Alcatel·Lucent

TECHNOLOGY WHITE PAPER

Overcoming VoWLAN Challenges

VoWLAN in the enterprise is poised to start living up to its original promise. Reaping the reward of Voice over WLAN requires an in-depth understanding of this complex technology. This white paper surveys the challenges IT professionals will encounter as they prepare to roll out VoWLANs, and documents the ratified and emerging standards and proprietary mechanisms that help ease VoWLAN deployments.

Table of Contents

Executive Summary

A few years ago, Voice over WLAN (VoWLAN) appeared to be just another overhyped wireless technology that never lived up to analyst expectations. True, it found a welcome reception in vertical segments like retail and healthcare, but it failed to make much of an impression on corporations and consumers.

A few years later, and VoWLAN is poised to start living up to its original promise. Vendors have beefed up the feature sets of their solutions. They're also addressing enterprise-class issues, like end-to-end quality of service and fast roaming, which lets end-users carry on conversations while they're on the move, without having to deal with degraded voice quality or dropped sessions.

At the same time, the IEEE is hard at work on a slew of VoWLAN standards — and vendors are adopting them as they're ratified. These new and emerging standards address everything from access control and call handoff to security and QoS.

Equally important, market projections this time around are based on steadily climbing sales and revenues that are already doubling from year to year.

An enhanced and extended technology; a series of business-class specs and standards; and market activity on a slow boil: It's time for IT professionals to start taking VoWLAN seriously.

This white paper will help them do exactly that — and more. It investigates the numerous complex challenges facing medium/large enterprises, that must be overcome to achieve a successful VoWLAN deployment. And there's no shortage of concerns and considerations. Essentially, VoWLAN runs voice over a wireless network that was built to carry data, which is far more forgiving of latency, jitter, retransmissions, dropped packets and a host of other conditions — any one of which can wreak havoc with voice transmissions.

There are no easy answers to these problems, but IT professionals that understand the issues fully won't be surprised or defenseless if and when they crop up.

This white paper thoroughly investigates VoWLAN challenges, starting with coverage requirements and site surveys and wrapping up with a review of alternative architectures.

Introduction

Early, enthusiastic predictions about the success of Voice over WLAN (VoWLAN) have fallen wide of the mark. A few vertical industries are putting the technology to work, but it's made little or no impression on the enterprise and consumer segments.

The situation is in flux, however. A number of vendors are enhancing their VoWLAN solutions: adding features, extending their architectures, and adopting new standards. Meanwhile, the IEEE and other industry organizations are moving ahead with emerging standards that help ensure fast roaming, conserve power, and tighten security.

In addition, vendors are starting to deliver dual-mode handsets that switch between the wireless and cellular networks. These enable VoWLAN to play a role in Fixed Mobile Convergence (FMC) solutions. Dual-mode devices are still expensive, but as prices drop, it will be easier for IT professionals to build a VoWLAN business case.

The widespread adoption of VoWLAN (also known as Voice over Wi-Fi, or VoWi-Fi) will be gradual, with the technology likely to go mainstream within two to three years. This timetable is reflected in the very healthy growth analysts expect to see across the wireless industry through the end of the decade.

According to Infonetics Research, the worldwide Wi-Fi phone market increased 116 percent between 2004 and 2005 and is projected to more than double in 2006 and every year thereafter until 2009, with nearly triple growth seen at times. Infonetics' latest report, "Wi-Fi Phones Biannual Worldwide Market Share and Forecast," predicts that the worldwide market will reach $3.7 billion by 2009 (up from $125 million in 2005). The "real growth", according to Richard Webb, directing wireless analyst with Infonetics, will come from "dual-mode Wi-Fi/cellular handsets."

That's good news for vendors of VoWLAN gear, but enterprise IT managers and service providers may have another point of view. With VoWLAN looming on the horizon (and solutions already available) they don't have much time to get ready for rollouts. It's already clear that IT and telecom professionals will have to grapple with a bewildering array of VoWLAN options. In addition, VoWLAN itself is a tricky technology to implement, especially when it comes to RF planning, mobility and quality of service (QoS).

What these professionals need (and what this white paper delivers) is a vendor-agnostic survey of VoWLAN challenges. Understanding these issues is a critical aspect of matching specific solutions to particular requirements.

Given the effort and focus IT professionals will have to invest in understanding VoWLANs, it's only natural that they want to know what benefits the technology offers. The simplest way to address this question is by taking a quick look at some of the vertical industries already putting VoWLAN to work:

- *Healthcare:* Doctors, nurses, and other healthcare professionals are always on the go, yet they also must remain reachable. VoWLAN ensures that they're always available via the hospital or healthcare organization's Wi-Fi network. This is particularly important since cellphones, which can interfere with a variety of equipment, are forbidden in many areas of a medical facility. In case of a medical emergency, VoWLAN can mean the difference between life and death.
- *Retail:* Sales personnel currently use wired or cellular phones to check inventory and order status at the warehouse. With a VoWLAN in place, employees can make these calls over the company's WLAN, reducing telecom costs significantly. A VoWLAN also enables personnel to utilize existing dialing/paging features of the PBX, increasing productivity and further reducing costs.

Existing corporate WLANs, which were mainly deployed to carry data traffic, will have to be reassessed and, in some cases, reinstalled in order to support voice. As noted, significant challenges must be overcome before Voice over WLAN can be used effectively in the enterprise:

- *RF Coverage and planning:* Most current data-centric WLANs have been designed for long range, low cost. VoWLAN, however, requires pervasive RF coverage wherever the mobile user may go. RF Site Surveys and simulation tools will play a key role in the planning stage.
- *Seamless mobility:* VoWLANs allow voice users to roam without restriction. Implementing this capability involves Layer2/Layer 3 roaming, in a very fast manner, and with strong security all the way.
- *Quality of Service (QoS):* Maintaining call quality and ensuring end-to-end QoS is not a simple matter. IT professionals will need to understand and deploy the recent 802.11e QoS standards and power-saving mechanisms. They also will need to map and extend QoS features across local and wide area networks.
- *Capacity:* Overburdened APs degrade overall voice quality and drop calls. These problems can be prevented using call admission control, load balancing, and other techniques.

- *Security:* Security is always an issue for IT professionals. It's even more of a concern when voice traffic is traveling over an airlink. Standards-based authentication and encryption (WPA, WPA2/802.11i) offer powerful protection. But other security concerns are not so easily addressed, including DoS attacks and other incursions, which require wireless IDS/IPSs and other safeguards.

As even this relatively short list demonstrates, successfully deploying a VoWLAN is a difficult, demanding undertaking. Furthermore, a VoWLAN is only one aspect of a company's communications infrastructure. As such, it will have to be integrated with other elements such VoIP; IP PBXs; or dual-mode services (DMS) that allow seamless roaming between VoWLAN and cellular networks, which calls for an in-depth knowledge of wireless, wide-area, and corporate networks.

As one of the leading network integrators worldwide, Alcatel-Lucent has firsthand expertise with the multivendor solutions deployed end to end to build complex, converged networks. Alcatel-Lucent also has extensive experience with both VoIP and legacy voice services. And as the primary architect of IMS and a driving force in the development of FMC solutions, Alcatel-Lucent has gained a deep understanding of the challenges that face today's IT professionals — and the appropriate solutions.

These capabilities also enable Alcatel-Lucent to offer a suite of professional services that can assist enterprises and carriers with any or all aspects of their VoWLAN initiatives.

VoWLAN Technical Challenges and Requirements

RF Coverage and Planning

Most current WLAN implementations were designed for data. Thus, they typically offer limited or spotty coverage in areas where users normally connect (for instance, desks, meeting rooms, reception). Also, applications like e-mail and Web browsing can tolerate marginal coverage for short durations and users are willing to reorient their laptops to obtain a better signal.

Wireless VoIP, on the other hand, requires pervasive coverage: complete, dense, and seamless RF coverage throughout the facility. In addition to normal working areas, places like elevators, stairwells, vending/cafeteria, and restrooms will need robust RF coverage in order to provide good quality, seamless voice service.

WLAN access points (APs) will need to be located so coverage cells overlap enough for voice users to roam without dropping calls. Proper placement will also enable high data rates, minimizing latency and providing enough capacity. APs normally operate at half or less of their maximum transmission power, creating smaller and denser coverage cells than those used for data-only deployments. This requires careful planning of AP power settings and RF channels to minimize interference from neighboring APs on the same or adjacent channels. In multi-story buildings, this represents a special challenge, as RF coverage needs to be provided between floors for stairs, elevators, or maintenance personnel working in ceilings, but at the same time addressing the interference between APs on different floors.

Typically, high-quality voice requires a minimum signal-to-interference ratio (SIR) of about 20 to 25 dB.

Signal-to-noise ratio (SNR) is another key variable that affects wireless voice quality and needs to be taken into account during planning and design. SNR is particularly important in locations with a great deal of electronic and RF equipment, such as healthcare facilities.

Besides SIR and SNR, other factors to be considered during design include throughput, capacity, and security perimeter (to avoid "spilling" RF outside the premises).

Site Surveys

Site surveys are essential to accurate RF planning and successful VoWLAN deployment. They can involve a number of methodologies and tools.

An RF site survey typically involves moving one or more APs while taking RF and network measurements (such as RSSI [received signal strength indicator], SNR, data rates, and retransmissions) throughout the facility. The collected data is then processed and analyzed, normally using specialized software, and a report is produced detailing the exact number and location of APs to be installed; antenna types and orientation; and channels and transmit power levels, along with coverage and performance information.

Spectrum analyzers also are used in the site survey to measure possible RF interference in the ISM (Industrial, Scientific and Medical) and UNII bands (2.4 GHz and 5 GHz) caused by cordless phones, microwave ovens, elevator motors, and other electronic equipment.

In addition, spectrum analyzers are used to reveal existing WLANs (rogue APs). Snapshots of narrowband or spread-spectrum bands also should be included in the survey report, with information detailing the source of interference.

Initial and periodic RF site surveys are a must when corporate policy calls for "0 percent coverage holes"; a building's RF characteristics vary throughout the coverage area; or significant RF interference exists. Note that a VoWLAN phone is expected to have the same QoS of a desk phone, not like a cell phone. We all expect dropped calls when using cell phones, but that will not be accepted at all for VoWLAN.

A VoWLAN site survey is a time-consuming activity. Specialized tools that automatically make the measurements, place them on the facilities map, and generate meaningful reports can make the process more efficient and accurate.

In many cases, the on-site survey can be complemented or even replaced by the use of predictive design simulation software, which offers a more streamlined and cost-effective approach to designing a VoWLAN. These tools take into account factors like physical environment, signal coverage, capacity, and interference. Some tools can even take direct wireless measurements, which can be used to calibrate and improve the simulation's accuracy.

A site survey may not always be necessary, however. Facilities with very simple and homogenous RF characteristics, such as the typical open office environment, may be able to use just the basic design guidelines normally provided by the WLAN vendor. One caveat: this approach is only possible with "self-healing" VoWLAN implementations that dynamically manage RF channel and power settings using real-time signal and interference measurements. If coverage or capacity problems arise, however, vendors of these advanced systems generally recommend adding more APs to the mix. This solution has several risks: Increases cost by adding APs, is unable to identify coverage holes it can't see (like on the perimeter of the building or caused by RF shielding/interference), and increases the possibility of excessive (automatic) adjusting of AP settings (reducing their ability to handle any traffic).

Finally, some innovative WLAN implementations eliminate cell-based planning by deploying single-channel blankets throughout a facility, using clever proprietary mechanisms to overcome interference and ensure some time-based access to the medium. Obviously the RF planning for these solutions is very simple; though again, they require very dense AP deployments to provide seamless coverage and adequate capacity.

Seamless Mobility

As VoWLAN users roam throughout the enterprise or a "hot zone," their calls will be handed off to multiple APs. If these APs belong to the same IP subnet, this handoff is performed at Layer 2; if the move is across subnets, the handoff is at Layer 3.

Roaming between APs inevitably involves some delay or *latency*. In a voice call, this latency should be less than 50 milliseconds; otherwise, the connection will be dropped or the call quality will severely degrade.

Layer 2 roaming latency is mainly due to three processes: scanning, reassociation, and reauthentication. Using current standards-based mechanisms (active scanning, 802.11F Inter-Access Point Protocol, and 802.1x authentication), handoff latency can vary from a few hundred milliseconds up to several seconds, clearly unacceptable for voice.

The most time-consuming process is 802.1x, which requires the mobile device to be reauthenticated with the RADIUS server every time a call is handed off between APs. This can take a few seconds.

In order to reduce latency to acceptable levels, vendors of centrally controlled WLANs have implemented several proprietary mechanisms. Some of these employ "pre-authentication" techniques, in which the controller distributes security/keying information, the cached Pairwise Master Key (PMK), to neighboring APs. Other schemes tunnel all 802.1x authentication (and all other) traffic from the APs up to the controller or switch so it can centrally and rapidly manage the mobility between APs.

With Layer 3 roaming, the mobile device must request and obtain a new IP address from a DHCP server, which again take several seconds. In order to avoid that delay, centralized architectures use various proprietary Mobile IP or Proxy ARP/IP tunneling techniques that enable the client to keep existing sessions and connectivity on the new subnet without having to actually change its IP address.

The IEEE is working on several emerging 802.11-based standards that will help achieve fast secure roaming. The main one is 802.11r (Fast Roaming/BSS Transition). It will be supplemented by 802.11i for pre-authentication and 802.11k (Radio Resource Management), which will enable the handset to make fast roaming decisions by prediscovering neighboring APs; their distances; and call capacities.

Until these standards-based solutions are ratified and implemented in commercial products (not before end of 2007 or beginning of 2008), proprietary centrally controlled schemes will remain the only option.

Quality of Service

Wired VoIP deployments have made it clear that call quality depends chiefly on the voice codecs used (such as G.711, G.729, or iLBC) and on end-to-end latency, jitter (variations in delay), and packet loss. VoWLANs are subject to the same end-to-end parameters. The main differences are that a WLAN relies on a shared airlink; uses different access mechanisms than wired Ethernet (CSMA/CA 802.11 vs. CSMA/CD 802.3), exhibits relatively limited bandwidth, and features higher packet-error rates and packet overhead.

WLAN QoS mechanisms are critical when voice and data share the same RF band. Data traffic typically consists of bursty transmissions and various-sized packets. Some of these can be very large (file downloads, for instance) and take more time to transmit over the airlink. This delays smaller, continuously transmitted voice packets, since all traffic contends for the shared medium using *collision avoidance*, and increases both latency and jitter.

QoS mechanisms rectify this situation by prioritizing voice over other traffic (data and video) and by providing voice with faster, more timely access to the medium.

Until recently there were no WLAN QoS standards, prompting some vendors to develop proprietary protocols. The most notable and widely deployed of these is SpectraLink Voice Priority (SVP), which has become a de facto standard and is supported by most WLAN infrastructure vendors.

SVP basically violates the 802.11 media access control (MAC) standard by assigning voice packets a *back-off value* of zero, which gives them absolute priority over other traffic. The downside is that if there are many wireless VoIP phones active on a single AP, there will be too many collisions. Moreover, the phones can monopolize available bandwidth and starve conventional data transmissions.

The IEEE ratified the 802.11e WLAN QoS standard in September 2005. The Wi-Fi Alliance has been certifying subsets of it that are being gradually implemented by handset and infrastructure vendors. Thus, proprietary mechanisms like SVP are likely to disappear.

802.11e basically defines two new medium access mechanisms: Enhanced Distributed Control Access (EDCA) and Hybrid Controlled Channel Access (HCCA). EDCA grants higher-priority traffic statistically faster access to the medium. It defines four access categories (ACs): voice, video, best effort and background. The applications and firmware on the mobile device map these ACs from user priorities defined in 802.1D standard (already in use), and consequently classify and prioritize packets bound for the Wi-Fi air link.

The voice AC is assigned the highest priority; packets are transmitted using the shortest *contention* and *arbitration windows*. This yields a higher probability that voice AC packets will be transmitted before lower-priority ones. Packets not assigned to a specific AC default to best effort priority.

HCCA is a centralized scheduling control mechanism that allows applications to reserve network resources based on their traffic characteristics (requests are sent by the client to the AP). HCCA provides a more parameterized QoS and better control of latency, scheduling, and bandwidth guarantees. It also allows a greater number of concurrent voice calls per AP than does EDCA.

The Wi-Fi Alliance launched the Wi-Fi Multi-Media (WMM) certification program in September 2004. It basically corresponds to the EDCA subset of the 802.11e standard. The alliance also has been working on the WMM Scheduled Access (WMM-SA) program, which will certify interoperability and compliance with the polling-based HCCA control mechanism.

There are, however, several hurdles to the widespread adoption of WMMSA. Most importantly, the lack of interest from WLAN infrastructure and handset vendors has forced the Wi-Fi Alliance to suspend WMM-SA certification. Also, applications and operating systems will need to explicitly support WMM-SA. Other difficulties are due to user-intervention requirements; lack of QoS fast roaming support; and limitations imposed by interference from other APs.

End-to-end QoS

In order to guarantee end-to-end QoS for wireless VoIP, different protocols and techniques need to be mapped and used jointly across the network. Applications and operating systems on client devices could use 802.1D and 802.11e/WMM to classify and prioritize voice traffic ahead of data and video. These devices also could connect to a voice-specific Service Set Identifier (SSID), or a wireless virtual LAN. The AP could map either WMM access categories or SSIDs to Layer 2 802.1p and (optionally) Layer 3 DiffServ Code Points (DSCP) tags before transmitting the packets over the Ethernet LAN. Some WLAN solutions can even directly recognize voice traffic flows and appropriately tag or retag packets and apply QoS mechanisms. The VoIP packets can then flow across different LAN, WAN, and IP backbones, where classes of services are based on 802.1p, DSCP, or

Multiprotocol Label Switching (MPLS) tags and different QoS (mainly queuing) techniques are used to prioritize voice packets over congested links.

Power Saving

Battery life for Wi-Fi phones, especially dual-mode (Wi-Fi/cellular) devices, is another key challenge to widespread VoWLAN deployments. Current talk and standby times for dual-mode handsets are far below those of cellular phones (something like 2/20 hours vs. 10/100 hours of talk/standby), though manufacturers and standards bodies are continuously working to improve Wi-Fi battery life. Next-generation devices are expected to attain more acceptable 5/70 figures. In general, in order to improve battery life, the Wi-Fi radio on the phone should wake-up for as short a time as possible. During a call, what will help most is the use of Unscheduled Automatic Power-Save Delivery (UAPSD). This enhanced power-saving mechanism, which significantly reduces the amount of time a station has to wake up in order to exchange frames, is part of 802.11e and was recently certified by the WFA as "WMM-Power Save."

Other helpful mechanisms include using higher data-rate protocols like 802.11g/a to transmit frames faster, thus reducing wake-up time. Transmit Power Control (TPC) also will be an asset, since it enables an AP to ask the client device to reduce its transmit power (thus reducing power consumption) when RF conditions are good enough.

During standby mode, which is where mobile devices spend most of their time, it is important to implement low-power techniques. Some are based on 802.11i/k/r to minimize the number of frames needed to be exchanged in order to maintain a WLAN association. Doing so results in more efficient and faster roaming. The proposed 802.11v "idle" mode also should help. Or Address Resolution Protocol (ARP) proxy techniques, which let the AP restrict the number of ARP packets sent to the client. Other creative mechanisms include automatically switching off the Wi-Fi radio when outside of predefined WLAN areas (for instance, using cellular location-based information).

Capacity and Call Admission Control

When planning a VoWLAN, network capacity is a crucial design parameter, since it determines the number of simultaneous calls that can be supported without sacrificing voice quality. Capacity depends on many factors, including the 802.11 standards and protocols that have been implemented, the specific RF environment, and the infrastructure and handsets being used.

Except for a few single-channel or array architectures, WLAN capacity is mainly determined by the number of available non-overlapping channels and the density of deployed APs. Aggregating several neighboring APs with non-overlapping channels increases capacity within a given area. If the channels do overlap, RF interference and packet collisions and retransmissions can result in overall performance being degraded instead of improved.

While 802.11b and high data-rate, backward-compatible 802.11g standards are currently supported by most Wi-Fi phones, they both operate in the 2.4-GHz frequency band and have only three non-overlapping channels, which can prove insufficient for high-density voice networks. In contrast, 802.11a operates at 5 GHz and offers anywhere from 8 to more than 20 non-overlapping channels, depending on a country's regulatory statutes. Thus, 802.11a supports higher-density AP deployment, mitigating the impact of co-channel interference and providing much higher system capacity.

In addition, although 802.11b/g radios cover a broader area than their 802.11a equivalents, this "advantage" is irrelevant in high-density deployments. As noted, APs need to operate at reduced transmit power mode (which translates into a smaller coverage area) in order to minimize co-channel interference.

What's more, since 802.11a or 802.11g APs operate at up to 54 Mbps, while 802.11b reaches its limit at 11 Mbps, the former can support many more voice calls. The exception is when using 802.11g with protection mechanisms needed to support 802.11b users, in which case call capacity is greatly reduced. The coming 802.11n standard, with data rates up to 600 Mbps, will significantly increase voice and data capacity.

Call Admission Control

Since VoIP codecs use relatively little bandwidth (the least efficient, G.711, consumes about 80 Kbps), an 802.11b AP could theoretically support up to 23 simultaneous calls. In practice, the high overhead and inefficiencies of contention-based 802.11, along with less than ideal RF and network conditions, reduce this number to 7 to 10, including moderate data traffic. If the number of calls exceeded the practical limit, the resultant MAC collisions and retransmissions would increase delay and degrade all voice communications.

All these reasons help explain why WLAN infrastructure vendors are implementing call admission *control* (CAC) mechanisms to limit the total number of calls an AP will allow. Subsequent requests are either rejected or redirected.

For now these mechanisms are basically proprietary, though some are ready to accept some traffic specification (TSpec) signaling from WMM-capable clients to admission control. Ultimately, WMM-SA-capable APs will only approve TSpec requests from clients when they have enough bandwidth and resources to meet the client's QoS requirements. Emerging standards like 802.11k and 802.11v also will assist handsets and infrastructure by enabling neighboring APs to take over some of the extra connections and thus share the load.

Security

Despite major advances in WLAN security standards and products over the past few years, security is still regarded by IT departments as the top challenge for WLAN deployments. Much of this feeling can be attributed to difficulties and doubts about optimally implementing available security solutions.

The first Wi-Fi security protocol, Wired Equivalent Privacy (WEP), quickly proved to be vulnerable to various attacks. In July 2004 the IEEE ratified the 802.11i standard, which provides a yet-to-be-hacked authentication and encryption solution. In parallel, the Wi-Fi Alliance launched Wi-Fi Protected Access (WPA) and WPA2 programs to certify parts of the 802.11i standard and validate interoperability between vendor products. WPA2 contains almost all 802.11i specifications; since March 2006 all new Wi-Fi certified products need to be WPA2-compliant. This will ensure that all new Wi-Fi and converged Wi-Fi/cellular handsets will support the strongest possible security standard; most first-generation handsets only support WEP.

In some cases enterprises or service providers (offering a hosted VoIP or FMC solution) opt to deploy upper-layer VPN solutions, typically based on IPSec, to protect voice communications end to end across LAN and WAN links, to overcome network address translation (NAT) issues, or simply to add to or replace 802.11 Layer 2 security. That, in turn, raises implementation challenges concerning availability and compatibility of VPN clients on mobile devices, performance and scalability issues, and potential difficulties recognizing and prioritizing voice packets because QoS tags have been encrypted (for example, in IPSec tunnel mode).

WPA and WPA2/802.11i implement robust authentication based on 802.1x, which prevents unauthorized access to the network (preventing a hacker from making free phone calls), and strong encryption (stopping hackers from eavesdropping on calls from the company parking lot).

There are, however, several other types of wireless attacks and security threats that are not mitigated by these standards or by use of VPNs. Denial of Service (DoS) attacks, which can easily bring down or degrade voice communications, "rogue" (unauthorized) APs, ad-hoc connections, and the like require the help of specialized wireless intrusion detection and prevention (WIDP) systems. These typically consist of distributed sensors (dedicated or incorporated in APs) that continuously scan traffic on all RF channels and a centralized appliance (again, dedicated or part of WLAN controller) that analyzes any unusual behavior, runs sophisticated detection algorithms, generates alerts, and detects and possibly prevents intrusions and attacks.

As mentioned, many enterprise IT managers are overwhelmed by the complexities of implementing end-to-end WLAN security policies. These challenges include choosing the right Extensible Authentication Protocol (EAP) and client for 802.1x authentication; deploying and managing certificates and public key infrastructures (PKI); and selecting, integrating, and managing VPN and WIDP solutions. As a result some IT professionals either postpone their WLAN deployments or rely on third-party services to assist them. The ITU-T Recommendation X.805, which is based directly on Alcatel-Lucent Bell Labs security model, is an excellent framework for systematically identifying security vulnerabilities and assessing and mitigating risks. It can be very valuable for evaluating VoWLAN security end to end across the enterprise.

Other VoWLAN Considerations

Besides the main technological challenges related to voice over WLAN, there are several other issues that should be carefully considered:

Handsets

As mentioned, the high price of WLAN handsets and the lack of requisite features have been major barriers to widespread VoWLAN adoption. This is likely to change with the introduction of dual-mode Wi-Fi/cellular phones and converged services. Other types of handsets include standalone Wi-Fi phones (either for enterprise and vertical industries like healthcare and retail or for homes and hotspots) like the recent Skype-enabled devices. Other platforms are PDA and laptop soft-phones. Those used by enterprises will require a much richer feature set, such as support for 802.11g and (ideally) 802.11a radios for increased capacity; WPA2 compliance for stronger security; low power consumption and WMM Power Save certification for enhanced battery life; and business-class features, user interfaces, and form factors.

Network Management

According to recent industry surveys, IT managers consider managing and troubleshooting the wireless infrastructure as their second-highest concern (after security). IT professionals need to deliver reliable and cost-effective service on an ongoing basis. This represents a major challenge in an environment where real-time voice users are free to roam while there may be coverage gaps, congested areas, and other problems.

Processes and tools are needed to provision and upgrade handsets, possibly managing certificates and VPN and VoIP clients, monitoring traffic to proactively identify capacity problems, overseeing the RF environment in real time to prevent or rectify coverage problems, and to address many other operational and WLAN management functions not specific to wireless voice. Depending on the size and architecture of the WLAN and specific equipment used, IT managers will need to choose between single-vendor management solutions (sometimes built into controllers) or third-party multivendor management platforms.

High Availability and Reliability

As with cellular and wired telephony, enterprise VoWLANs require high availability and reliability. It is unacceptable to pick up a phone and not have a dialtone. That means VoWLANs must deploy redundant components and automated failover mechanisms. Some WLAN solutions already provide this type of redundancy; emerging standards will enhance and standardize the process.

Emergency Calls and Location-based Services

Depending on country and state regulations, VoWLANs may need to comply with emergency calling mandates, such as FCC enhanced 911 (E911). When a VoWLAN user dials 911 (or the equivalent number outside the U.S.), the WLAN system should be able to accurately predict the location of the Wi-Fi calling device to within a few meters. Most current centralized WLAN solutions provide location-tracking services, using either triangulation or RF fingerprinting, that comply with E911. These location-based services (LBS) also are typically used for many other purposes such as enhanced security (for instance, locating rogue APs) and asset tracking.

Alternative Architectures and Solutions

One of the key decisions IT departments face when planning a VoWLAN deployment is which infrastructure vendor will best meet their requirements for applications, performance, security, scalability, manageability, costs, and so on. Many enterprise WLAN solutions that support voice use different architectures and offer various feature sets. Mainstream solutions have evolved during the past few years from standalone ("thick") APs, which handled all 802.11 and networking processing, to centralized ("thin") APs that almost act as dumb radios, tunneling all 802.11 frames to a central switch or controller, which handles traffic and manages security, mobility, QoS, RF, and the like.

Some vendors, claiming performance and scalability advantages, have implemented hybrid architectures that combine "intelligent" APs to handle some functions locally with centralized controllers that manage things like secure fast roaming and RF optimization. Finally, a few startups have come up with innovative architectures based on single-channel blankets, which use proprietary deterministic access schemes to solve co-channel interference and fast roaming problems. Other newcomers address scalability challenges with a "WLAN Array" that consists of many APs with sectorized antennas plus a controller collapsed into a single box.

Conclusion

Voice over WLAN is ready to jump from a few vertical industries to the enterprise. Solutions from multiple vendors are out there, using both proprietary and standards-based mechanisms and architectures to deliver business-class functions. Dual-mode Wi-Fi/cellular handsets are becoming available and will soon deliver the right features at the right price, allowing IT departments to build a strong VoWLAN business case.

IT professionals, however, will face numerous technical challenges when planning and implementing a VoWLAN, which has very different requirements than a data-only wireless LAN. Some of the key areas they'll need to address are security, mobility, RF planning, and QoS.

Alcatel-Lucent can help enterprises and service providers assess the array of VoWLAN options and select the right infrastructure and handset. Alcatel-Lucent also offers a broad portfolio of professional services to plan, design, implement, optimize, and manage VoWLANs end to end, while integrating them with VoIP, PBXs, other corporate IT systems, and carriers FMC solutions.

About The Authors

Gil Arumi

Gil Arumi is a senior member of the consulting staff in Alcatel-Lucent's IP Transformation Center. Arumi has served as the lead Wi-Fi and WiMAX Solutions Architect for EMEA, supporting and developing business throughout the region. While at Alcatel-Lucent, he has also planned, designed, and integrated several large enterprise and service provider IP networks, focusing on internetworking, routing, VoIP, and IP VPNs.

Before joining Alcatel-Lucent, Arumi managed the IP network and services for NTT Europe (London). He also has worked as a network systems engineer in several European and American companies.

Gil holds a BS and MS in telecommunications engineering from the Universitat Politecnica de Catalunya (Barcelona); did post-graduate work at the University of North Carolina (U.S.); and was a guest researcher at the University College London (U.K.). His certifications include CWNA, CCNP, CCDP, and JNCIA.

Theresa Buthmann

Theresa Buthmann is the director of Wireless Solutions for Alcatel-Lucent Services. She leads the development of robust wireless solutions that balance the gains of productivity with concerns around security, quality of service, and cost. Buthmann applies the knowledge gained from holding several diverse positions within AT&T and Alcatel-Lucent in the CFO, marketing, and business development organizations to enable multiple facets of the wireless solutions business across many technologies including optical transport, VoIP, Wi-Fi, in-building optimization, and mobile IP. Buthmann holds a BA in Business Administration from Kean University.

To learn more about our comprehensive portfolio, please contact your Lucent Technologies Sales Representative or visit our web site at http://www.lucent.com.

This document is for informational or planning purposes only, and is not intended to create, modify or supplement any Lucent Technologies specifications or warranties relating to these products or services. Information and/or technical specifications supplied within this document do not waive (directly or indirectly) any rights or licenses — including but not limited to patents or other protective rights — of Lucent Technologies or others. Specifications are subject to change without notice.

www.alcatel-lucent.com

Alcatel·Lucent