2004 Wireless LAN

FEBRUARY 2004

State of the Market Report

By Joanie Wexler and Steven Taylor

Produced By:

Webtorials

Sponsored By: NORTEL NETWORKS™

2004 Wireless LAN State of the Market Report

Introduction

Webtorials, the computer-networking industry's premier educational Web site, surveyed its subscribers in December 2003 about their perceptions of wireless LANs (WLANs) and their plans to deploy them. The responses provide a multifaceted snapshot of enterprise trends in this emerging and complex market.

In summary, the Webtorials subscriber base paints the following picture of the current wireless landscape:

- **There are a respectable number of WLANs installed today.** A substantial number of respondents (53%) have already deployed WLANs or are currently in the process of doing so.
- **Enterprises are incrementally building out their networks.** This conclusion stems from the finding that the number of users with WLAN access (or planned access) in respondent organizations is significantly smaller than the total number of employees in those organizations.

  Of the survey respondents, for example, 62% say they are supporting or will support fewer than 100 wireless users. More than a third (36.5%) say they are supporting or will support fewer than 50 users. Yet 71% of the survey respondents work in companies with more than 100 employees; in fact, 38% work in organizations with more than 2,000 employees. These figures indicate that enterprises are growing their wireless networks conservatively, rather than rolling them out en masse to their entire user population.
- **Existing users are fairly satisfied.** Respondents with WLAN implementations already in place expressed a medium to high level of satisfaction with their products and WLAN experience in general.
- **The primary enterprise deployment goal is to improve the productivity of mobile knowledge workers.** "Anywhere, anytime" access to email and Web-based applications for knowledge workers was chosen by the most respondents (68%) as a benefit they hope to gain with WLAN use.

Webtorials State of the Market Reports

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

Design/Layout Artist
Debi Vozikis
dvozikis@rcn.com

Copyright © 2004
Distributed Networking
Associates, Inc.

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

Professional Opinions Disclaimer
All information presented and opinions expressed in this Webtorials 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.

- **The biggest deployment hurdle remains security.** By far the biggest inhibitor to WLAN implementation today is user concern about wireless security—whether real or perceived.

Market Background

Wireless LANs have been around for well over a decade. But until fairly recently, proprietary technologies and slow speeds have kept them largely confined to specific niches within enterprises.

WLANs have long thrived, for example, on retail floors, in warehouses, and on loading docks. In these environments, tasks such as inventory checks and product code scans require broad coverage but not much bandwidth.

The first IEEE WLAN standard, 802.11, was ratified in 1997 and met these requirements. Early products ran at just 1 Mbps or 2 Mbps, depending on the modulation scheme used in vendor implementations. However, these speeds were not robust enough for mainstream business applications—particularly considering that bandwidth in WLANs is shared, not switched, which renders per-user throughput even lower.

Today, however, enhanced versions of those early 802.11-based WLANs (now also known as "Wi-Fi" networks) suddenly represent one of the greatest areas of networking technology investment. Among the reasons are that the maturation of Wi-Fi technology and enterprise requirements for user mobility are finally intersecting on a fairly grand scale.

Technology contributors to the uptake in WLANs include the following:

- The availability of products supporting higher-speed (11 and 54 Mbps) IEEE 802.11-based standards, making wireless networks more suited to mainstream business applications
- Successful industry cooperation to fix known security holes unique to radio-frequency (RF) networks
- The emergence of management-centric WLAN architectures, which make networks easier to scale
- 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

On the enterprise demand side:

- The convenience of wireless networking in the home has driven corporate users to demand the same flexibility at work.
- Knowledge workers spending most of their workdays in meetings need access to corporate resources and the Internet so that they can collaborate more effectively and receive urgent communication.
- The emergence of 802.11-based "hot spots" in public places extends an enterprise's investment in 802.11 technology off the campus to users who are traveling.

Survey Methodology and Demographics

The Webtorials subscriber base was contacted by email twice and asked to participate in a 30-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.

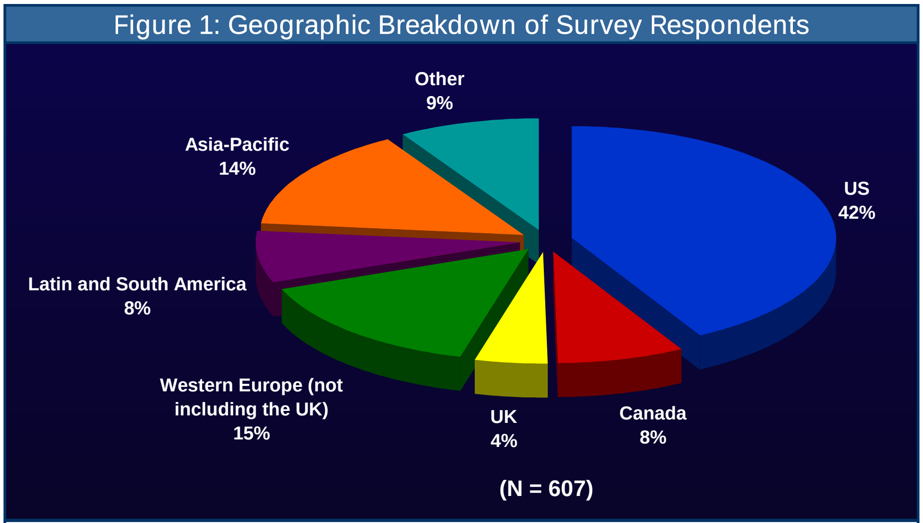
The order of the multiple choices rotated randomly so as not to bias the survey respondent by the order in which the options were presented.

The Webtorials survey was conducted in December 2003. A total of 623 respondents participated, though not all respondents answered all questions.

Nearly 80% 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 in terms of the number of enterprise sites to be supported (about a third each for fewer than 10 sites, 10 to 99 sites, and 100 or more sites) and the industries in which the respondents participated. However, the number of respondents in the non-computer manufacturing and processing, education, and

Figure 1: Geographic Breakdown of Survey Respondents



The regional distribution of survey respondents offers a global view into the WLAN marketplace.

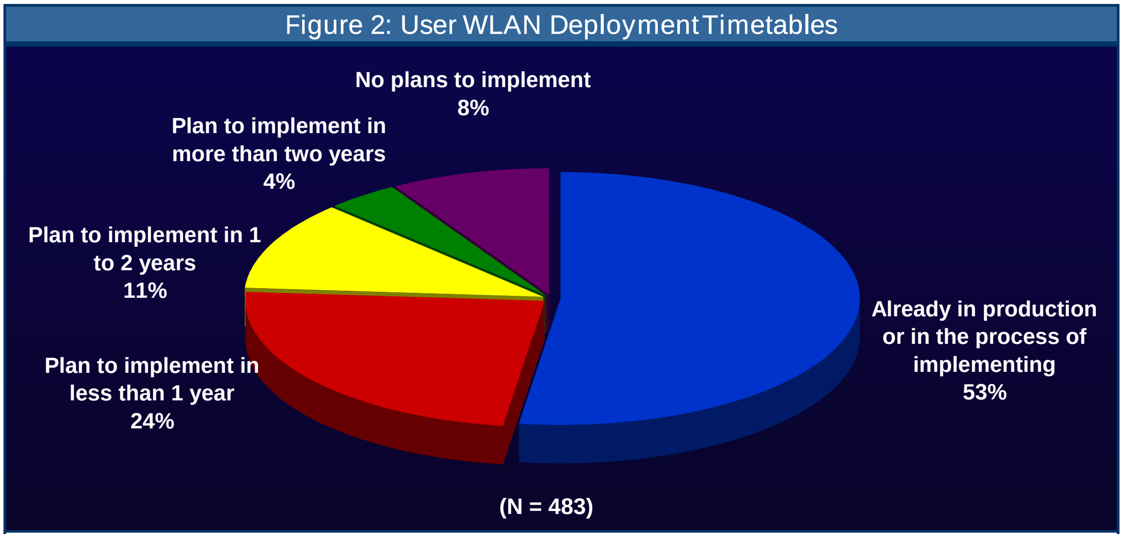
government sectors slightly outpaced respondents in the finance, medical, legal, and utilities arenas.

Geographically, Webtorials subscribers in the U.S. responded in the greatest numbers, representing 42% of the survey base. They were followed by 15% in Western Europe (excluding the UK, which represented 4%) and 14.5% in the Asia-Pacific region (Figure 1).

Enterprise Perceptions and Plans

More than half of the Webtorials survey respondents have already deployed WLANs or plan to do so in the near future (Figure 2). Those that already have some WLAN installations under their belts indicated that they are fairly satisfied with their product deployments: More than half gave their satisfaction level a ranking of 5 or better on a scale of 1 to 7 (Figure 3).

Figure 2: User WLAN Deployment Timetables



The outlook for WLAN deployment among the Webtorials subscriber base appears bright, as most survey respondents indicated that they have already installed a wireless network or plan to do so in the foreseeable future.

Technology Preferences

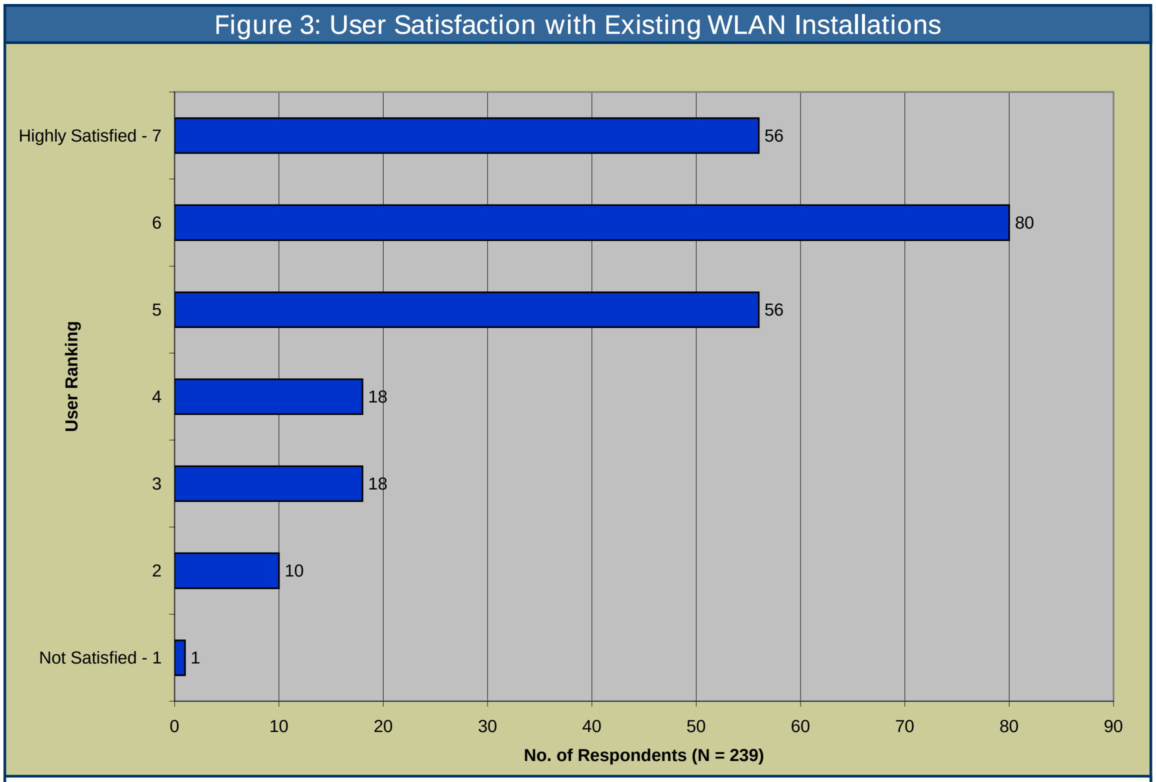
It stands to reason that 11-Mbps 802.11b technology ranked high on user deployment lists, given that this is the only multimegabit-speed wireless technology that has been available for several years (the 802.11b standard was ratified in 1999). Users also indicated a fairly high interest level in deploying 54-Mbps 802.11g, either by itself or in dual-mode products with 802.11b.

Interest in 802.11g is most likely due to the perception of investment protection. 802.11g runs in the same frequency band as 802.11b (2.4GHz). Because they share a common frequency and thanks to some IEEE standards specifications, 802.11g is backward-compatible with 802.11b.

What is surprising, if not distressing, however, is the relatively low indication of 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, this technology represents a crucial component for large-scale wireless implementations in general and the success of voice over IP (VoIP) over WLANs (VoWLANs) in particular.

802.11a brings to the table the additional channels needed to avoid interference. Use of the technology will likely also contribute to improved quality of service (QoS), as network implementers can potentially put real-time voice conversations on certain channels and data on others.

Figure 3: User Satisfaction with Existing WLAN Installations



Users with existing WLAN experience rate their satisfaction levels fairly high.

Another issue is that in mixed 802.11b and 802.11g networks, when an 802.11b client associates to an 802.11g access point, throughput for all members of that basic service set (BSS)—defined as one access point and some number of client devices associated with it—falls back to the shared 11-Mbps speed of 802.11b. In other words, the presence of even a single 802.11b client compromises the throughput benefits of the 54-Mbps 802.11g network for all 802.11g users in that BSS.

Yet 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 (Figure 4).

What many users do not realize is that both 802.11b and 802.11g have just three nonoverlapping channels available to them in the 2.4GHz band, while 802.11a has approximately 24 in the 5GHz band. (The number of 802.11a channels available varies slightly by geographic region and local telecom regulatory rules.)

Because each 802.11-based access point is tuned to a channel, only three 802.11b or 802.11g access points can occupy a given coverage area before you must tune the next access point to the same channel as the first. Depending on the reach of the access points, interference could become an issue.

Once you add 802.11a's 24 nonoverlapping channels into the mix, however, by the time you have to repeat channels, the two access points sharing the same channel will be so far apart that there will be a small likelihood of interference. In a mixed 802.11b/a or 802.11g/a network, for example, the number of channels available is 27: 3 in the 2.4GHz band plus 24 in the 5GHz band.

On the other hand, running a dual-radio 802.11a/g access point (or simply a mix of standalone 802.11g and 802.11a access points) would provide the maximum number of channels with the maximum throughput in each channel while supporting all industry-standard clients.

Product Preferences

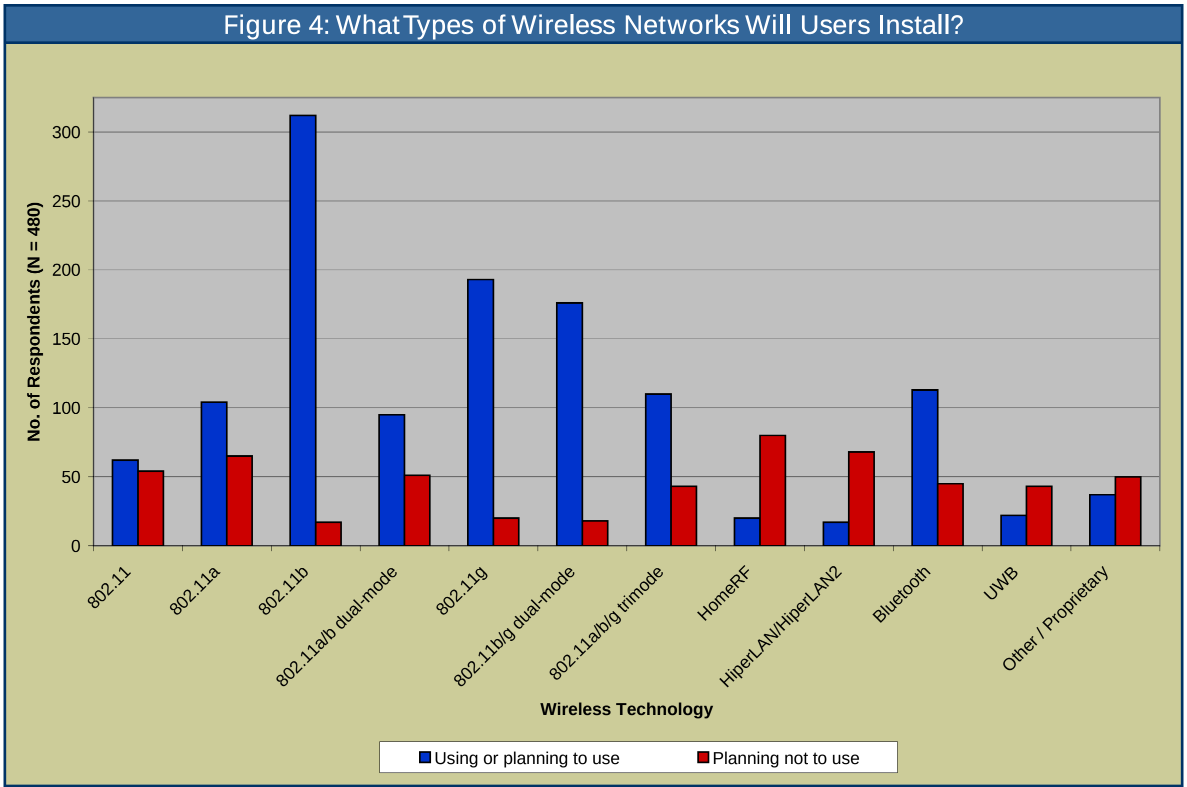
Understandably, the vast majority of respondents intend to use notebook computers as their WLAN client device of choice (82% within 18 months). Such devices are most broadly equipped with WLAN connections today. Most notebooks now ship with an integrated Wi-Fi network interface card (NIC) option for a negligible price premium.

In addition, mainstream knowledge workers are accustomed to the workings of their laptops and the generous size of the laptop screen for using traditional business applications.

Personal digital assistants (PDAs) ranked second as representing a significant component of WLAN installations, likely due to the mobile nature of their form factor. Surprisingly, desktop computers (46% within 18 months) followed PDAs as targets for Wi-Fi connectivity. Presumably, the impetus is to reduce cabling materials and installation costs.

Vertical-industry devices, such as scanners, ranked low as a significant component of WLAN installations (Figure 5). This is odd, considering that this application has to date been the mainstay of the WLAN business. Many organizations such as transportation companies tracking packages at the loading dock, for example, simply would not be able to meet their business's expectation levels without the mobility benefits afforded by WLAN technology.

Figure 4: What Types of Wireless Networks Will Users Install?



As the longest-standing multimegabit-speed standard WLAN technology, 802.11b is the most broadly deployed WLAN type today. Survey respondents expressed enthusiasm for migrating to its 54-Mbps cousin, 802.11g, but interest in 802.11a ranks low. Users should rethink these strategies, in that they gain an eight-fold improvement in the number of available, nonoverlapping channels with 802.11a technology.

Surprisingly, a substantial number of respondents expressed little knowledge of a product category that combines so-called "wireless LAN switches" with "lightweight access points" to centralize the management of certain WLAN functions and thereby enhance network scalability.

This finding was quite interesting, given the rash of product announcements from both startups and traditional WLAN vendors during the past 18 months in this product category—announcements that have been made with much fanfare. Still, more than a third (34.4%) said they'd heard of this product category, but didn't know enough about these products to comment on the possibility of using them.

What's Driving WLAN Demand?

Webtorials respondents indicated both tactical and strategic reasons for their interest in implementing wireless networks. When asked to choose the two greatest benefits they hoped to gain from a WLAN implementation, top-scoring choices reflected both applications of the technology that empower employees in new or different ways and uses that simply allow organizations to achieve the same capabilities at a lower cost.

Improved Knowledge-Worker Access

As noted in the findings summary in the introductory section of this report, the overwhelming vote for the biggest benefit of using WLANs was to improve knowledge-worker productivity by enabling access to corporate resources for more hours of the day from more locations.

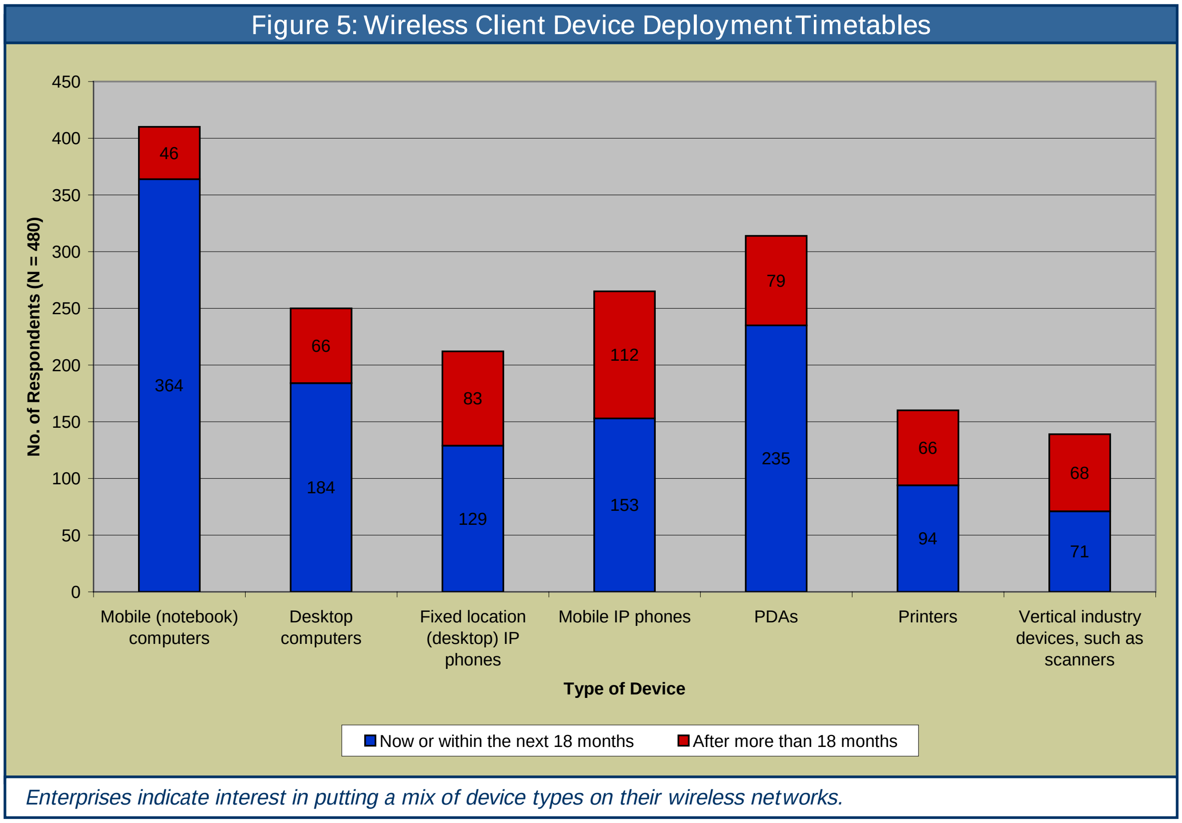
Some respondents noted that support of temporary or part-time workers was also an impetus for installing WLANs. Users were also interested in applying wireless to enhance specific business processes (such as improving inventory management).

Reduced Cabling Costs

Respondents also showed enthusiasm for using wireless to reduce cabling costs. Generally, industry consensus is that a single cabling drop costs about $150. Multiplied by the number of employees, it's evident how these costs quickly add up in large enterprises.

And given the high level of interest in putting wireless NICs in desktop computers, as referenced in Figure 5, the fact that nearly 40% of users were interested in reducing the operational expenses of cabling with a wireless solution jibes with respondents' selection of wireless products they intend to deploy.

Figure 5: Wireless Client Device Deployment Timetables



Enterprises indicate interest in putting a mix of device types on their wireless networks.

Despite these perceived benefits, less than a quarter of respondents (22%) had been able to calculate a hard return on investment (ROI) for WLANs; the others had either been unable to do so or had not attempted the exercise (Figure 6). Apparently, the hard payback of knowledge worker mobility is either difficult to attach to a price tag or the cost of ownership is low enough that users don't feel they need to formally justify implementing WLANs.

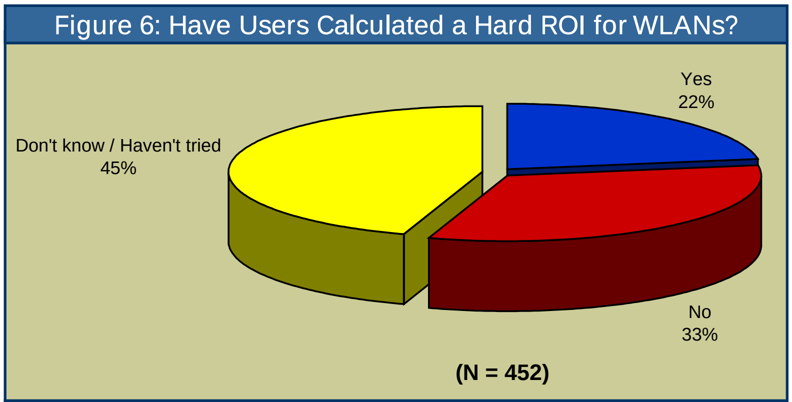
Webtorials respondents also showed a healthy interest in running voice over their wireless networks. Let's take a closer look at wireless VoIP perceptions and trends.

Wireless Voice Strategies

About a fourth of Webtorials respondents indicated that running VoWLANs was one of the two most important benefits they hoped to gain from a Wi-Fi implementation. There are likely multiple forces at work here.

Wireless local networking and the conversion from TDM to packet telephony are perhaps the two biggest potential projects under review in many enterprises. And they are related. If an organization has made the commitment to move to a packet-voice infrastructure and has also decided that the data-productivity and reduced-cabling benefits of WLANs make wireless an intelligent choice, the next natural step will be to combine the two efforts.

Figure 6: Have Users Calculated a Hard ROI for WLANs?



It appears challenging to put an ROI number on WLAN installations that users say will primarily aim to improve the productivity of mobile knowledge workers.

Why? Convergence saves on capital and operational expenses not only at the network element level, but also at the client-device level. With VoIP phones (whether they are wired or wireless) costing several hundred dollars, it potentially pays to make that phone a wireless VoIP phone that can be used both at fixed workstations and when locally mobile. Accessing the corporate VoIP network using the "free" WLAN allows users to be mobile without having to pay cell phone charges when they are within the enterprise. It also gives them access to XML applications from the wireless handset when mobile but without their laptops.

Most respondents pointed to the ability to contact locally mobile users and to conserve cell phone costs as the two biggest benefits they would hope to gain with VoWLANs (Figure 7).

Paradoxically, however, when respondents ranked the overall importance of various networking technologies, WLANs and VoIP separately ranked fairly high, while VoWLANs ranked substantially lower. This result indicates that some users haven't put two and two together yet on the benefits of converging the two technologies as they merge voice and data on the wired side of their networks.

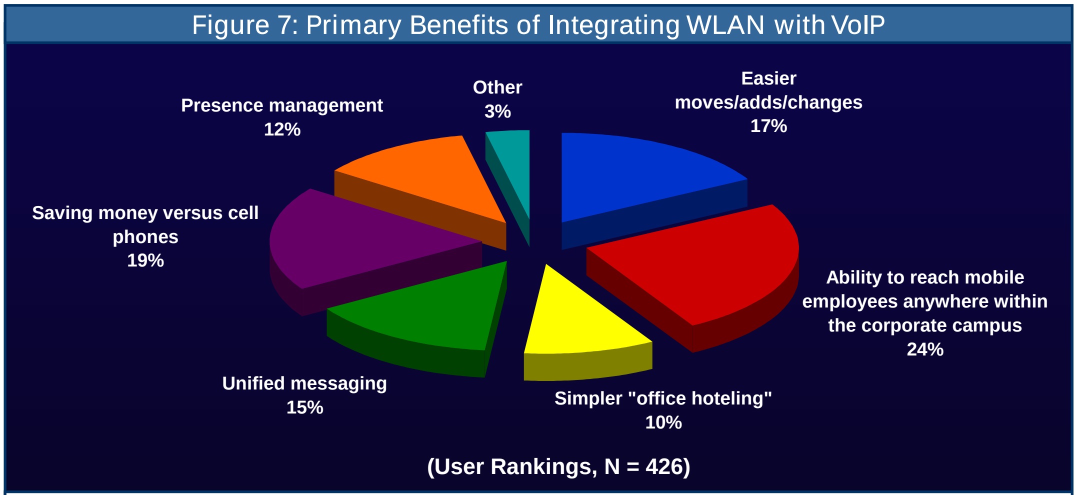
The move to VoWLANs will likely further heat up as handsets that support both 802.11 and cellular WAN connections become widely available this year. Using such handsets, a single device can support local mobility with no airtime charges, and then switch to the cellular network when the user roams off campus.

Note, though, that at this juncture, there are strides that still need to be made in the IEEE to prepare 802.11-based technology for QoS in heavily loaded wireless networks. The 802.11e standard for QoS—which addresses traffic prioritization marking and queuing, as well as polling to manage the latency introduced by bandwidth contention—is currently on track for ratification in June 2004.

And a new IEEE study group, the Fast Roaming Study Group, just formed in January 2004 to tackle the issue of latency introduced as users roam among access points in different subnets, which requires them to re-authenticate.

And speaking of security, user perceptions are that WLANs still have vulnerabilities that wired networks do not. As discussed in the section below, security ranks at the top of WLAN deployment challenges.

Figure 7: Primary Benefits of Integrating WLAN with VoIP



Some users are grasping the synergies between the mobility aspects of wireless networks and converged packet voice/data networks.

Deployment Impediments

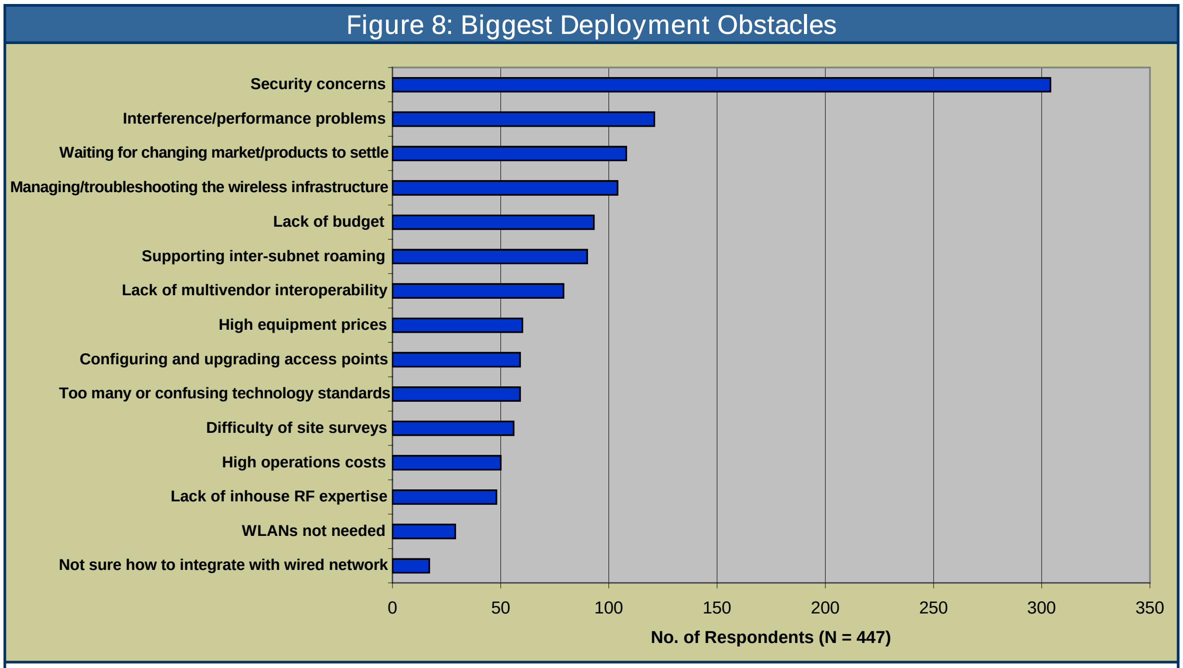
When asked to rank the three biggest factors challenging their WLAN deployments, Webtorials respondents indicated a surprisingly low level of worry about capital and operations costs. They also expressed little concern about their ability to scale and manage large WLAN installations.

Predictably, however, user trepidation about wireless security persists. In fact, perceived security issues far outpaced all other potential deployment impediments (Figure 8).

Security Perceptions

Users simply might not yet be convinced by vendor claims that they have plugged well-known wireless security gaps. The vendor point of view on WLAN security is basically that the known vulnerabilities in the 802.11 standard have "been solved."

Figure 8: Biggest Deployment Obstacles



Security concerns far and away present the biggest obstacle to WLAN deployments, followed by worries about interference and performance problems.

The fixes include the industry's replacement of static encryption keys in the Wired Equivalent Privacy (WEP) component of the standard with dynamic, rotating keys. They also include use of the industry-standard 802.1x authentication framework and an IEEE mandate for products to migrate from RC4 to Advanced Encryption Standard (AES) encryption.

In addition, vendors have created their own ways of detecting and blocking "rogue," or unauthorized, access points to prevent session hijacking.

It is also possible that users may believe that the technology exists to run a secure WLAN, but may not feel confident in deploying the various components to create a secure overall infrastructure. More respondents consider security of the "wireless infrastructure" a major problem than do those who break out the relative weaknesses of specific technologies, such as encryption or authentication algorithms (Figure 9).

Given that RF signals radiate in three dimensions and through walls, secure management of the signals must be in place to ensure that outsiders do not steal packets in transit or piggyback onto legitimate user connections. And some users worry about using standard "best practices" for security, figuring that if approaches to wireless security are standardized and known, hackers will quickly learn to circumvent them.

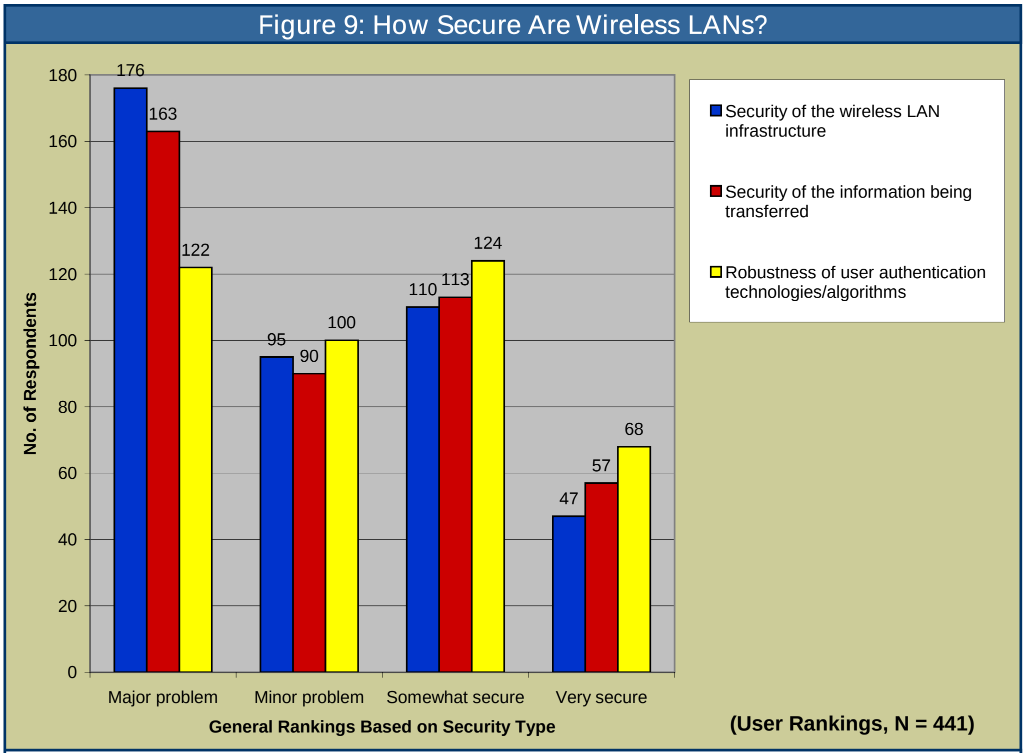
Consequently, most respondents who have deployed WLANs indicated that they are using virtual private network (VPN) technology (IPSec or SSL encryption) to protect their wireless connections. As Layer 3 and 4 technologies, IPSec and SSL are outside the scope of 802.11 standards. But consultants recommended VPN use with Wi-Fi networks for many years while Layer 2 security issues were being solved.

What is necessary to turn the corner on the security hurdle is for the industry to educate users about the various components of securing a wireless network and present them with a high-level decision tree of all the pieces they need to address. Users might choose to implement different technologies and products to fulfill the various security requirements, but at least they could feel confident that hadn't left any security stones unturned.

Ultimately, will security concerns be a deal-breaker for WLANs? Likely not.

"All of the wireless security initiatives to date have been proven flawed," wrote one survey-taker. "However, the business perception of wireless as an enabler continues to drive the requests for Wi-Fi."

Figure 9: How Secure Are Wireless LANs?



More respondents worry that their data will be stolen in transit than they do about an unauthenticated intruder gaining access to their corporate data via the Wi-Fi network.

Interference and Performance Problems

Second on user worry lists was the impact of interference on network performance. About 27% of Webtorials respondents cited this as one of the three most important factors challenging their deployments today. Note that while this factor ranked No. 2, security was cited more than twice as often, with 68% pointing to security as a challenge.

The problem of interference and its impact on performance grows, somewhat, in step with the size of the Wi-Fi installation. As mentioned in the section, "Enterprise Perceptions and Plans: Technology Preferences," the three-channel limitations of 802.11b—the most broadly deployed technology today—and the newer 802.11g render the danger of interference and its impact on application performance greater than in 802.11a networks.

Because 802.11a products, which support up to 24 channels, have only recently begun shipping from multiple vendors, users have not yet warmed up to using them strategically to help mitigate their interference problems.

Meanwhile, providers of access points, access point component technologies, and standalone RF management tools are meeting the interference problem head-on. Some Wi-Fi system makers offer tools that allow users to import floor-plan blueprints and build simulations of their work environments. These tools instruct wireless implementers as to the optimum locations to place access points to avoid interference from one another and from other types of wireless devices.

And system components are being developed—both in hardware and software—to enable WLANs to self-adjust to changing environmental conditions. For example, access points will soon get "smarter" and be able to automatically change channels, adjust power output, and redirect traffic to other access points in the face of interference.

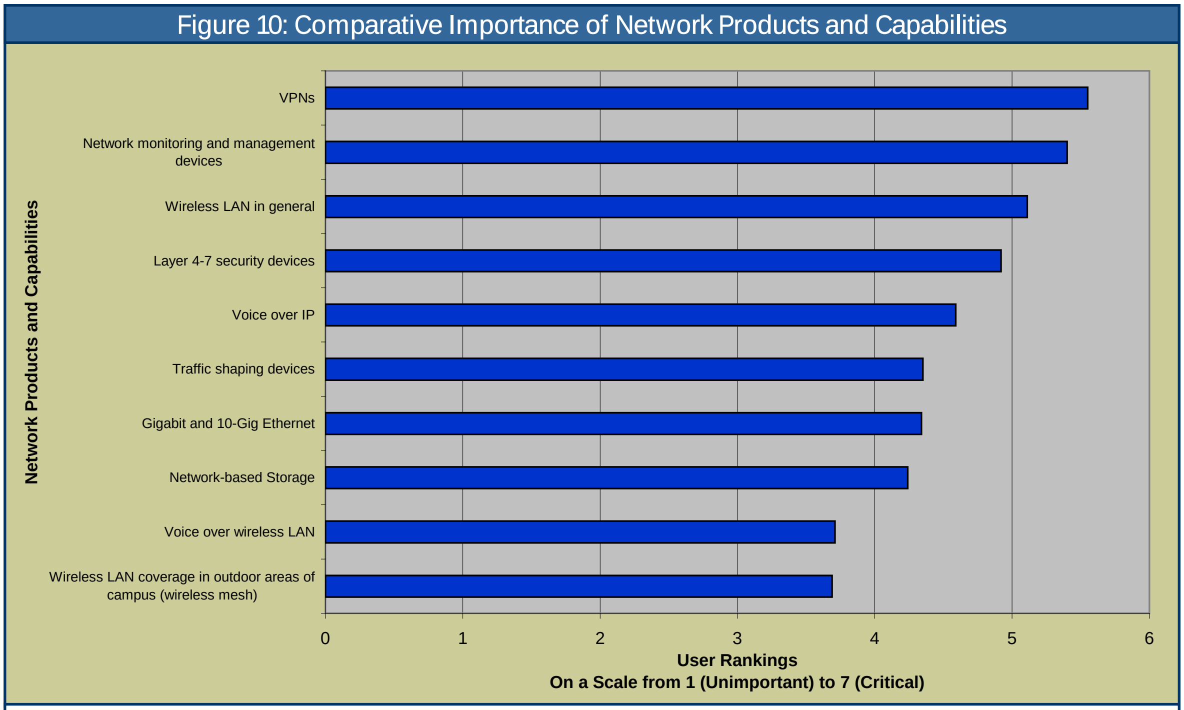
Because of these advances, it is likely that future "State of the Wireless LAN Market" surveys will show interference and performance decreasing on users' lists of concerns.

Conclusions

In general, Webtorials readers who participated in this study have embraced the idea that local wireless networking has significant business benefits. Indeed, most have already implemented WLANs or are planning to do so fairly soon. And WLANs rank a fairly close third to VPNs and network management/monitoring products in user assessments of the overall importance of network products and capabilities (Figure 10).

Note that these three product categories are not mutually exclusive; for example, many respondents cited VPNs as a necessary accoutrement to WLANs, and network management and monitoring apply to the wireless side of networks, as well as to the wired side.

Figure 10: Comparative Importance of Network Products and Capabilities



WLANs occupy a respectable third place in user rankings of the relative importance of many kinds of networking products and capabilities.

The Webtorials survey indicates that most organizations using WLANs have wisely started small and are building their networks incrementally. Wireless networking allows this luxury. Because WLANs offer an additional type of access to the wired network, they currently are perceived by some organizations as a "nice to have" rather than a "must have" in horizontal installations. So some companies can afford to get their feet wet with the technology before committing to wholesale implementations.

In addition, Wi-Fi technology continues to mature. Solutions to interference problems, QoS, and fast roaming are still emerging. So enterprises that would like to see where the technology settles before committing to large-scale deployments can install a few access points now in locations where they know they will get an immediate benefit.

If technology changes and those access points need to be replaced in a year or two, the impact on the enterprise is negligible. This is because capital prices have already become quite affordable, as reflected in user rankings that capital (and operations) costs are not of top concern to them.

Because enterprises have bought into the benefits of WLANs, it's now up to the vendor community to solve the outstanding challenges—perceived or real. They need to distinguish their products in straightforward ways that don't confuse—and, as a result, paralyze—enterprise customers. If vendors succeed on the education front, the WLAN uptake should accelerate at a rapid pace during the next 24 months.

About the Authors

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 *Business Communications Review* and *Computerworld*.

Steven Taylor is president of Distributed Networking Associates and publisher of the Webtorials networking-education Web site, which conducted the survey for this report. 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. His articles appear in *Business Communications Review* and *Network World*, and he co-authors the "Convergence" and "Wide-Area Networking" newsletters distributed by *Network World Fusion*.

Solving Wireless LAN Security Concerns

By Tony Rybczynski,
Director of Strategic Enterprise Technologies, Nortel Networks

From the Sponsor

NORTEL NETWORKS™

Wireless LANs (WLANs) extend and leverage the ubiquity of Ethernet networks and the Internet. WLANs also extend the plug-and-play nature of Ethernet to locations where wiring may be difficult, impractical, or expensive. They also enable mobility, allowing users to retain access to corporate resources when in meetings or otherwise on the move.

So why, then, haven't enterprises fully embraced WLANs as an intrinsic part of their IT infrastructures?

The primary obstacle has been concerns surrounding security.

WLAN signals are transmitted via radio waves. Because signals are airborne and do not require line of sight to reach their destinations, they have no physical barriers to protect them from outsiders. Consequently, intruders can intercept the signals of non-secure access points (APs) from outside a building using "war-driving" and "war-chalking" methods, exposing the enterprise's confidential resources. The insertion of "rogue" APs—malicious or otherwise—can also create vulnerabilities.

Wired Equivalent Privacy (WEP), the primary security mechanism that has long shipped with most WLAN products, has proven insufficient to protect networks against unauthorized access, session hijacking, eavesdropping, and other threats. Roaming is another issue: WLAN users cannot generally roam between IP subnets without re-authenticating themselves to the network. And inter-subnet roaming may simply not work in some multivendor WLAN environments.

'Olde Worlde' Security Solutions

Not surprisingly, enterprises have not taken these threats sitting down. They have adopted several solutions to their security concerns, including the following:

- **DMZ isolation.** This approach uses virtual LANs (VLANs) to segregate the WLAN traffic and connect WLAN users to certain enterprise servers in a DMZ area outside the corporate firewall. This prevents unauthorized users from using the corporate WLAN for Internet access and protects the corporate LAN.

- **RF isolation.** This approach attempts to isolate the WLAN radio signals from the outside world. With a high-gain directional antenna, outsiders can gain unauthorized access to a WLAN from many miles away. One way to combat this threat is to provide a physical barrier that RF signals cannot penetrate to simulate a "secure zone."

  Another method of blocking unauthorized outsiders from taking advantage of the open-air availability of the signal is to surround the perimeter of the corporate grounds with APs that are not connected to the internal network. An outsider is blocked from seeing the internal WLAN because the outside APs operate at the same frequency as the internal ones and offer greater signal strength to the outsider. In effect, the external WLAN "jams" the internal signal for the outsider. The disadvantages of this approach are that it is expensive and is not 100% effective.

- **Proprietary WLANs.** Some WLAN vendors have developed their own security solutions. Most are vaguely standards-based, but cannot interoperate with other vendors' solutions. Customers are thus locked in a single-vendor scenario, which comes with a high price tag and a complete dependence on the vendor's strategy and development cycle. Often the intelligence in these solutions is implemented in the APs, complicating management, increasing costs, and at times requiring hardware upgrades to support new features if processing power is insufficient to handle the added capabilities. Clearly, these stopgap approaches incur a total cost of ownership penalty and are difficult to evolve.

- **IP virtual private networks (VPNs).** IP VPNs were developed to initially meet the needs of secure remote access over the Internet. Enterprises have favored this technology for adding security to WLAN deployments either by leveraging their investments in secure IP services gateways, such as Nortel Networks Contivity*, or by deploying additional VPN units closer to the WLAN APs.

> ***"Centralized security management forms an important part of 802.11i."***

IP VPN-based wireless security is platform- and radio technology-agnostic; the client system establishes a connection to the network via the WLAN, and the VPN takes over from there. Users trying to access the network via the WLAN are first authenticated by the WLAN network and then by the VPN server (exactly as if they were accessing the enterprise across the Internet). Their information is encrypted, and all communication is logged by the VPN system. This approach solves many enterprise WLAN security challenges. In fact, it is a solid standards-based element of Nortel Networks WLAN security architecture, which is discussed later.

These approaches to securing WLANs solve some, but not all, elements of the security conundrum. What works best is the use of solid WLAN standards combined with a WLAN architecture that is functional, secure, and manageable.

Putting IT Back in Control

The foundation of today's WLAN solutions is standards. The IEEE 802.11 committee has responded to the needs of WLAN users by undertaking the development of a number of new standards, which complement IEEE 802.11a, 11b, and 11g. Most notable among these is the still-emerging 802.11i, which establishes a robust WLAN infrastructure for security.

802.11i and Wi-Fi Protected Access (WPA), a subset of 802.11i, provide an alternative to WEP. They introduce access control based on the IEEE 802.1x authentication framework, dynamic re-keying, per-session key-distribution mechanisms, and strong cryptographic algorithms. Centralized security management forms an important part of 802.11i. IEEE 802.1x provides authentication/access control for the APs through use of the Extensible Authentication Protocol (EAP), a set of messages for authentication negotiation. Enterprises have a choice of several authentication transport methods between client and server for use with EAP.

So how do enterprises go about implementing a solid standards-based WLAN architecture? Winner of the Security award at SuperComms' 2003 SuperQuest awards, Nortel Networks WLAN 2200 Series has a secure and open WLAN architecture based on a tiered approach both physically and functionally. It offers an optimal distribution of functionality and security for better performance and a lower total cost of ownership.

Nortel Networks WLAN 2200 Series builds on Nortel Networks Unified Security Framework; in particular, on the principles of variable-depth security, closed-loop policy management, and uniform access management. Nortel Networks Unified Security Framework provides a conceptual, physical, and procedural framework of best recommendations and solutions for enterprise network security and serves as an important reference guide for IT professionals responsible for designing and implementing secure networks.

"We offer complete end-to-end architecture for all existing cellular standards. Because of this wireless experience, we knew how important it was to also get the WLAN security issues addressed at the foundation of our architecture," says Atul Bhat-

6th Annual
SUPERQuest
Awards

nager, vice president and general manager of enterprise data networks at Nortel Networks.

APs are the first tier of Nortel Networks WLAN architecture, providing wireless connectivity to roaming mobile users equipped with laptops, PDAs, and mobile telephones. Nortel Networks WLAN 2200 Series Access Points are designed to evolve to support new wireless standards and technologies for more effective use of the radio spectrum and greater security over the radio link. Nortel Networks WLAN 2200 Series Access Points support a broad range of security features, including WPA support, multiple filters, and multiple authentication mechanisms.

The second tier of Nortel Networks architecture is wired Ethernet networking. Nortel Networks switches include support for IEEE 802.3af-standard power over Ethernet (PoE), VLAN segmentation, and quality-of-service (QoS) capabilities. The advantage of using these proven high-performance devices is that the enterprise has the choice of where and how it wants to integrate WLANs into the basic wired Ethernet infrastructure. It also allows a common PoE technology to be used consistently across both wired and wireless environments.

The third tier in the architecture provides networking and application-aware security at Layers 2 through 7 of the OSI model: Nortel Networks WLAN Security Switch 2250. This product is a WLAN-optimized, purpose-built Layer 2 – 7 secure platform. The WLAN Security Switch 2250 is standards-based and AP-agnostic, allowing APs to evolve independently and thus future-proofing enterprise investments when non-Nortel Networks APs are already deployed. The WLAN Security Switch 2250 sends an authentication request to the user’s browser, allowing the user to enter his/her credentials, which it matches against information in a directory. Users can be authenticated via a built-in database or via existing central authentication servers such as Lightweight Directory Access Protocol (LDAP), Remote Access Dial-In User Service (RADIUS), Windows NT Domain, and Active Directory.

> ***“SSL VPNs, operating at the session layer, encrypt information exchanges through Web applications and limit access.”***

The WLAN Security Switch 2250 supports a wide range of authentication methods. These include passwords, smart cards, certificates, and tokens, as well as combinations of these methods. If the user fails to authenticate, custom actions can be taken. For example, the user can be redirected to a locally stored Web page with an error message, requesting the user to contact support or reset a password.

Once the user has been authenticated, access control mechanisms ensure that the user only has access to resources specified in a policy server. Enforcing who can access your network via the WLAN is a vital component to any security policy.

Nortel Networks WLAN Security Switch 2250 supports a range of encryption techniques, including IPSec and SSL VPNs (and in the future, 802.11i-standard AES). IPSec VPNs, operating at the network layer, are application-agnostic, and require client software. For example, an IPSec-based VPN connection can be used to access email, interact with self-serve human resources applications on the intranet, and browse the network.

SSL VPNs, operating at the session layer, encrypt information exchanges through Web applications and limit access. They don’t require any special client software other than a Web browser. The SSL VPN approach is particularly attractive when the enterprise wants the lowest-cost security solution for limited application access. It is also useful when the enterprise doesn’t own or control the remote-access devices, as in the case of visiting customers, contractors, or suppliers.

Nortel Networks WLAN Security Switch 2250 can terminate IPSec VPN tunnels or provide IPSec passthrough to the installed base of secure IP services gateways. The advantages of this approach are consistency for remote, branch, and WLAN users; simplified management; and investment protection. In cases where IPSec VPN support is the only requirement, secure IP services gateways can continue to be used in the architecture. The WLAN Security Switch 2250 can be added at a future date when guest support through a captive portal and inter-subnet roaming become a requirement.

Nortel Networks tiered WLAN architecture provides a high degree of flexibility while meeting the needs of the enterprise for secure WLAN access. It is complemented by access control—which authenticates all users and authorizes which network resources are accessible—and by network management for both the wireless and wired portions of the network.

Summary

The 2003 SuperQuest award underlines Nortel Networks understanding of the security challenges faced by businesses in embracing WLANs for extended business connectivity, increased employee mobility, and productivity.

“Nortel Networks 2200 Series has been created to meet the needs of enterprises as they move through the process of WLAN adoption,” Bhatnager says. “The products will grow with enterprises as the WLAN becomes a ubiquitous component of their network infrastructures.”

> ***"Central to Nortel Networks vision is the principle that security is inherent to all applications and services, whether accessed by a wired or wireless connection."***

Nortel Networks WLAN 2200 Series, including mobile adapters, the WLAN Access Point 2220, and the WLAN Security Switch 2250, allows seamless voice and data roaming within and across IP subnets and between 2.4GHz and 5GHz radio frequencies. Sessions remain uninterrupted even across subnets and frequencies. Central to Nortel Networks vision is the principle that security is inherent to all applications and services, whether accessed by a wired or wireless connection.

The WLAN 2200 Series delivers high-end, enterprise-class security at both the network and application levels, consistent with Nortel Networks layered Unified Security Framework. This includes WPA based on IEEE 802.1x with per-user, per-session keys and key rotation for added security. This portfolio also supports an extensive set of QoS, bandwidth management, and access controls for wireless users. Comprehensive network management is complemented by failsafe business continuity through redundant AP and security switch configurations.

Nortel Networks envisions APs distributed across the enterprise with WLAN security integrated into the enterprise infrastructure (such as embedded in campus router/switches) with users roaming seamlessly among enterprise WLANs, cellular networks, WLAN hotspots and mobile WLANs.

Nortel Networks WLAN solutions allow enterprises to securely offer a new dimension in productivity for users-—without compromising the IT department’s control over the networking infrastructure.

**Nortel Networks, the Nortel Networks logo, the globemark design, and Contivity, are trademarks of Nortel Networks. All other trademarks are the property of their owners.* *Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.*