2006 Wireless LAN State-of-the-Market Report

AUGUST 2006

By Joanie Wexler

Produced By:

Webtorials

Sponsored By:

ARUBA™
The Mobile Edge Company

2006 Wireless LAN State-of-the-Market Report

Introduction

The productivity benefits associated with general user mobility are becoming increasingly apparent to businesses, as evidenced by the growth in wireless LAN (WLAN) deployments in mainstream enterprise environments. In April 2006, Webtorials surveyed its subscriber base for the third consecutive year concerning WLAN deployment plans, attitudes, and experiences. This report is a summary and analysis of those findings, compiled from Web-based survey responses of 350 subscribers.

Respondents' Sphere of Influence

Eighty percent (80%) of this year's respondents said they played a role in the decision-making process of WLAN purchasing and installation, either as decision-maker, recommender, or influencer. About 44% of respondents worked in companies with more than 2,000 employees.

This year's findings indicate that responsibility for WLANs is moving increasingly into the enterprise network manager's job description: More than half (55%) described themselves as traditional enterprise network managers—a figure that is up 14% over those who saw themselves in that role in 2005. The remaining respondents were nearly evenly split into the categories of "RF Expert" (22%) and "Wireless Hobbyist/Home User" (23%).

For additional demographics and other data, see Appendix, pp. 20-25.

Webtorials State-of-the-Market Reports

Produced By
Webtorials, a venture of
Distributed Networking
Associates, Inc.
Greensboro, N.C.
www.webtorials.com

Editor/Publisher
Steven Taylor
taylor@webtorials.com

Design/Layout Artist
Debi Vozikis

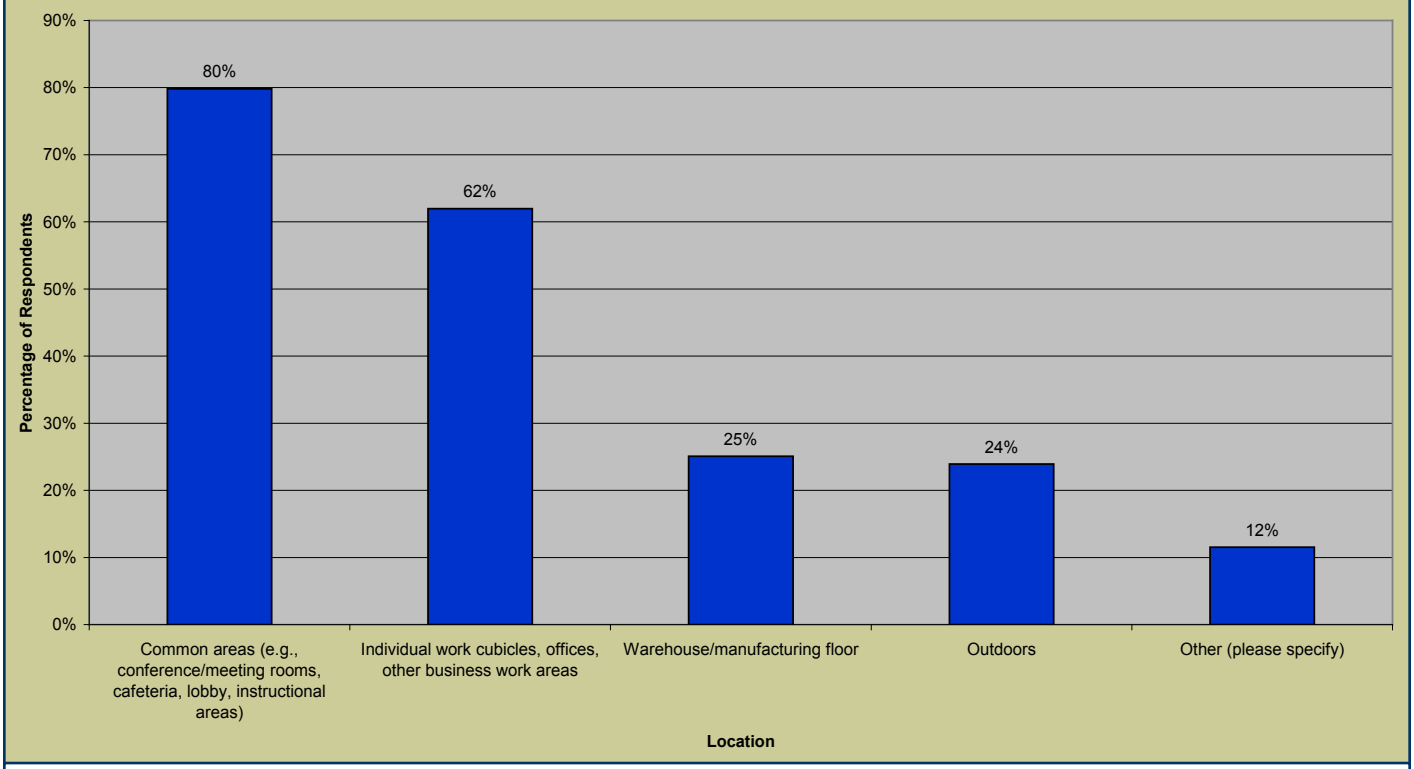
Key Findings

The 2006 Webtorials survey revealed the following other key enterprise WLAN deployment and usage trends:

- **Mainstream business WLAN implementations are widespread.** Eighty percent (80%) of respondents this year had already deployed business-class WLANs or were in the implementation process at the time of the survey. This figure represents a 14% increase in WLAN deployments from last year (70%) and is up 51% from 2004 (53%). In addition, 80% of 2006 respondents have deployed WLANs (informally known as "Wi-Fi" networks) in common areas of their organizations, such as conference rooms, lobbies, and cafeterias. Another 62% have also extended Wi-Fi to individual work cubicles and offices, as well as to other business work areas, a sign that Wi-Fi is moving out of niche installments and into more dense deployments for mainstream, horizontal business applications (see Figure 1).

- **802.11b growth is waning, and 11g deployment plans currently outstrip those for more mature 802.11a networks.** About 64% of respondents have deployed 11b, but only 5% have plans to continue deploying it. This is not a surprise. Higher-speed (54 Mbps) 802.11g network connections, which work in the same frequency band as 802.11b (2.4GHz), are now pervasive in client devices for communications with multi-mode access points (APs). And still faster 802.11n (100 Mbps and up) standards, which will be backward-compatible with all existing 802.11a/b/g networks, promise more capacity in the relatively near term. 802.11a installations and plans lag those

Figure 1. Where Is Wi-Fi Deployed?



Wi-Fi is becoming more densely deployed, reaching beyond common business areas and into individual work spaces.

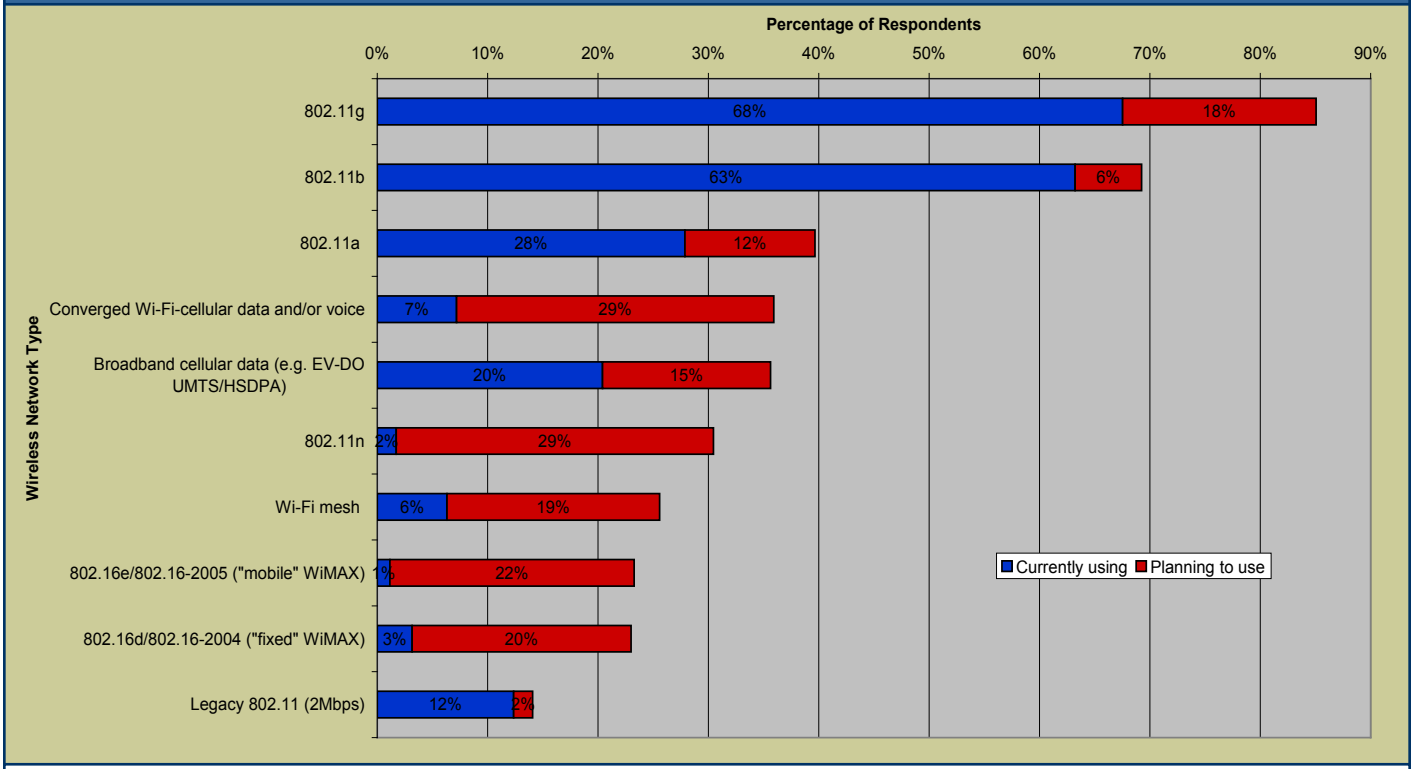
for 802.11g by 46%. (See section, "WLAN Architecture Trends," "Which Network?" on page 8.).

- **Centralized management architectures are quickly gaining traction.** Overall, survey responses indicate a 48% increase in the use of thin-AP architectures, which bundle management and security functions into a centralized controller, and a roughly 15% decrease in the use of standalone intelligent APs.

- **Plans for converged Wi-Fi/cellular networking are strong.** Though commercial use of converged networks and devices is currently low (8%), a primary reason is simply the scarce availability of converged services and products. However, user *plans* to merge the two technology types (29%) tied with plans to use emerging 802.11n networks as the highest-ranked wireless technologies in terms of growth. Mobile WiMAX (802.16e/802.16-2005) also made a reasonably strong showing on enterprise network blueprints, appearing in 23% of respondents' plans. The interest in mobile WiMAX is likely related to enabling user roaming across multivendor networks using a single technology (see Figure 2).

- **Confidence in wireless security is growing, but is far from rock-solid.** There was a significant dip this year in the percentage of Webtorials 2006 respondents who felt that WLANs simply "are not secure." Just 10% of this year's respondents chose this statement as best reflecting their feelings about Wi-Fi security, compared with 18% last year. Security, however, remains the business market's biggest Wi-Fi challenge.

Figure 2. Enterprise Technology Implementations and Plans



802.11n and converged Wi-Fi-cellular networking show the greatest potential for growth.

- **Voice over Wi-Fi deployments haven't increased much, but enthusiasm persists.** Twenty-three percent (23%) of 2006 respondents have deployed real-time voice over their Wi-Fi networks, compared to 21% last year. Another 45% of this year's survey-takers intend to deploy Wi-Fi voice; 44% said they planned to do so last year. One probable reason for lack of progress in this area is the remaining latency challenge imposed on real-time applications by roaming and re-authentication.

Market Background and Update

The IEEE 802.11 standards-based WLAN market continues to evolve in multiple dimensions. Technology is developing faster than industry interoperability consortia can certify it and faster than users can learn about it and deploy it. Each year seems to bring new WLAN technologies, security mechanisms, wireless architectures, and applications to consider. A mix of approaches to building scalable, enterprise-wide WLANs is installed, and additional architectures continue to be invented. Included in enterprise architecture considerations are how and where radio-frequency (RF) interference is addressed (e.g., single-channel versus multi-channel architectures); how (and how fast) a system addresses roaming, particularly for real-time voice traffic; and the provisioning, security, and management features of a given system.

As noted in the introduction, however, among the survey respondents, there is a trend toward the use of enterprise thin-AP architectures deployed in conjunction with centralized controllers and away from traditional distributed APs that house all the system intelligence (see section, "WLAN Architectures"). It is likely that these plans and deployments are reflective of organizations' movement toward covering large areas of geographic space using additional numbers of APs (which continue to drop in price) to improve capacity and coverage. Both broader and denser deployments make the centralized management and security control afforded by thin-AP architectures increasingly necessary. The reason is that there are significantly more APs to be installed, provisioned, and controlled.

As in previous years, survey respondents acknowledge that, for the most part, it is difficult to calculate a hard return on investment (ROI) for providing WLAN connections to general business employees, partners, and contractors. Twenty-eight percent (28%) of respondents said they had not been able to calculate such an ROI, but 27% said that a soft ROI was justification enough. Just 13% had been able to calculate a hard ROI for WLANs, and another 32% either didn't know whether they could or they hadn't tried.

Without the bottom-line justification, what's fueling the deployment ramp-up?

Business Drivers

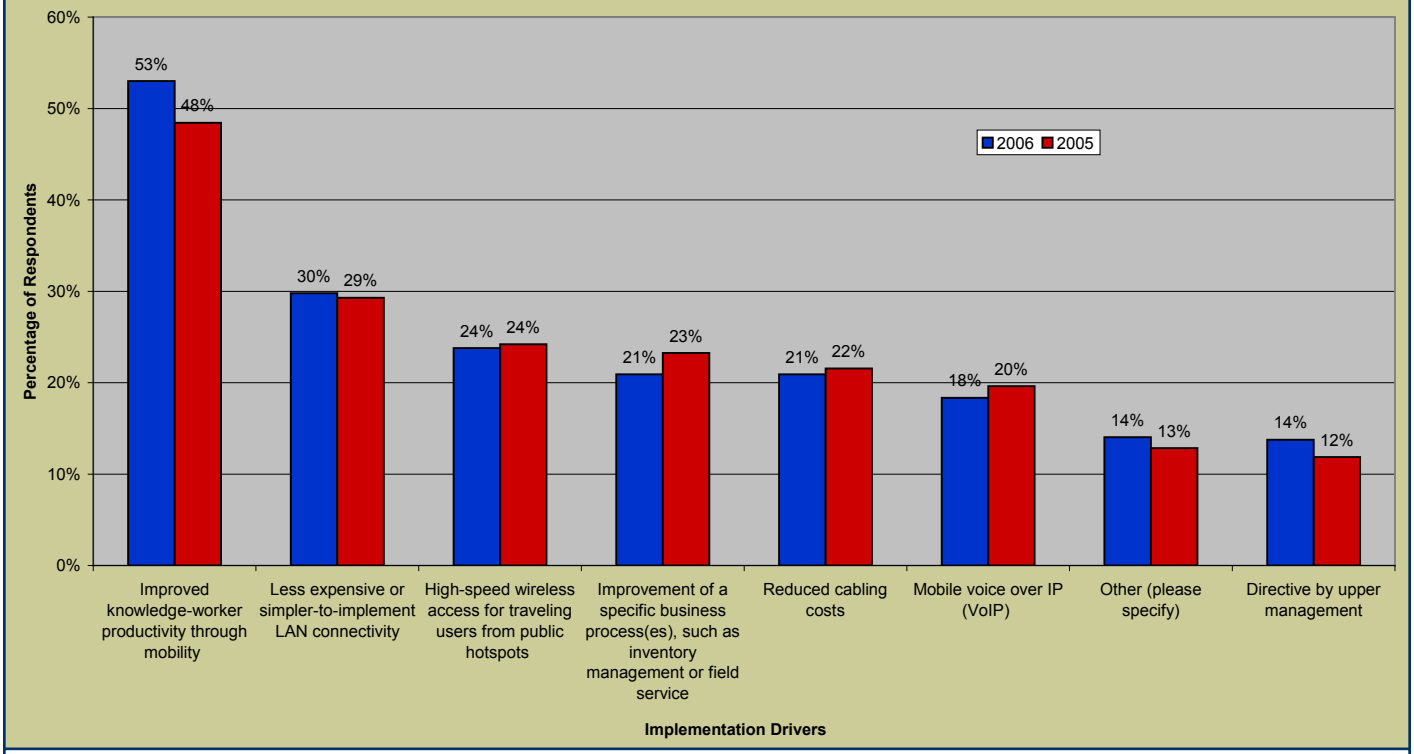
At this juncture, growth in the "carpeted" areas of enterprises—aimed at mobilizing business personnel—is outpacing growth in vertical applications. As in past surveys, "improved knowledge worker productivity through mobility" still far outranks any other driver as rationale for deploying WLANs (53%). A distant second reason (30%) is less expensive or simpler-to-implement LAN connectivity (see Figure 3).

These are among the reasons that 38% of survey respondents said they have deployed Wi-Fi that is accessible by at least half of their employees enterprise-wide or plan to do so within the next 12 months.

Technology Drivers

Among the technology developments during the past year that have likely affected survey responses:

Figure 3. Market Motivators



Organizations continue to look beyond hard-ROI justifications to the soft improved access and productivity benefits associated with mobility.

- **802.11n—**The IEEE Draft 1.0 specification for the 802.11n standard for high-speed (100 Mbps and above) WLANs arrived in January 2006. The promise of 802.11n may be stalling 802.11a deployments. 802.11a got a negative reputation for a few years because its range was limited to about 50 feet at full speed and it didn't perform well through walls. At this juncture, however, the technology has been improved such that 11a's range is close to that of 802.11g networks (about 100 feet).

  Still, enterprises lose nothing by implementing 11a and, in fact, gain more flexibility in network design by having more available channels to use in the "checkerboard" layouts of overlapping cell sites they build. These additional channels help avoid interference—cited by survey respondents as the third largest challenge to WLAN deployments (37%) after security (70%) and managing and troubleshooting the wireless infrastructure (38%).

  Because 11n specifies backward-compatibility with 802.11a/b/g standards, any product that becomes 802.11n-certified by the Wi-Fi Alliance industry consortium will also pass 11a/b/g certification, the alliance has stated. Though the Draft 1.0 802.11n first ballot did not receive final confirmation from the IEEE during a late-April 2006 vote to advance in the standards process toward "sponsor ballot" status, a ratified 802.11n standard is still expected by mid-2007. The Wi-Fi Alliance expects to start product interoperability certification testing in fall 2007.

- **Unified communications—**Users are expressing increased interest in converging Wi-Fi and cellular mobile networks and devices for the productivity benefits of unified communications across network

types. Unified communications includes being reachable by a single business number and having just one wireless (and wired) voicemail box to check.

- **Wireless intrusion detection/prevention (WIDP)**—Maturing WIDP systems architectures, increased product choice, and an increase in enterprise security needs at the RF layer are fueling installation of WIDP systems.

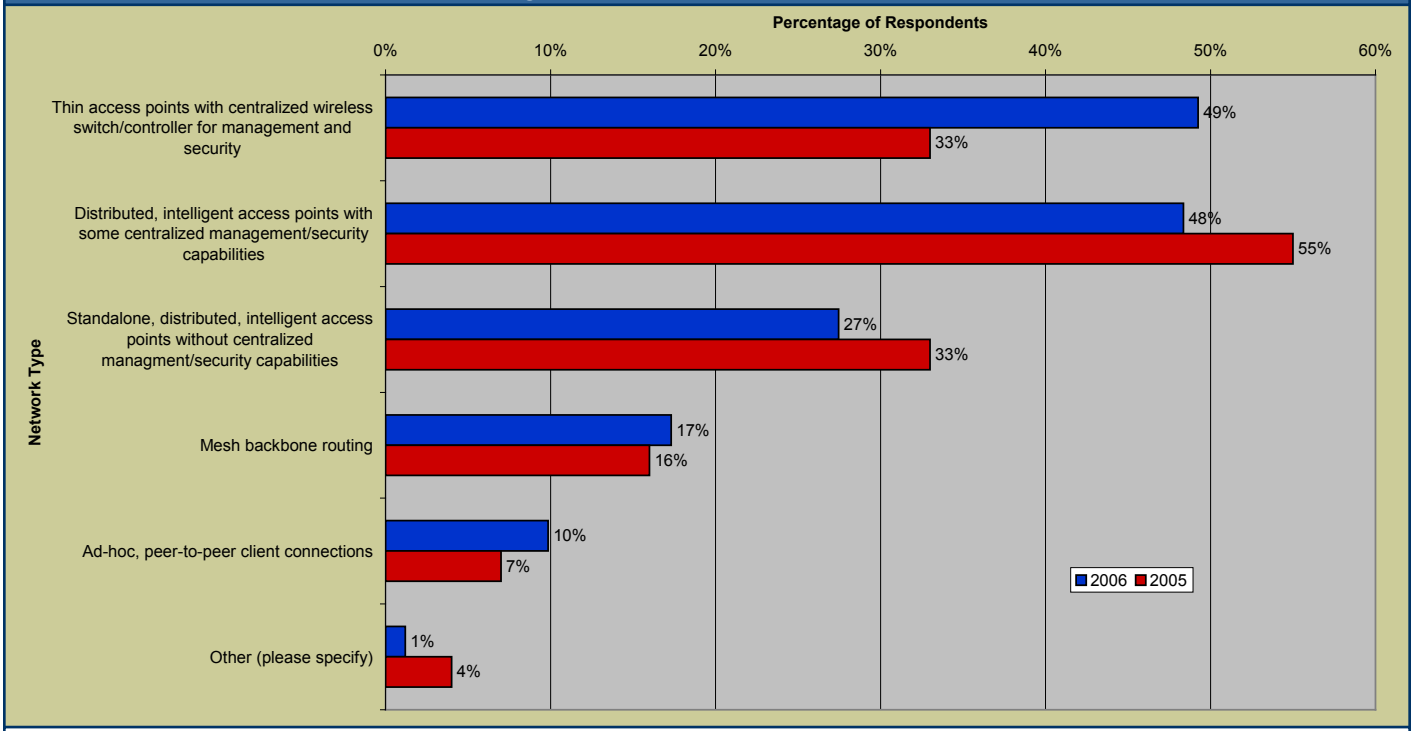
  Some non-Wi-Fi enterprises use intrusion detection systems to enforce "no wireless" policies; others, to differentiate legitimate users and traffic from unwanted activity. Without such systems, wireless' inherent tendency to "bleed" through walls, ceilings, and floors and for wireless devices to naturally auto-associate with other wireless devices—authorized or not—potentially opens the door to data hijacking, eavesdropping, and piggybacking onto corporate network connections.

WLAN Architecture Trends

As mentioned, there is a notable trend away from distributed standalone APs that are managed and secured on an individual basis and toward APs dependent on a centralized controller for more scalable group control.

Still, multiple types of architectures will persevere depending on the size and nature of a given business. Small businesses running one or two APs might find it more economical to go with the intelligent, standalone AP; companies that make frequent topology changes or have difficult-to-wire environments are the most likely candidates to adopt mesh environments. Mesh networks allow APs to communicate directly to one another over the air, rather than requiring each one to be cabled

Figure 4. Architecture Preferences



Respondents show a preference for centralized management and security as they move away from standalone intelligent access points that must be provisioned and controlled individually.

back to a LAN switch or wireless controller. Some organizations will run different architectures in different sites, depending on the requirements and physical characteristics of each location.

Toward Centralized Management

Survey-takers were asked to check all of the architecture types that they intended to deploy in their environments. This year, nearly half (49%) the survey respondents said they are using or are likely to use thin APs with a centralized controller for management and security in their Wi-Fi environments. This represents an increase of 48% over the number of respondents who last year said they were using or planning to use thin-AP Wi-Fi architectures (33%).

The use of intelligent standalone APs (with no centralized controller) fell from 33% to 27% compared with last year (an 18% decrease), and plans to use intelligent standalone APs with some centralized management and security capabilities decreased by about 13%, from 55% last year to 48% this year (see Figure 4).

Which Network?

802.11g networks continue to find much broader acceptance than 802.11a networks, despite the fact that both run at the same theoretical maximum speed. 802.11a offers four to five times the number of non-overlapping channels in the 5GHz band for flexibility in building out networks with less interference and for segregating traffic types (such as voice and data). However, 19% of respondents said they specifically planned NOT to use 802.11a going forward; in fact, 802.11a ranked second only to legacy 802.11 networks (34%), built on the 1997 version of the standard and running at just 2 Mbps, as missing from user plans.

Survey responses may not yet account for Intel Corp.'s January 2006 release of its Centrino Duo mobile architecture for laptops. If accepted widely by laptop makers, the dual-frequency connections (802.11a/b/g) could mean that 802.11a clients proliferate rapidly by default and 802.11a use will pick up.

A contributing reason to 11a's slow adoption, at least until now, is that worldwide spectrum regulations for use of the 5GHz spectrum historically have been fairly inconsistent around the world, primarily because of interference issues with local military radar. A great deal of harmonization has now been achieved in the 5GHz band globally, though several countries in the Middle East, as well as Morocco, Thailand, Romania, and Russia, don't allow 5GHz networking at all. Some in South America allow limited 5GHz Wi-Fi networking across just a portion of the band. This has been a deal-breaker for some global businesses that wish to standardize on a single product SKU worldwide.

As noted earlier, 802.11a might also be feeling competitive heat from forthcoming 802.11n networks, as well as from a trend toward the use of four channels in the 2.4GHz band (1, 4, 7, 11) as an alternative to limiting a 2.4GHz network to its three non-overlapping channels (1, 6, 11). When APs are installed in appropriate locations, users can gain the flexibility of another channel with little corresponding interference.

Finally, while 802.11a is recommended in converged voice/data Wi-Fi deployments for segmenting real-time traffic as a quality-of-service (QoS) technique, the industry remains in the same chicken-and-egg situation it was in last year: At the time of this writing, there still are no 802.11a VoIP handsets commercially available. Intel's third-generation Centrino Duo architecture and other connections with 802.11a/b/g dual-frequency connections could support VoIP softphone capabilities on laptops. In this scenario, users would run IP telephony software on their laptops, rather than carrying a VoIP-

enabled Wi-Fi handset, and laptop-generated VoIP traffic could be segmented onto 802.11a networks for QoS.

Intrusion Prevention Systems

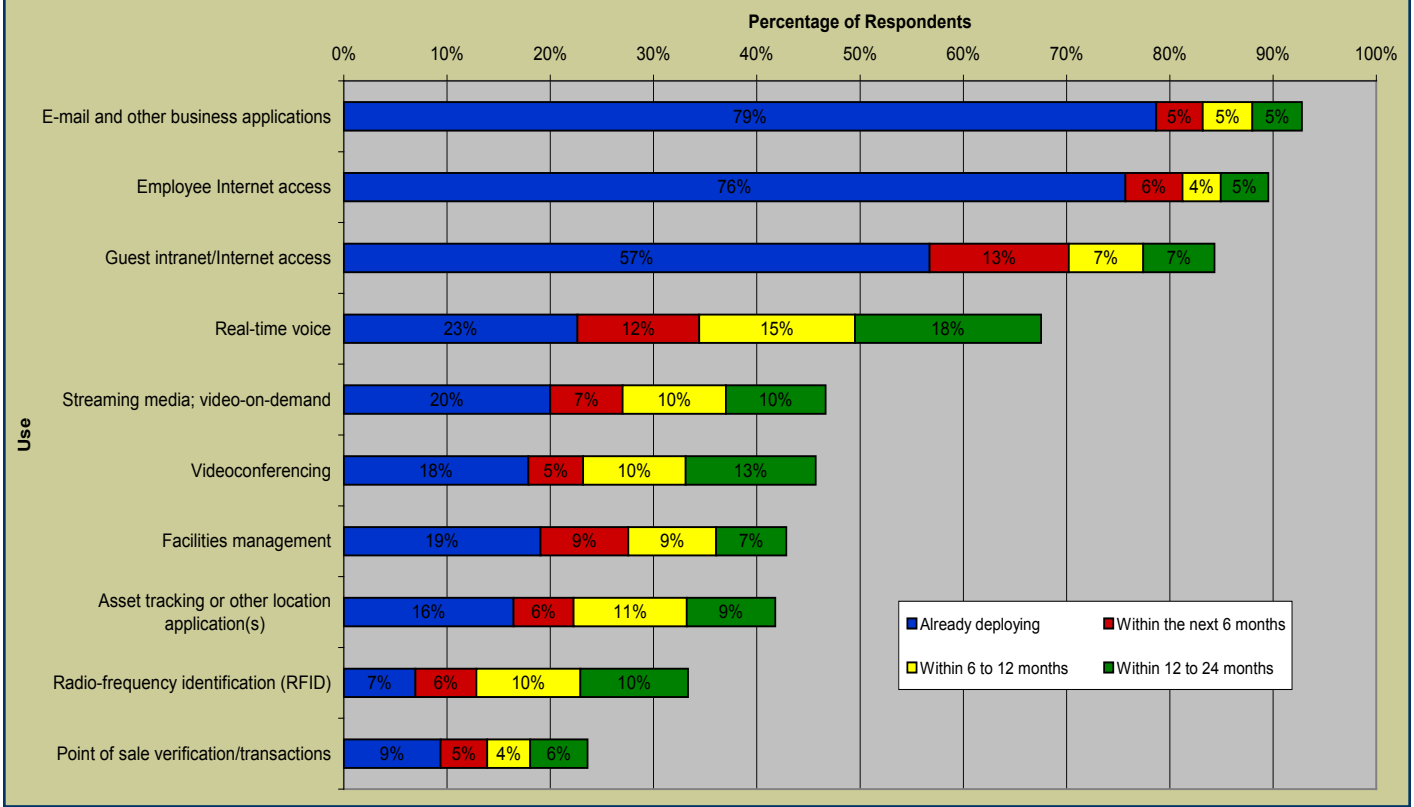
IT departments also appear to be moving toward WIDP systems for enhanced security. WIDP systems ranked third after personal digital assistants (75%) as equipment playing a significant role in the infrastructure (a survey option not available last year).

There are various architectures for deploying WIDP systems. Seventy percent (70%) of respondents indicated existing or imminent use of a WIDP system that has been integrated with the respondents' existing WLAN systems, for example. Another 52% said they are or will soon be deploying "overlay" WIDP systems—standalone appliances or servers that correlate security events reported by specialized, distributed radio sensors and take automated, policy-based action.

What's Running on Wi-Fi?

E-mail, other general business applications, and employee and guest Internet access remain the primary uses for Wi-Fi networks today and in the near-term (see Figure 5). Still, voice over IP over Wi-Fi (Vo-Fi) outpaces the other applications in terms of growth potential, while radio-frequency identification (RFID) applications used in asset and location tracking still rank fairly low on user radar screens for the next two years.

Figure 5. Existing and Planned WLAN Applications



Traditional e-mail, Internet access, and other business communications applications are the top apps using Wi-Fi networks today, though voice shows the greatest potential for growth.

As noted, the survey reflected large growth potential in dual-mode Wi-Fi-cellular handsets and internetwork roaming. From a user mobility perspective, Wi-Fi-cellular convergence would eventually give users a single universal phone number with features that would follow them around and work the same way wherever they are. Combined with presence management, chat, and text capabilities, wireless net convergence could begin to eliminate some of the phone tag productivity problems that plague workers who use multiple networks today.

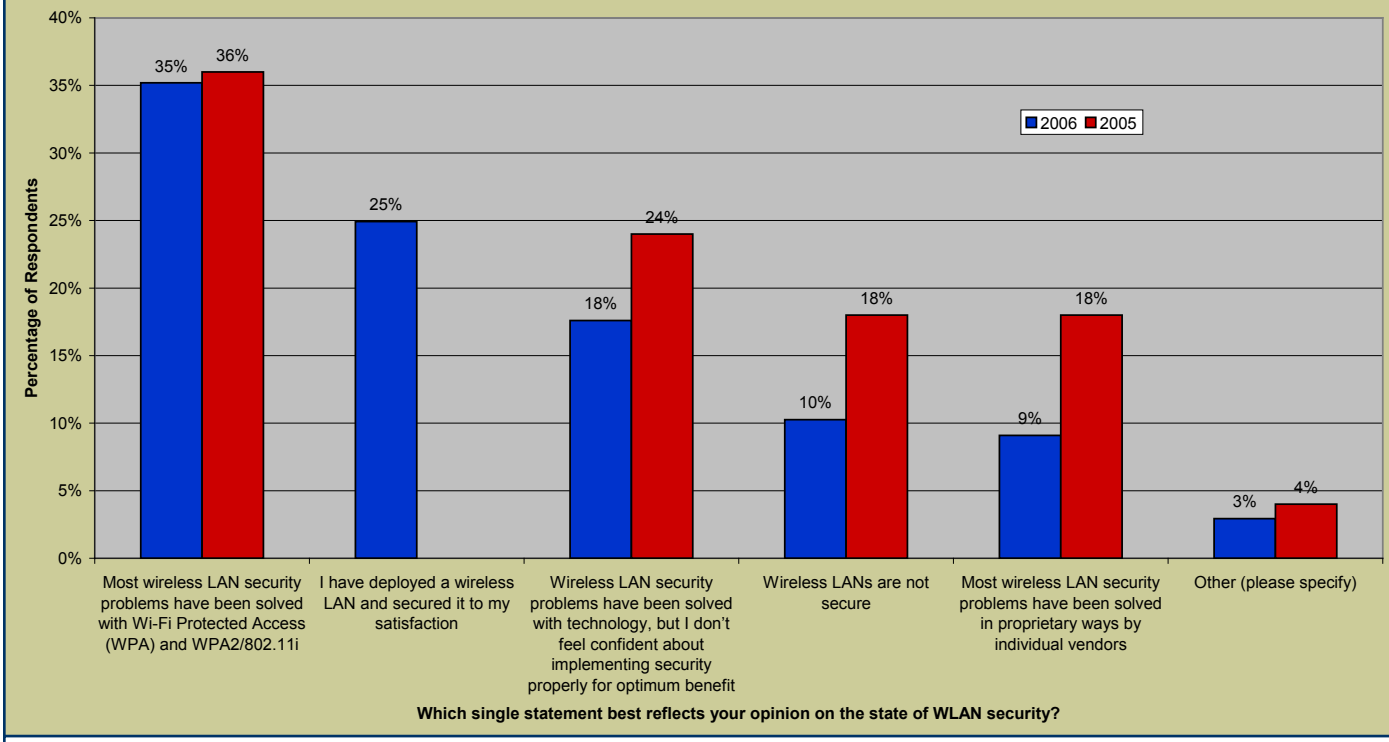
Enterprise Challenges

Respondents again ranked their three top wireless challenges in this year's survey. While "security concerns" dipped slightly—from 73% in 2005 to 70% in 2006—security continues to top the list. The next greatest challenge, cited by 38% of respondents (about the same as last year), was managing and troubleshooting the Wi-Fi network. This figure is up from 23% in 2004, presumably because networks are growing larger. As a result, enterprises are feeling the requirement for associated management and security that scales in step with the size of their networks.

Security: Forever a Question Mark?

IT departments are becoming more confident about deploying effective wireless security, but still have a ways to go. When asked which single statement best reflected their attitudes toward Wi-Fi security, 35% said that they believed most security problems had been solved with the advent of the 802.11i security standard suite (a.k.a. Wi-Fi Protected Access 2, or WPA2). And while 25% said they felt satisfied that they had properly secured a WLAN that they had deployed, 18% still said

Figure 6. Attitudes Toward Security



IT confidence in securing Wi-Fi networks has improved significantly; still, respondents indicate they could use more training and expertise.

they lack confidence in optimally implementing the security products and technologies available (see Figure 6).

The Wi-Fi Alliance has made noises about certifying Wi-Fi products for simple, secure configuration and setup—a motivation to get vendors to simplify the tasks associated with the many layers of security required in RF networks.

Within enterprises, progress is being made, too. While upper-layer VPNs continue to be the most broadly deployed form of WLAN security (41%), link-layer WPA and WPA2/802.11i have made great strides over last year. WPA2 is in use in 38% of the enterprises represented in the 2006 survey, up from just 22% last year. WPA2's predecessor, WPA, also a very secure option, has also increased in use since last year, from 29% to 36% (see Figure 7).

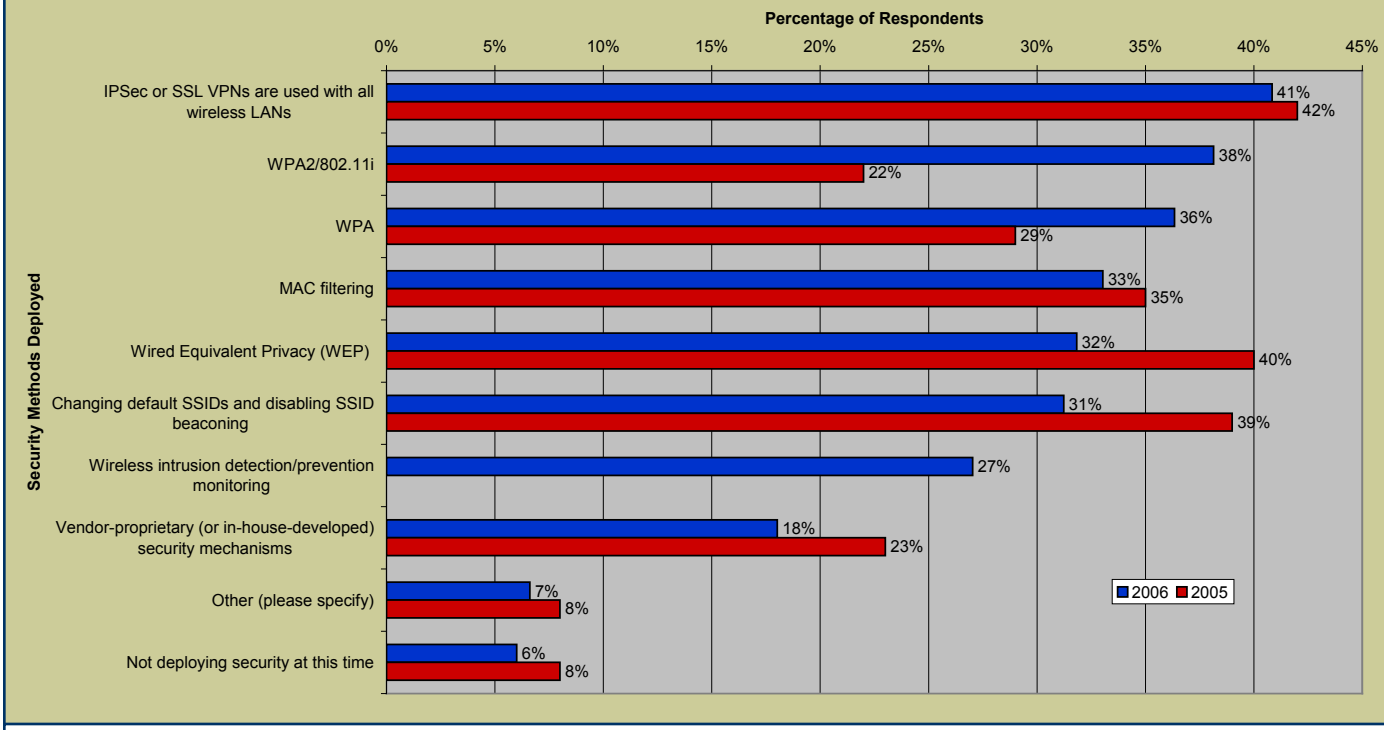
Wireless Voice Status

For the past two years, Vo-Fi has garnered more attention and hype than deployment action. Within the 2006 survey sample, deployment progress didn't change much, with existing deployments remaining about the same at 23% (Figure 5). Plans to implement Vo-Fi over the next two years, however, are high (45%).

Technology advances will help this application. Since last year, the call admission control (CAC) portion of the 802.11e QoS standard was ratified, which completes the technology specification. However, the Wi-Fi Alliance product interoperability certification testing for CAC-enabled Vo-Fi devices will not begin for enterprise-class products until mid to late 2007.

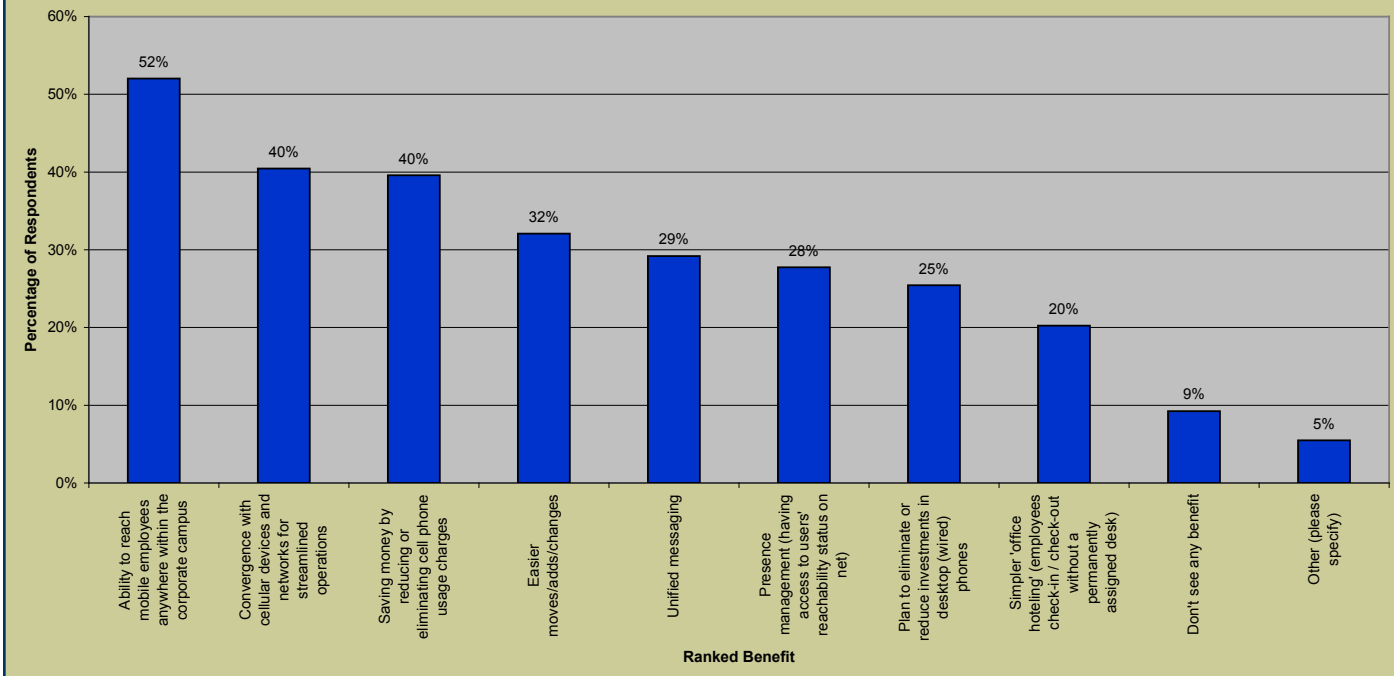
Vo-Fi still faces challenges in roaming latency (an issue addressed somewhat, but not completely, by the

Figure 7. Security in Use



While higher-layer VPNs continue to be the most broadly deployed form of WLAN security, link-layer WPA and WPA2/802.11i have made great strides over last year.

Figure 8. Benefits of Merging Wi-Fi and VoIP



Improving mobile worker accessibility, including merging Vo-Fi with cellular for single-number access, are among the biggest perceived advantages of integrating Wi-Fi networks with VoIP.

authentication piece of the 802.11i security standard). In addition to CAC, the issue of latency induced by roaming is being addressed by two related 802.11 working groups (Task Group R and Task Group K), which expect relevant ratified standards in mid-2007. Interoperability certification tests are expected to begin at about the same time.

The primary interest in Vo-Fi is similar to that of WLAN deployments in general: More than half of the respondents want to improve the accessibility of mobile employees roaming around the corporate campus (see Figure 8). The other two highest-ranking reasons for deploying Vo-Fi seem to fall in the area of convergence: 40% say that converging Vo-Fi with cellular networks and devices for streamlined operations is a motivator. And 40% also said they wished to save on cellular phone charges by using Vo-Fi when possible.

Nascent solutions to converging Vo-Fi and cellular are already on the market, mostly in the form of enterprise-based servers that extend PBX numbers, as well as related calling features and applications such as presence, out to the cellular network. Most are available from IP PBX vendors, some of whom have struck partnerships with voice-centric software startups. In addition, early cellular services recently began rolling out that extend PBX dial plans and features to the wide area and offer a better cellular calling rate when users are on their own enterprise premises. The mobile operators offering them say they are testing dual-mode Wi-Fi-cellular versions of these services, but that it is too early to say when they will become commercially available.

Conclusions

The pace of WLAN adoption is picking up in the enterprise, in part because of faster networks, more powerful client devices, and higher levels of confidence about wireless security. Mostly, however, organizations that have gotten a taste of the accessibility benefits associated with mobility realize that there's simply no turning back.

Most 2006 respondents have already implemented WLANs to support Internet access, email, and other traditional horizontal business applications in the hopes of making the average knowledge worker more productive and accessible when roaming around campus. A high number expressed interest in running voice on their Wi-Fi networks, preferably integrated with dual-mode Wi-Fi-cellular devices to further enhance accessibility.

User confidence in wireless security is strengthening, now that robust security technology is here and the industry gains experience deploying it. Many respondents believe that the technology solutions have been delivered by the industry to build secure wireless networks—just 10% flat-out believe that wireless networks simply are not secure. Many express less confidence in their personal abilities to actually build secure Wi-Fi networks than they do in the industry's support of appropriate products and technology to do so, but this number is starting to fall.

Additional data compiled from survey responses is presented in the Appendix, pp. 20-25.

About the Author

Joanie Wexler is an independent technology analyst and editor who reports on trends and issues in the computer-networking and telecommunications industries. She authors the "Wireless in the Enterprise" newsletter for *Network World* and contributes frequently to industry trade publications such as *Computerworld* and *Business Communications Review*.

About the Publisher

Steven Taylor is editor and publisher of the Webtorials networking education Web site, which conducted the survey for this report. An independent analyst, author, and teacher since 1984, Mr. Taylor is one of the industry's most published authors and lecturers on high-bandwidth networking topics.

Scaling Wireless LAN Deployments

By Keerti Melkote, Co-founder and Vice President of Marketing, Aruba Wireless Networks

From the Sponsor

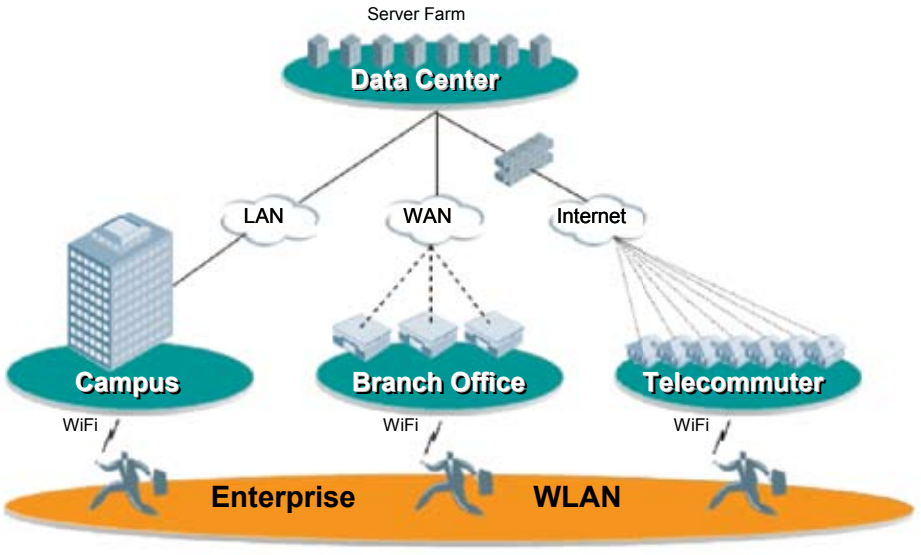
ARUBA™
The Mobile Edge Company

Introduction

Enterprise wireless LANs (WLANs) have expanded rapidly over the past few years, moving from small hot-spot-style deployments in conference rooms and other common areas to pervasive enterprise-wide deployments that span campuses, branch offices, telecommuters, and even nomadic remote offices. As these wireless networks grow in size, their scalability is primarily determined by the underlying architecture of the WLAN and its interworking with the wired architecture.

Enterprise WLAN design has evolved from a distributed to a centralized model. It is clear that centralized WLAN architectures are here to stay and will be the dominant method of building enterprise wireless networks. However, not all centralized architectures are created equal. Customers are faced with two architectural options even with centralized architectures. One option is to embed centralized WLAN capabilities into the existing network infrastructure. This requires an upgrade to the fixed, or wired, edge of the network to address the challenges associated with mobility. The other option is to create a new mobile edge that extends beyond the existing fixed edge and allows users to connect from any location at any time. A mobile edge requires an overlay network model that delivers mobile connectivity across the corporate network and the public Internet.

Figure 1. Mobile Edge Architecture for a Common User Experience across LAN, WAN, and Internet



Determining which products and solutions available today can address this fundamental architectural difference can be difficult since most of the industry rhetoric seems similar. One key area of differentiation is scalability. Traditional scalability metrics of centralized WLAN architectures have focused on controller throughput and the number of thin access points (APs) supported by centralized WLAN controllers. While these are important metrics, real-world experience in deploying high-end enterprises has yielded fresh insight into scaling requirements for WLANs. The challenges of scaling

enterprise WLANs fall into three primary categories:

- Campus WLANs with hundreds to thousands of users and devices
- Branch office wireless LANs with 10 to 100 users and devices
- Telecommuter and nomadic office WLANs that have between one and 10 users

Scaling Campus WLANs

As the enterprise workforce becomes increasingly mobile, user counts on campus WLANs are constantly on the rise. With the proliferation of Wi-Fi-equipped personal handheld devices, device counts are increasing even more rapidly. The key challenges of scaling a campus WLAN are caused by the density of users and devices, instantaneous loads caused during peak-hour usage, and the mobility of users between different areas on the campus. The associated technical challenges relate to the scaling of RF capacity, AAA services, and VLAN architecture for mobile networks.

Scaling RF Capacity with Multi-Channel RF Architecture

All centralized WLAN architectures today incorporate some level of RF management functionality, which is designed to automate the site survey process. However, in most implementations, RF management is limited to pre-planning and makes use of heavy- duty RF planning software. Other vendors claim to eliminate the entire planning process by moving to a single-channel architecture. Both approaches leave much to be desired when it comes to delivering high-capacity WLANs.

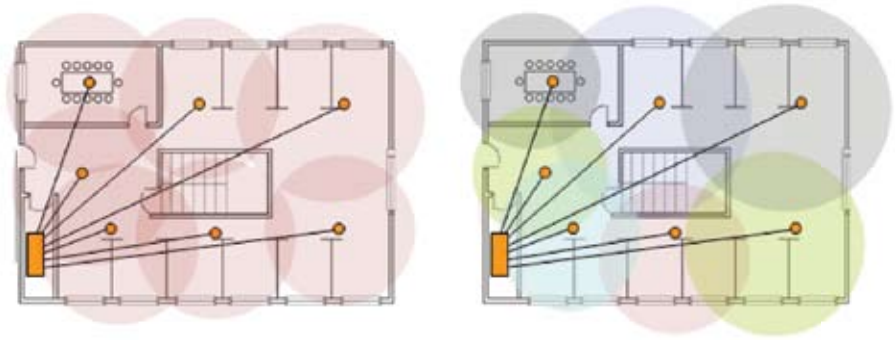
In the first instance, planning AP placement based on building materials and other models is fundamentally flawed, because the RF characteristics are dynamic and change constantly. This results in a failure to adjust to ambient RF conditions or, worse, in sub-optimal results, when assumptions regarding building materials and other variables are flawed. Single-channel architectures, while eliminating the planning problem, introduce an issue related to client density. When all clients are operating on the same channel, co-channel interference increases significantly, resulting in poor performance. Multi-channel RF architectures are inherently better suited for high-density usage, because they utilize all available channels in the spectrum to reduce co-channel interference. However, multi-channel architectures must be completely automated from a deployment standpoint. New techniques such as Adaptive Radio Management (ARM) are emerging in the industry to completely automate the deployment of multi-channel RF architectures and reduce co-channel interference. This leads to much higher RF capacity and better RF performance of WLAN networks.

As density increases, enterprises are employing strategies to migrate to 802.11a, which operates in the 5GHz band and offers 4 to 5 times more capacity than the 2.4GHz band. The 5GHz band is also inherently much cleaner with respect to interference, yielding better and more consistent channel performance. The 2.4GHz band will continue to be the first choice for equipment manufacturers of most handheld mobile devices such as voice-over-Wi-Fi, or "Vo-Fi", phones; PDAs; dual-mode phones; barcode scanners, and active RFID tags because of the greater maturity, lower cost, and lower power demands of 802.11b/g silicon. However, laptop manufacturers have finally caught up and are now implementing new power management efficiencies and adding support for 802.11a. The newer laptops with 802.11a/b/g network interface cards autoselect and, wherever possible, opt for, the 5GHz band. This, in turn, is resulting in a hybrid approach, using the 5GHz band for

laptops and the 2.4GHz band for other handheld devices.

In addition, enterprises are increasingly using four-channel architectures in the 2.4GHz band instead of the traditional three-channel approach, as the extra channel yields additional capacity. This approach is especially valuable in dense deployments.

Figure 2. Multi-Channel RF Delivers Up To 3 Times the Capacity of a Single-Channel RF Architecture



Single channel architectures increase client contention and co-channel interference

Self-tuning multi-channel architectures reduce client contention and co-channel interference

Scaling AAA Services with Hardware Acceleration of 802.1X Authentication

Even with additional RF capacity and a successful 802.11 association, devices in large enterprise networks may still be unable to connect to the network. This is often the result of heavy loads on the back-end authentication, authorization and accounting (AAA) server. This situation is being compounded with the implementation of new authentication practices as part of 802.11i.

802.11i, which requires all users and devices to authenticate to the WLAN using the 802.1X authentication protocol, is established as an industry best practice for securing enterprise WLANs. The National Institute of Standards and Technology (NIST), responsible for setting government standards, has, in fact, mandated the use of 802.11i in securing WLAN networks.

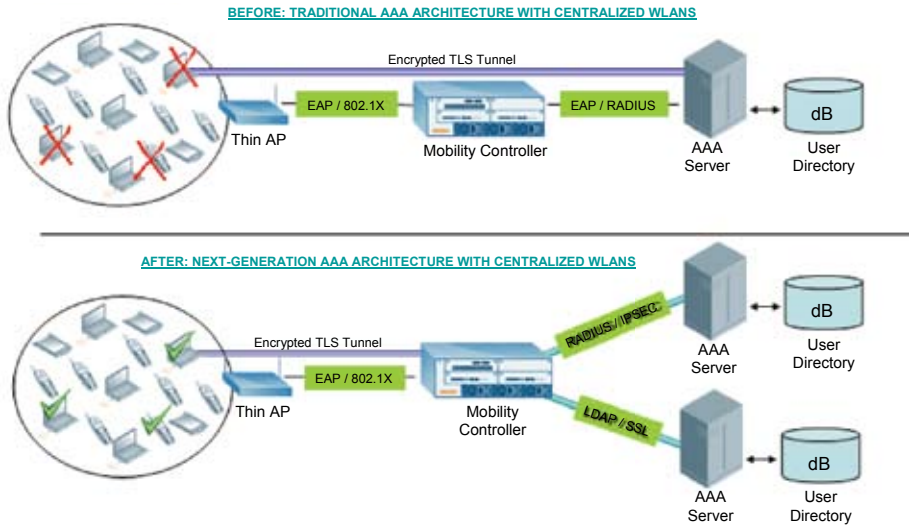
Traditionally, in centralized WLAN architectures, the controller only serves as an authenticator in the 802.1X authentication process. The actual AAA transaction of verifying a username and password combination is carried inside an encrypted Transport Layer Security (TLS) tunnel between the wireless client and the AAA server. Typical tunnel types used today are PEAP and EAP-TLS, with PEAP as the dominant method.

The introduction of 802.11i forces AAA servers to take on an even greater computational burden. The AAA server is given the responsibility of both terminating encrypted authentication network protocols such as EAP-PEAP, as well as generating the encryption keys that are used by WLAN clients and APs for secure wireless 802.11 communications.

As user density and the number of login requests per second go up, the backend AAA server's ability to process cryptographic information with consistent response times while simultaneously authenticating and authorizing users becomes a bottleneck. Users in heavily loaded wireless networks end up with slow, variable response times during network login and may even experience network disconnects due to timeouts. Customers who have experienced this problem end up having to set up multiple AAA proxy servers to scale AAA processing capacity in the network. The extra proxy servers and associated network redesigns increase network complexity and add both capital and operational expense.

Solutions to this problem are emerging from some centralized wireless LAN vendors whose WLAN controllers are architecturally capable of absorbing the fixed, but immense, overhead of the 802.1X authentication process. These controllers incorporate purpose-built hardware encryption processors to

Figure 3. Before-and-After Comparison of AAA Services with Hardware Acceleration



terminate the PEAP/TLS tunnels and centrally compute the crypto keys for secure wireless communications. This offloads the back-end AAA server from this significant processing burden and leaves it free to perform the tasks of AAA. This approach, known as AAA FastConnect, results in more than 1,000 authentications per second–a tenfold increase–eliminating the issue of slow connect times and failed login attempts.

AAA FastConnect not only results in faster and more predictable connect times, but also greatly simplifies the integration of secure WLANs with various back-end servers. In traditional AAA architectures, back-end AAA servers must be upgraded to handle 802.11i security, because centralized controllers are just a pass-through relay in the authentication phase. With AAA FastConnect, a mobility controller can interoperate directly with an AAA server using RADIUS or LDAP, given that all AAA-related 802.11i security requirements are absorbed by the mobility controller. Furthermore, RADIUS packets can be encrypted in an IPsec tunnel, while LDAP transactions can be encrypted in SSL to keep the entire AAA transaction encrypted end-to-end. Such flexibility is not possible with traditional AAA architectures. This enables the entire WLAN to operate as a secure overlay without requiring any additional investment to upgrade or add security to the wired network, thereby cost-effectively solving the scalability problem.

Scaling Branch Office Wireless LANs

The primary challenges associated with branch office WLANs are the cost and complexity of deploying WLANs in a large number of branch offices, centrally managing a large number of branch offices distributed across a wide-area network (WAN), and keeping users connected to the branch WLAN even when the WAN link goes down.

Self-Configuring Mobility Controllers for Automated Large-Scale Deployments

Branch offices typically lack skilled IT personnel to set up and operate secure WLAN networks. Yet, users expect a consistent and secure mobility experience regardless of their location. To deliver a consistent user experience at the lowest operating cost for a branch WLAN, mobility controllers must provide simple self-configuration. This capability allows for the mobility controller to be centrally provisioned and drop shipped to a branch location for plug-and-play operation.

Self-configuring mobility controllers dynamically obtain an IP address from the branch firewall/router or broadband access provider using a built-in DHCP client or a PPPoE client. Upon obtaining the IP address from the network, the local branch

controller automatically synchronizes its configuration with a centrally located configuration server (master mobility controller). This capability allows a non-technical employee to bring up a secure WLAN by simply plugging the mobility controller into the branch network, eliminating the cost and hassle of sending skilled IT staff to branch offices.

Automating configuration of branch office wireless LANs drastically cuts the total cost of deployment and is a critical first step in enabling a large-scale branch WLAN deployment.

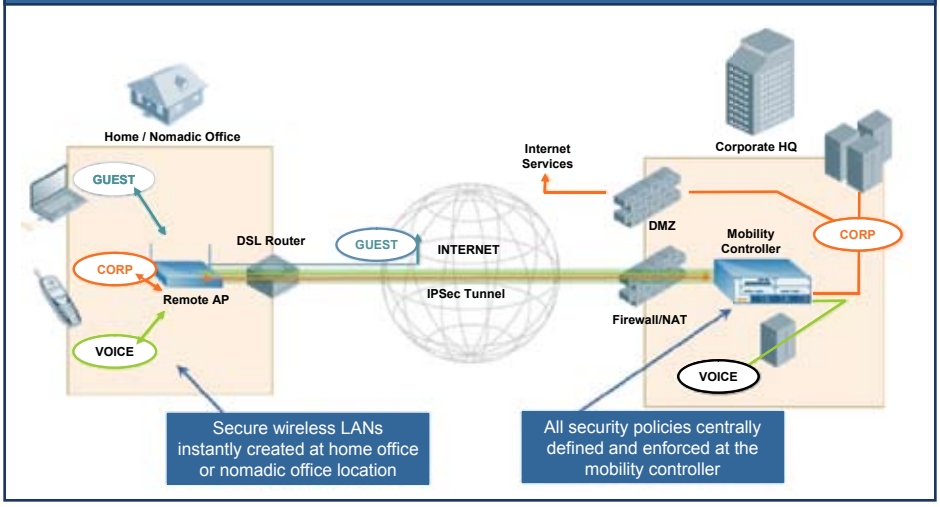
Scaling Telecommuter Wireless LAN Connectivity

Telecommuters increasingly demand access to corporate voice over IP (VoIP) and data resources from their home offices. The requirement is for a simple and secure solution that users can just plug into their home networks to gain instantaneous, secure access to the corporate network over the Internet. However, telecommuter wireless LAN deployments have depended on either difficult-to-manage, stand-alone enterprise APs or completely unmanaged, highly vulnerable consumer APs.

Similar to the telecommuter WLAN requirement, there is an ever-increasing need for nomadic offices, which require setting up a temporary network that lasts for a few weeks, a few days, or even just a few hours. This is a very common and critical requirement in the construction industry, where access to corporate resources is needed from remote building sites. Trade shows are another example of a nomadic office where multiple users need secure access to corporate resources from the show floor.

Remote APs deliver the benefit of securely and easily extending enterprise WLANs to home offices and nomadic office locations. Remote APs are plug-and-play devices that require only very basic one-time provisioning by the IT department. Once provisioned to discover the central mobility controller over the Internet, remote APs allow mobile workers to take the enterprise wireless LAN with them wherever they go, securely accessing corporate VoIP and data services from any location. Large deployments of remote APs are possible at the lowest operational and capital costs since they are simple, secure, and plug-and-play.

Figure 4. Remote APs Instantly Create Secure Enterprise WLANs for Telecommuters



Conclusion

As workforce mobility becomes pervasive, enterprises are increasingly considering large-scale deployment of secure wireless LANs. Enterprises are faced with two architectural choices: extend the fixed edge of the existing network or create a new mobile edge that spans the LAN, WAN, and Internet. The mobile edge architecture not only delivers ubiquitous and secure

mobile access, but also delivers unprecedented scalability. Unique capabilities, such as AAA FastConnect, VLAN Pooling, and Remote AP, created based on the needs of actual, large-scale enterprise WLANs, are essential to delivering a reliable, cost-effective, and operational enterprise wireless network.

About Aruba Wireless Networks, Inc.

Aruba Networks is a fast-growing enterprise infrastructure company enabling the Mobile Edge, an evolutionary network architecture that represents a new approach to transitioning enterprise networks from a fixed, port-based architecture to an architecture centered on secure, identity-based mobility. The Mobile Edge simultaneously delivers mobile data and VoIP services, as well as a common user experience to mobile workers in the office, at home, and on the road by creating a secure mobility overlay that spans the LAN, the WAN, and the Internet. To deliver the Mobile Edge, Aruba manufactures and markets a complete line of fixed and modular mobility controllers, wired and wireless access points, an advanced mobility software suite, and a mobility management system. Privately held and based in Sunnyvale, California, Aruba has operations in the United States, Europe, the Middle East, and Asia Pacific and employs staff around the world. To learn more, visit Aruba at http://www.arubanetworks.com.

Appendix

Methodology and Demographics

The Webtorials subscriber base was asked to participate in a 22-question online survey about their experiences with and plans for deploying WLANs. All questions were in a multiple-choice format and included a "Don't Know," "Not Applicable" or "Other (please specify)" option.

Whenever appropriate, the order of the multiple choices rotated randomly so as not to bias the survey respondent by the order in which the options were presented.

The Webtorials survey was conducted in April 2006. A total of 350 respondents participated. The survey base was fairly well distributed across industries, though the number of respondents in professional services, government, education, and the non-computer manufacturing and processing sectors slightly outpaced respondents in the finance, medical, legal, and utilities arenas.

Figure A1. Which of the following best describes your expertise with wireless LAN technology?

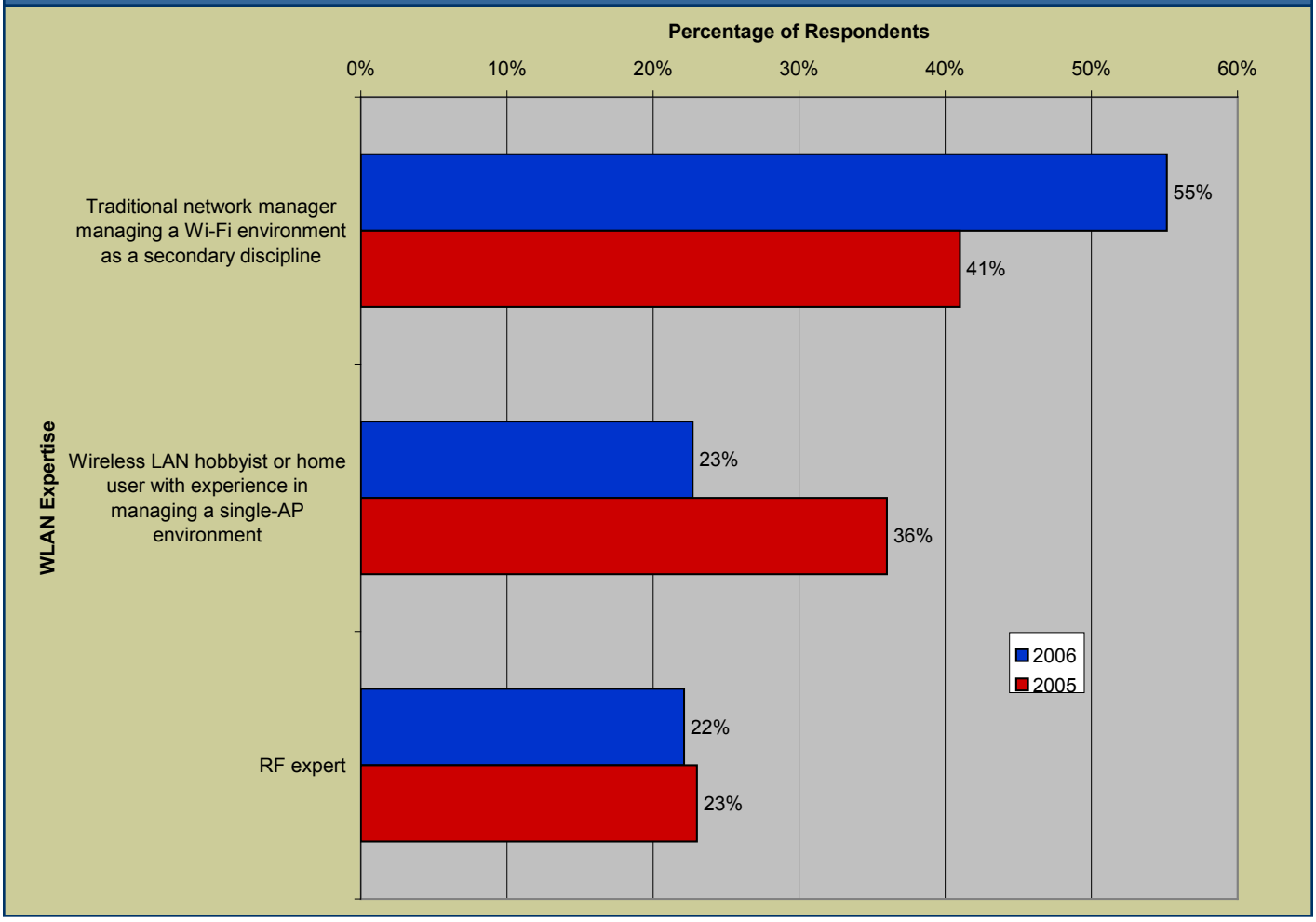


Figure A2. Please rank the importance of deploying each of the following mix of wired and wireless technologies in your network over the next 18 months on a scale of 1 (unimportant) to 7 (critical).

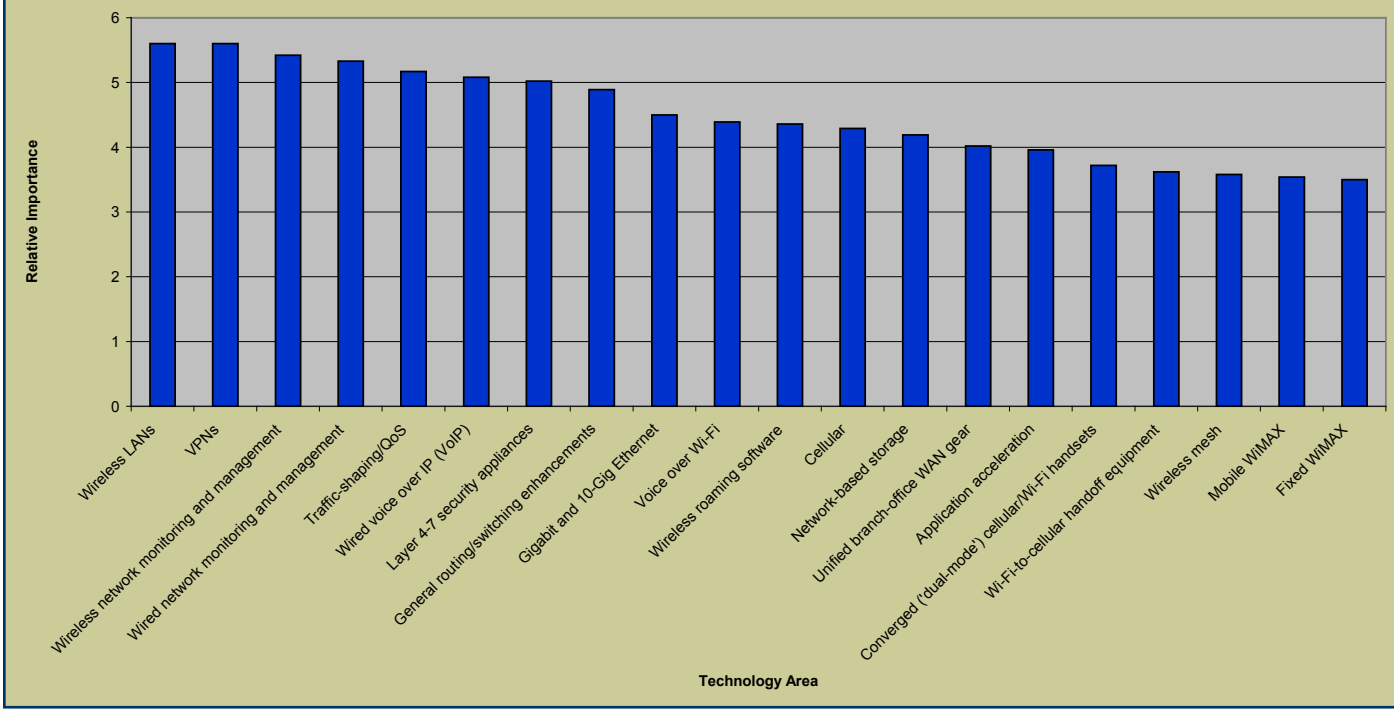


Figure A3. How many employees are there in your organization?

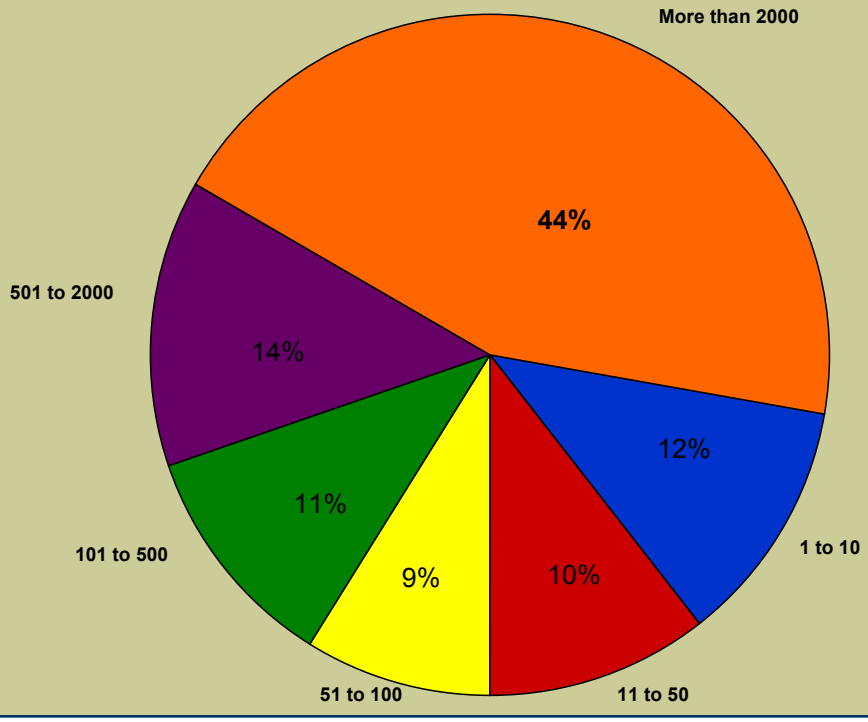


Figure A4. What are the THREE most challenging factors in justifying or deploying wireless LANs? (Top factors only shown here.)

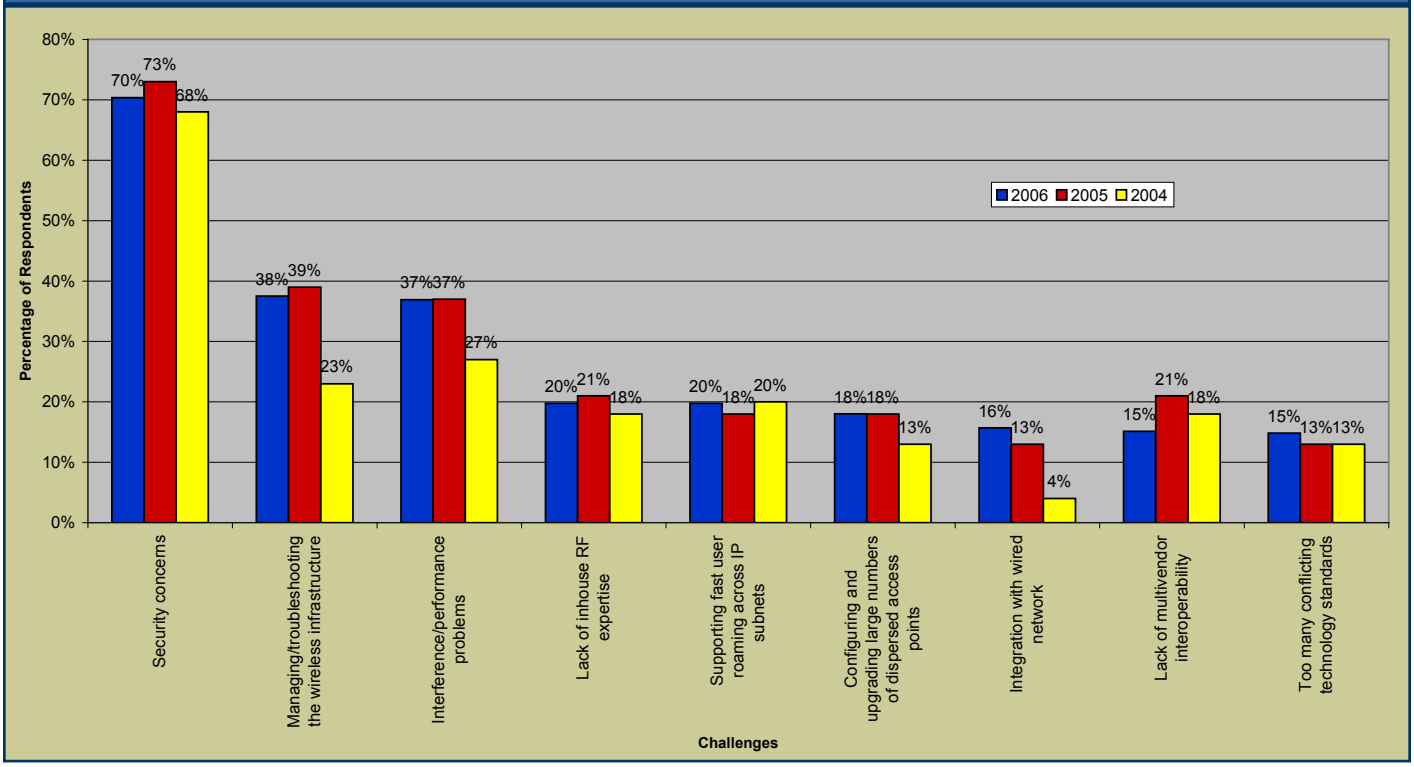


Figure A5. How would you rate your company relative to how rapidly it adopts new technology?

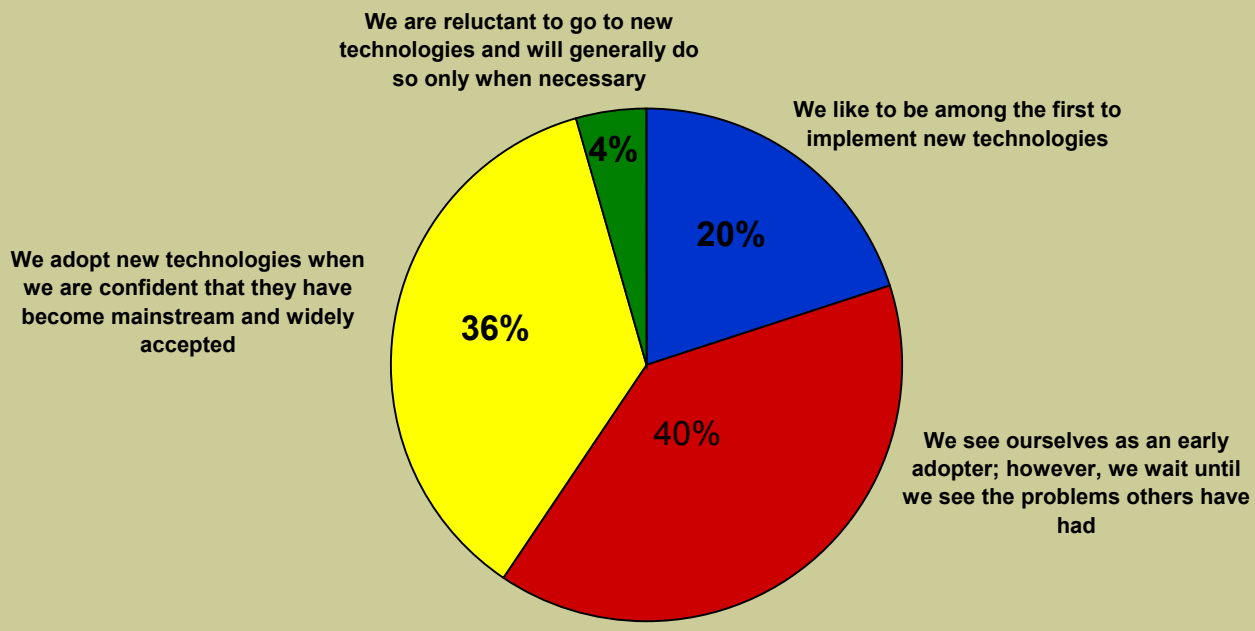


Figure A6. Please indicate the timeframe in which you expect each of the products below to be a SIGNIFICANT component of your wireless LAN implementation.

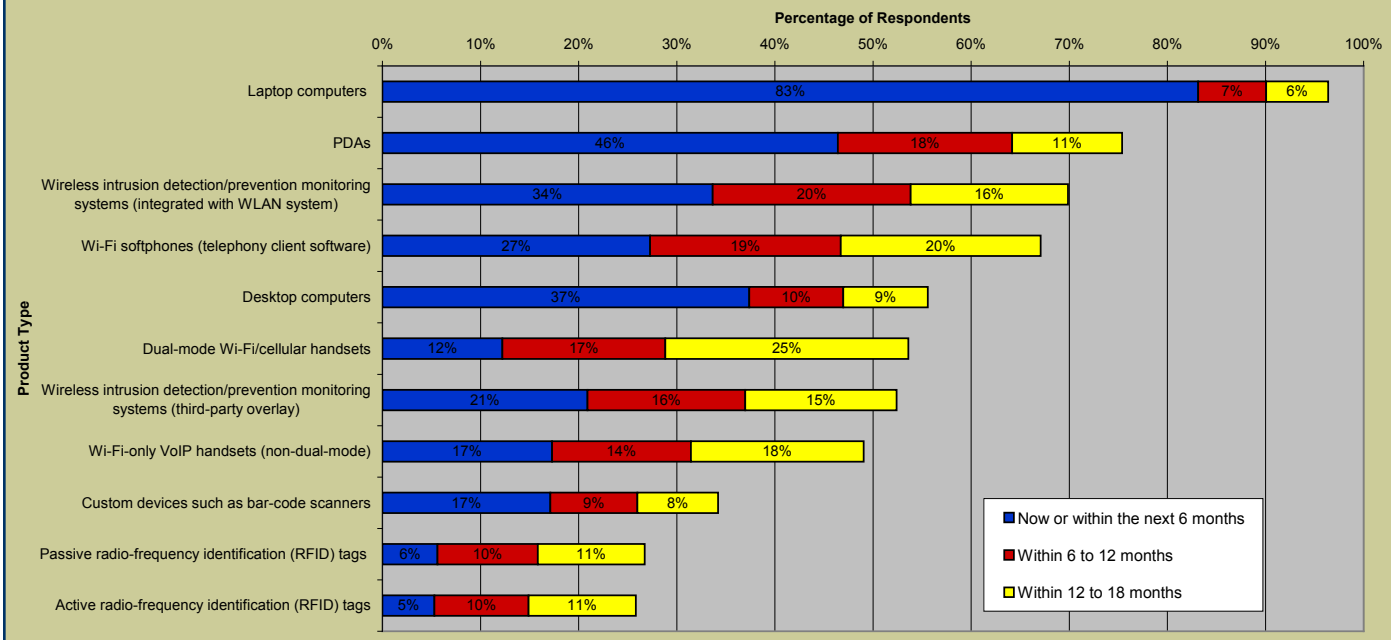


Figure A7. The company you work for most closely fits into which one of the following categories?

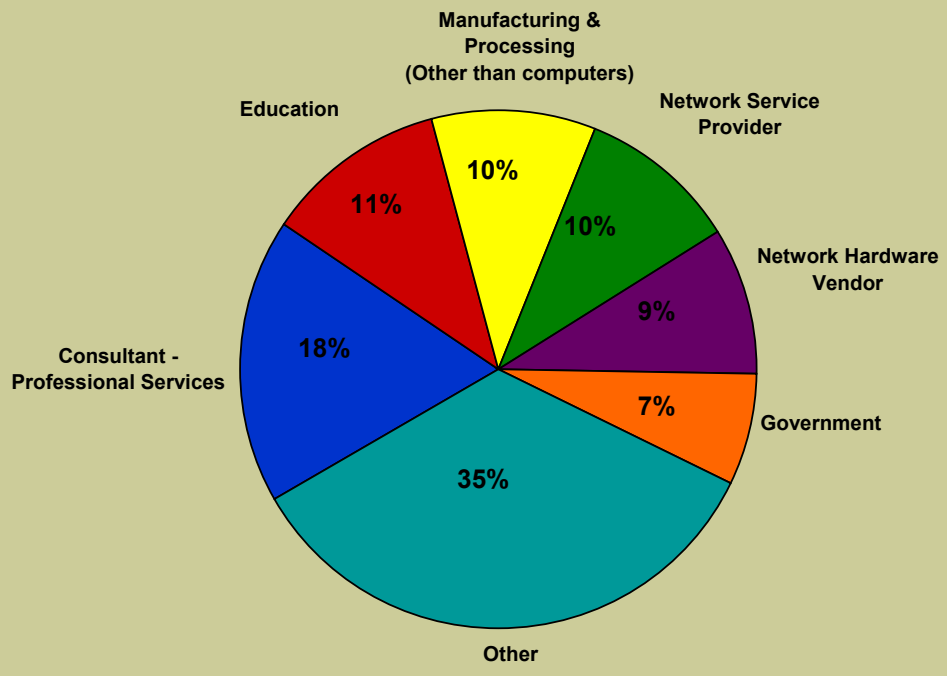


Figure A8. Have you been able to calculate a hard ROI/payback with an existing or planned wireless LAN implementation?

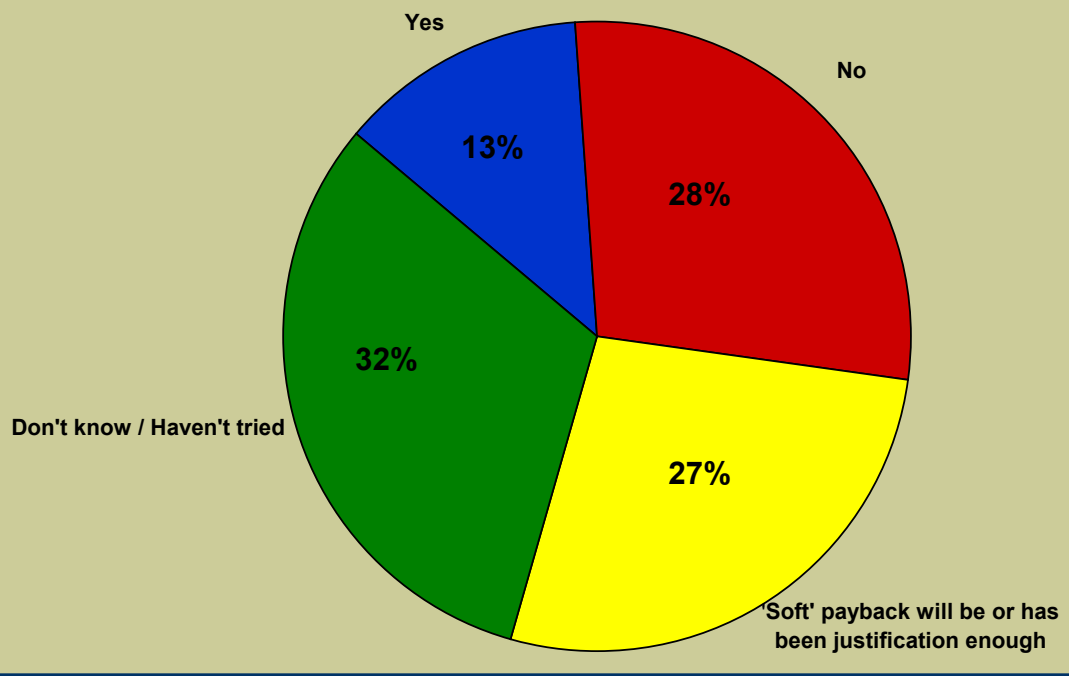


Figure A9. What is your role in your company's wireless LAN implementation?

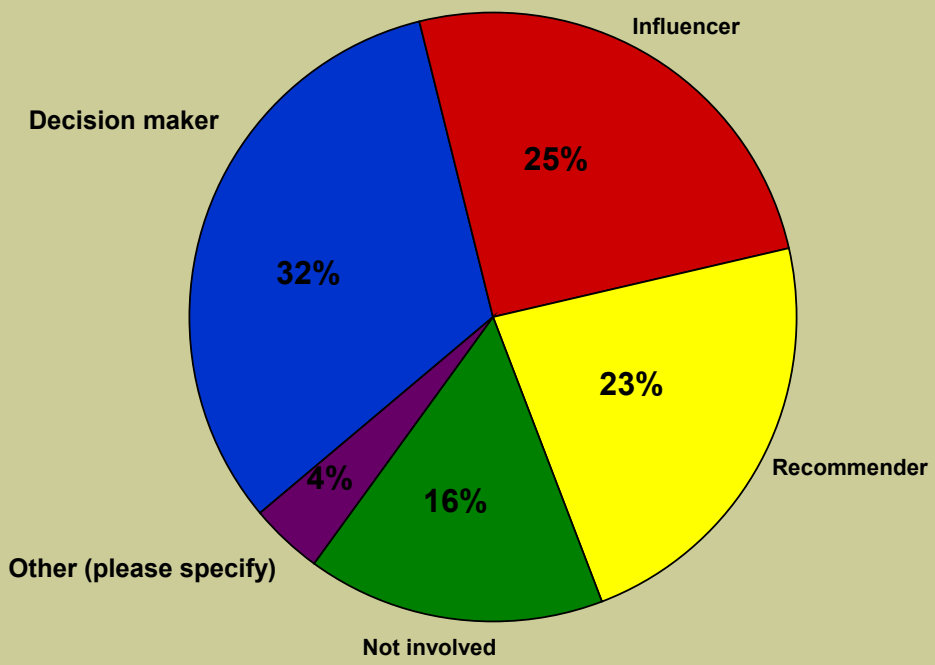


Figure A10. Where is your company headquartered?