APRIL 2005

2005 Wireless LAN State-of-the-Market Report

By Joanie Wexler

Produced By:

Webtorials

Sponsored By:

Colubris NETWORKS

2005 Wireless LAN State-of-the-Market Report

Introduction

The Webtorials second annual Wireless LAN State-of-the-Market Report reveals that significant progress has been made in wireless deployments and wireless security advances in the past year. Webtorials surveyed its subscribers in March 2005 about their status with deploying wireless LANs (WLANs) and the applications and devices driving WLAN usage. Well over a third of this year's 419 respondents were network managers learning to manage a business WLAN environment (as opposed to RF experts or solely home users), and over a third worked for companies with 2,000 employees or more. Their roles in WLAN implementation were fairly equally divided among decision maker, influencer, and recommender, though weighted slightly toward the role of influencer.

The 2005 Webtorials survey unveiled the following trends in the current WLAN arena:

- **WLAN deployments are approaching hockey-stick growth.** Nearly 70% of respondents this year had already deployed business-class WLANs or were in the implementation process at the time of the survey. This figure was significantly up from just over half the respondents (53%) answering the same question last year (**Figure 1**).
- **A variety of WLAN architectures will persevere in enterprise deployments.** Among the respondents in this survey pool, intelligent access points continue to play a strong role. More than half of the respondents said they planned to use intelligent access points with some centralized management/security capabilities. A third said they would use standalone intelligent access points, and a third said they would use a thin access point/wireless switch architecture. Another 16% intend to use mesh routing in their backbones—a fairly healthy reply, given the nascent nature of mesh today. Note that responses were not necessarily mutually exclusive; multiple architectures could be at work in a given enterprise environment.

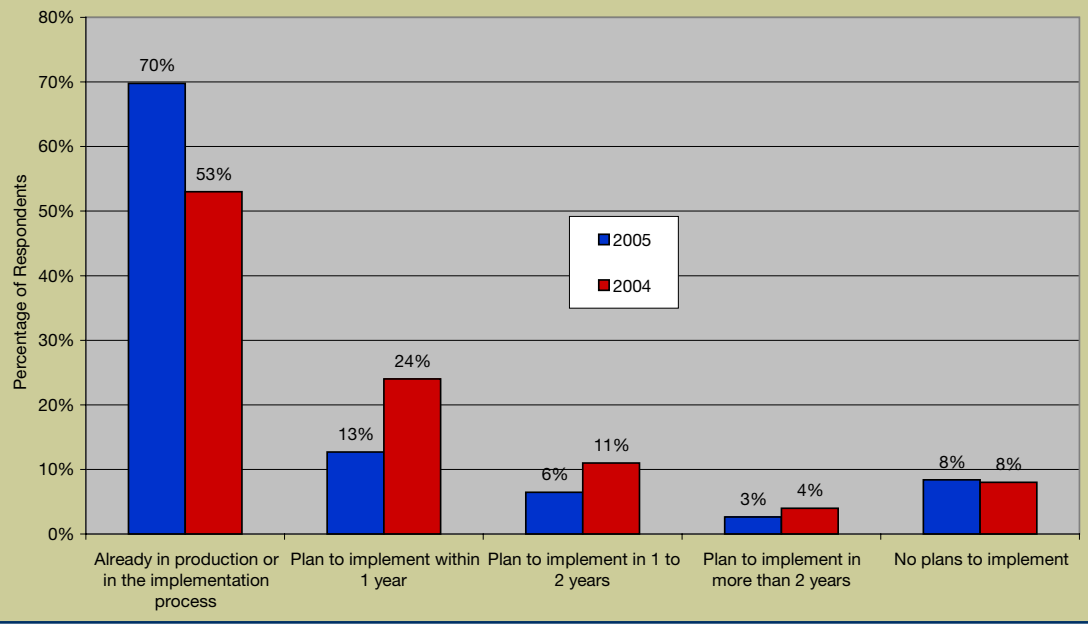
Webtorials State-of-the-Market Reports

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
dvozikis@rcn.com

Figure 1. User WLAN Deployment Timetables



WLAN deployment among the Webtorials subscriber base is quickly moving beyond vertical-application niches and into the "carpeted areas" of the enterprise. The past year has seen a 32% increase in businesses that have WLAN network installations already in place or under way.

- **Improved knowledge-worker productivity and accessibility through mobility still drives most business-class WLAN deployments.** With 48% of respondents citing this factor as one of the two biggest drivers behind their WLAN implementation, it would appear that WLAN deployments have officially moved beyond vertical application niches and into mainstream business use. By comparison, less expensive or simpler-to-implement LAN connectivity was a healthy but distant second WLAN driver cited by 29% of survey respondents.
- **The state of WLAN security is a paradox.** The biggest inhibitor to WLAN implementation today remains wireless security concerns. At the same time, though, most respondents said they now believe that wireless security problems have been solved with available products and technology.
- **Voice over Wi-Fi plans exist, but seem dependent on industry progress.** Responses about deploying 802.11-based handsets and softphones were strewn among survey-takers who were already doing it, planned to be doing it after six months, and were uncertain as to their plans for wireless voice. Similar scores came in for those wishing to deploy dual-mode cellular/Wi-Fi handsets. Given that the devices and applications for such deployments aren't fully cooked yet from a standards and integration perspective, it seems natural that the interest would exist, with commitments contingent on industry support.
- **802.11a's popularity remains limited.** Surprisingly, not only has a low percentage of respondents implemented 802.11a to date, few have plans to deploy it. An even higher percentage specifically plans not to use the 54-Mbps technology, despite the merits of its many nonoverlapping channels.
- **Businesses aren't inclined to pay a lot for Wi-Fi hot spot use.** When asked what service payment model they preferred for their company's use, more than half of the respondents said they prefer their users to either "pay by the drink" or that they allow users to only use services that are available as an amenity. A significantly smaller percentage was interested in committing to wireless service subscriptions.

Market Background

The past few years have seen many changes in the WLAN market. A bevy of startup companies emerged with new system architectures and products aimed at solving the scalability, device management, radio-frequency (RF) monitoring and management, and security challenges that threatened to rear their heads as WLANs positioned themselves to grow into large, mainstream enterprise deployments. A variety of architectures remain, and more continue to emerge.

It is becoming clear that no single architecture will "win" for all environments. Large installations require solutions that allow them to quickly manage and secure hundreds or thousands of access points at an affordable price and to monitor and manage the RF airspace in an automated manner. However, there are, to quote a cliché, a number of ways to skin a cat.

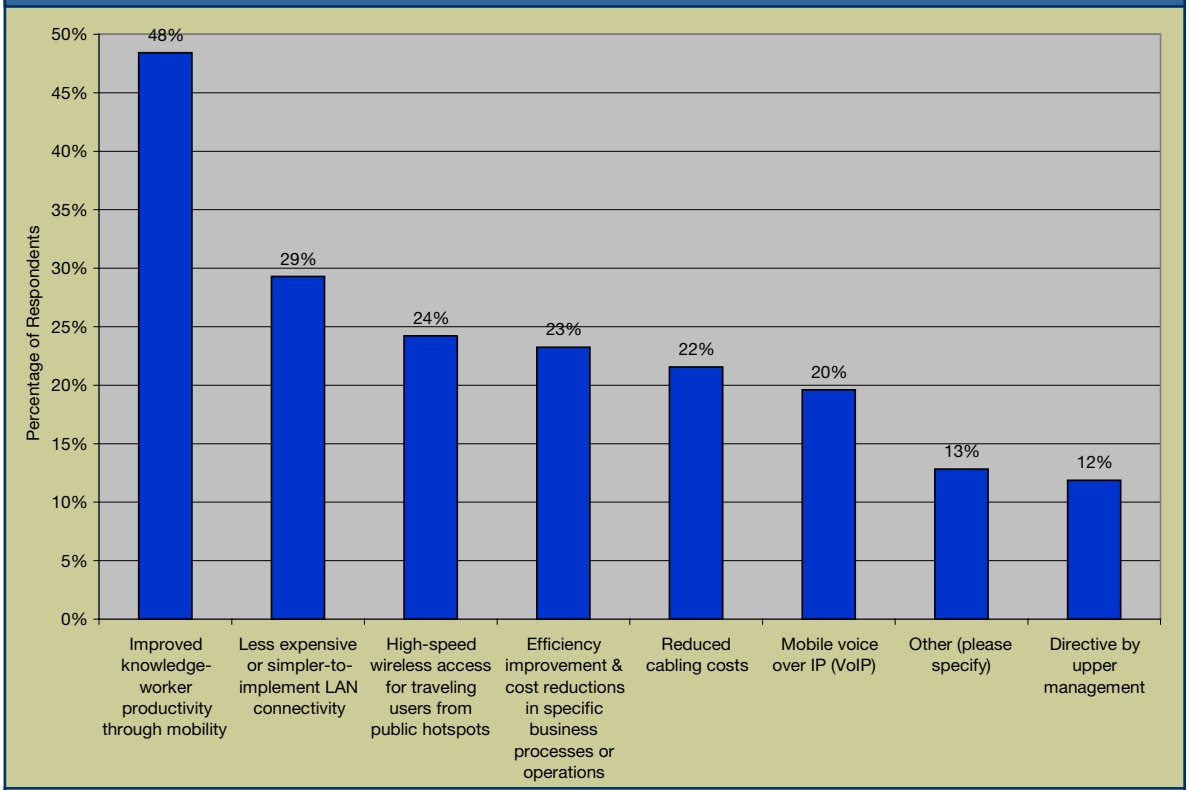
A key milestone this past year was the ratification of the 802.11i security extension, which seems to have hypothetically quelled user fears about wireless security. Many such fears stem from wireless' inherent tendency to "bleed" through walls, ceilings, and floors and for wireless devices to naturally auto-associate with other wireless devices—authorized or not—potentially opening the door to data hijacking, eavesdropping, and piggybacking onto corporate network connections.

802.11i includes an Advanced Encryption Standard (AES) mode of operation for WLAN use, preauthentication of users for fast, secure roaming, and peer-to-peer communications security. It also requires products to rotate encryption keys on a per-packet basis and, in enterprise environments, use the industry-standard 802.1x framework for authentication with an Extensible Authentication Protocol (EAP) algorithm of the network operator's choice.

The past year has also experienced hype in the area of voice over IP (VoIP) over 802.11, a.k.a "Wi-Fi" networks. The standards progress here has been slower, though a portion of the key quality-of-service (QoS) standard, 802.11e, has been completed. The Wi-Fi Alliance, an industry consortium organized to hasten Wi-Fi use and standards adoption, took action similar to what it did when 802.11i was being developed in pieces. Last fall, it began certifying product interoperability among the completed component of the 802.11e standard for packet-prioritization—dubbed Wi-Fi Multimedia, or WMM—so that the industry could begin benefiting from some of the advancements.

Still, integration and development work between WLANs and IP PBX call-routing platforms will be necessary before VoIP-over-Wi-Fi deployments can truly ramp up. The general lag in this effort could be why respondents to the 2005 WLAN State-of-the-Market Survey showed a measure of ambivalence about their VoIP-over-Wi-Fi deployment plans.

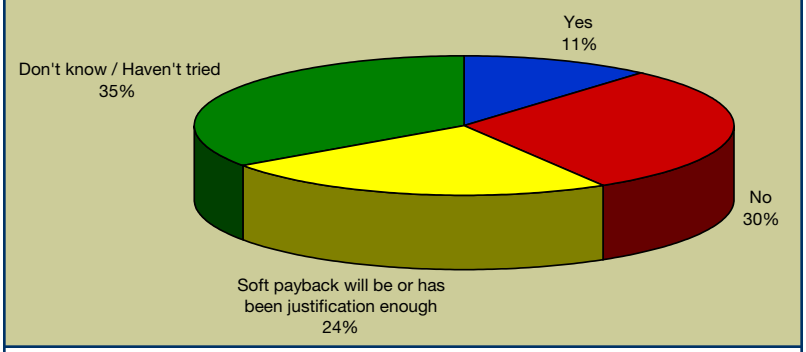
Figure 2. Primary WLAN Deployment Drivers



Enterprises' primary motivation for deploying WLANs is to empower knowledge workers. Implementations seem to be somewhat grass-roots-oriented, because "directive by upper management" ranked dead last as a driver.

To date, the two areas of technology have largely remained isolated; bringing the intelligence of the two together, however, would enable important functions like extending busy signals reflecting crowded airwaves out to Wi-Fi phones and providing IP PBXs with the location-tracking information needed to extend E911 emergency calling services to 802.11 callers.

Figure 3. Have Users Calculated a Hard ROI for WLANs?



Most enterprises don't feel they need to justify WLAN deployment with hard payback numbers.

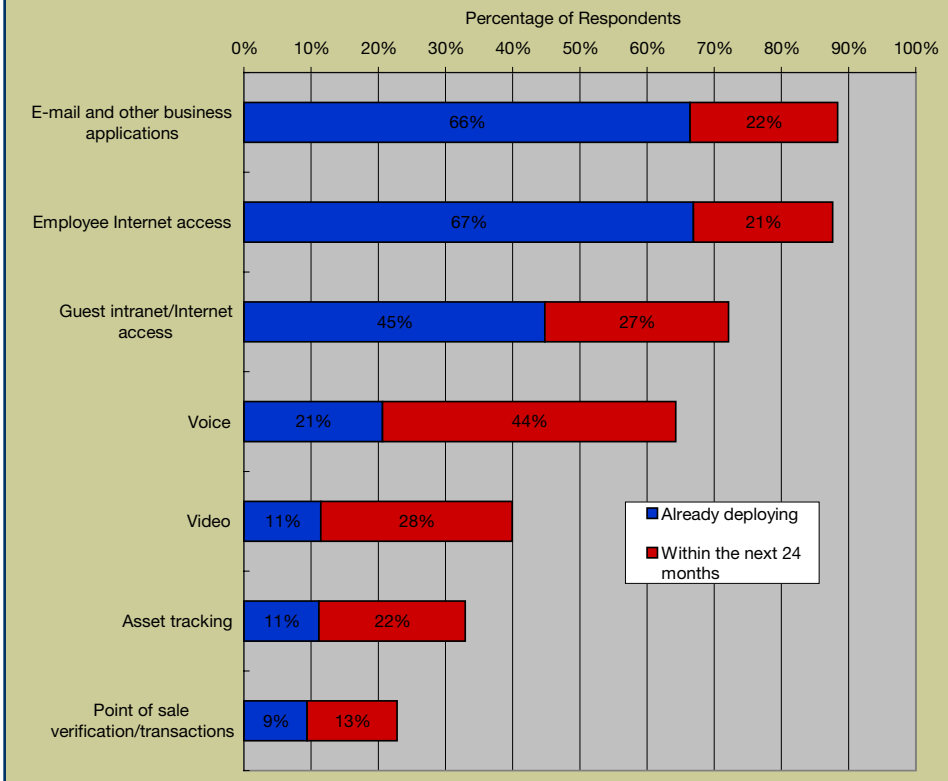
Why Enterprise Deployments Are Booming

Nearly 70% of the Webtorials survey respondents have already deployed WLANs or are in the implementation process, a significant jump from last year's 53%. There are a number of technology and market contributors to this progress:

- WLAN maturity, particularly of 802.11b and g, whose chip prices have reached commodity status, and the promise of forthcoming 802.11n, which will surpass 100-Mbps speeds
- Centralized network management and RF monitoring systems for large installations have both matured and proved in, providing enterprises with the tools they need to affordably scale, manage, and secure large numbers of wireless access points and clients
- Ratification of 802.11i and the perception that most security issues associated with wireless are now solvable with multiple layers of technology
- Further emergence of wireless tools that discover and, now, offer the option to set policy to automatically disable unauthorized, or rogue, devices connecting to WLANs
- The availability of automated RF tools to help networks "self-adjust" to environmental conditions, reducing the level of RF expertise and manual labor required by customers to install and maintain WLANs

Aside from these product and technology advances, however, there is a general perception that, with wireless

Figure 4. Plans for WLAN Applications



Wirelessly enabling traditional IP apps, along with providing guest Internet access, are currently top priorities for 802.11-based rollouts.

laptops and, increasingly, handheld devices shipping with embedded 802.11 connections, WLANs have simply become a natural part of everyday work life. Ironically, many companies that have elected not to install production WLANs, in fact, run WLAN sensor networks for security reasons. The point of these sensor networks is to detect rogue wireless devices that might be connected directly to their Ethernet switches.

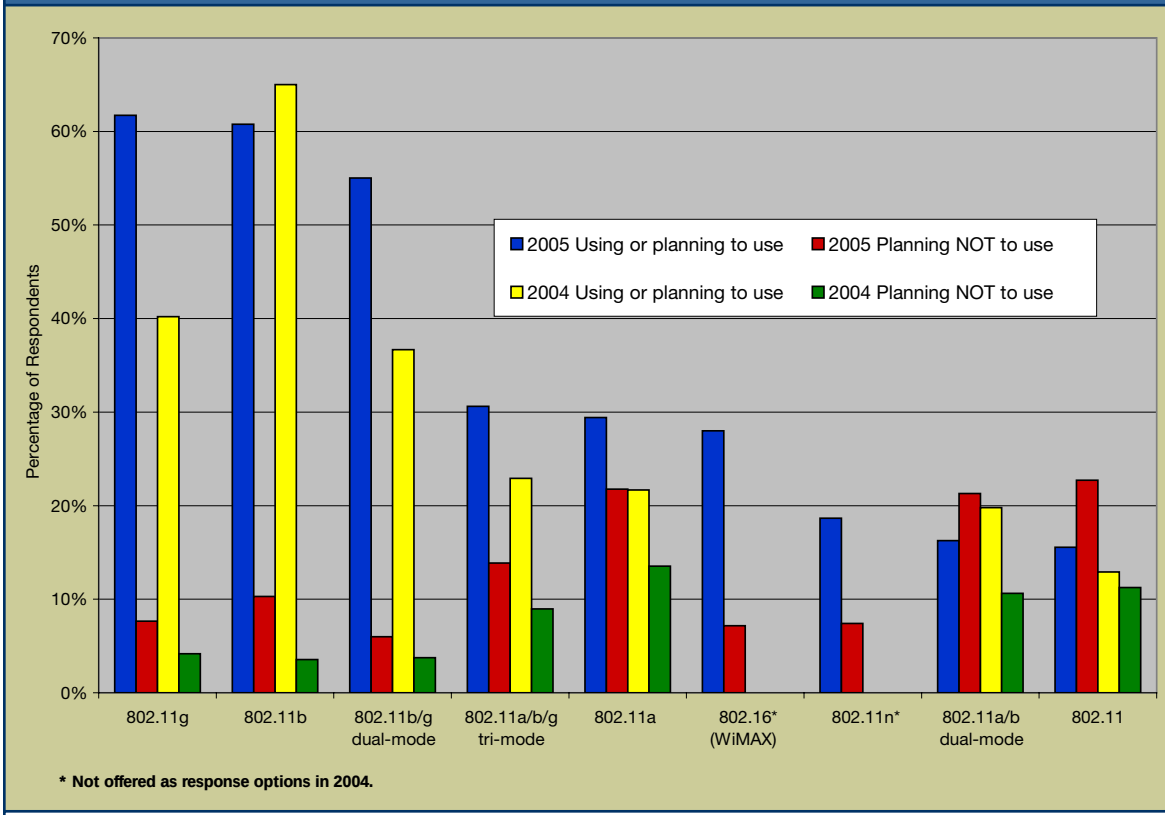
Business Drivers

Companies have long operated WLANs for specific healthcare, inventory and retail management applications. Wi-Fi networks at this juncture appear to be permeating traditional office corridors so that employees who tend to be mobile by nature—often in attendance at meetings, for example—can improve their productivity and accessibility when away from their fixed work spaces. Survey respondents acknowledge that, for the most part, it is difficult to calculate a hard return on investment (ROI) with using WLANs to extend email, Internet access, and other traditional business applications—as well as "guest Internet access" to contractors, business partners, and others—yet, the soft ROI apparently is worth the investment for most Webtorials survey-takers.

Technology Drivers

IEEE 802.11b networks, which run at a theoretical maximum of 11 Mbps, are installed in the majority of respondents' networks. This is natural, as 802.11b, ratified as a standard in 1999, is the only multimegabit-speed wireless technology that has been available from multiple sources for several years. (Though the 802.11a standard was ratified the same year, as a more complex standard, 802.11a products didn't begin shipping from multiple sources until 2003.) However, 802.11b's 2.4GHz cousin, 8021.11g, is quickly catching up, with a majority of users saying they had deployed the 54-Mbps WLAN and nearly half noting that they had installed dual-mode 802.11b/g radios. 802.11g was ratified as an IEEE standard in mid-2003.

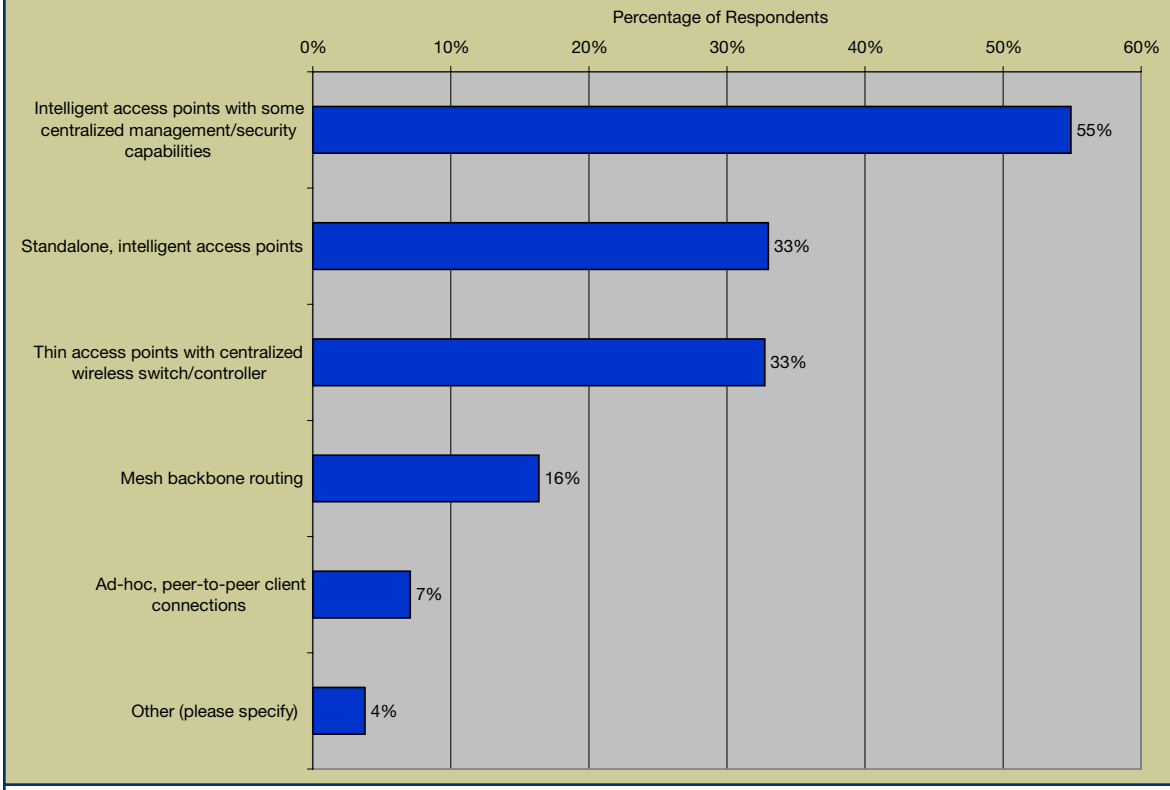
Figure 5. What Types of Networks are Users Deploying?



802.11a has not raised its profile much in the past year. Users considering running real-time traffic or needing more than a few megabits of capacity before 2007 or 2008 when 802.11n kicks in should reconsider their aversion to 802.11a. Its eight-fold improvement in the number of nonoverlapping channels offers better immunity to interference, as well as traffic segmentation for QoS.

The perception of investment protection is most likely at the root of 802.11g's popularity. Because the two networks share the same fre-

Figure 6. WLAN Architecture Preferences



Enterprises seem likely to use a mix of wireless architectures. It appears that enterprises haven't universally bought in to the concept of slimmed-down access points and WLAN switches.

quency band and due to some IEEE standards specifications, 802.11g is backward-compatible with 802.11b, able to service both 802.11g and 802.11b clients. However, in part because of the limitation of three nonoverlapping channels in the 2.4GHz band, in which both networks operate, most 802.11g network infrastructures suffer performance degradation in the presence of 802.11b clients, many failing back to 802.11b's 11-Mbps performance rates. (Note, though, that some vendors have designed ways around this problem.)

Yet there remains a relatively low interest in deploying 802.11a, which runs in the 5GHz band at the same theoretical maximum speed as 802.11g (54 Mbps). While 802.11a networks are not backward-compatible with 802.11b clients, the additional channels available with 802.11a and its high speed in a separate band bode nicely for large-scale wireless implementations in general and the success of VoIP over Wi-Fi and other real-time traffic.

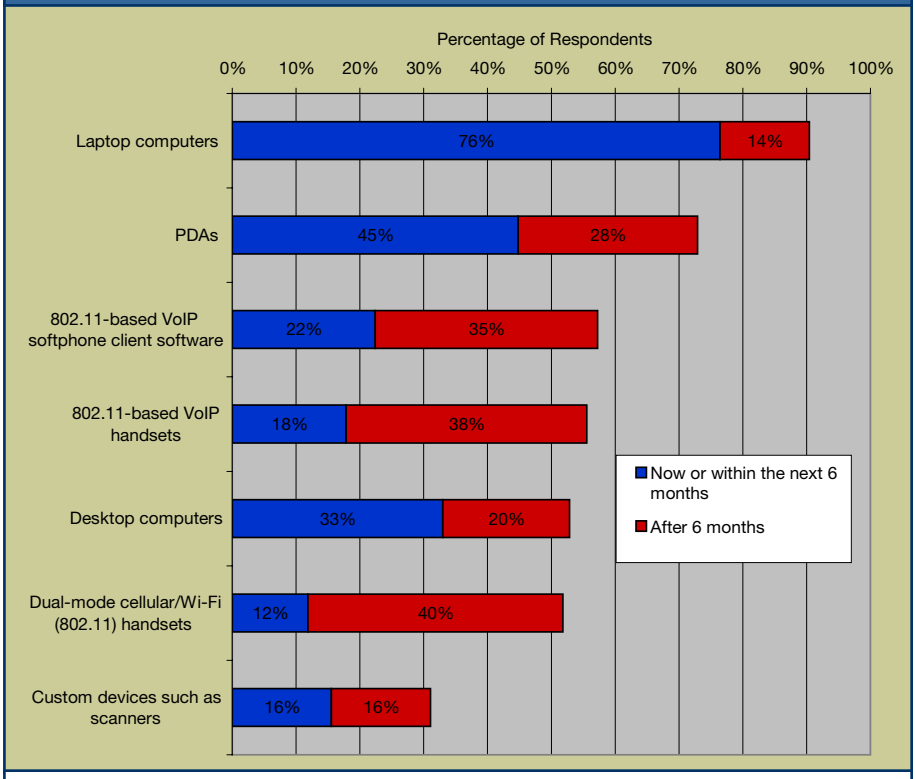
802.11a brings to the table the additional channels needed to avoid interference—cited by survey respondents in Figure 8 as the second largest challenge to WLAN deployments next to security. Use of the technology will likely also contribute to improved QoS, as network implementers can potentially put real-time voice conversations on certain channels and data on others. It could be that 802.11a will simply be passed over for 802.11n (though standards-based 802.11n products won't be available until at least 2007) or even WiMAX (802.16), an alternative network type, as respondents indicated more aggressive plans to implement these two types of networks than 802.11a.

Only about a quarter of the respondents indicated plans to deploy 802.11a, and nearly a third said specifically that they will not deploy it (see **Figure 5**). A chicken-and-egg reason could exist: One of the primary benefits of 802.11a, as mentioned, could be for segmenting real-time traffic, such as VoIP, as a QoS technique. However, at the time of this writing, there are no 802.11a VoIP handsets on the market.

Architecture and Product Preferences

From an architecture perspective, it seems that enterprises still wish to retain some intelligence in their access points, yet preferences seem to embrace the gamut of intelligent and at least somewhat slimmed down access points. Certainly, there is a preference for centralized management for scaling large deployments. Survey-takers were asked to check all of the architecture types that they intended to deploy in their environments, and more than half (about 55%) said they would use intelligent access points with some centralized management and security capabilities (see **Figure 6**).

Figure 7. Wireless Client Device Deployment Timetables



Enterprises will connect a mix of device types to their wireless networks for both strategic and operational reasons.

On the client side, 90% of respondents are either using laptop computers as a significant component of their WLAN implementations or plan to. Given that most notebooks now ship with an integrated Wi-Fi network interface card (NIC) for a negligible price premium, it would be difficult not to have notebooks play a role in a WLAN installation. Personal digital assistants (PDAs) are a strong second in the mix.

Desktop computers ranked third, which, combined with a healthy vote for using wireless to reduce cabling costs and for less expensive or simpler-to implement LAN connectivity (Figure 2) indicates that WLANs are not exclusively about mobility, but also have some purely operational and cost motivation behind them. Generally, industry consensus is that a single cabling drop costs about $150. It's easy to see how these costs quickly add up in large enterprises.

Interestingly, dual-mode Wi-Fi/cellular handsets have appeared on the scene. While such devices are in scarce supply today, 40% of respondents indicated they intend to deploy them after six months, presumably when the industry makes them available after solving some of the tricky hand-off challenges between cellular and Wi-Fi networks. Some service provider business models are expected to emerge whereby carriers, for example, blend wide-area and local-area mobile phone service, invisibly transferring cellular calls to the enterprise local WLAN (with local IP PBX features supported) and to WLANs in public hotspots for a consolidated monthly fee.

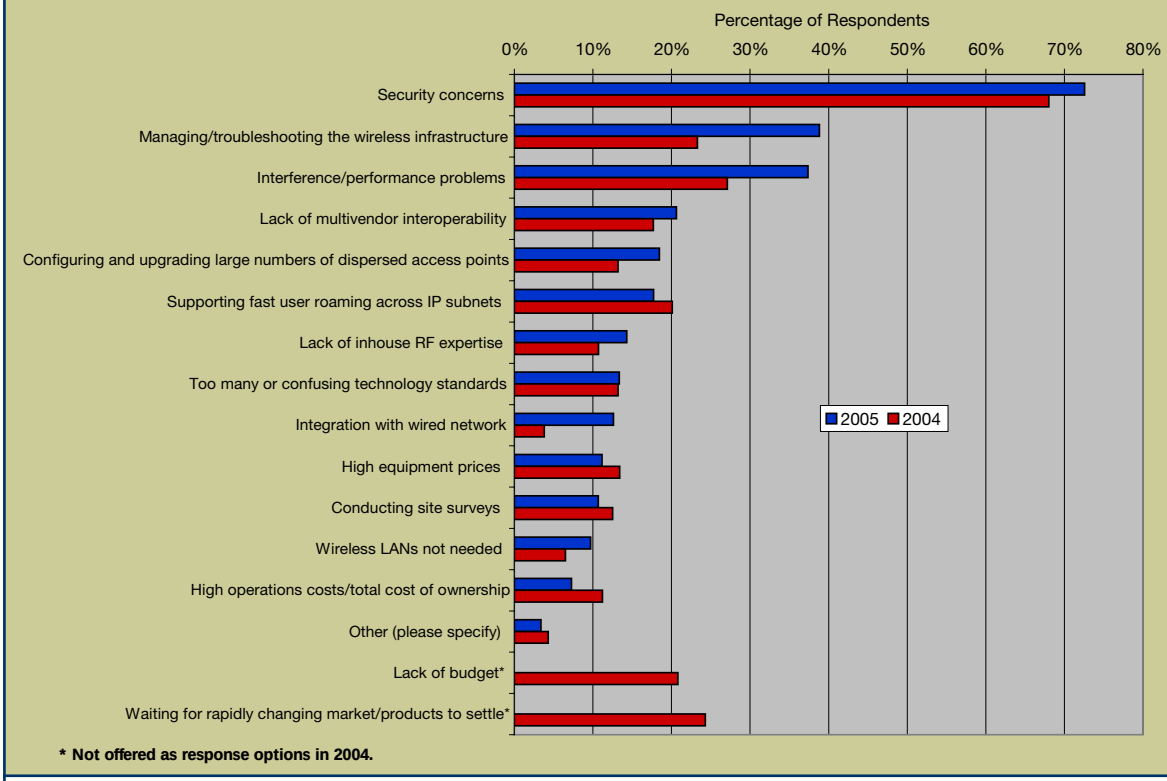
From a user mobility perspective, this would eventually work to truly give users a single universal phone number with features that would follow them around and work the same way wherever they are, along with "presence management" capabilities that could begin to eliminate some of the phone tag productivity problems that plague many workers today.

Security: The Good News and the Bad News

A healthy number of survey respondents (well over a third) state that they believe that most WLAN security problems have been solved with technology, such as Wi-Fi Protected

Access (WPA) and WPA2/802.11i. Paradoxically, however, users continue to cite security concerns as the largest impediment to WLAN deployments (see **Figures 8 and 9**).

Figure 8. Top-Ranking Challenges in Deploying or Justifying WLANs



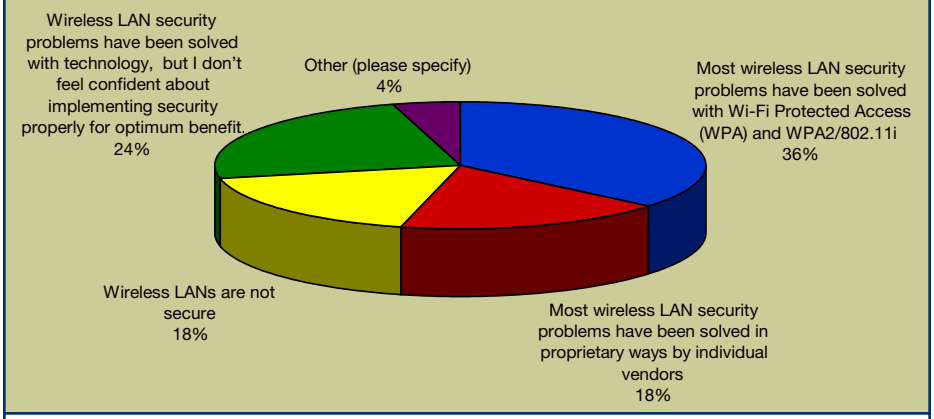
Security concerns still present the biggest perceived obstacle to WLAN rollouts.

Accounting for the seeming discrepancy in these answers is the fact that nearly 24% of respondents also stated that they don't feel confident about implementing security properly for optimum benefit. In other words, while the user community believes that the technology exists to build a secure wireless network, its confidence levels in getting the i's dotted and t's crossed to feel truly secure is shaky at this point.

Still, most respondents seem to be taking the right precautions; 42% are using virtual private network (VPN) technology with all WLANs today. A solid mix of strong security approaches is in use, including a fairly impressive deployment of 802.11i (22%), given that 802.11i-compliant products only became available within the past half-year or so.

It is incumbent upon the vendor community to better educate users about the various components of securing a wireless network and present them with a high-level decision tree of all the threats that need addressing and the options available for doing so. Even handier will be vendors' further automating the process of "turning on" these components as network administrators set corporate policies.

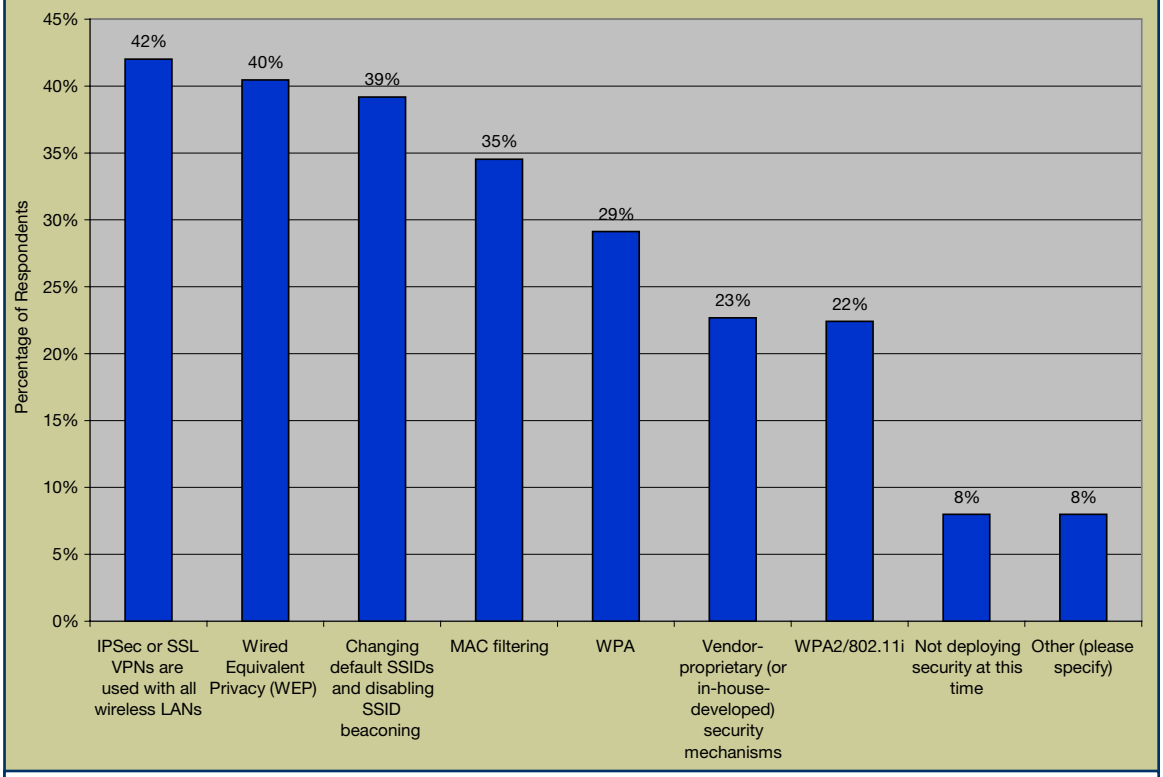
Figure 9. User Opinions on the State of WLAN Security



Users seem more concerned about security implementation than about the strength of available technology.

In addition, regular security audits of the WLAN (and wired LAN) are a recommended enterprise best practice by The SANS Institute, a Bethesda, Md., organization that offers information security training and certification. This involves regularly checking each AP's configuration to make sure it accurately reflects the organization's internal security policies and using RF analysis to verify that airborne packets are indeed using the EAP algorithm selected.

Figure 10. How Users Are Securing their Wireless Networks



Despite low confidence levels in executing wireless security strategies, survey respondents seem to be using an appropriate mix of defensive measures to protect their networks.

And continual scanning for rogue devices that are not authorized to be connected to the network is also becoming a de facto best practice. Scanning can be performed by a separate, overlay monitoring sensor network or by more recently available access-point networks that perform double-duty forwarding traffic and conducting scans.

Wireless Voice Ambivalence

Wireless VoIP is on users' radar screens, but concrete plans for deployment seem elusive. A look at Figure 2, for example, shows mobile VoIP near the bottom of the list of wireless LAN implementation drivers. Figure 4 reveals that fewer than a quarter of respondents are already deploying wireless voice, but if you add up user plans over the next couple years, the application does gain traction. As mentioned earlier, what's likely going on here is that enterprises without a specific vertical market need are concerning themselves first with the data portion of the rollout and awaiting QoS and roaming standards and solutions to be completed by the industry (and possibly 802.11a handsets) before tackling voice.

The primary motivation for VoIP over Wi-Fi, according to the survey, 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 11**). Still, saving toll charges compared with cell phones, the simplification of moving user work stations, and the potential for presence management (having other users' reachability status across the network) were all reasons to deploy wireless voice. These motivators all scored high last year, as well, but each gained additional percentage points this year (multiple responses were allowed both years), indi-

cating that their perceived value has increased in the eyes of the respondents.

Conclusions

In general, Webtorials readers who participated in this study are rapidly embracing WLANs for general business benefits. Indeed, most have already implemented WLANs, and Internet access, email, and other traditional horizontal business applications are the first to go mobile, as organizations hope to make the average knowledge worker more productive and accessible when roaming around campus.

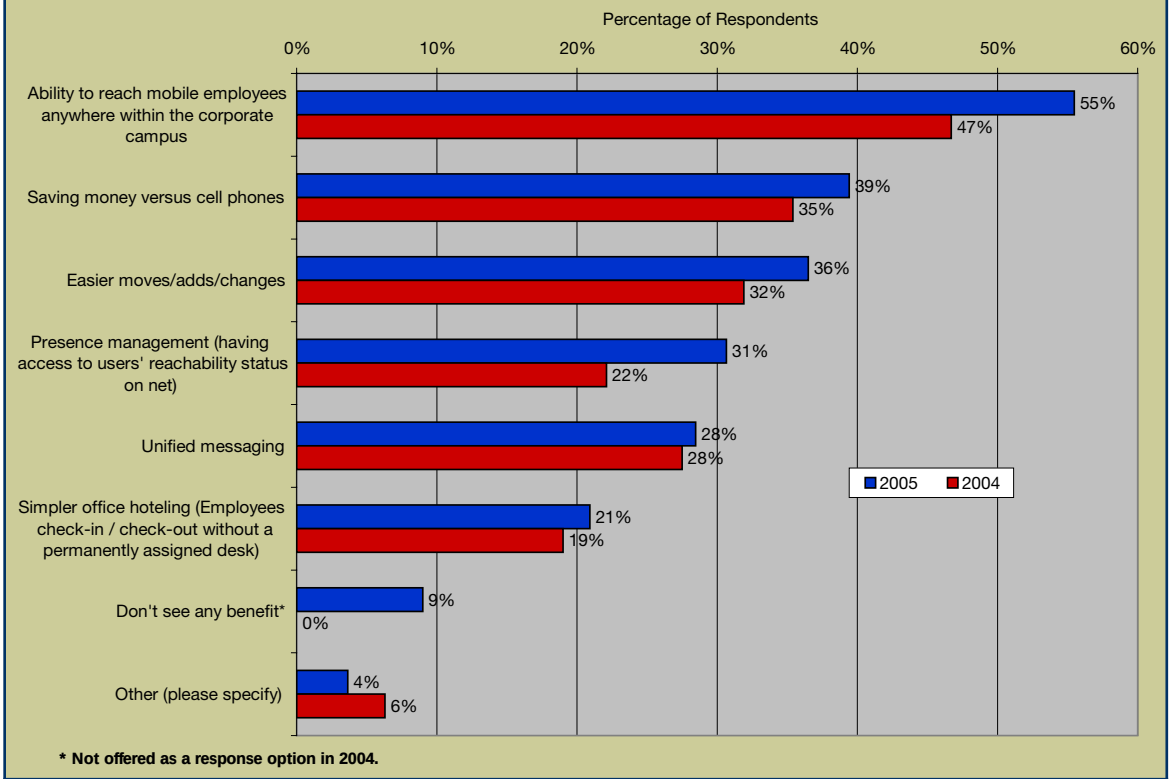
Among the other drivers are the maturation of 802.11-based technology, commodity prices for Wi-Fi chips, the trend toward office mobility in general, and the operational savings associated with wireless connectivity and moves, adds, and changes.

Respondents expressed some ambivalence about wireless security and voice. Most believe that the technology solutions have been delivered by industry to build secure wireless networks, for example; however, they express less confidence in their personal abilities to actually build them without leaving a door open somewhere. Better industry education and automation in security technologies and products and training in best practices are needed to help users accurately implement and audit their products and configurations for optimum impact and confidence.

At first blush, interest in VoIP over WLANs seems anemic, compared to industry hype. However, aggregating user intentions to deploy VoIP over WLANs during the next two years shows that two-thirds of the respondents intend to put voice on their WLANs during that time frame. The reason here could simply be that the industry itself lags in the necessary technology for high-quality wireless VoIP, in the areas of standardized QoS, roaming and handoff technologies (particularly among disparate network types). Also missing are integrated Wi-Fi and cellular client devices, which are capturing a high interest level as users look forward to streamlining their many methods of communications as they grow unwieldy and costly.

In the grand scheme of networking priorities, WLANs continue

Figure 11. User-Perceived Benefits of WLAN-VoIP Integration

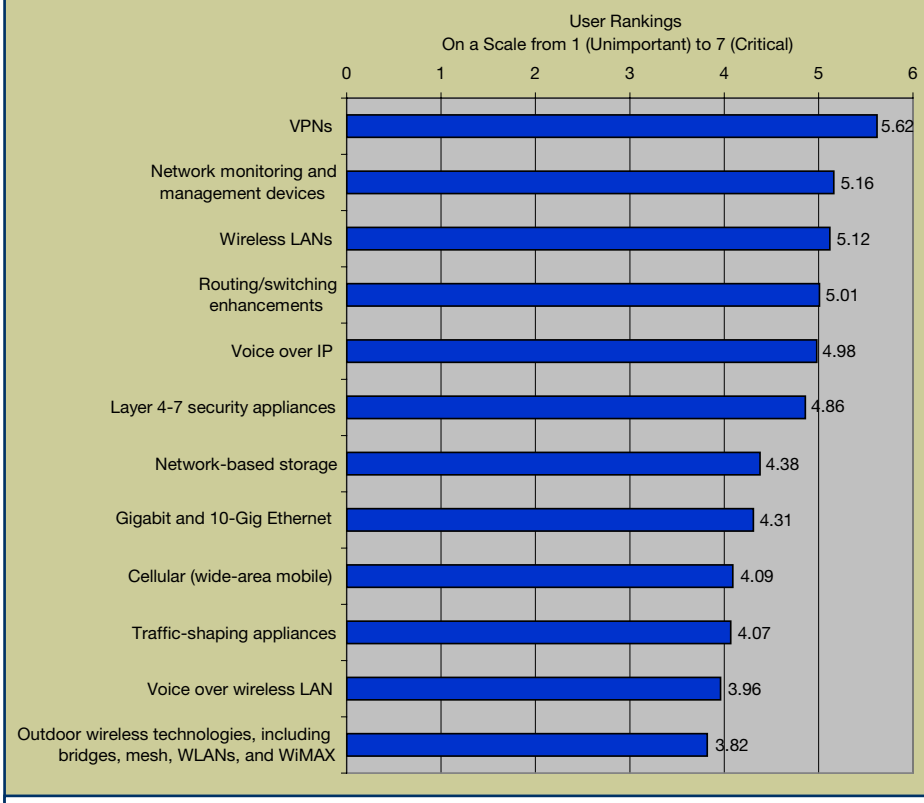


Survey respondents seem to see more benefits this year to the many potential attributes associated with converging VoIP onto the WLAN.

to rank a fairly close third to VPNs and network management/monitoring products in user assessments of the overall importance of network products and capabilities (see **Figure 12**).

The probable reason is that, like it or not, wireless and mobility have become an integral piece of both business and personal life. IT and networking departments really have no choice but to address the technology, much as they were forced to embrace the PC 20 years ago. Hopefully, the vendor community, which has come a long way on innovation and solving security and interference problems, will further beef up its efforts to ease deployment and maintenance of wireless networks, including inter-network roaming and support of real-time traffic, so that the business community will feel comfortable adding more strategic applications to their networks.

Figure 12. Comparative Importance of Network Products and Technologies



WLANs remain one of users' top three networking priorities.

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 Fusion* and contributes frequently to industry trade publications such as *Computerworld* and *Business Communications Review*.

About Webtorials

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.

The Unified Services Network

Merging wireless and wired network infrastructure, management and services: How to get there from here

From the Sponsor

Colubris NETWORKS

No longer an "emerging" technology, wireless LANs (WLANs) have become a widely accepted access medium for both public and private networks. Still, compared to wired LANs, many WLAN solutions fall short in terms of security, quality of service (QoS), cost and scalability. Their overlay design meets only limited business objectives and provides only partial support for valuable new services like voice over IP (VoIP).

Colubris Networks, a leading provider of intelligent WLAN solutions for service providers and enterprises, envisions a future in which wireless and wired LANs come together to form a Unified Services Network. In these unified networks, wired and wireless LANs deliver equivalent price/performance, QoS and security, removing current business limitations and enabling a new generation of untethered applications.

This white paper describes the Colubris vision. It begins with an evaluation of today's WLAN solutions. Then, after describing the Unified Services Network, the paper suggests how today's WLANs will evolve to reach that goal. Finally, the white paper offers a brief look at Colubris Networks' product rollout plans.

Today's WLANs: Separate and Unequal

Wireless LANs are popping up everywhere. WLAN hot spots in airports, hotel lobbies and coffee shops make public Internet access quick and easy. Affordable WLAN routers let home users enjoy broadband cable and DSL services without pulling Ethernet cable through their walls. Enterprise-class WLAN solutions give business users more convenient access to company resources and enable valuable new applications.

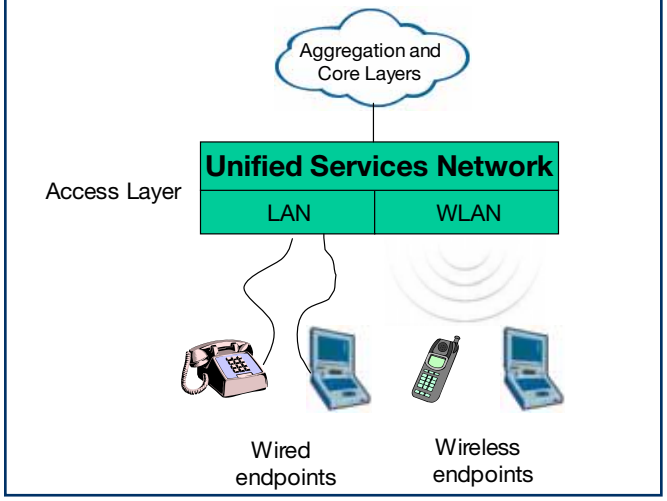
But today's WLANs don't always measure up to wired LANs. The QoS features needed for real-time services like VoIP are not widely available in wireless implementations. Inconsistently applied security policies expose corporate networks to hackers and other threats. Roaming is limited, not only by QoS and security issues, but also by slow handoff times between access points (APs).

The overlay architecture of many popular WLAN solutions presents additional challenges. Because it requires special WLAN switches or appliances operating in parallel with conventional Ethernet switches, the overlay model doubles network management and operations costs and boosts amortized capital expense to over $1,000 per AP. Moreover, the "sweet spot" for performance is only 36 to 72 APs per switch, severely limiting WLAN scalability.

These shortcomings affect enterprises and service providers alike. Without consistent QoS control, for example, today's WLANs can't support converged cellular/WLAN telephony in office buildings or in public venues. Likewise, limited scaling and poor mobility make it difficult for service providers to expand their managed services to include WLANs.

For wireless LANs to become as useful and ubiquitous as wired LANs, these problems must be solved. Today's WLANs must evolve to create Unified Services Networks in which wireless and wired LANs provide equivalent, fully functional access to enterprise backbones and public network services and are managed as a single, integrated network facility.

Figure 1. The Unified Services Network merges wireless and wireline switching into a unified platform.



The Colubris Vision

In the Colubris vision, the Unified Services Network is a single, integrated wired/wireless access network for delivering best-in-class business services (**Figure 1**). With the Unified Services Network, it doesn't matter if an end-user device is wired or wireless, because there are no longer any restrictions on wireless applications. Both access methods support the same array of consistent, unified services:

- QoS – Guaranteed support for multiple real-time and non-real-time applications.
- Security – Layered authentication, encryption, intrusion detection and prevention, anti-virus safeguards, network access control and access lists.
- Application – Full support for voice, video and data applications.

The unified infrastructure supports multiple simultaneous services, with each service tuned to meet specific application requirements. Plus, wireless access supports seamless roaming and location-based services.

The Unified Services Network is created, in part, by merging wired and wireless LAN switching into a single platform that can be deployed throughout the access layer of the enterprise or service provider network. It distributes intelligent policy enforcement to the network edge, where it can be most effective. And by adhering to IEEE and IETF standards for switching, routing, QoS, virtual LAN (VLAN) traffic management, etc., the Unified Services Network integrates compatibly with existing aggregation and core networks. Forward-thinking commercial silicon designers share this vision and have begun shipping chipsets that enable this vision. Unlike the proprietary silicon used by some WLAN switch vendors, these commercial chipsets will deliver next-generation price/performance that enables wide-scale network deployment.

Key services like QoS and security will be built into the unified platforms, amortizing the cost of processing power across large numbers of wired/wireless ports and users. Moreover, the unified switching platform will greatly reduce operations cost and complexity by letting enterprises and service providers purchase wired/wireless access solutions that are manageable from a single network management system (NMS).

Figure 2. Today's WLAN solutions take two forms.

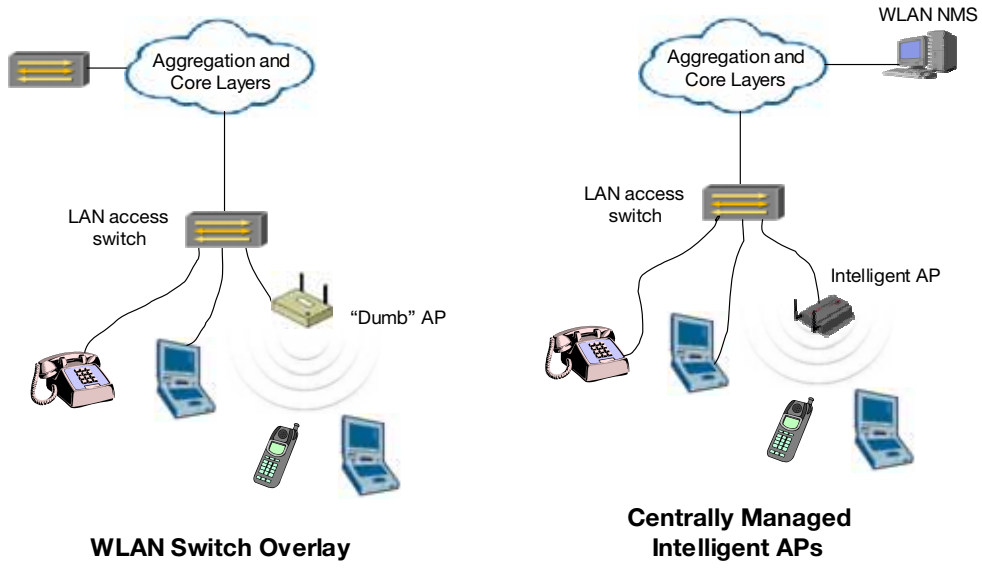
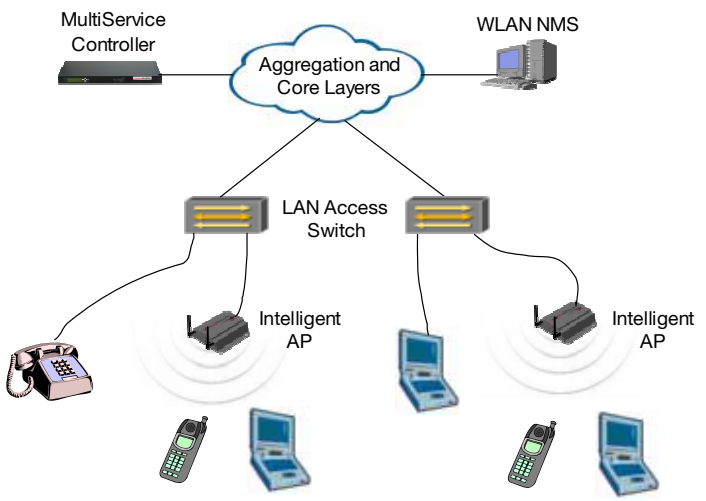


Figure 3. Intelligent APs and a multiservice controller replace the WLAN switch/appliance.



Distributed WLAN Switching

Getting There From Here

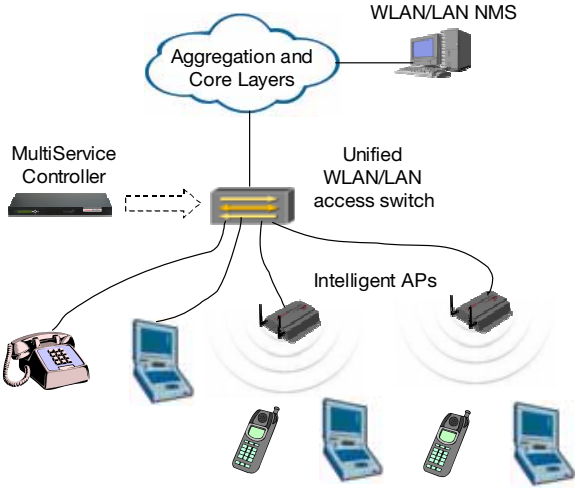
The migration path from today's WLANs to the Unified Services Network has two starting points: the overlay model and the intelligent AP model (**Figure 2**). With the overlay model, traffic between "thin" APs and WLAN switches is tunneled through the wired LAN, making individual flows invisible to the LAN switch. Often, the WLAN switches are deployed in a data center, several "hops" removed from the APs. The switches handle encryption, security and QoS policies, while MAC-layer processing is split between the switches and the thin APs. Since QoS policies are applied at the WLAN switches and not at the APs, outgoing wireless traffic is subject to latency and jitter caused by congestion on the radio-frequency (RF) medium. Each access network—wired and wireless—is managed separately.

In the intelligent AP model, as delivered by Colubris today, no special WLAN switches are required. The APs link directly to Ethernet access switches using standard 802.1p/Q VLAN security and QoS protocols—similar to the trunks between Ethernet switches. The APs are centrally managed from the Colubris NMS. The intelligent APs process the full 802.11 MAC-layer protocol and apply centrally defined QoS and security policies at the wireless edge, avoiding the weaknesses of the overlay model and leveraging the existing wired infrastructure for superior scalability and economy. Individual flows are visible to the LAN switch, enabling it to apply its rich QoS and security processing features to the traffic.

Figure 3 illustrates Distributed WLAN Switching, the first step towards the Unified Services Network. Intelligent APs and a multi-service controller (MSC) preserve the strengths of the two earlier models while eliminating the weaknesses. Conventional LAN switches, which boast much greater switching capacity than today's WLAN switches, handle both wired and wireless traffic directly, while the intelligent APs bring security and QoS enforcement to the wireless edge. (Of course, this is true today with Colubris WLANs.) The MSC provides the centralized control required for seamless roaming, plus RF management and security, but without the scaling constraints of a WLAN switch. The result is a highly scalable, truly multiservice WLAN infrastructure.

One more step completes the migration to the Unified Services Network, as the LAN access switch is replaced with a unified LAN/WLAN access switch (**Figure 4**). The intelligent APs and the MSC remain, although in some implementations the MSC may be integrated with the unified switch or

Figure 4. A unified WLAN/LAN switching platform and a unified NMS complete the migration.



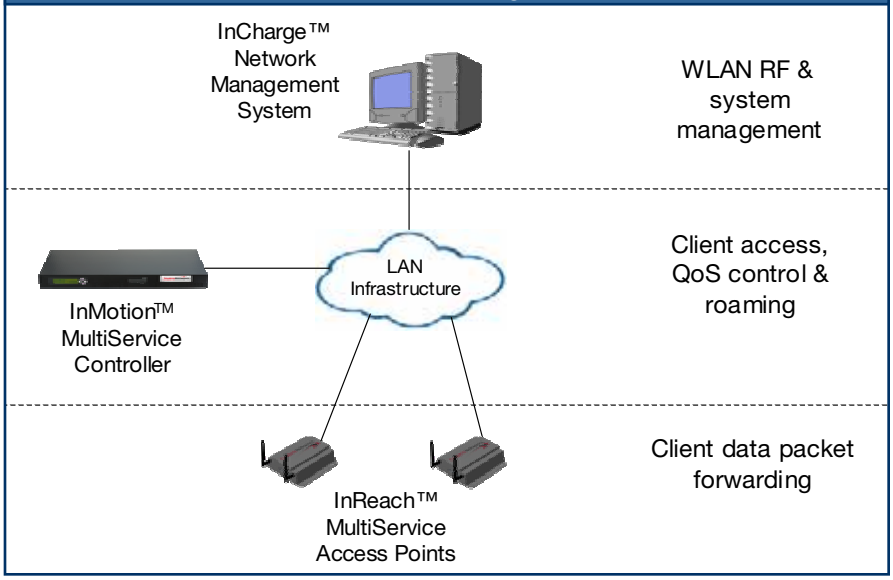
Unified WLAN/LAN Switching

tucked away in a LAN core switch. Leading-edge silicon in the unified switch applies advanced QoS and security controls to both wired and wireless traffic. For dramatically simplified network operations, a unified NMS oversees both types of access traffic.

The Colubris Migration Plan

Colubris Networks has had great success furnishing both service providers and enterprises with WLANs based on centrally managed intelligent APs. Now Colubris has mapped out a product evolution path to the Unified Services Network that parallels the steps described above.

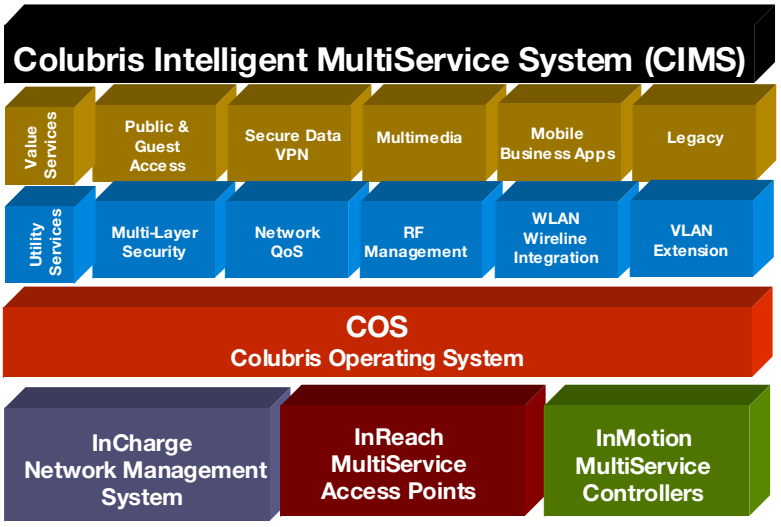
Figure 5. Colubris will introduce its first distributed WLAN/LAN switching solution.



Distributed WLAN/LAN Switching

In 2005, Colubris will introduce its first distributed WLAN/LAN switching solution (**Figure 5**). In this product suite, intelligent InReach™ MultiService APs leverage commercial silicon for highly scalable, highly cost-effective WLAN access. The InMotion™ MultiService Controller supports WLAN QoS, security and seamless roaming without the scaling constraints of a WLAN switch. A protocol interface between the APs and the MSC facilitates auto-discovery and configuration of the APs, RF management and location services. Based on IETF Control And Provisioning of Wireless Access Points (CAPWAP) specifications, the interface ensures interoperability and investment protection. An enterprise or service provider could, for example, add high-speed 802.11n APs in the future without replacing the InMotion MSC. Similarly, existing InReach 802.11a/b/g APs can be used with future unified switches.

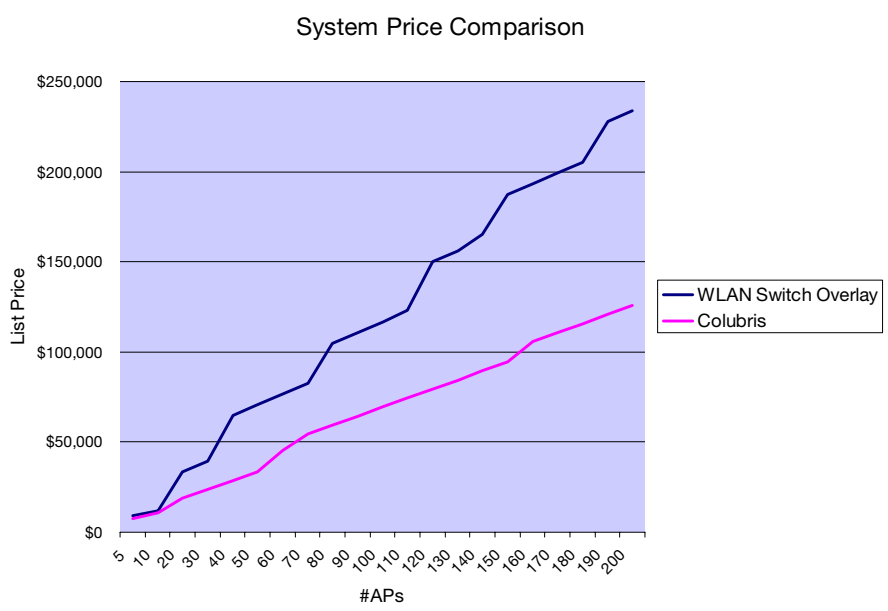
Figure 6. The Colubris Operating System integrates all the components into a single system.



The Colubris Operating System, embedded in the InReach APs, the InMotion MSC and the InCharge NMS, unites the components as a single system and brings the WLAN to true multi-service status (**Figure 6**). Utility services provide the basic "plumbing," including multi-layer security, QoS, RF management and VLAN extension. Building on this foundation, value services furnish higher-layer capabilities such as public and guest access, secure virtual private networks (VPNs), multimedia transport and mobile business applications. Tunable parameters let enterprises and service providers configure WLAN support for still-valuable legacy devices.

Compared to popular overlay solutions, the Colubris distributed WLAN/LAN solution cuts total system cost in half while yielding 10 times greater scalability. This pay-as-you-grow design is complemented by the low opera-

Figure 7. Total cost for the Colubris solution is nearly 50% less than popular overlay solutions.



tions cost of the InCharge™ NMS, which can manage thousands of WLAN elements as a single system.

Unified WLAN/LAN Switching

In 2006, Colubris—in partnership with a leading chip and/or LAN switch vendor—will introduce a unified WLAN/LAN switch that provides consistent access to network services for all users, whether wired or wireless. Ports on the unified switch will accommodate links to WLAN APs as well as personal computers, servers and other standard Ethernet devices.

WLAN functions will be distributed among the unified switch, the MSC and the intelligent APs. The switch, for example, will implement VLAN tagging, L3—L7 intrusion detection and prevention, authentication and wireless mobility. The MSC will handle layer 2 and IP subnet roaming, plus client access control. The APs will implement wireless encryption processing, RF intrusion detection and prevention and a full 802.11 MAC layer. Standard interfaces will ensure interoperability among the WLAN/LAN elements.

The unified access network will enforce QoS at every hop. APs will enforce 802.11QoS protocols at the network edge—where they should be enforced—and translate between 802.11 and 802.3 protocols for consistent hop-by-hop performance. The MSC will provide central control of WLAN QoS policies, monitor QoS performance and cooperate with the switch to load-balance among the APs.

The unified switching platform will take advantage of commercial WLAN/LAN chipsets for reduced capital expense (**Figure 7**). A unified WLAN/LAN management system will minimize operations costs and further enhance network scalability. Overall network security will be strengthened with features like strong authentication of the wireless APs and automatic disablement of switch ports upon detection of wireless rogues. The result will be a best-of-breed Unified Services Network solution—the ultimate merger of wired and wireless into a consistent, fully capable, centrally managed access network.

Conclusion

The handwriting is on the wall. Wireless LANs are no longer an exotic species that exists separately from wired LANs. Instead, based on the latest silicon, wired and wireless LANs are coming together to create a unified, centrally managed platform for best-in-class business services. These new Unified Services Networks will transform WLANs into full-featured counterparts to wired LANs for access to both enterprise and service provider networks. With its intelligent InReach MultiService Access Points, InMotion MultiService Controllers and the InCharge Network Management System, Colubris Networks is not only providing the industry's most advanced WLAN solution today, but is also taking the first major step towards the Unified Services Network of tomorrow.

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 March 2005. A total of 419 respondents participated. Eighty-two percent (82%) of all respondents said they played a role in their company's WLAN efforts, either as decision-maker, influencer, or recommender.

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.

Geographically, Webtorials subscribers in the U.S. responded in the greatest numbers, representing 45% of the survey base. They were followed by 17% in Western Europe (excluding the UK, which represented 7.5%), 12% in the Asia-Pacific region, and 4% in Latin and South America.

Figure A1. What is your Role in your Company's WLAN Implementation?

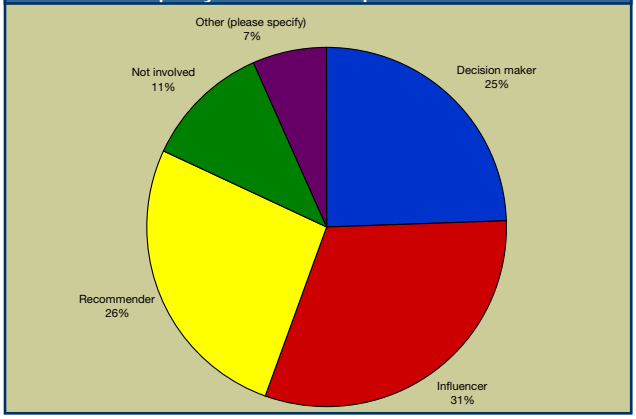


Figure A2. How would you Rank your Expertise with WLAN Technology?

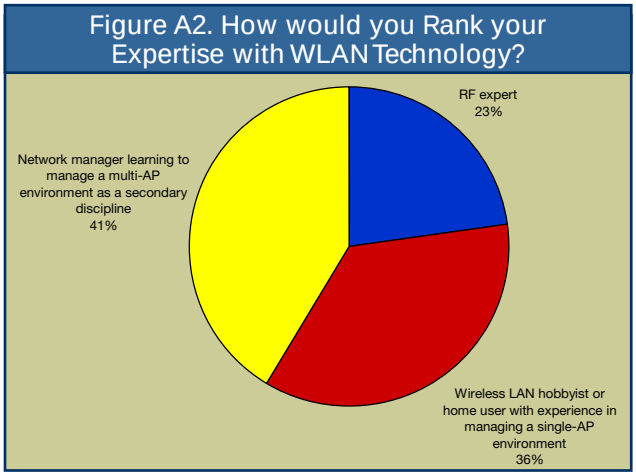


Figure A3. How Many Employees are in your Organization?

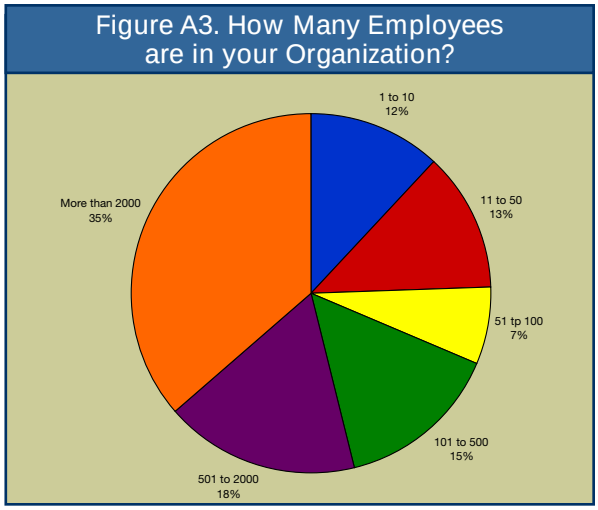


Figure A4. How would you Rate Your Company Relative to how Rapidly it Adopts New Technology?

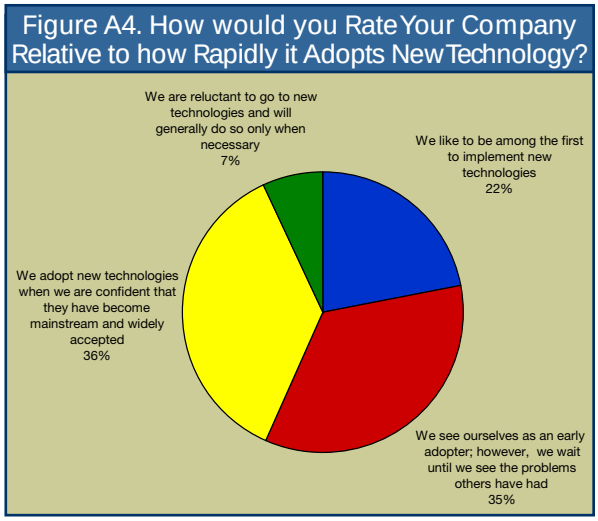


Figure A5. Where is your Company Headquartered?