

Taming
the Wild,
Wireless LAN
June 2002

Custom
Consulting
Analysis

Table of Contents

Taming the Wild, Wireless LAN

*Management Software
Becomes Critical, as Wireless Local
Area Networks Grow in Size, Complexity*

Sections	Section 1	Growing Complexity Drives Need for Automated Management	2
	Section 2	Elements of WLAN Management.....	4
	Section 3	Wavelink Solutions	6
	Section 4	Management in Action	9
	Section 5	Strong Returns.....	11
 Figure	 Figure	 Elements of Effective WLAN Management Software	 5

NOTE: This report is based upon information believed to be accurate and reliable. Neither Summit Strategies, Inc. nor its agents make any warranty, express or implied, as to the accuracy of the information or the opinions expressed. We shall have no liability for any errors of fact or judgment or for any damages resulting from reliance upon this information.

Trademarked names appear throughout this report. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, Summit Strategies uses the names only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

© 2002. Reproduction in whole or in part is prohibited except with the written permission of the publisher.

Unauthorized use or sharing of this document is strictly forbidden.

Taming the Wild, Wireless LAN

*Management Software
Becomes Critical, as Wireless Local
Area Networks Grow in Size, Complexity*

Wireless Local Area Networks (WLANs) based on the IEEE 802.11b standard have been one of the great technology-industry success stories during the past couple of years. The combination of a stable standard and unregulated radio spectrum has brought broad vendor support and sparked a positive feedback loop that delivers performance, innovation and falling prices. In record numbers, WLANs are being deployed in three basic types of situations:

1. To provide network connectivity to workers beyond the reach of wired LANs;
2. To help mobile workers access corporate data from home, public places or other offices; and
3. To reduce the cost of “moves, adds and changes” in enterprise IT infrastructure.

While discussion has focused on rapid growth of the WLAN market, little attention has been paid to a related set of changes: As they grow in number, WLANs are also changing in size, scope and complexity—and in their strategic importance to the companies that deploy them.

Growth inevitably requires management, and WLANs are no exception. In fact, as more organizations are discovering, management is the dark secret of WLANs—easy to underestimate, even ignore, until it rears its head. Many organizations are learning to their chagrin that, although their wireless networks are delivering promised benefits, they also require lots of attention and upkeep. Furthermore, these organizations are finding out that WLAN management is complex and requires skills that are not only rare, but expensive. But, if it is not properly addressed, the result can be poor performance and reliability, as well as risk of intrusion that puts sensitive information at risk.

The solution, we believe, is software that simplifies and automates the deployment, oversight and continuing maintenance of WLANs to optimize their performance and reliability while minimizing cost of ownership. One of the pioneers in this field is Wavelink, whose Mobile Manager and Avalanche offerings address management issues that many customers—and vendors—are only now beginning to notice.

In this white paper, we discuss the growing complexity and strategic importance of WLANs, and how those factors are driving the need for automated management capabilities. We describe the elements of effective WLAN management, then present an overview of Wavelink's WLAN management solutions and the benefits they deliver in both initial deployments and continuing network oversight. Finally, we offer some concluding thoughts on the return that customers can anticipate from an investment in WLAN management tools.

Section 1 Growing Complexity Drives Need for Automated Management

Wireless networking has a long history in certain specialized markets—factories, warehouses and distribution centers, some retail concerns—where connectivity was needed, but traditional networks were impractical. The combination of improved performance and falling prices has dramatically expanded these existing markets and, at the same time, spawned entirely new markets in fields such as health care (in hospitals and clinics); education (especially at the university level, but also in secondary and even K-12 institutions); on corporate campuses; and in public areas such as airports, convention centers and cafes.

Just as important, but less obvious, are some fundamental changes in how WLANs are deployed:

- *Size.* Not only are wireless networks more numerous, but individual WLANs are becoming larger. In the past, a typical WLAN might have involved a dozen access points and a few dozen wireless-enabled devices. Today, it is not uncommon for a WLAN to involve hundreds of access points and thousands of end-user devices, and some are larger than that;
- *Scope.* Besides increasing in size, WLANs are becoming more far-flung. In the past, a company might have had WLANs in its warehouses; but, today, it deploys them throughout the organization—in retail stores, manufacturing centers and offices, as well as warehouses. As this occurs, individual WLANs are more geographically dispersed and far from the organization's central IT staff, which nonetheless wants to manage them consistently, according to established policies for access and security; and
- *Strategic importance.* As they become established throughout an organization's departments and locations, WLANs become part of its core

IT infrastructure and gain mission-critical status. Failure of a factory-floor WLAN could interrupt production, while a WLAN security breach in a retail store could endanger sensitive corporate information.

Inherently Different

WLANs also differ from wired LANs in both structure and operation. Their fundamental units—radio access points—are distributed throughout the organization, not centralized in a wiring closet. They may be hidden behind ceiling panels, or hung from the high ceiling of a warehouse or factory where a mechanized lift is required to reach them. True, administrators can use Telnet, or a browser, to manage them remotely; but this is a device-by-device process—often cumbersome, expensive and error-prone.

Because they allow mobility, WLANs are also much more dynamic than wired LANs in terms of bandwidth consumption. As users move and congregate, they may overload a portion of the network and cause its performance to suffer. To avoid this, and to maximize performance, requires careful capacity planning followed by active monitoring and management of the WLAN.

Nor are WLANs a one-size-fits-all proposition. Even within one company, WLANs may have different uses and raise different concerns. In a warehouse, for example, the WLAN may primarily support specialized handheld devices equipped with bar-code scanners for inventory tracking, with users transmitting small amounts of data, such as product numbers and inventory levels. The top priority is 24x7 availability, because downtime equates directly to lost production. One of the nation's largest retailers, for example, estimates that a WLAN outage in one of its distribution centers costs \$66,000 per minute—the value of goods the company cannot ship to stores to be sold.

In a corporate office, by contrast, a WLAN may support mainly executives using laptops and personal digital assistants (PDAs) to send and receive e-mail with attachments that include large documents, spreadsheets and presentations. This traffic, unlike that of the warehouse, involves large chunks of data that consume substantial amounts of bandwidth. Reliability is still important, even though not directly related to production levels; but the top priority may well be security of the corporate information, such as marketing or acquisition plans, contained in the data being transmitted.

Adding more complexity, WLANs within a single organization may include equipment from a variety of different vendors. This can happen in corporations because of acquisitions or department-specific needs, for example, or in universities where individual departments deploy WLANs independently, without central coordination.

In any of these situations, IT managers may have different priorities than business managers. Whereas a sales manager might rely on the WLAN to keep employees in contact with each other and help the manager meet quarterly goals, IT's top concerns might be to ensure that the WLAN equip-

ment meshes properly with the rest of the company's infrastructure, and to ensure security and reliability by keeping firm control of individual devices. IT oversight and control may be relatively easy in a factory environment, where workers turn in their handhelds at the end of each shift, but difficult in a medical center where doctors and nurses use handhelds for access to critical patient data and are loath to relinquish them for upgrades or maintenance. From a financial standpoint, removing a device from service reduces the "productive use" of that asset, because the worker who was using it is less efficient—perhaps even idle—until it is returned.

Operating Requirements

Finally, WLANs have some specific requirements that entail significant costs when managed device by device. For example, when access points are first deployed, they must be configured with specific versions of firmware, radio settings, and lists of the users and devices entitled to connect through them. End-user devices must be similarly configured, and also must be loaded with software such as anti-virus applications and job-specific programs. Once deployed, WLANs are subject to frequent change as manufacturers update firmware and introduce new products; new employees are hired; new stores and offices are built; security codes are updated, and the like. Each of these changes requires an administrator to "touch"—physically or electronically—each access point or device that connects to the WLAN.

These chores are manageable in a small WLAN, but can be daunting in the extreme in a large enterprise. A case in point is a global retail clothing company that uses Wavelink software to manage WLAN access points throughout its 3,300 retail stores. Each network has two or three access points and multiple handheld devices. Many companies, even if they have sophisticated IT departments, are not well versed in wireless network technologies. And, even if they have these skills in their central offices, almost inevitably they do not have them in the field. Nor is it feasible to hire for these skills at the scale these organizations need. Although WLAN equipment itself has become relatively inexpensive, network administrators are not—especially those with wireless training.

For all of their attractions in terms of performance, flexibility and affordability, then, WLANs also pose management challenges very different from those of wired networks. Moreover, these challenges increase geometrically as WLANs grow in size, scope and complexity. The solution, we believe, is to automate these management tasks. In Section 2, we discuss how this can be accomplished.

Section 2 Elements of WLAN Management

An effective WLAN management solution has two fundamental capabilities. First, it provides real-time visibility into the entire network, including all access points and end-user devices. It displays the specifics of their con-

figurations—such as firmware, radios, security and software—and it shows the network’s status in terms of traffic levels, bottlenecks and overall health and performance.

Second, an effective WLAN management solution provides automated, policy- and agent-based control from a central location of all elements in the network, across multiple sites. It provides this capability both for initial deployment, and for ongoing operation and maintenance of the network or networks. Simply put, if someone in Tallahassee plugs in a new access point, an administrator in Seattle should see it happen. If the new device is authorized, the administrator would simply configure it to function as intended; if not, the administrator would disable it.

Beyond these two requirements—visibility and control—certain other attributes are desirable (see Figure). For one thing, the management tool should support as many different types of equipment as possible, in terms of both access points and devices, to minimize “blind” spots. It should be easy to use, with an integrated interface, so that administrators don’t have to learn different menus and commands to perform similar functions on different vendors’ equipment. At the same time, it should “understand” that different devices have different capabilities—in terms of alerts and notifications, for example—and allow administrators to take full advantage of them.

These multi-vendor WLANs are more the exception than the rule, though far from rare. A retail company, for example, may have installed equipment from one vendor in its stores and from another in its warehouses, and now want

Figure

Elements of Effective WLAN Management Software

Visibility	Provides detailed information on both access points and end-user devices, regardless of location
Control	Provides fine-grained control in both initial deployment and ongoing operation
Flexibility	Allows central or distributed management, with permissions set by policy
Ease of use	Includes simple interface that allows network devices to be managed in groups, or individually, as needed
Multi-vendor support	Allows customers to choose different equipment for different needs without sacrificing management capability
Integration	Meshes easily with existing network-management frameworks, such as OpenView, UniCenter, Tivoli
Source: Summit Strategies, Inc. www.summitstrat.com	

central control over both. This type of diversity is likely to persist, and even increase. Some companies will standardize their WLAN equipment, but so many factors work against standardization—specialization for specific needs and requirements, emerging technologies such as 802.11a and 802.11g, mergers and acquisitions, to name some of the most important—that heterogeneous environments will remain at least as common as they are today.

Another desirable attribute is flexibility that allows for central or distributed management, with permissions set by policy. For example, a district-level IT administrator might have control over WLANs within a particular district, while a corporate-level administrator would have control over multiple districts.

It is worth noting that many WLAN management requirements—from initial configuration and security settings to roaming oversight—are beyond the scope of traditional network-management systems. These tools have only limited visibility into end-user devices, and were not designed with mobility in mind. For example, they don't notice when a handheld device roams from one building to another on the WLAN and acquires a new IP address. Nor can they handle the not-infrequent case when an administrator needs to update settings or applications on a handheld device, but finds that someone has changed a setting so the handheld cannot connect to the network. An effective WLAN management solution should augment standard network-management tools and integrate with them through standard application-programming interfaces.

As noted earlier, any of these functions can be performed manually, either through physical interaction with the device or through remote interaction via the Telnet protocol or a browser. The point is that the devices are becoming so numerous, and the management steps so frequent, that manual management can be extremely costly and inconvenient, to say nothing of being error-prone. Tools that automate this management can not only reduce the administrative overhead associated with WLANs, but also improve their performance, reliability and security.

Section 3

Wavelink Solutions

Wavelink's core value proposition is to reduce the total cost of WLAN ownership by enabling the central management of large numbers of access points and end-user devices. It does this via two key products: Mobile Manager for access points, and Avalanche for end-user devices, whether laptops or handhelds, and the network equipment installed on them. Each of these Wavelink products provides distinct benefits on its own, but, used together, provide even greater value. In this section we discuss the products, their functions and benefits, separately and together.

Mobile Manager

Mobile Manager provides the detailed network visibility and control capabilities discussed in Section 2. It also supports equipment from multiple

vendors, including Cisco Systems, Symbol Technologies, Nortel, 3Com, Ericsson and Intel. (Wavelink plans to support other vendors as well, including Lucent/Avaya.) Mobile Manager provides an integrated interface for all of these access points, but also includes support for vendor-specific features. This allows customers to unify the management of disparate WLANs, while retaining flexibility to choose WLAN equipment based on price, features or application support without giving up interoperability. Mobile Manager integrates with existing network-management systems and uses standard models to integrate with enterprise products, such as Hewlett-Packard's (HP's) OpenView, Computer Associates' UniCenter and IBM's Tivoli. Beyond standard integration, Wavelink has established a partnership with Computer Associates and made Mobile Manager a "plug-in" to UniCenter. It is working with HP, Tivoli and other enterprise network-management system vendors to establish the same sort of relationship and deeper level of integration with those frameworks. These partnerships are mutually beneficial, giving Wavelink access to the framework vendors' installed bases, and allowing them to offer sophisticated WLAN management capabilities more quickly than they could through internal development.

Mobile Manager's remote detection and configuration capabilities play a critical role in both the initial deployment and the ongoing operation of the WLAN. Administrators can define profiles and settings for groups of access points, and have Mobile Manager apply them automatically when it senses that new ones have come online. Once the WLAN is operating, Mobile Manager checks each access point regularly—10 minutes by default, but customers can specify any desired interval—to make sure it remains within specifications and established policies. If it finds an abnormality, Mobile Manager can be configured to alert a network administrator and/or to change the settings automatically. It can do the same thing for bandwidth utilization, continuously monitoring network performance and adjusting settings and resources to ensure optimum performance and efficiency. When access-point manufacturers release new firmware, Mobile Manager can automatically install the new version, maintaining standardization across the network.

Mobile Manager's auto-detect feature also allows it to detect many so-called "rogue" access points—unauthorized devices that can compromise the security of an entire network, wired and wireless. Rogue access points have emerged as a key vulnerability of 802.11b networks because they can be plugged into any standard network jack, and their built-in security capabilities can be defeated or disabled with relative ease.

Mobile Manager takes advantage of the self-identification feature that most enterprise-focused vendors build into their access points. When its auto-detect feature finds a new one, Mobile Manager can identify it as authorized or unauthorized, and automatically shut it down or apply preset profiles and settings so the access point functions according to policy. This does not provide total protection, however, because not all access points identify themselves. Vendors such as D-Link that primarily serve the residential and small-office/home-office markets omit the self-identification

feature to reduce the cost of their equipment. Wavelink is developing other methods for detecting even these “invisible” access points; they will be added to future versions of Mobile Manager.

To ensure security, WLAN administrators must augment rogue detection with additional tools, such as firewalls; encryption hardware and software; physical security measures; and clear policies for employee behavior.

Although access points are critical, end-user devices can impose a greater management burden—partly because they are more numerous, but also because they are more diverse, ranging from standard laptops and PDAs to specialized devices equipped with things like bar-code scanners or temperature sensors. Moreover, these devices often include end-user applications that require installation, maintenance and upgrades—in addition to the firmware, radio and security settings that they have in common with access points. Wavelink’s device-management offering, called Avalanche, is similar to Mobile Manager in that it provides visibility and granular control. It can manage devices over any IP-enabled connection—the WLAN itself, a wired cradle or docking station, or even a wireless wide-area network, as is increasingly common with PDAs.

Avalanche

Avalanche maintains connection logs that help enterprises track their mobile assets, showing an administrator when a particular device is logged in or, if not, when it last connected. Wavelink plans to develop this capability further by adding the ability to log associations between access points and devices to give administrators more information on each device’s specific location. This capability could speed the recovery of a mislaid inventory scanner, for example, by limiting the search to the area around its associated access point. Avalanche currently supports a wide variety of mobile platforms, including Palm OS; Windows CE and Pocket PC; Windows 98/NT/2000/XP; and industrial handhelds and bar-code scanning devices from numerous vendors.

Mobile Manager and Avalanche provide strong benefits individually, but their value is even greater when used in tandem. For example, when an end-user reports poor performance, the cause might be a faulty radio in an access point or a handheld, or an unusually large number of users concentrated on one access point and overtaxing it. Separately, either Avalanche or Mobile Manager would provide important data and clues as to the root cause. But, only by analyzing data from both can an administrator make a precise determination. Network security also will benefit from the two products working together to continually refresh the encryption keys on both access points and mobile devices. This addresses what has become an important security concern for many companies deploying WLANs—that hackers can decode the encryption keys with relative ease, but not quickly enough to penetrate the network if the keys are changed often.

This “dynamic key management” capability is built into both Mobile Manager and Avalanche. At the moment, it must be coordinated manually; but Wavelink is already testing a new version that simplifies the process by integrating key management across both products. The new version is scheduled for release in the third quarter of 2002.

Section 4 Management in Action

So far, we have discussed the factors driving the need for automated WLAN management; the elements of an effective solution; and Wavelink’s approach and offerings. In this section, we look at WLAN management in the way that customers often do—first in terms of an initial deployment, then in terms of continuing operation and maintenance.

Regarding initial deployment, a case in point is Wavelink’s work earlier this year with CeBIT, the annual computing trade fair held each spring in Hannover, Germany. For this year’s event, held in March, CeBIT wanted to provide wireless Internet access for many of the expected 700,000 participants. This meant installing, configuring and managing more than 200 access points spread across more than two-dozen venues. Event organizers chose Cisco Aironet 350 access points and began configuring them manually.

Days before the show began, as time ran short, Cisco contacted Wavelink for help. Wavelink personnel used Mobile Manager to define access-point profiles and then remotely configure the new access points as they were plugged into switches in the various exhibit halls. Wavelink’s software worked in tandem with Cisco’s discovery protocol to automate identification and configuration of the access points across four different subnetworks. Wavelink automatically configured 90 percent of the access points in less than two days, and also detected and reconfigured a number of access points that had been misconfigured during the earlier manual deployment.

Different Priorities

Clearly, in a short-term deployment such as CeBIT, the benefit of Wavelink’s technology stems mainly from its auto-configuration capabilities. This would also be the case for any organization planning a broad WLAN rollout across hundreds or thousands of locations. The latter situation would involve at least two key differences, however.

First, whereas CeBIT’s goal was to provide access to as many visitors as possible, the retailer would have a much greater need for data security and making sure only authorized employees had access to the network. Meeting this need would also draw on Wavelink’s auto-detection capabilities, but in a different way. Instead of detecting and configuring a new access point or handheld device for use, Wavelink’s software can detect the new

equipment, identify it and compare it to a list of authorized users before determining what action to take. Even in the absence of new equipment, Mobile Manager and Avalanche can work in tandem to maximize security by periodically distributing new encryption keys to access points and end-user devices. The security problem posed by “static” encryption keys is less important for companies that use WLANs to transmit relatively innocuous data, such as part numbers; but it has become a major concern as companies rely more often on WLANs to transmit sensitive corporate and customer data (such as point-of-sale or credit-card information).

The second major difference between CeBIT and most WLAN deployments involves change, which, over time, affects almost every facet of a WLAN deployment. Physical layouts change as businesses grow and reorganize. Access points occasionally fail and must be replaced. And the technology itself is evolving rapidly. Whereas most networks today are based on the 802.11b standard, vendors are beginning to offer faster, higher-capacity equipment based on the 802.11a variant—and yet another, 802.11g, is in development. Most observers foresee the development of WLAN equipment that supports two, or even three, different radio technologies, so that organizations can take advantage of higher speeds without abandoning their investment in 802.11b equipment. Security standards are also evolving, which entails periodic firmware updates as well as the rotation of encryption keys mentioned earlier.

Continuous Monitoring

Besides such periodic updates, WLANs require continuous monitoring for unexpected events of various types. Before an access point fails, it may show early signs of trouble that, if detected, could alert a network administrator that trouble is imminent. Lightning or a power surge can corrupt their settings, disabling one or more units and even blocking remote access via Telnet or browser. And, of course, human error is always a factor. Curious employees can hack into an access point and disable it inadvertently; even network administrators sometimes make mistakes. If this happens at 2 a.m. in a round-the-clock manufacturing operation, several hours' worth of production might be lost before an administrator arrives to address the problem manually. Mobile Manager can solve problems on its own, by detecting and resetting incorrect access-point settings automatically, without any human intervention.

Once again, most, if not all, of these tasks could be performed manually, even remotely, on a device-by-device basis. Even if each task takes only a few minutes, however, manually maintaining even a modest-sized WLAN with a few dozen access points could easily be a full-time job for more than one administrator. Simple multiplication—many devices times many required actions—demonstrates that automated management of both deployment and ongoing operation is the most effective way to maximize performance and security while minimizing cost.

Section 5 **Strong Returns**

For all of their advantages in terms of flexible, cost-effective network access, WLANs require more oversight and maintenance than many companies had suspected. These tasks can be expensive to perform manually, and dangerous—as well as expensive—to ignore. Left undone, they can degrade the WLAN's performance and/or leave it prone to intrusion.

Furthermore, the need for automated WLAN management is destined only to grow. The networks themselves will continue to increase in size and scope—unless limited by management overhead. The enabling technologies will rapidly evolve, prompting many companies to deploy multiband equipment. End-user devices will become ever more specialized. Applications will remain diverse, some involving large chunks of data that tax network bandwidth, and others that are less demanding. The same is true of users' priorities: some will be security-driven, others hungry for speed. These diverse devices, applications and priorities will drive heterogeneous deployments, as administrators choose one vendor for the warehouse WLAN, another for the corporate office and a third for the retail stores.

The strongest solution should automate WLAN management by providing real-time visibility and central control in both initial deployment and ongoing operation. It should provide seamless support for multiple vendors' equipment, to give customers maximum choice and flexibility. Both visibility and control should be as fine-grained as possible, and must encompass both access points and end-user devices—one without the other is less than half of a solution. The bottom line, of course, is return on investment (ROI): How quickly will WLAN management software pay for itself?

We know of no comprehensive study that addresses this question. On the other hand, IDC has documented strong ROI from conventional LAN-management software. We believe the value equation is even stronger for wireless LANs because of the greater number of tasks and variables involved.

Wavelink invites prospective customers to estimate the benefits of Mobile Manager for themselves, using an Excel-based tool that helps them define such factors as the hourly costs of business interruption, backup systems and IT support, and then puts those estimates into an ROI equation. In a hypothetical distribution-center deployment with 30 access points at each of 18 sites, Wavelink estimates an annual savings of approximately \$700,000, and a payback period of about five weeks. In a 500-site retail operation with two access points per site, Wavelink estimates a payback of 90 days (compared to oversight by a remote IT staff)—and just four days if the retailer hired IT support for each of the 500 sites. In an office setting, Wavelink estimates payback in 11 days, if Mobile Manager replaces on-site IT support; five months if that support is remote.

The calculator tool doesn't model payback for device management with Avalanche. But, at a list price of approximately \$80 per client device, Ava-

lanche could pay for itself in a single update, given the shipping, downtime and IT-support costs if each device had to be serviced individually at a central location. These devices are already expensive enough; studies have found that support costs often reach \$3,000 per year or higher for each unit, dwarfing their purchase cost. Actual mileage may vary, of course. But, clearly, the need for automated WLAN management is strong and growing. We believe that Wavelink, with its robust offerings, is well positioned to play a strong role in this emerging market.

Warren Wilson
wwilson@summitstrat.com

Contact information:
Wavelink Corp.
11332 NE 122nd Way, Suite 300
Kirkland, WA 98034-6936
Phone: 425-823-0111
Fax: 425-823-0143
www.wavelink.com