STATE-OF-THE-MARKET REPORT | OCTOBER 2007

2007 Wireless LAN

By Joanie Wexler

SPONSORED BY

NORTEL

DISTRIBUTED BY

Webtorials

PRODUCED BY

Kubernan
Guiding Innovation
www.kubernan.com

2007 Wireless LAN

Introduction

In June 2007, Kubernan surveyed the Webtorials subscriber base for the fourth consecutive year concerning wireless LAN (WLAN) deployment plans, attitudes, and experiences. This report is a summary and analysis of those findings, culled from a Web-based survey response pool of almost 300 Webtorials subscribers. Only fully completed questionnaires from individuals actively involved with their companies' WLANs have been included in this analysis.

Improved access to mobile employees is the primary driver behind mainstream WLAN enterprise deployments, according to results of the Kubernan 2007 Wireless LAN State-of-the-Market survey. Nearly half (46%) of respondents cited this benefit as one of two top reasons for using WLANs. A related benefit, improved knowledge-worker productivity, was the next biggest driver, specified by 24% of survey respondents.

Overall, enterprise Wi-Fi deployments seem to have leveled off: this year, 76% of respondents said they have installed Wi-Fi infrastructure in common business areas, compared to 80% who said so last year. Similarly, 59% said they have deployed the infrastructure in individual work areas, about the same number as those who said last year that they had done so (62%).

Continued growth in Wi-Fi seems to rest squarely with the arrival of next-generation 802.11n networks, which will support at least 100Mbps (and likely 300Mbps) in early products and will operate in both the 2.4GHz and 5GHz unlicensed frequency bands. For example, while 86% of respondents said they are currently running today's fastest Wi-Fi networks using 802.11g technology, which operates in the 2.4GHz band at 54Mbps, only 9% plan to deploy 802.11g in the future. Meanwhile, though only 6% of respondents have deployed 802.11n, 64% plan to deploy it. 802.11a, which figures in the future deployment plans of 15% of respondents and operates at 54Mbps in the 5GHz band, has already been deployed by 50% of respondents.

KUBERNAN STATE-OF-THE-MARKET REPORT

Published By
Kubernan
www.Kubernan.com

Design/Layout Artist
Debi Vozikis

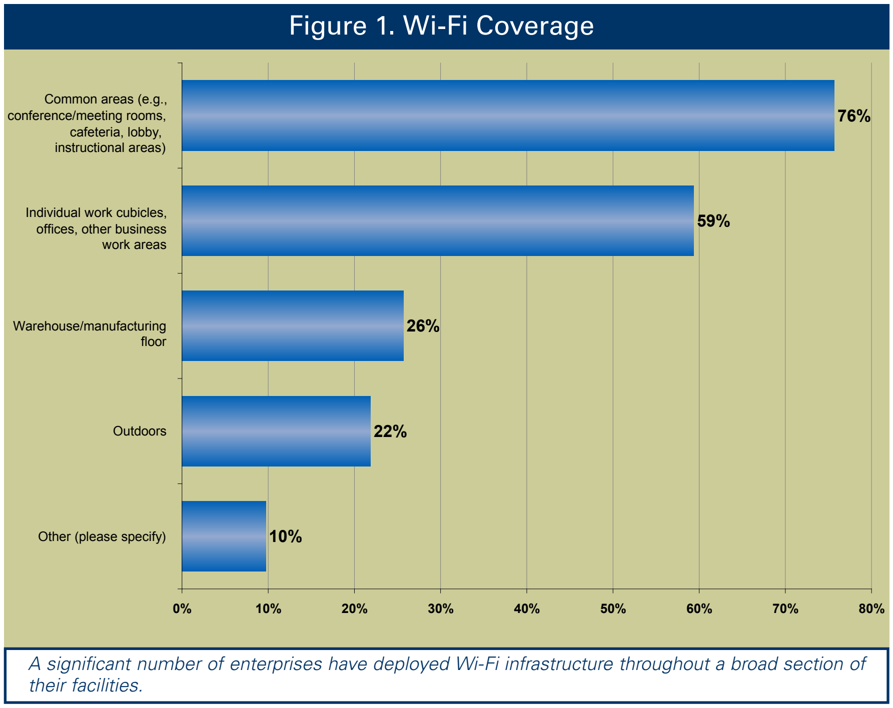
For Editorial and Sponsorship Information
Contact Steven Taylor,
taylor@webtorials.com

Professional Opinions Disclaimer
All information presented and opinions expressed in this Kubernan State-of-the-Market Report represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

Respondents' Sphere of Influence

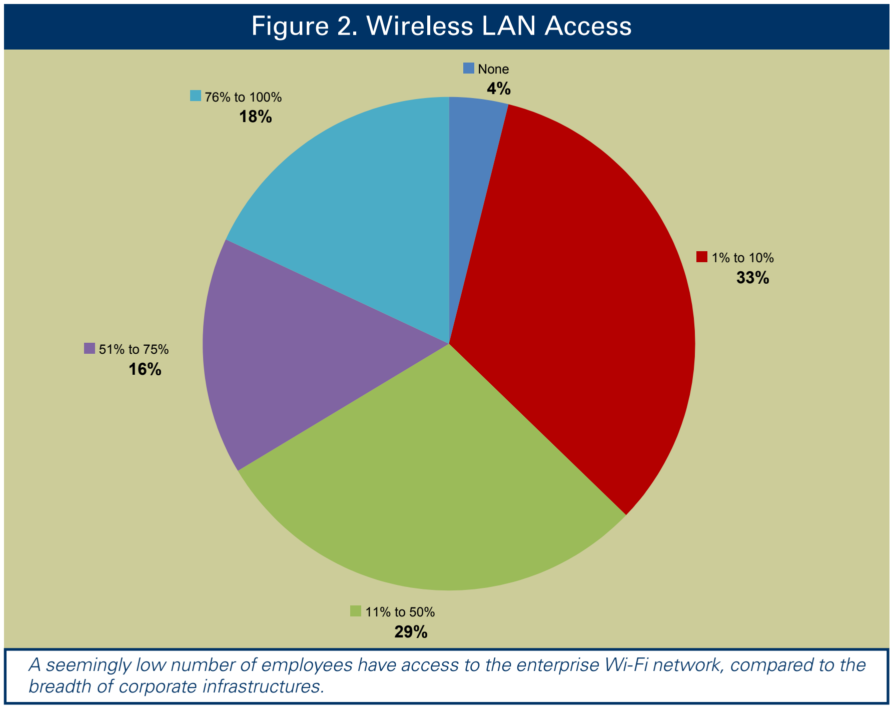
Nearly four out of five (79%) of this year's respondents said they played a role in recommending WLAN products. A third or more said they were involved in securing, installing, managing, or supporting WLANs, and 29% said they have WLAN purchasing responsibilities. Both large and small businesses were represented: 21% worked in companies with 10,000 to 100,000 employees; 20% worked in companies with 1,000 to 5,000 employees; and 20% worked in organizations with 50 or fewer employees, for example. More demographic detail is available in the Appendix at the end of this report.

Figure 1. Wi-Fi Coverage



A significant number of enterprises have deployed Wi-Fi infrastructure throughout a broad section of their facilities.

Figure 2. Wireless LAN Access



A seemingly low number of employees have access to the enterprise Wi-Fi network, compared to the breadth of corporate infrastructures.

Key Findings

The 2007 survey revealed several primary enterprise WLAN deployment and usage trends, described below.

- **Enterprise Wi-Fi infrastructure expansion is significantly outpacing user Wi-Fi access.** A large number of respondents have deployed WLAN infrastructure (radio access points) throughout their organizations. About three fourths have covered the common areas of their companies, such as conference rooms, cafeterias, and lobbies. More than half say they cover individual business work areas, such as cubicles and offices, and nearly another quarter have even deployed infrastructure out of doors.

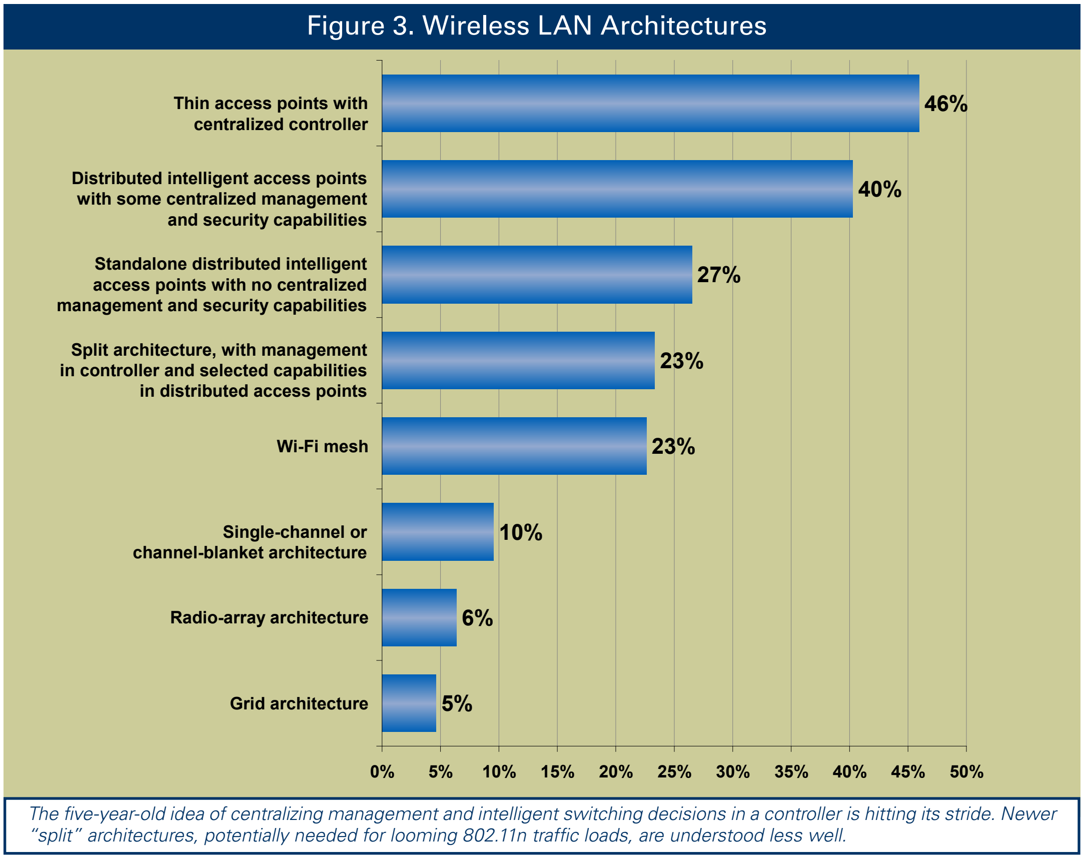
On the other hand, survey respondents also report that a comparatively small number of employees have Wi-Fi access. More than a third (37%) say 10 percent or fewer employees actually have access, and another 29% say just up to half (11% to 50%) of their users have access (see Figures 1 and 2). In other words, two-thirds of respondents said that half or fewer employees currently have WLAN access.

There are a few potential reasons for these seemingly paradoxical findings. It's possible that a significant number of organizations' infrastructure efforts are simply outpacing their client-device deployments. Infrastructure must be in place before Wi-Fi clients can gain access, so perhaps the discrepancy has to do with IT departments simply needing to catch up on the client side.

Another explanation could be that some organizations might have built out their networks broadly but not yet densely. In other words, they might have installed access points in some of the areas they indicated, but not in all of them. For example, perhaps only a small percentage of conference rooms and user workspaces have been covered.

- **Newer Wi-Fi architectures that split processing duties between a central controller and distributed access points haven't registered on most user radars.** Five years ago, the industry got the idea of using a centralized switch or controller in conjunction with dis-

Figure 3. Wireless LAN Architectures



The five-year-old idea of centralizing management and intelligent switching decisions in a controller is hitting its stride. Newer "split" architectures, potentially needed for looming 802.11n traffic loads, are understood less well.

tributed lightweight access points to scale and configure access points without having to touch each one. The user community is finally implementing this architectural change in significant volume. However, the industry has realized that increased network traffic loads will soon be driven by the greater capacity of 802.11n (which could push traffic off wired LANs and onto wireless LANs) and the eventual need to support real-time multimedia traffic.

As a result, still newer, next-generation "split" or "hybrid" architectures are emerging just as enterprises are picking up steam with the five-year-old centralized controller/lightweight AP architecture. About half as many respondents are currently using or planning to use the distributed/centralized combination architecture as with the controller-only setup (see Figure 3).

- **Voice-over-IP-over-Wi-Fi ("Vo-Fi") deployments have grown, but future implementation plans are a question mark.** Slightly more than a third of Wi-Fi shops (35%) said they are using Vo-Fi now, compared to 23% in 2006. This is a significant jump, given that Vo-Fi deployments remained fairly static the previous year, growing from 21% in 2005 to 23% in 2006.

  About another third of the Webtorials respondents (30%) haven't decided if they'll deploy Vo-Fi at all, while about another third (35%) say they plan to deploy Vo-Fi within the next 12 months. Note, though, that the percentage of respondents "planning" to deploy Vo-Fi within the year has hovered at about a third in Kubernan research for the past several years, indicating that some Vo-Fi plans have been postponed or reconsidered more than once.

  A number of factors are driving mixed enterprise strategies when it comes to Vo-Fi. Among them:

  1. Those already using Vo-Fi tend to be in specific industries with very localized mobile voice needs, such as nurses on a single hospital floor. A single access point can often serve such user groups, so secure fast roaming between access points (see below) isn't an issue.

  2. The status of secure fast-roaming technology, which ensures that voice sessions won't get dropped as users re-associate to a different access point as they roam, is a mixed bag. Some vendors that make both WLANs and Wi-Fi handsets have their own proprietary secure fast-roaming scheme. In these cases, enterprises generally must use infrastructure and handset from the same vendor or the vendor's infrastructure and vendor partner's handset that has been certified for use on its WLAN.

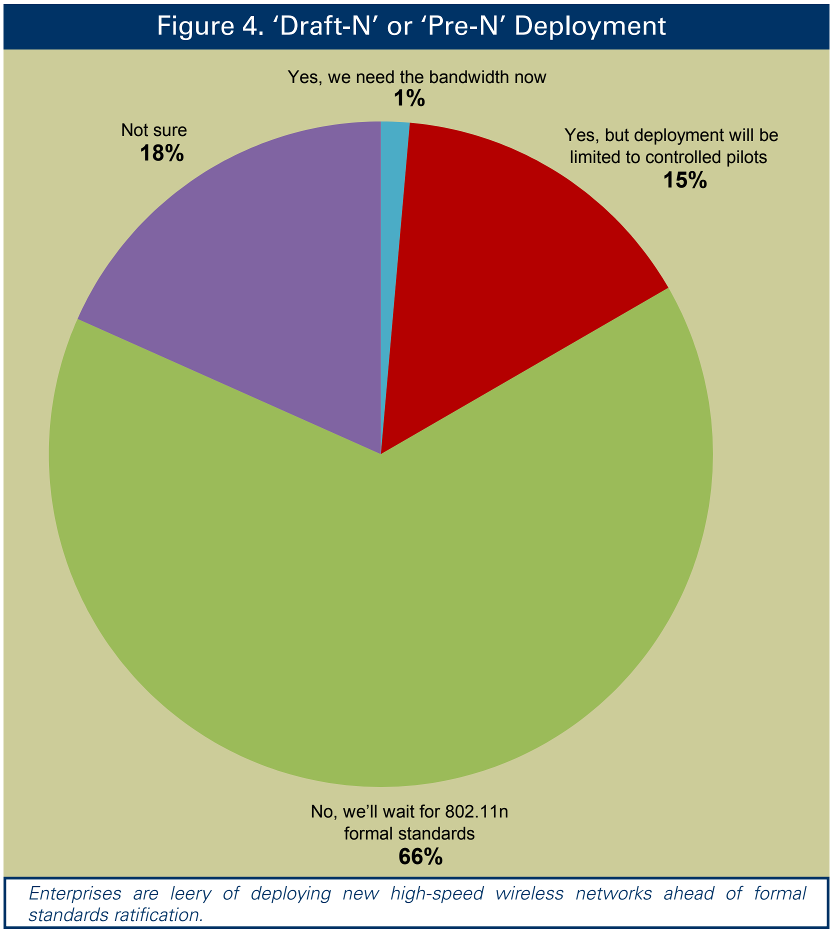
     However, as WLANs proliferate, the Wi-Fi community wants secure fast roaming to become standard across systems. 802.11r, the secure fast-roaming standard in development, isn't due for ratification until next year, with products to follow.

3. Finally, there are many emerging approaches to achieving mobile voice. For example, in-building cellular services with PBX extensions are emerging, and some companies already ingrained in a cellular culture might be anticipating those.

- **Enterprises plan to wait for final 802.11n standards before deploying the high-capacity Wi-Fi networking technology.** The survey reflects a strong enterprise aversion to deploying 802.11n ahead of formal standards ratification. Only 1% of respondents said they need the bandwidth now and would go ahead and deploy pre-standard products in production environments. By contrast, 65% said they intend to wait for ratification by the IEEE of formal 802.11n standards (expected in late 2008).

One might note a seeming discrepancy here: 1% said they would deploy pre-standard products, while, as mentioned earlier, 6% stated that they had already deployed 802.11n. However, the earlier question did not differentiate between 802.11n use in full production mode and controlled pilots. So it is possible that some of the 15% of respondents indicating they would limit 802.11n deployment to controlled pilots (see Figure 4) have already done so, accounting for the 1% to 6% differential.

Figure 4. 'Draft-N' or 'Pre-N' Deployment



Enterprises are leery of deploying new high-speed wireless networks ahead of formal standards ratification.

Market Background and Update

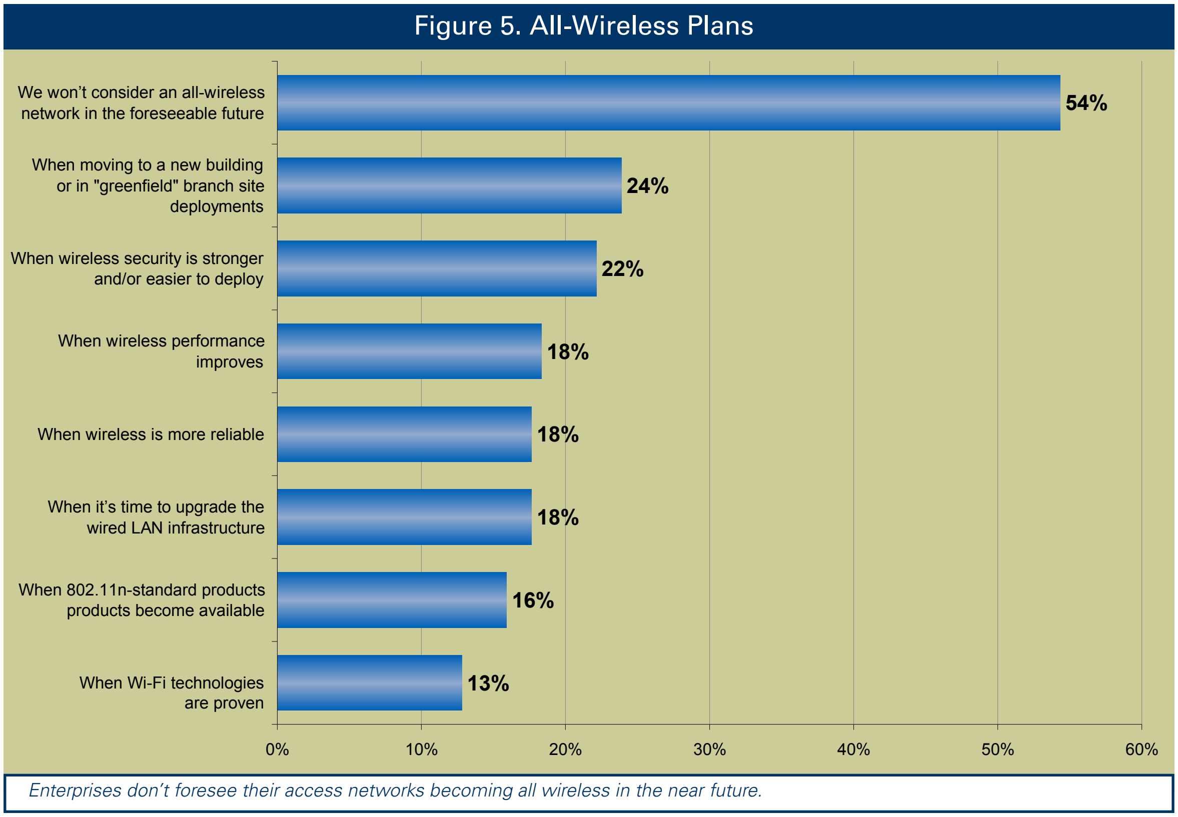
Perhaps the biggest anticipation in Wi-Fi advances lies in the arrival of high-speed 802.11n networks, which significantly increase the throughput of today's 802.11a/b/g networks to rival wired Ethernet-to-the-desktop speeds. The emergence of standard 802.11n products implies that some enterprises might eventually operate all-wireless LAN access networks to reduce costs associated with cabling materials and labor and to ease and accelerate the adds, moves, and changes of user work stations and phones.

Still, many enterprises will have to upgrade their wired Ethernet switches to support the gigabit-speed uplinks that 802.11n access points support. They might require significantly greater aggregate backplane capacity in their WLAN controllers, as well, which usually requires replacing the controllers. Also, because 802.11n radios use multiple transceivers, they require more power than existing WLANs. So companies with access points plugged into power-over-Ethernet (POE) ports will require a different POE source to accommodate the additional power requirements.

Because of the necessary infrastructure upgrades required, the move to all-wireless access networks in established companies might take several years. More than half (54%) of respondents said they wouldn't consider an all-wireless network in the foreseeable future, though 24% said they would consider it when moving to a new building or in Greenfield branch site deployments. Another 22% said they would consider it when they felt that wireless security was stronger and/or easier to deploy (see Figure 5).

With 802.11n's forthcoming capacity increases, additional applications will join the Wi-Fi network. In anticipation of this, interoperability and integration efforts are moving beyond the component-level interoperability efforts of the Wi-Fi Alliance, an industry consortium that certifies basic connectivity among different vendors' access points and client devices. As

Figure 5. All-Wireless Plans



Enterprises don't foresee their access networks becoming all wireless in the near future.

users begin to deploy additional WLAN applications, such as IP voice, location/tracking, and intrusion detection, some vendors are striking interoperability partnerships with makers of IP PBXs, application servers, and application appliances. The idea is to ease integration headaches associated with inconsistent software configuration commands among different types of systems. This type of ecosystem cooperation will be necessary at least until such time that industry-standard application programming interfaces (APIs) emerge that allow WLANs to communicate with various upstream application servers and appliances and downstream client devices in a common format.

Business Drivers and Trends

Growth in the "carpeted" areas of enterprises continues to outpace growth in vertical applications, which have long relied on older and slower WLANs for such applications as warehouse picking and product scanning. As noted, improving access to mobile employees ranked at the top of enterprise business drivers (46%), followed by "improved knowledge worker productivity through mobility" (24%). Other drivers were "reduced cabling costs (20%), "improvement of a specific business process" (18%), and "as a step toward fixed-mobile convergence" (14%).

While locally mobile voice capabilities is a driver for some organizations, Vo-Fi has not hit its stride as the dominant compelling application for the reasons mentioned in the "Key Findings" section. Still, about one third of respondents (30%) report use of Vo-Fi handsets in their organizations and nearly half (49%) report use of telephony software on Wi-Fi-enabled user laptops to make mobile calls.

Technology Drivers and Trends

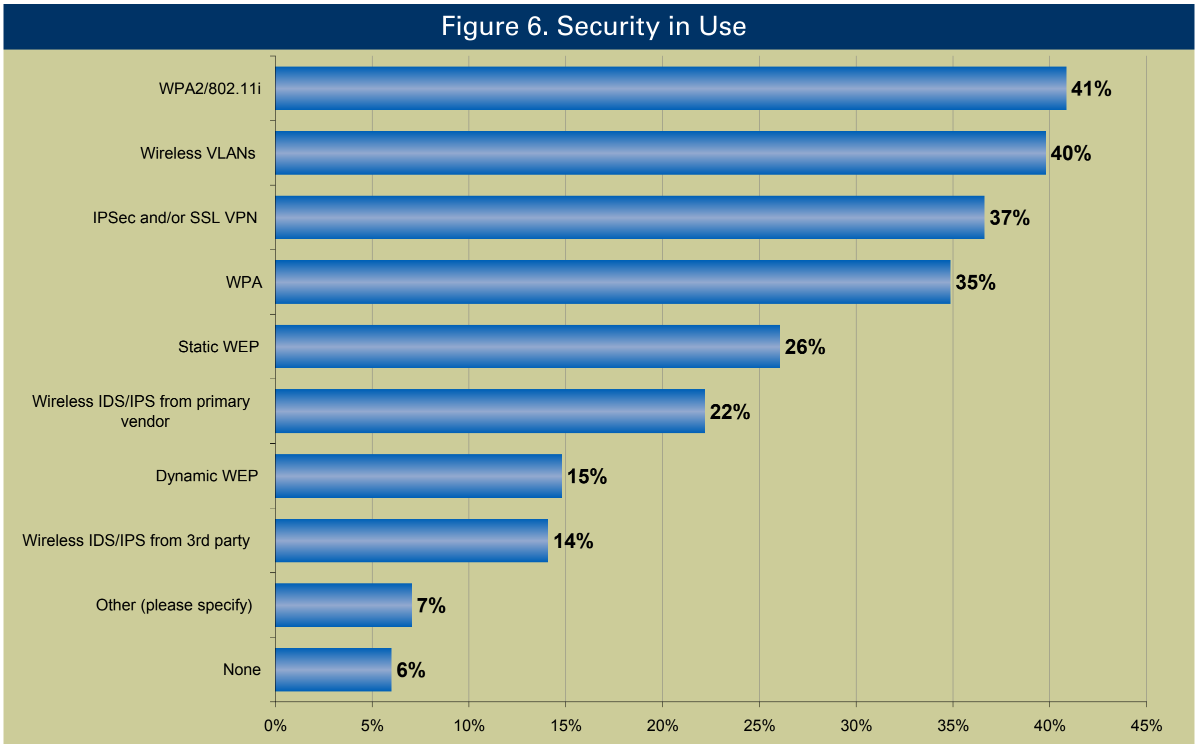
Helping drive Wi-Fi deployments are the maturation of wireless security technology, the promise of tomorrow's 802.11n technology, and the uptake of centralized architectures, which are now in mainstream deployment.

- **Security: The good news and the bad.** Security remains the largest challenge to Wi-Fi implementations, according to 53% of the respondents. But this number has dipped significantly, down from 70% in 2006. About 41% of the 2007 respondents use the strongest form of Wi-Fi security—802.11i/WPA2—in their networks, which represents about the same number of users who said they had deployed these sophisticated encryption and authentication standards in 2006 (38%). By contrast, just 22% had deployed 802.11i/WPA2 in 2005.

  One possible reason for the stagnation of 802.11i/WPA2 security deployment is that 37% of respondents said they use IPSec and/or SSL VPNs over their wireless networks, which they might feel is adequate. Also, many budget-conscious retailers and warehouses using Wi-Fi-enabled legacy handhelds, such as bar-code scanners, can't upgrade to 802.11i/WPA2 because of memory and processing constraints in the older devices.

Enterprises are taking other security measures, too. About 14% are using wireless intrusion prevention systems (IPSs) from a third-party vendor, while 22% are using similar capabilities embedded in their primary WLAN vendor's system (see Figure 6). Wireless IPSs identify when an unauthorized device is connected to the corporate network or when an authorized client device has associated to an unauthorized access point, and they alert systems administrators or take automated action. Such systems also have built-in auditing systems to help enterprises determine if they are in compliance with the wireless security aspects of relevant regulatory mandates.

Figure 6. Security in Use



Enterprises worry about Wi-Fi security, but are doing many things right in their implementations.

- **The promise (and pitfalls) of 802.11n.** The deployment of 802.11n will likely drive multimedia and all-wireless access networks, but few enterprises intend to deploy early 802.11n products that don't guarantee compatibility with the final IEEE 802.11n standard. Most of the enterprise-grade Wi-Fi makers have announced pre-standard products that advertise compliance with Draft 2.0 of the IEEE 802.11n standard (the latest draft). The Wi-Fi Alliance officially began certification testing for Draft 2.0 products in June 2007. At the time of this writing, only one enterprise-class vendor had received Wi-Fi certification for its pre-standard products, though a number of other vendors were expecting Wi-Fi certification by year-end 2007.

Though a few enterprises will deploy enterprise-class 802.11n networks ahead of standards, the majority of those say their installations will be limited to controlled pilots, and the lion's share of enterprises intend to wait for formal standards ratification. The primary inhibitor to 802.11n, said 44% of the respondents, is that final standards and standards-based products are still at least a year away. Wi-Fi infrastructure upgrade costs were cited by 39% of respondents as the second biggest inhibitor to 802.11n deployment.

The Draft 2.0 enterprise-class product announcements can likely be explained by the primary suppliers wanting their customer base to know that they will be ready and waiting with compliant and tested infrastructures when the standard is ratified. While 802.11n will be backward-compatible with 802.11a/b/g networks, performance degradation of mixed-mode deployments likely will be significant unless organizations aggressively replace legacy clients with 802.11n devices. One potential approach is to install an overlay of 802.11n-capable access points on a separate 5GHz channel plan, because the 5GHz band is far less cluttered than the 2.4GHz band used by 802.11g/b networks and several other wireless device types.

- **Architecture acceptance.** Enterprise acceptance of lightweight AP architectures used with centralized controllers is ramping up as installations grow larger, and provisioning, management, and security enforcement becomes increasingly unwieldy using traditional distributed access points that house all system intelligence. It is likely that these deployments reflect organizations' expanding coverage. Both broader and denser deployments make the centralized management and security control afforded by centralized architectures increasingly necessary.

WLAN Architecture Trends

Now that deployments are going mainstream, broader and denser coverage is needed, and potentially hundreds or thousands of access points are required. Included in enterprise architecture considerations are where system processing and traffic-forwarding decisions are made; how and where radio-frequency (RF) interference is addressed (e.g., single-channel versus cell-based, multi-channel architectures); and how well a system addresses session handoffs from access point to access point as users roam.

Survey-takers were asked to check all of the architecture types that they intended to deploy in their environments. This year, 46% of the survey respondents said they are using or are likely to use lightweight access points with a centralized controller for management and security in their Wi-Fi environments. This is about on par with the number of respondents who last year said they were using or planning to use such architectures (49%).

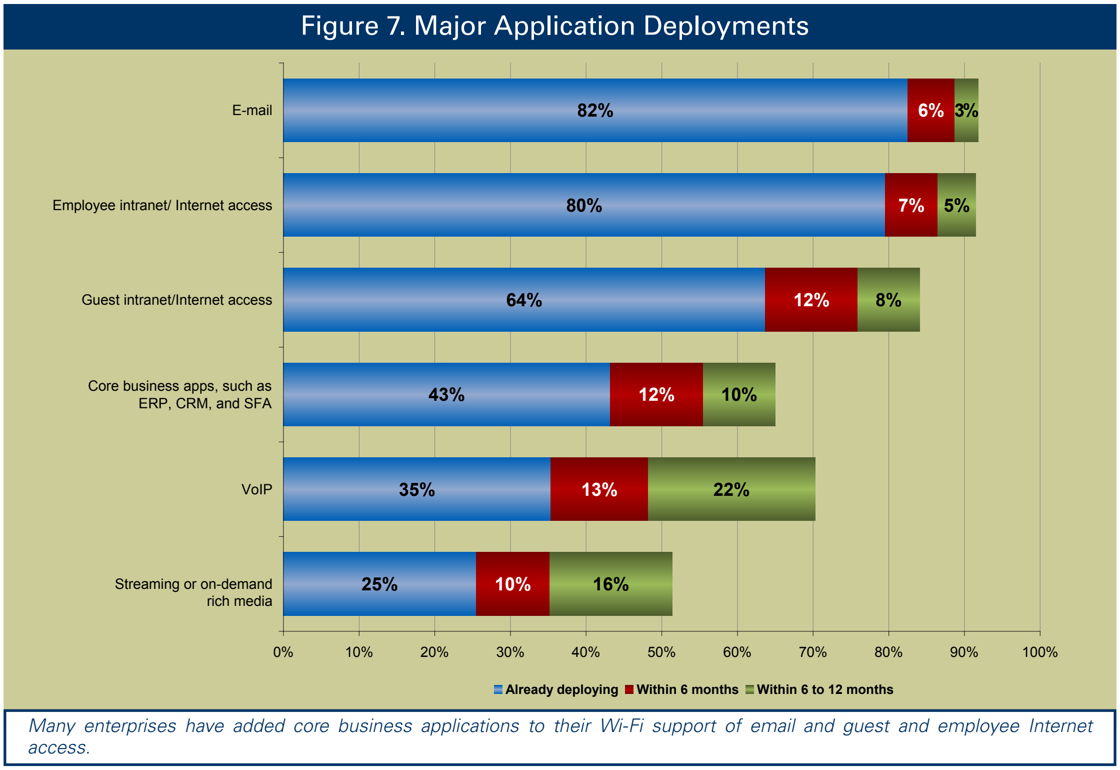
The use of intelligent standalone access points with no centralized controller and no centralized management or security remained consistent with last year (27%). Plans to use intelligent standalone access points with some centralized management and security capabilities decreased slightly from 48% last year to 40% this year.

From an architectural perspective, those enterprises looking ahead to 802.11n and Vo-Fi applications might consider the eventual impact of latency on a peer-to-peer voice call that must traverse a centralized controller before making its way from Client A to Client B. This is one reason for the emergence of part-distributed, part-centralized architectures, which enable some forwarding decisions to be made in distributed devices. Again, only about half as many respondents expressed plans to use these newer hybrid architectures as those using or planning to use the fully centralized model.

Wi-Fi Applications

E-mail and employee and guest Internet access remain the primary uses for Wi-Fi networks today. However, core business applications are beginning to make a respectable showing, as well, with 43% of respondents saying they run the likes of enterprise resources planning, cus-

Figure 7. Major Application Deployments



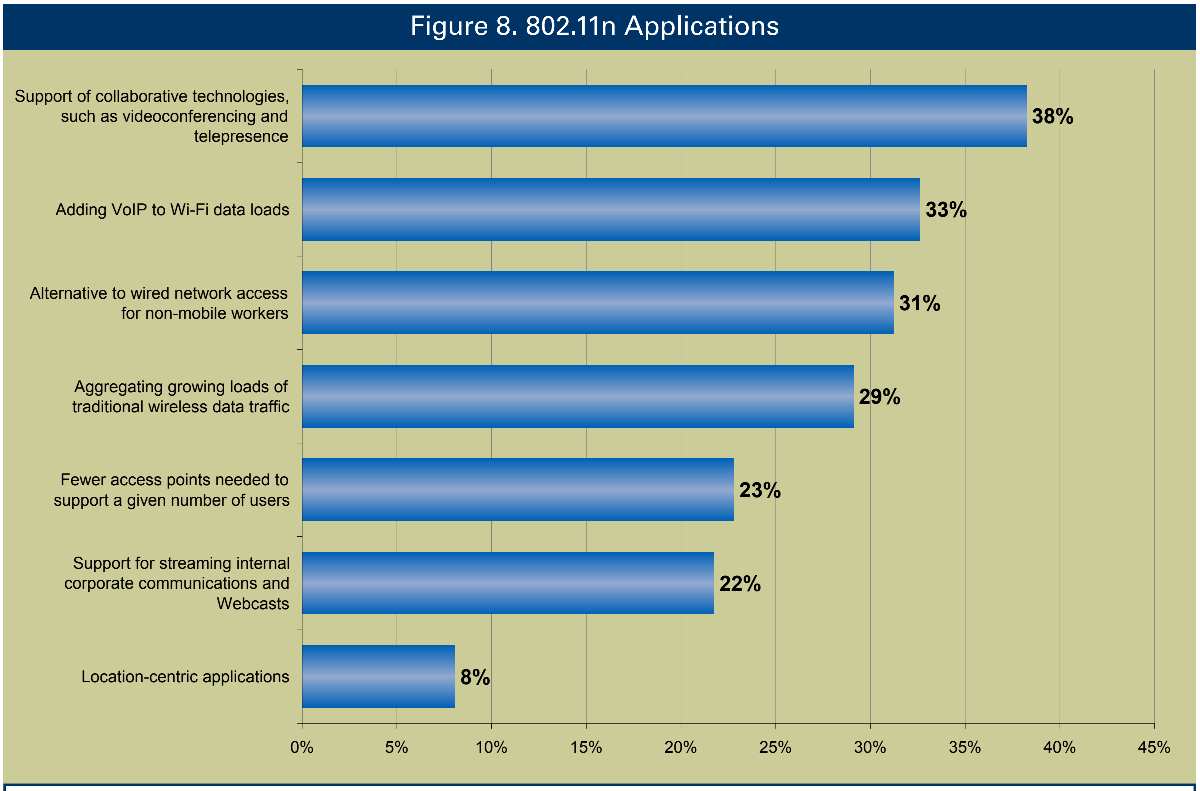
Many enterprises have added core business applications to their Wi-Fi support of email and guest and employee Internet access.

tomer relationship management, and sales force automation applications over their networks today (see Figure 7).

As noted earlier, Vo-Fi deployment jumped from 23% last year to 35% this year. Other collaborative applications and rich media are also growing in popularity, while the lowest-scoring applications were radio-frequency identification, or RFID (10%), and point-of-sale (POS) transactions (11%). The seeming low deployment rate of RFID and POS could be attributable to the cross-industry breadth of the Kubernan survey response base. RFID applications tend to be used primarily in retail/supply chain management and healthcare applications, for example, and POS is used almost exclusively in the retail industry.

802.11n, in particular, showed the highest ranking for supporting collaborative applications. More than a third of respondents (38%) said they anticipate that the primary business application for the next-generation Wi-Fi technology will be support for collaborative technologies such as videoconferencing and telepresence (see Figure 8).

Figure 8. 802.11n Applications



Collaborative applications such as videoconferencing are a primary driver behind anticipated 802.11n deployments.

Conclusions

The pace of WLAN adoption has flattened as enterprises have accepted the five-year-old centralized architecture but also await standards-based 802.11n, due in about a year. 802.11n promises to deliver the increased throughput and range needed to potentially create all-wireless access networks and to support multimedia, collaborative applications. However, 802.11n will require new Wi-Fi gear, upgrades to wired infrastructure, and possibly new combination centralized/distributed architectures, with which many respondents are not yet familiar.

Enterprises have installed Wi-Fi primarily to improve access to mobile workers and to boost knowledge-worker productivity. Security concerns still top the list of user challenges with Wi-Fi. A good number of enterprises, though, have deployed the industry's most stringent standard encryption and authentication mechanisms, 802.11i/WPA2. Many continue to use VPN technology over their WLANs and a respectable number have deployed some form of wireless IPS to detect and deter unauthorized wireless device associations.

The use of voice over Wi-Fi remains strong in niche industries where users require no long-distance phone capabilities or off-campus mobile voice services to perform their jobs. Its future is uncertain in mainstream environments, however, in part because not all QoS and secure fast-roaming issues have yet been solved in a standardized way. In addition, cellular hovers as a potential competitor for internal voice calling, and enterprise decisions will likely hinge on the degree to which wireless carriers step up to the plate to extend IP PBX features and calling plans at reasonable in-house calling rates.

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 Editor

Steven Taylor is a co-founder of Kubernan and Editor/Publisher of Webtorials. An independent consultant, author, and teacher since 1984, Mr. Taylor is one of the industry's most published authors and lecturers on high-bandwidth networking topics

Integrated Architectures Will Replace WLAN Overlays

By Seth Atkins
CTO, Mobility Solutions, Nortel

From the Sponsor

NORTEL

Network design concepts are rarely revised, but often added to. When new applications or technologies arrive on the market that don't fit cleanly into current design paradigms, like a square peg in a round hole, the typical solution is to bolt it on as an overlay. However, history has taught us that when there is a strategic advantage to revising network design concepts, it forces positive industry change and upheaval. This trend usually takes the form of true integration of what was once the "new" technology, and it happens along product generational lines.

When wireless LAN (WLAN) architectures shifted to controller-based approaches a few years ago, nothing less happened. And we have come to accept the network bolt-on approach, also known as the overlay, as standard fare in wireless deployments. The industry has clearly accepted the benefits of the controller-based architecture as being worth the extra expense and complexity of having a true network overlay, so much so that the preeminent debates within the industry relate to which overlay architecture is best. Central encryption or distributed encryption? Central forwarding or distributed forwarding? Extremely "thin" access points (APs) or "chubbier" APs containing some network intelligence? Rarely is the issue of the overlay approach itself debated or questioned.

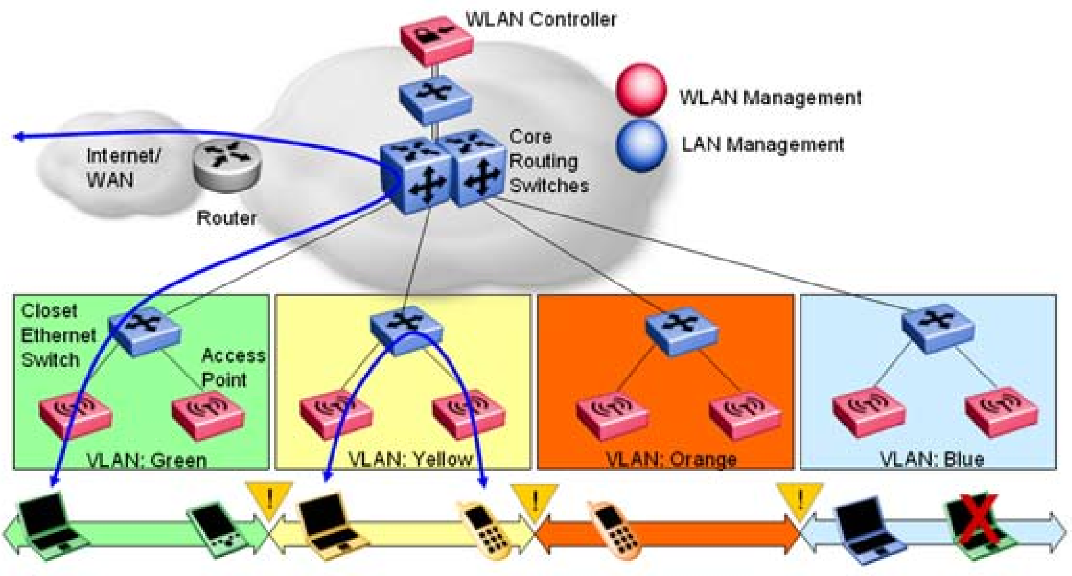
The Architecture Continuum

These architectural discussions tend to be oversimplified. The architecture component labels "fat," "thin" "centralized," and "distributed" are rarely 100% accurate when describing a given system. Rather, most architectures fall somewhere along a continuum spread between the endpoints. For example, most current WLAN APs are somewhere between fat and thin—with less intelligence than the autonomous, fully intelligent APs of yesterday, but with more intelligence than a dumb radio that is controlled 100% by a centralized device. The APs on the continuum differ by which functions reside centrally in a controller versus in the AP.

The three primary axes to consider are control, encryption, and forwarding. Control has the greatest degree of variability among different architectures; in other words, no two WLAN systems are exactly the same in terms of how much or little is centralized. Forwarding functions can also be centralized or distributed, but many products allow a customized mix of the two depending on AP location and other variables. The reason is clear: completely distributed forwarding sacrifices mobility. To support mobility, typically, you have to allow for a mix of central and distributed forwarding. The location of encryption functions is the only black-and-white choice among different architectures.

That said, there is also now a fourth axis to consider: integrated versus overlay.

Figure 1: Completely distributed forwarding sacrifices mobility



Moving traffic forwarding to the access points in an overlay WLAN system can help scale system capacity but can also restrict user mobility to individual network segments.

CAPEX/OPEX to Drive Shift

A few years from now the industry will look back at overlay products as a closed chapter in the history of WLAN evolution. One key reason is that OPEX and CAPEX concerns inevitably play a critical role in the natural selection of the optimum product architecture. But until then enterprises are plagued with the issues of purchasing extra devices to control APs, extra servers to manage the WLAN apart from the LAN, extra devices to maintain WLAN security (even to the point of having an overlay sensor network on top of the overlay AP network), special quality of service (QoS) features, and extra network administrators to keep it all running. Lowering OPEX demands management and maintenance simplicity, and lowering CAPEX demands integration of capabilities into fewer devices.

Managing an overlay WLAN almost always requires a separate standalone application and has very limited integration into a holistic management application framework. For security, functions such as policy enforcement and intrusion detection and prevention (IDS/IPS) are also handled in separate silos, further complicating operations and increasing cost. Lastly, the

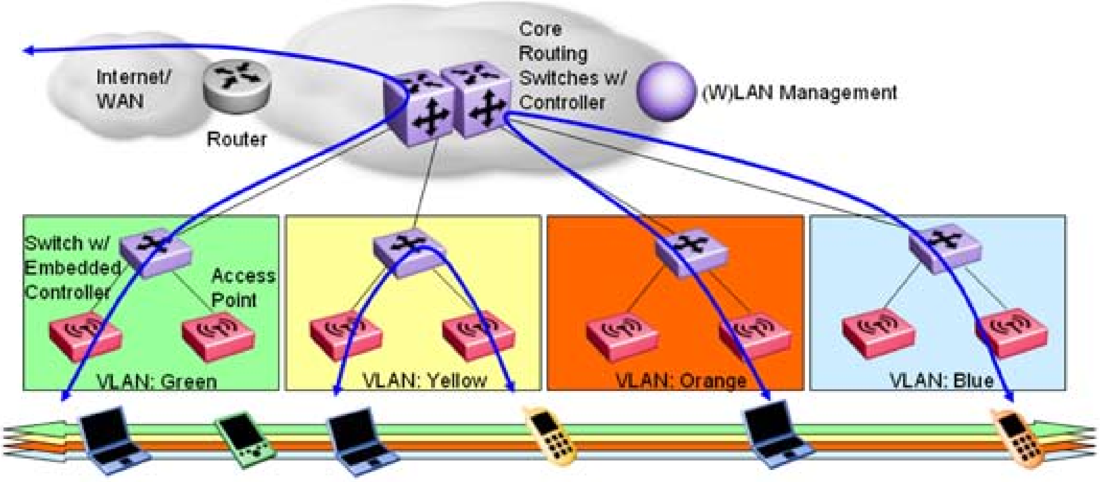
WLAN traffic is tunneled and invisible to the LAN for much of its travel across the network to the central controller. This makes QoS and filtering more challenging and diminishes the value of the important functionality that resides in the edge switching equipment.

It is for this last reason that distributing the forwarding functions makes a great deal of sense. However, distributing forwarding all the way out to the AP, as many vendors are trying to do, is suboptimal. All WLAN traffic from an AP comes in through a port on a line-rate 10/100/1000 Ethernet switch containing a very rich feature set including filtering and QoS, as well as advanced functions such as network access control. This switch should logically be the common gatekeeper for converged wired/wireless networking, because it is positioned at the edge of the network and contains the required LAN traffic-handling capabilities.

Security will benefit from this architecture as well. Most filtering of wired traffic is performed at the perimeter. With wireless traffic in most of today's systems, this principle is violated; traffic is sent back to the network core just to be filtered by a different device such as a stateful firewall. A converged edge switch, by contrast, allows the wired policies to be applied to wireless traffic, too, at the perimeter, eliminating the need for extra filtering devices in the core. The network is simultaneously simplified and made more secure.

Many vendors have hyped the performance advantages of distributed forwarding when the forwarding functions reside in their APs, stating that this is good for delay-sensitive traffic

Figure 2: The Converged Wired/Wireless Network



A truly converged wired/wireless architecture results in a simplified network that's easier to manage and provides wireless scalability without compromising mobility.

like VoIP. What is typically left unsaid is that when a phone is in a mobile state (not local to its native subnet), the traffic is tunneled to the central controller—or, even worse, is dropped. With converged wired/wireless switching, the starting point of the tunnel is the ingress edge switch, and the mobility tunnel always takes the shortest path to the destination subnet. So performance is always optimized regardless of the traffic type, device type, or location.

The logical end to this architectural evolution is to further merge the control functions into the converged wired/wireless switch that is in the wiring closet. This removes the last vestiges of the controller overlay, separate management of devices, and separate administrators. But a word of caution: this means true unification at all levels of the product. This is not the type of unification where two separate devices are simply stacked and wrapped in a single piece of steel resulting in a 2RU box with two command-line interfaces. The latter offers none of the CAPEX or OPEX advantages and in fact is less resilient than having the two devices separated.

A simple way of concluding is to say that converged wired/wireless switches combine all the unique advantages of all types of WLAN architectures and eliminate the unique limitations of each of those architectures. It returns us to the day when there was just "the network" to manage, not collocated networks. And that benefits everyone.

For a technical tutorial on converged wireless-wired architectures, listen to the 2007 WLAN State-of-the-Market Webcast, in which Kyle Klassen, a director in Nortel's enterprise wireless group, presents the issues of WLAN overlay architectures and how they can be solved. The Webcast and accompanying presentation with educational diagrams can be accessed at http://www.webtorials.com/abstracts/KubernanSOTM07-03.htm.

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 June 2007. A total of almost 300 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.

Geographically, Webtorials subscribers in the U.S. responded in the greatest numbers, representing 44% of the survey base. They were followed by 16% in Western Europe (excluding the UK, which represented 9%), 16% in the Asia-Pacific region, 3% in Canada, and 7% in Latin and South America. The remaining 5% described themselves as being located elsewhere.

Figure A1: What is your role in your company s wireless LAN implementation? (Please check all that apply.)

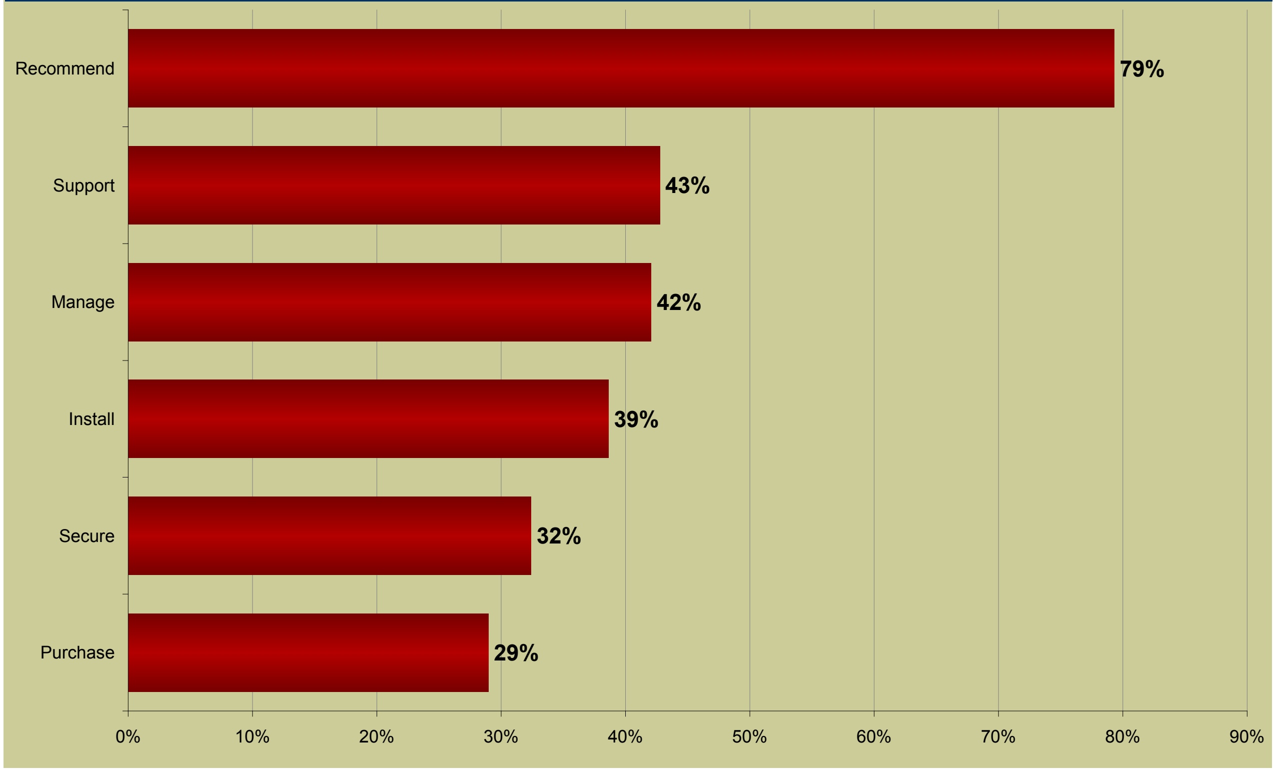


Figure A2: How many employees are there in your organization?

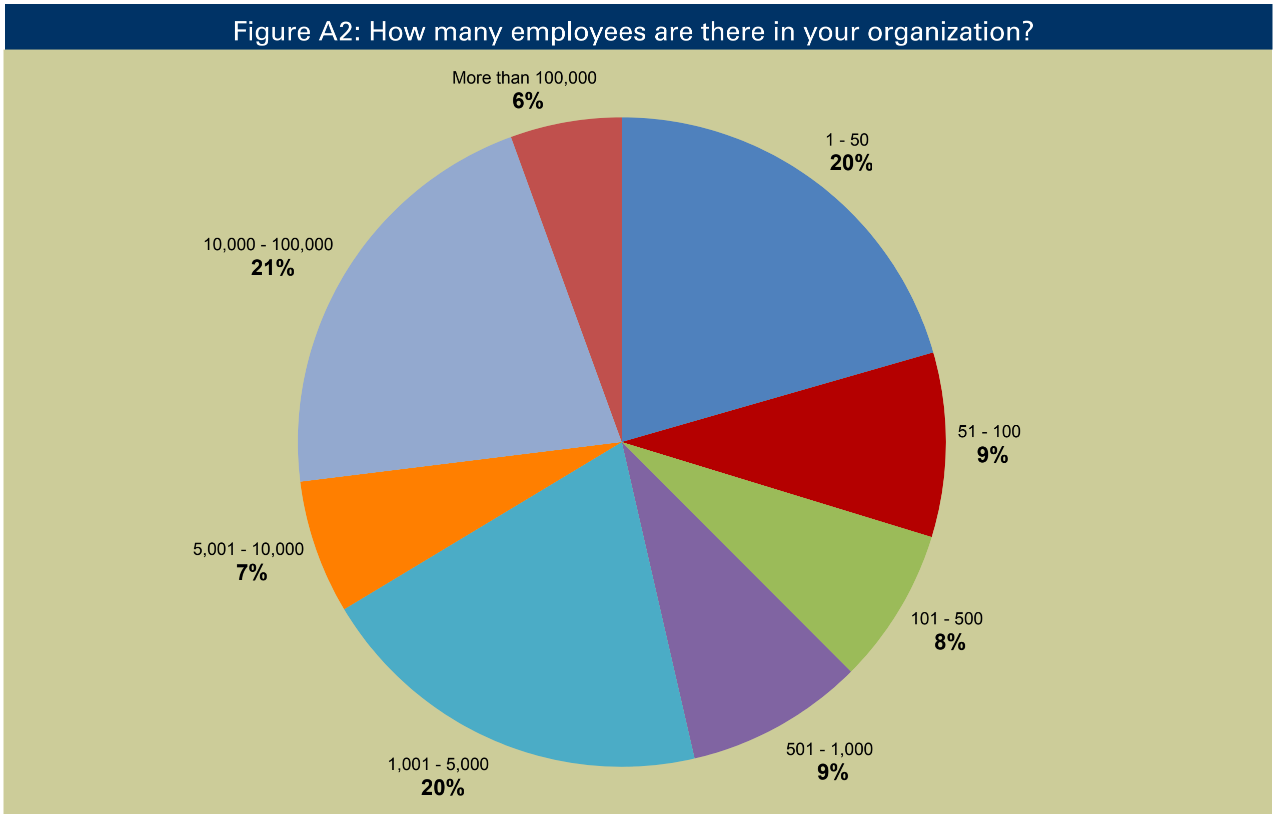
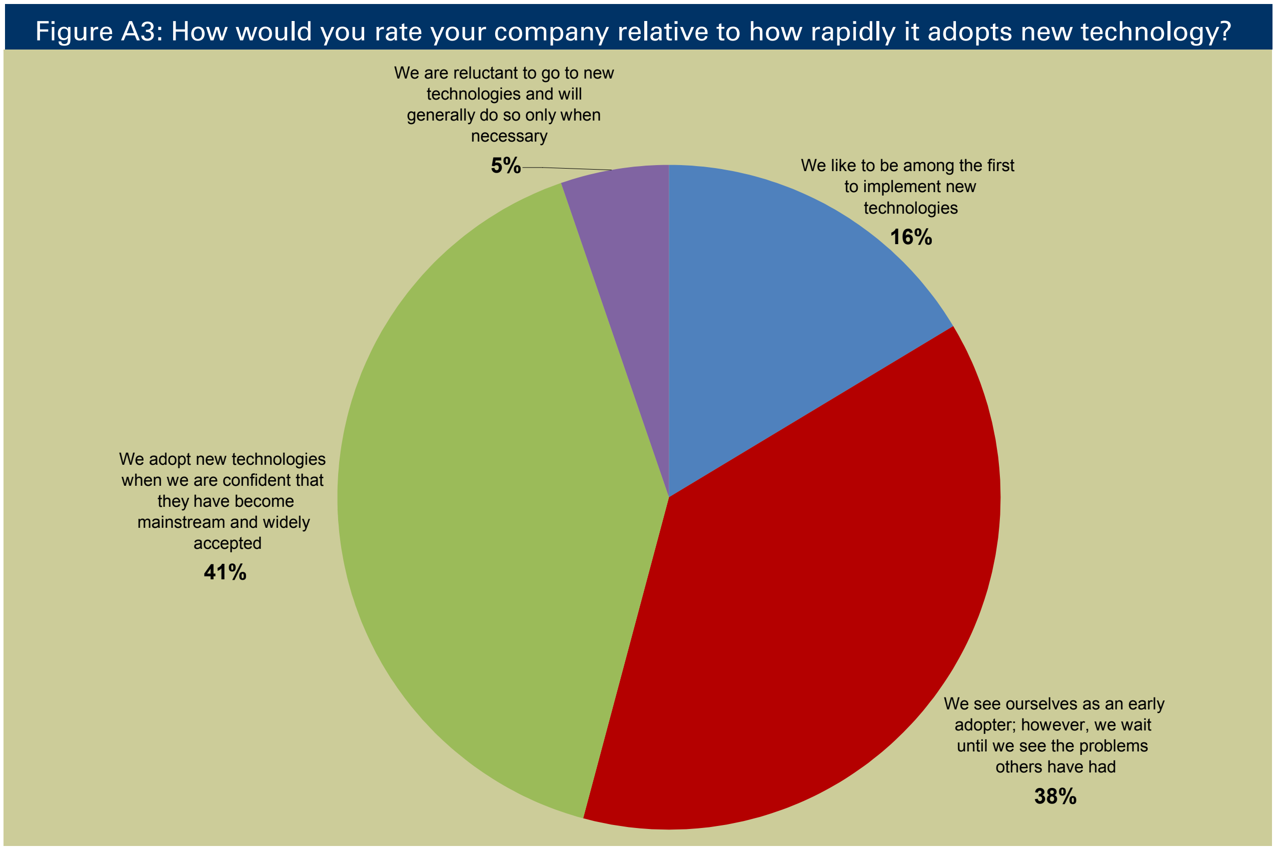


Figure A3: How would you rate your company relative to how rapidly it adopts new technology?


We are reluctant to go to new technologies and will generally do so only when necessary
We like to be among the first to implement new technologies
We adopt new technologies when we are confident that they have become mainstream and widely accepted
We see ourselves as an early adopter; however, we wait until we see the problems others have had