

Rapid
Payback:
Managing
Wireless LANS
for Maximum
ROI

White
Paper



Table of Contents

Rapid Payback: Managing Wireless LANS for Maximum ROI

Sections	Section 1	WLAN Complexity Overwhelms ROI.....	1
	Section 2	Wavelink Solutions.....	4
	Section 3	How WLAN Management Delivers ROI	6
	Section 4	Conclusions	8
 Figures	Figure 1	Savings Summary, Small Health-Care Provider	6
	Figure 2	Savings Summary, Large Logistics Company	7

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.

© 2003. 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.

Rapid Payback: Managing Wireless LANS for Maximum ROI

In today's economy, when companies have to watch every penny and justify every investment, wireless local-area networks have found success and grown dramatically in popularity. Inexpensive, easy to deploy and providing good performance, WLANs make intuitive sense as a way for companies to save on networking costs and cost-effectively link people with applications, data and colleagues. As prices fall and performance improves, WLANs are spreading in early markets such as retail and distribution, and taking root in a variety of new settings—from hospitals to corporate offices to university campuses, even fast-food restaurants.

Many companies have enjoyed promising results with their early, limited forays into wireless networking. As they venture further into this new territory, however, many companies are finding that WLANs aren't as foolproof as they once seemed. As wireless networks grow larger in size and scope, they become vastly more complex and expensive, both to deploy and to maintain. Left unmanaged, these complexities can degrade or interrupt a network's performance, and/or expose the company to security risks. Managing these complexities can be very costly, however, weakening or negating the benefits on which the WLAN investment was justified.

Fortunately, effective solutions exist in the form of network management software that improves WLAN performance and security while dramatically minimizing management overhead. Many of these solutions can quickly pay for themselves and allow WLANs to deliver maximum benefit. This paper outlines the issues that companies face as WLANs grow in size and complexity and describes the elements of an effective management solution. It then describes Wavelink Corporation's approach to addressing these issues with its Wavelink Mobile Manager™ and Wavelink Avalanche™ products. The paper concludes with some examples of WLAN deployments that illustrate in more detail the savings and return on investment these products can provide.

Section 1 **WLAN Complexity Overwhelms ROI**

As WLANs proliferate, they are growing along several axes. Most obviously, they are growing in size, measured in terms of the number of access

points and end-user devices. WLANs of two or three access points and 10 or 12 end-user devices have become quite common in small businesses. But a growing number of companies, including large retailers, manufacturers, logistics companies and even IT industry leaders such as Microsoft and Cisco Systems, are deploying WLANs that span hundreds or even thousands of access points, and tens of thousands of end-user devices. At the same time, WLANs are growing in geographic scope.

Companies are deploying WLANs in multiple buildings on a corporate campus, for example, or within company facilities located around the country. WLANs are also growing in complexity, often comprising access points from multiple vendors and supporting a wide variety of wireless-enabled end-user devices, from laptops to PDAs to specialized handheld computers with built-in bar-code scanners or magnetic-stripe readers.

As if this were not complex enough, WLANs are increasingly being used to support business-critical applications—for example, managing a company's supply chain or a distribution system, where a network failure can quickly lead to lost production or missed deliveries. On the horizon are demanding, bandwidth-intensive applications such as video- and voice-over-WLAN, whose performance can suffer noticeably from stresses such as network overload and radio-frequency interference. Moreover, the fact that access points are so easy to plug into a corporate network means that they can compromise network security, potentially exposing sensitive corporate data to hackers.

What many companies do not fully appreciate as they plan larger, more complex wireless networks is that WLAN access points and end-user devices require frequent attention. Initially, someone must configure each piece of equipment with identification information, radio settings and data-encryption keys, a process that can easily take 15-20 minutes or more for each device. Thereafter, access points periodically must be updated with new firmware (basic instructions programmed onto a memory chip)—sometimes just once a year, but often as frequently as once every two months. Security keys or access control lists must be changed periodically, the more frequently the better. End-user devices also require new drivers and firmware periodically, as well as new applications, antivirus updates, patches and other “fixes.”

Such management and maintenance are time-consuming even if the devices are all local, within a single building. When they are spread out around the country, it is often cost-prohibitive for IT managers to visit them all, and impractical or risky to have the work done by less-skilled people on-site. Even within central IT shops, many companies lack sufficient expertise to manage these needs efficiently and effectively. Taken together, these support requirements—for both initial deployment and ongoing operation—require time, money and people to execute. This can place significant and unexpected strains on IT budgets, and even delay rollouts or technology upgrades once the equipment is purchased.

In even a modest deployment, these management needs can easily require the full-time attention of one or more IT specialists; large deployments can require several. Estimating conservatively, this staffing requirement could amount to at least \$50,000 per person in salary alone, let alone the cost of travel to remote sites, or express-shipping malfunctioning devices back and forth for service and repair.

Clearly, manual administration is an expensive way to address the complexity of large WLANs and groups of WLANs distributed across large areas. What are needed are automated solutions that have two core capabilities. First, they should provide real-time visibility into the wireless network (or multiple distributed networks), displaying not only device-level information but network status and performance data. Second, these solutions should provide fine-grained control, from a central location, of all elements in the network, wherever they happen to be—in the same room or spread out around the globe.

In addition to visibility and control, a management tool should support equipment from as many vendors as possible. It should be easy to use, with a single, simple interface that doesn't require much training. At the same time, it should "understand" that different vendors' devices have different capabilities—in terms of alerts and notifications, for example—and allow administrators to take full advantage of them.

Multi-vendor WLANs are more than the exception than the rule, although they are common enough in settings such as universities, where multiple departments may have implemented WLANs independently, and in companies that have grown through acquisition. Some organizations will no doubt attempt to standardize, but so many factors work against standardization—including specialization for specific needs and requirements, new variants of the 802.11 standards, and mergers and acquisitions—that heterogeneous environments will remain common.

WLAN management software should also be flexible enough to support either central or distributed oversight, so that, for example, a district-level IT administrator could control only the WLANs within his district, while a corporate-level administrator would have control over multiple districts.

Finally, WLAN management solutions must plug into traditional network and systems management tools, which provide little visibility into wireless access points or end-user devices, and were not designed with mobility in mind. For example, traditional tools don't notice when a handheld device roams from one building to another on the WLAN and acquires a new IP address. They can't update the settings on an access point or the applications on a mobile access device. Notwithstanding these limitations, traditional network and systems management tools are not only common in enterprise networks but crucial to their operation, so WLAN management software must mesh easily with them through standard application programming interfaces.

As noted earlier, many of these management and maintenance functions can be performed manually, device by device, either hands-on or remotely via Telnet or a browser. But wireless devices are becoming so numerous, and the management demands are so frequent, that manual approaches can be extremely costly and inconvenient, to say nothing of error-prone. Tools that automate this management can not only improve the WLAN's performance, reliability and security, but they can dramatically reduce administrative overhead—thereby allowing the WLAN to deliver the benefits on which the investment was justified.

Section 2 Wavelink Solutions

Wavelink, one of the earliest companies to focus on WLAN management and a market leader with several thousand customers, reduces the cost of WLAN ownership by enabling fine-grained, remote 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. Wavelink also offers an Enterprise version of Mobile Manager, which integrates the two products to provide both access point and mobile device management. These products eliminate much of the time and expense of manually deploying and managing WLANs and therefore yield strong ROI for customers. In this section we discuss Wavelink's products and their functions.

Wavelink Mobile Manager

Mobile Manager provides visibility and control of access points from a wide range of vendors, including Cisco Systems, Symbol Technologies, Proxim, HP, Dell, and others. It unifies the management of these diverse products in a single interface, but doesn't "dumb them down"—because it supports most of the features and capabilities unique to each vendor's product. This capability simplifies management of heterogeneous WLANs, while still giving customers the flexibility to choose equipment based on price, features or application support. Plug-ins allow simple integration with major systems management systems such as Hewlett-Packard's OpenView and Computer Associates' UniCenter. Wavelink recently struck a strategic agreement with access-point maker Proxim, which holds about 30 percent of the enterprise market, in which Mobile Manager will become Proxim's default network management solution.

Mobile Manager simplifies both initial deployment and ongoing operation of WLANs. Initially, administrators can define profiles and settings and apply them to multiple access points simultaneously. Once the WLAN is operating, Mobile Manager senses when a new access point comes online and applies the proper settings automatically. It also checks each access point at user-defined intervals to make sure it remains within specifications and established policies. If it finds an abnormality, it can alert a network administrator and/or change the settings automatically.

When manufacturers release new firmware—which some do as often as every month or two—Mobile Manager can automatically install the new version, maintaining standardization across the network and eliminating the time and expense of manual updates. If the new firmware proves “buggy,” Mobile Manager can automatically roll each access point back to the previous version, again eliminating substantial time and cost.

Mobile Manager’s auto-detect feature enhances network security by detecting unauthorized or “rogue” access points and either shutting them down or applying pre-set profiles and settings so the access points function according to policy. These capabilities will be enhanced through a new relationship with access-point manufacturer D-Link, a major player in the residential market that is beginning to target small- and medium-sized businesses. In the deal, D-Link will add new functions to its firmware that turns each end-user device into a “probe” that scans the network and reports its findings to Mobile Manager, which in turn determines whether the activity is authorized. In addition to this specialized solution, Wavelink plans to enable other WLAN adapter cards to monitor wireless traffic for rogues.

Wavelink Avalanche

While access points are critical, end-user devices can be even more burdensome to manage. They are both more numerous and more diverse, spanning everything from standard laptops to PDAs to specialized devices equipped with magnetic-stripe readers and bar-code scanners. They are also mobile, which, as noted, introduces a range of management and security concerns. Moreover, end-user devices often include end-user applications that must be installed, maintained and upgraded, in addition to their firmware, radio and security settings. 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 network connection—the WLAN itself, a wired cradle or docking station, or a wide-area network, wired or wireless.

Avalanche currently can manage a variety of handheld devices running both Microsoft and Palm operating systems, including those from Symbol Technologies and Intermec, as well as the various Windows laptop platforms.

Mobile Manager and Avalanche provide significant benefits individually, but even more when used in tandem. For example, when an end-user reports poor performance, the cause might be a faulty access point or handheld device, or an unusually large number of users concentrated on one access point and overtaxing it. Separately, either Avalanche or Mobile Manager would provide relevant information, but only by analyzing data from both can an administrator precisely determine the cause. The two products also work together in security, coordinating the distribution and

updating of encryption keys on both access points and mobile devices (in addition to identifying rogue access points, as discussed earlier).

Section 3 **How WLAN Management Delivers ROI**

Now that we know how they work, let’s look at some examples of how these Wavelink products actually reduce WLAN management costs. Savings depend on several customer-specific variables, but fall into a handful of categories—costs associated with deploying and maintaining access points, end-user devices, security management, and business productivity.

First let’s consider the case of a small health-care provider with a hospital-based WLAN that includes 90 mobile devices and 75 access points. The company plans to install 50 more devices and 50 more access points over the coming year. (All of the customers mentioned in this section declined to be identified, citing competitive concerns.)

In addition to daily support and trouble-shooting, the company plans to upgrade the software and firmware on its mobile units three times each year, and assumes this would require 30 minutes per device. At a labor rate of \$30 an hour, upgrade costs would total about \$4,000 a year. Counting collection and distribution time, each device would be out of service for two hours. The company estimates the value of this “availability loss” at \$3,400 a year. These device-related costs would total \$7,400.

Looking next at access points, the customer estimates it would take about 60 minutes to install each new access point. Again using a labor cost of \$30 an hour, the total cost to install 50 new units would be about \$1,500. To upgrade software and firmware on 100 access points (assuming half the new ones won’t require upgrades), at a half-hour per device, would cost an additional \$4,500. Costs related to access points would total \$6,000.

The customer plans to update security-related settings (WEP keys, ESSID numbers, etc.) three times a year on each device and each access point, and estimates the chore would require an average of 30 minutes per

Figure 1 Savings Summary, Small Health-Care Provider

90 mobile devices, 125 access points (50 new), labor = \$30/hour	
Access point installation, upgrades	\$6,000
Mobile device upgrades	\$7,400
Security management (WEP, ESSID, etc.)	\$8,500
Productivity	\$5,600
Total savings & productivity gain	\$27,500

device. This would cost a total of about \$4,000 for all the mobile devices and \$4,500 for all access points, or a total of \$8,500.

Once acquired and deployed, the Wavelink products automate all of these tasks, reducing their costs to nearly zero, generating savings of \$22,700.

Finally, the customer estimated productivity lost in the event of an access point failure. For this category, it assumed 75 operational access points, with an average of one access point failure each year, and an estimated operational value of \$7,500 an hour. Without Mobile Manager, the company figured it would take 1.5 hours to detect, locate and replace or repair a failed access point, which worked out to an estimated annual loss in this category of about \$8,400. With Mobile Manager, it could address the failure in just 30 minutes, cutting the loss by two-thirds and saving an additional \$5,600.

In total, the health-care provider estimates Wavelink’s solutions will save a total of \$27,500 in the first year—and pay for themselves well before that year is over. The payback equation gets even better in subsequent years, as licensing fees disappear. Savings remain high, and are offset only by maintenance fees.

Next consider the case of another Wavelink customer, a large logistics company with WLANs deployed at multiple sites around the world.

Figure 2

Savings Summary, Large Logistics Company

2,500 mobile devices, 1,000 access points (250 new), labor = \$30-\$50/hour	
Access point installation, upgrades	\$28,100
Mobile device upgrades	\$236,600
Security management (WEP, ESSID, etc.)	\$1,080,000
Productivity	\$104,000
Total savings & productivity gain	\$1,448,700

The first category the company considered in calculating its return on investment in Wavelink solutions involves the 2,500 mobile end-user devices it has already deployed. It identified three sub-categories of savings: upgrade costs, shipping costs and lost productivity when devices are out of service.

The company assumed it would have to upgrade each device four times a year, and that each upgrade would take 10 minutes. It estimated its labor costs at \$30 an hour. On this basis, upgrades would cost \$50,000 a year. Shipping to and from a facility where the upgrade would be per-

formed would cost another \$10 per device, four times a year, for a total of \$100,000 a year. Assuming a three-day turnaround time for each upgrade, and a device cost of \$667 a year, the time value of out-of-service devices would be about \$61,600. The company also estimated about \$25,000 in additional overhead (besides labor). In total, it figured device-related costs would total about \$236,600 a year.

Next the company considered costs related to access points, of which it has already deployed about 1,000. It estimates it would have to upgrade them three times a year, at about 15 minutes per device. If labor again costs \$30 an hour, access point upgrades would cost a total of about \$22,500 a year. The company also estimated that about 10 percent of access points would fail at some point during the year and that each failure would take 30 minutes to repair or replace, at a labor rate of \$50 an hour (instead of \$30) because of the greater degree of technical knowledge required. This sub-category would total \$2,500.

Finally, the company estimates it will install 250 new access points a year, a process that would take 15 minutes per device done manually, at the higher labor rate of \$50 an hour—for a total cost of about \$3,100 a year. Total savings related to access points comes to \$28,100.

The largest category involved costs related to security management. The company assumed it would upgrade device identifiers and encryption keys four times a year on each access point and mobile device, and estimated its cost to do this manually at \$1,080,000.

Finally, the company considered the cost of productivity lost due to access-point malfunctions. It estimated a 10 percent annual failure rate, then assumed that with built-in redundancy, there was only a 1 percent risk that an access-point failure would cause the entire WLAN to fail. Using this conservative assumption, and applying various other internal metrics for the value of its operations, it calculated an annual productivity cost of \$104,000.

Across all four categories, the company estimated that Wavelink's solutions would save it \$1,448,700 a year, and pay for themselves in less than a year.

As a rule of thumb, Wavelink says, its solutions typically pay for themselves in the initial deployment of WLANs that include 100 or more access points and devices—their cost is equal to or less than what the customer would have paid to configure those access points manually. The payback is even greater if the customer's environment encompasses several WLANs distributed over multiple sites. In that case, because of higher travel costs, Wavelink estimates its solutions pay for themselves on initial deployment of just 50 access points and devices.

Section 4 Conclusions

This discussion has focused narrowly—and conservatively—on the cost savings and productivity gains that result from effective WLAN manage-

ment. However, these are by no means the only benefits to consider when weighing WLAN deployments.

As mentioned earlier, WLANs are increasingly popular because they enable cost-effective connections among people, applications and data that were not possible, or not cost-effective, in the past. For example, WLAN-based applications can enable fine-grained management of supply and distribution chains to improve their efficiency and reduce overhead. WLANs can also enable entirely new business processes. To cite but one example, hospitals are using WLAN-enabled point-of-care applications to reduce errors and improve overall patient care.

WLAN management solutions provide a variety of other benefits can be substantial but difficult to measure. For example, they can protect corporate data by preventing intrusion through rogue access points. They help control salary costs, by allowing IT staffs to manage larger networks without adding staff. And they can improve overall network management by integrating with customers' existing systems, such as OpenView and UniCenter. Fortunately, it isn't necessary to measure these benefits to justify investing in WLAN management solutions, which can quickly pay for themselves simply by minimizing time-consuming deployment and administrative chores.

Many companies are only now discovering the challenges that arise as WLANs grow in size, number and strategic importance. These challenges will only grow as more wireless networking standards emerge, and as companies seek to deploy performance-sensitive applications such as voice- and video-over-WLAN. Furthermore, end-user devices will become increasingly complex, supporting more powerful applications and becoming more specialized for specific job functions.

Clearly, WLAN management can't be ignored. Rather than tackle it manually, device by device, companies will find a much better solution in solutions such as those offered by Wavelink that provide continuous monitoring, address problems pro-actively and allow administrators to remotely manipulate multiple devices at once. We believe that companies considering deploying or expanding their use of WLANs should strongly consider such solutions.

Warren Wilson
wwilson@summitstrat.com