a plane and travel across the continent. Laptop computers, cell phones, and network-enabled PDAs are commonplace.

On the home front, the Centers for Disease Control and Prevention just released a study based on a survey of 13,056 households. CDC found that 25 percent of Americans between the ages of 18 and 24, and 30 percent of adults 25 to 29 live in cellphone-only households; overall, 233 million Americans are cell phone users. The country and world at large are becoming unstrung.

Today's workers may be working at their desk (desk-bound), collaborating with others who may be on site (knowledge workers/campus nomads), or off-site (road warriors/teleworkers). Most enterprises have most, if not all, of these types of workers. In some enterprises, as many as 80 percent of employees are mobile somewhere on-site during the business day.

To be maximally effective and productive, these on-site mobile workers require and expect on-demand connectivity with critical business assets, be they organizational assets (systems, knowledge and processes); other on-site personnel including employees, on-site consultants, suppliers and customers who have been granted secure guest access to network resources; as well as location information for physical assets. With location capabilities, businesses have the ability to track assets and people and integrate that location knowledge into business processes.

Wireless LAN (WLAN) technology, commonly referred to as Wi-Fi, was developed to enable all these things. WLANs are rapidly becoming a fixture in the enterprise. For example, Infonetics Research notes that worldwide WLAN hardware revenue hit $697.2 million in 3Q06, up 19 percent from 2Q06. In addition, many enterprises are simultaneously deploying voice over IP (VOIP) systems in hopes of gaining expanded telecom features and lower costs. Infonetics expects worldwide IP-PBX revenue to hit $1.9 billion in 3Q06, up 8 percent from 2Q06. Revenues for 2009 are forecast to reach $11.1 billion and $3.8 billion, respectively, in the WLAN and IP-PBX markets.

Improved knowledge worker productivity through mobility is the obvious objective for the deployment of Wi-Fi capability—both for data and, increasingly, for voice. The proper integration and deployment of these two technologies, called voice over WLAN (VoWLAN) or voice over Wi-Fi (VoWi-Fi), enables the delivery in a campus environment of communications-enabled business processes, and can provide superior, more cost-effective indoor coverage compared with cellular.

All key IEEE standards supporting VoWLAN will be in place in 2008, which is also when the Wi-Fi Alliance's (WFA) enterprise voice certification program will be in operation. Today, the leading vendors engaged in setting those standards are supporting successful VoWLAN deployments in enterprises and vertical markets such as hospitals, hospitality, retail stores, education and general industrial settings including manufacturing, warehousing and distribution facilities, and even libraries.

Within the enterprise environment, VoWLAN supports the following generic business goals:

(1.) Drive revenue by providing an exceptional customer experience.

(2.) Meet customer needs efficiently and effectively (i.e., do the right things the right way to control cost and enhance customer satisfaction).

(3.) Maintain a safe and secure environment.

In addition, the VoWLAN system must seamlessly integrate with the organization's current PBX, and offer employees full PBX feature set availability, desk set voice quality, and ease of use. IT managers also want systems with acceptable manageability, security, reliability and scalability. The sidebar ("Some VoWLAN Cases") highlights some VoWLAN deployments within the key verticals.

Why VoWLAN?

It's certainly reasonable to ask why VoWLAN outranks cellular as today's solution of choice.

Paul B. Robinson, PhD and David H. Yedwab are founding partners at Market Strategy and Analytics Partners.

Cellular networks were designed to provide wide area outdoor service to large numbers of users. We have all experienced its spotty coverage, especially in buildings. The cellular network was simply not built either to penetrate buildings with voice or high speed data, or to handle high-density in-building traffic that requires many smaller cells. WLANs, on the other hand, were specifically designed to replace data cables and provide mobile services in the workplace and at home.

Both cellular and WLAN have evolved to serve additional needs. But neither alone provides the best solution for the mobile executive who wants one device with one phone number that is fully integrated into the corporate telecom network for always-on, anywhere connectivity.

However, no U.S. carrier has announced a dual-mode service (termed FMC for fixed/mobile convergence)—one that combines Wi-Fi and cellular—for businesses. On the contrary, some carriers have discouraged the spread of converged services by disabling or barring Wi-Fi functions on the phones they sell. And in the case of T-Mobile's dual-mode HotSpot at Home service, expected to be rolled out nationwide this summer, the initial cellular-to-WLAN handoff fee is $20

Neither cellular nor WLAN alone is sufficient for most mobile users

Some VoWLAN Cases

Vendors such as SpectraLink, now a part of Polycom, have had success with VoWLAN since 1999 in key verticals such as health care, hospitality, manufacturing and retail. In these markets, the business case for employee mobility has long been documented. The following cases demonstrate how wireless telephone systems have long helped make employees more responsive, accessible and productive.

Health Care

The University of Southern California University Hospital (USCUH) is a private, 293-bed research and teaching hospital located near downtown Los Angeles. The hospital has been using VOIP-based wireless telephones since early 2002 and has deployed more than 275 handsets. The handsets operate with radio signals well below industry-accepted levels for hospital environments and avoid interference with sensitive electronics found in many biomedical devices used for patient care.

Because the wireless telephones are integrated into the hospital's existing telecom and wireless communications backbone, the hospital gains significant savings on future telecommunications resources as data traffic is migrated to the network. Additionally, moving, adding and changing telephone extensions are made easier for telecommunications managers by the quick transfer capabilities of wireless telephone extensions for new and relocated hospital staff.

Hospitality

In August 2005, the management of Pelican Bay, Grand Bahamas resort decided to deploy Wi-Fi-based telephones. The wireless handsets allow resort employees to communicate from anywhere on the property using the resort's existing PBX system and WLAN, accessing features such as dial-by-extension, caller ID, call transfer and multiple line appearances. Additionally, the wireless telephones provide two-way text messaging capabilities, allowing integration with hotel management applications such as CRM, security and HVAC systems.

Staff—including management, bellmen, maintenance and security employees—share 16 handsets in the 24-hour, multi-shift work environment. Several handsets provide a push-to-talk feature, allowing users to communicate by broadcasting over shared channels similar to traditional two-way radios.

Response times to guest inquiries improved dramatically. Staff can now locate each other on the first try from anywhere on the property and communicate privately on sensitive issues. Coverage is provided throughout the facility, including the adjacent Lucaya marketplace.

Retail

GIANT Food Stores have deployed Wi-Fi handsets in 98 stores in Pennsylvania, Maryland, Virginia and West Virginia. The installation in each store consists of 10 wireless telephones per store, mainly used by store management and department heads. Inbound telephone calls are sent from the store's PBX through a digital gateway to the Ethernet LAN and transmitted via radio waves from the wireless LAN access points to the individual handsets. The installation process for all 98 stores was completed in less than three months.

Customer service and operational efficiencies have been greatly improved. Customers receive more attention on the shopping floor and spend less time waiting in the checkout line for price checks and cashiers. With the wireless telephones and text messaging capabilities, cashiers can now select a function directly from their handset to send a non-disruptive text message to a particular department head's wireless telephone for a price check or to a front-end clerk for a cash run without leaving the register.

Store management has also seen a dramatic increase in the time they are able to spend on the selling floor (up from 40 percent to more than 75 percent), ensuring the store is running smoothly□

Two of the four key standards for QOS and security are in place

per handset per month, so there's no free lunch there, either.

FMC is clearly coming, but the future is a ways off. In December 2006, Frost & Sullivan forecast that single-mode VoWLAN device shipments will dominate the marketplace in North America through 2010. Moreover, even in 2009, single-mode shipments will be twice as large as that of dual-mode devices.

Michael Finneran's column, "Clearing Up Fixed-Mobile Confusion" (*BCR*, May 2007), provides an informative discussion of FMC solutions. In conclusion he notes: "If anything, we should be looking beyond simple voice calls to solutions that mobilize the entire user experience, including text messaging, paging, email, and network access, rather than just a sleight-of-hand trick with a phone call." Today, single-mode VoWLAN handsets offer PBX integration, text messaging and push-to-talk (PTT) capabilities, as the sidebar cases indicate. With such productivity benefits available now, why wait?

VoWLAN is a proven technology that has been in place for years. But a successful implementation requires that certain unique aspects be taken into account. When implementing both VOIP and Wi-Fi over one network, performance, quality of service (QOS) and security must be taken into consideration. The combination of these unique applications often means that end users must work with multiple vendors to find a best-in-class solution. Fortunately, the industry has come together through organizations such as the IEEE and the WFA to define performance standards and address interoperability concerns.

Workplace VoWLAN Requirements

Voice and data traffic flows have different network requirements. Latency and jitter associated with the transmission of bursty data packets becomes a major issue for voice transmission, which requires a steady stream of audio packets in order to ensure a satisfactory user experience.

In addition, most data applications can withstand some network packet loss because TCP/IP supports retransmission of lost packets for reliable delivery. Retransmissions, however, can introduce perceptible delay in real-time communications by breaking the flow of a voice conversation, thereby degrading audio quality.

Moreover, VoWLAN deployments must anticipate voice clients' mobile nature. This means that QOS must support a user's need to roam throughout a building and campus while on an active call. As the user roams, the WLAN access point (AP) must be able to seamlessly hand off the client device to another AP without degrading voice quality or dropping the call. Bottom line, VoWLAN must be transmitted with acceptable levels of latency, packet loss, jitter, and AP handoff. The essential QOS performance measures for VoWLAN applications are shown in Table 1.

Four IEEE standards are central to supporting the QOS and security requirements of enterprise VoWLAN deployments. Two of these four—802.11e (QOS) and 802.11i (security)—are already in place.

802.11e (ratified in 2005) has led to the Wi-Fi Alliance (WFA) QOS specification consisting of the following three elements:

- Wi-Fi Multimedia (WMM), which describes four relative priorities for the Wi-Fi traffic: voice (highest), video, background, and best effort (lowest). Prioritizing the forwarding of voice traffic minimizes the latency, packet loss and jitter that affect voice quality.
- WMM Power Save (PS) extends Wi-Fi client battery life. The client device can "doze" between packets to save power, while the AP buffers downlink frames. The application chooses the time to wake up and receive data packets to maximize power conservation without sacrificing QOS.
- The forthcoming WMM Admission Control (AC) mechanism (expected early 2008) lets APs reject calls when the call load exceeds available capacity. Without such call admission control, oversubscription would introduce excessive collisions and packet loss, which would degrade audio quality for all voice transmissions associated with the overloaded access point.

Call AC partially addresses roaming latency. The issue of latency induced by roaming is also being addressed by upcoming standards 802.11k and 802.11r, both of which should be available by early 2008 as well (see below).

Prior to standards approval, equipment vendors implemented proprietary QOS mechanisms for supporting VoWLAN. Before 802.11e, the de facto standard for voice QOS has been SpectraLink Voice Priority (SVP), a proprietary QOS mechanism, created by SpectraLink (now part of Polycom), that leading AP vendors (i.e., Aruba, Cisco, Meru, Motorola/Symbol, Trapeze and several others) have adopted. SVP accomplishes the same things as the three WFA QOS elements described above, although optimized for SpectraLink handsets.

The other key standard that's complete is 802.11i, which was specified as Wi-Fi Protected Access 2 (WPA2) by the WFA; this security stan-

TABLE 1 Essential QOS Performance Measures For VoWLAN Applications

Latency	(Time taken to get information through a network)	Maximum latency < 50 ms
Packet loss	(Packets lost due to collisions or retransmissions)	Maximum packet loss < 1%
Jitter	(Variation in latency for different packets)	Maximum jitter < 5 ms
AP handoff	(Time client takes to reassociate/reauthenticate at Layer 2)	Maximum AP handoff < 50 ms

dard has been in place since 2004. It includes intelligent security protocols, such as pre-authentication, to reduce roaming time by enabling the handset to authenticate with neighboring APs before roaming. In enterprise mode, Advanced Encryption Standard (AES) is used for all traffic. This entails:

- Using IEEE 802.1x and Extensible Authentication Protocol (EAP) to prevent unauthorized network access, by verifying network users through an authentication server.
- A technique called Robust Security Network (RSN) for keeping track of associations.
- AES-based CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), to provide confidentiality, integrity and origin authentication.

The two standards in process, mentioned briefly above, are:

- 802.11k (finalization expected 2007): This Radio Resource Management protocol is intended to improve the way traffic is distributed within a network. In a WLAN, each device normally connects to the AP that provides the strongest signal. With 802.11k, if that AP is loaded to its full capacity, the WLAN client would connect to one of the underutilized APs, improving overall throughput, even though the signal may be weaker.
- 802.11r (Finalization expected by early 2008): This fast roaming protocol allows a wireless client to establish stringent security (802.11i) at a new AP before the call is actually handed off, which minimizes connectivity loss and application disruption. The objective is sub-50ms AP handoff (the interval that is detectable by the human ear) while maintaining a secure connection. In the interim, Aruba, Cisco and Meru, for example, have developed proprietary methods to deal with the shortcomings addressed by 802.11r.

WLAN RF Infrastructure Alternatives

The selection of WLAN technology has significant impact on the overall configuration and layout of the WLAN infrastructure. WLAN capacity is mainly determined by the number of available non-overlapping channels and the density of deployed APs. If the channels do overlap, RF interference, packet collisions and retransmissions will result in overall performance degradation. Consideration of AP configuration options is a must before performing a site survey and deploying a VoWLAN infrastructure.

In addition to the existing 802.11a/b/g standards, Draft 2.0 for the higher-bandwidth 802.11n standard was approved in March 2007. Some enterprise vendors have already announced Draft 2.0-compatible products and will begin shipping in 3Q07. Almost everyone will have a Draft 2.0-compatible product by 4Q07 or the early part of 1Q08 at the latest. All four standards are summarized in Table 2.

In the 2.4 GHz band where 802.11b/g APs operate, there are three non-overlapping channel #'s—1, 6 and 11—for North America. There are four non-overlapping channels (#'s 1, 5, 9 and 13) in European countries. However, in the 5 GHz band (802.1a/n APs), all 23 channels are technically considered non-overlapping, since there is at least 20 MHz of separation between the center frequencies of each channel. However, since there is some frequency overlap on adjacent 802.11a channel sidebands, RF engineers leave at least one cell separating adjacent channels and two cells separating the same channel.

The 802.11a standard is approved in the U.S., Japan and EU. Lack of worldwide regulatory support for use of the 5 GHz band has dampened adoption.

Since 802.11a/g APs operate at up to 54 Mbps,

Lack of worldwide regulatory support for the 5-GHz band has hurt 802.11a adoption

TABLE 2 Infrastructure Standards Comparison

Specifications	802.11b	802.11g	802.11a	802.11n Draft 2.0
Approved	July 1999	June 2003	July 1999	March 2007
Frequency Band	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz / 5 GHz
Channel Width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Supported data rates (Mbps)	1, 2, 5.5, 11	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54	6, 9, 11, 12, 18, 24, 36, 48, 54	6.5 Mbps–600 Mbps
Typical throughput (Mbps)	4–6	25 when .11b is not present	25	~100
# channels/non-overlapping	13/3	13/3	23/23	26/26 at 20MHz
Transmission type	DSSS/CCK	DSSS/CCK and OFDM	OFDM	MIMO/ODFM
Typical range per AP indoor/outdoor (M)	~35/110	~35/115	~30/100	~70/160
Impacts				
Frequency congestion	Med-High	Med-High	Low	Lowest
Signal propagation	Better	Good	Fair	Best
Site planning flexibility	Least	Moderate	Better	Best
Call capacity	Good	Better	Better	Best
Market penetration	High	Moderate	Low	None

The Wi-Fi Alliance is developing a voice certification program

while 802.11b reaches its limit at 11 Mbps, the former can potentially support many more voice calls. The forthcoming 802.11n standard, which promises data rates up to 600 Mbps, will significantly increase voice and data capacity. Realistically achievable data rates are lower, however, and range from the mid-20 Mbps for 802.11a/g to 4-6 Mbps for 802.11b and about 100 Mbps for 802.11n.

Higher-frequency RF signals used by the 5 GHz band do not propagate as well through air, or through obstacles. This typically means that more APs will be required to provide the same level of coverage on 802.11a (or .11n when operating in the 5-GHz band) than with 802.11b/g, though in high-density deployments this factor is significantly mitigated.

Because the overall bandwidth is dynamically shared across all the users on a channel, 802.11b cards can operate at 11 Mbps, but will scale back to 5.5, then 2, then 1 Mbps (also known as Adaptive Rate Selection), if signal quality becomes an issue. The ability to drop to lower data rates is common to all the WLAN standards as environmental interference challenges communications.

The 802.11g modulation scheme supports data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. When operating at 1, 2, 5.5 and 11 Mbps, 802.11b characteristics apply, such as when using .11g with protection mechanisms needed to support .11b users. In this case, call capacity is greatly reduced.

The 802.11a protocol supports maximum raw data rate of 54 Mbps. The data rate is reduced to 48, 36, 24, 18, 12, 9 then 6 Mbps if required.

The emerging 802.11n specification differs from its predecessors in that it provides for a variety of optional modes and configurations that dictate different maximum raw data rates. An 802.11n WLAN may well become the default mobile triple-play LAN for voice, video and data. One caveat, however: unifying wired LANs and 802.11n WLANs requires that the wired LAN support Gigabit Ethernet. You'll definitely swamp a 100 Mbps wireline Ethernet connection with 802.11n.

Some of 802.11n's key features are:

- Performance ranges from as low as 6.5 Mbps to 600 Mbps, with typical throughput in the range of 100 Mbps.
- Based on MIMO/OFDM. Multiple Input/Multiple Output or MIMO harnesses a technique known as space-division multiplexing, which improves performance by parsing data into multiple streams transmitted through multiple antennas. Orthogonal Frequency Division Multiplexing (OFDM) is a digital multicarrier modulation scheme, which uses a large number of closely-spaced orthogonal sub-carriers.
- Effectively doubles data rates by doubling channel bandwidth from 20 MHz to 40 MHz, though 20-MHz channels may still be used in the 2.4-GHz band.
- Supports dual spectrum; can use 2.4 GHz for data, 5 GHz for voice, for example.

Status Of WFA Enterprise Voice Interoperability Certification

The WFA is developing a voice certification program. The work is progressing in two phases: (1) consumer, which is expected to launch later in 2007 and (2) VoWLAN in the enterprise, which is planned to be available during 1H08.

WFA certification testing programs are generally based on the IEEE standards. The Alliance does not test for compliance to those standards; they test for interoperability among products. The three pillars of the enterprise voice certification program will likely rest on interoperability across the physical layer 802.11a/b/g/n, QOS (WMM, WMM-PS) and security (WPA2).

The WFA enterprise voice certification will include WMM-AC (Admission Control), the missing QOS element, as well as those elements of 802.11k and 802.11r standards-in-progress bearing on QOS and security. In addition, products that become enterprise voice certified will also have to meet performance minimums such as those described in the section above on "Workplace VoWLAN Requirements."

The WFA has certified about 3,500 products appearing in a searchable database on their website, www.wi-fi.org. Included are about 100 voice devices, the bulk of which are dual-mode (Wi-Fi and cellular) consumer handsets. These devices are certified for basic Wi-Fi interoperability, the same as a data client, but not specifically for voice.

In the absence of an enterprise voice certification program and the missing Admission Control QOS element, vendors have relied on their own programs. Two such proprietary programs are Cisco's Compatible Extensions Program for WLAN Client Devices (CCX) and Polycom's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program. Cisco and Polycom lead the single-mode Wi-Fi handset market, according to Infonetics Research.

A Solution Whose Time Has Come

Enterprise adoption of both VOIP and WLAN technologies, coupled with the continued growth of anywhere/anytime business is a sign that a business case can be made for placing VoWLAN in the enterprise and on the campus. Table 3 shows three "waves" of workplace wireless evolution, and shows that we're currently at the end of the second or Convergence Wave, and will enter the Open Standards Wave in early 2008.

In his March 2006 *BCR* article (pp. 48–53), Greg Collins of the Dell'Oro Group calculated the Internal Rate of Return (IRR) of a 1,000-phone greenfield VoWLAN deployment at 11 percent

TABLE 3 The Workplace Wireless Evolution

Core Issues	Proprietary Wave	Convergence Wave	Open Standards Wave (2008 And Beyond)
PBX Interface	Analog/Digital	Analog/Digital/IP	IP
RF Infrastructure	Proprietary	Wi-Fi (802.11a/b/g)	Wi-Fi (802.11a/b/g/n), DECT, Mesh, WiMAX
Security	Proprietary	WPA2	WPA2 + 802.11r
Enterprise Voice QOS Certification		SVP	WMM+PS+AC
New Markets	Verticals	Enterprise	Enterprise and SMB
Price/User	$1,200+	$600+	$400+

after three years, with breakeven achieved midway through the second year. With a voice-capable WLAN already in place, deployment costs obviously drop.

Key assumptions were that the cost of the Wi-Fi handset was $400 per user (or 57 percent of the total deployment cost), with productivity gains/cost savings at $30 per month per user. These savings are not out of reach, just considering the cost avoidance in office cellular usage, which Collins estimates as $18–$30 per user per month.

VoWLAN technology is available and deployable today with acceptable cost/benefit tradeoff for those enterprises with strong in-building or on-campus needs for mobile voice communications. The evolution of the market will only make such implementations more valuable in the future. FMC, when broadly available, can use the already-deployed VoWLAN infrastructure to provide great in-building capability with little incremental investment, except for the handsets□

Companies Mentioned In This Article

Aruba (www.arubanetworks.com)
Cisco (www.cisco.com)
Meru (www.merunetworks.com)
Motorola (www.motorola.com)
Polycom (www.polycom.com)
T-Mobile (www.t-mobile.com)
Trapeze (www.trapezenetworks.com)