

WLANs: The Next-Generation Business Case A 3Com ROI Series Document

WHITE PAPER

CONTENTS

Real Savings Out of Thin Air	1
A Personal Trainer for Your Access Points	2
A Fit AP = a Fit Wallet	4
Better, Faster and Cheaper	4
Is that WLAN Secure?	5
Fit AP Architecture and Security.....	6
Not Your Father's Site Planning Process.....	7
Out with the Old, but Not the Good	9
<i>Improving Productivity... With a Smile.....</i>	9
<i>A Bridge Over High Trenching Costs</i>	11
<i>Turning Wired LAN's Inside Out</i>	14
Prime Time for a Change.....	16

Real Savings Out of Thin Air

As organizations often at the vanguard of science and technology, it's not surprising that the higher education community was one of the first to embrace Wireless Local Area Network (WLAN) technology. Not only did the original WLAN systems accommodate the mobile lifestyles of students and teachers, they also offered substantial cost savings to the budget-strapped educational institutions.

In 1997, for example, Hofstra University Law School spent \$50,000 installing 120 Ethernet access points. Four years later, it accommodated the same number of users on a new WLAN for about 25% the cost: \$12,000¹. Indeed, Hofstra wasn't the only educational institution to get the WLAN religion. The Campus Computing Project, an on-going study that tracks technology use in higher education, reported in 2003 that over 90% of public universities use some kind of wireless LAN, and more than 10% have campus-wide wireless access².

Public schools are similarly availing themselves of wireless LAN benefits, with nearly two-thirds of school districts employing wireless LAN technology today. Further, that same study reported that primary and secondary education spending on WLANs is increasing at about 60% annually (\$500M invested in 2001-2002³). A recent WLAN study shed some light on why WLANs have been particularly popular in Primary/Secondary schools and Universities:

"With wireless LANs they [schools] were able to save money by buying fewer computers. The solutions ranged from using cart-mounted computers wirelessly hooked to the wireless LAN. The carts could be moved to the classrooms where they were

needed. The schools saved money by buying fewer computers as well as wiring to a central hub. The savings can be attributed to the utilization of cart-mounted computers and fewer network drops as a result of the wireless LAN. With carts, fewer rooms would have been required to be networked and populated with computers."⁴

The use of WLAN technology in education is anything but surprising: college tuition costs continue to rise between 6% and 10% annually, more than double or triple the rate of general inflation⁵, while public school budgets are constantly under assault from weary taxpayers, even in the most affluent school districts. At first glance, the picture is somewhat bleak, but there is a silver lining in that cloud: educational and other institutions can continue to go to the WLAN well for additional cost savings.

Just because an institution has deployed a WLAN does not mean it has exhausted all opportunities for cost savings from that technology. In fact, next generation WLAN architectures are not only providing customers with much improved capabilities, they're also yielding much improved cost savings over the initial, rather clumsy, first generation LANs.

San Antonio Community Hospital (SACH) understands this as well as any organization. The 350-bed healthcare facility in California recently upgraded its first-generation wireless system with a state-of-the-art WLAN solution. Irv Hoff, Converged Networks Manager at SACH, and Jan Snyder, Senior Communications Consultant at the facility, estimate that the updated WLAN system will save the hospital 70%-90% over the previous system in labor, operations, and support costs. "Total cost of ownership was the clincher," said Hoff."⁶

1 http://www.mobileinfo.com/Wireless_LANs/business_case.htm

2 <http://www.wifizonenews.com/publications/page207-594084.asp>

3 "Wireless vs. Hard-Wired Network Use in Education," Dr. Sylvia Charp, The Journal., <http://www.thejournal.com/magazine/vault/A4212.cfm>

4 "Wireless LAN ROI," <http://www.wlana.org/learn/roi.htm>

5 "Report: College Costs Soar Again," CNN.com. July 9, 2004, <http://www.cnn.com/2004/EDUCATION/07/09/college.costs.ap/>

6 http://www.trapezenetworks.com/solutions/vertical/healthcare/casestudy/SACH/SACH_casestudy3.asp

Next generation WLAN systems are clearly ringing the bugs (and excessive architecture costs) out of the first WLAN systems. Let's take a closer look at what these new designs look like, and how they've improved considerably on a very good idea.

A Personal Trainer for Your Access Points

The vast improvements in WLAN design and architecture have been the primary result of a new concept of access point (AP) functionality. In the parlance of the industry, the choices are "Fat" APs, "Thin" APs, and "Fit" APs.

The primary change in design convention is the best place to locate wireless network control (for example, routing and network management), and therefore what functions to maintain on the AP. The newest and best-available architectures pull the best from both the Fat and Thin AP strategies, centralizing management functions, but keeping the most time-sensitive processing at the "edge" of the network, on the AP.

First, let's look at the major functions of APs:

- Signal reception, amplification, and transmission
- Ethernet interfacing
- Authentication
- IEEE 802.1x processing
- Encryption
- SSID⁷ processing
- Signal routing decision-making processing

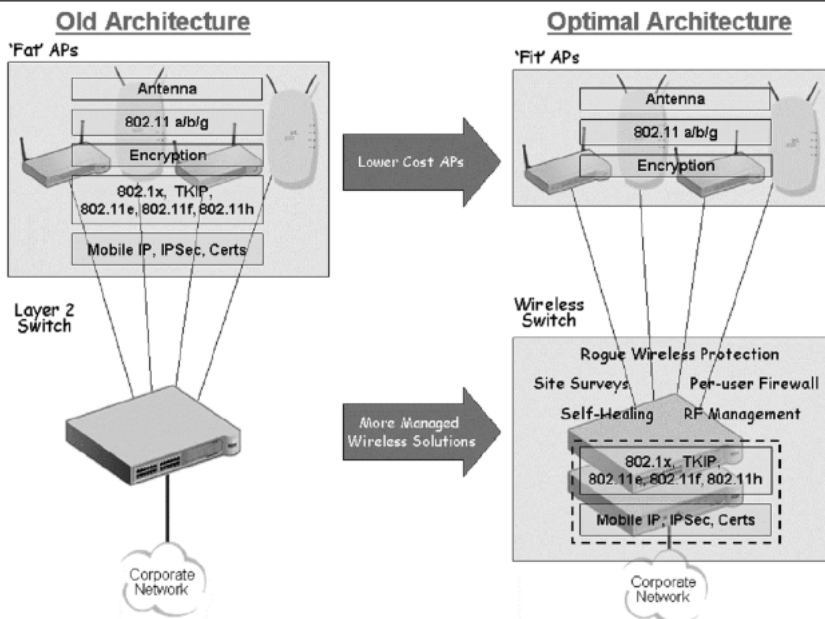
As might be expected, Fat APs perform the most functions, often including encryption, SSID, and signal routing for AP-to-AP hand-offs. Thin APs may be so thin that they are only a transmitter/receiver with an Ethernet interface, too dumb to accept commands or relay information. Fit APs, conversely, attempt to perform only the functions needed for optimum performance and financial value, while moving all other WLAN functions to the wireless switch. For example, Fit APs retain encryption functions (to provide better security and decrease latency), but move other functions (like AP routing and handoffs) to the switch.

Most wireless networks today use "Fat" access points (APs). This means that each individual AP includes support for one or more wireless radios (IEEE 802.11 a/b/g), associated antennas, authentication software, encryption hardware and software, and a host of complicated wireless security features. As more WLAN standards and security features are added to an AP, the memory, processing, and power requirements increase. This makes each AP fatter and more expensive. In addition, managing all of these AP features in a large wireless network can become time consuming and complicated.

A WLAN architecture with "Fit" APs, as illustrated in Figure 1, offers a compromise solution that optimizes hardware and maintenance costs by decreasing the amount of software in each individual AP and by centralizing AP functions into a wireless switch. At the same time, performance and efficiency increase.

7 SSID - Short for service set identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network.

FIGURE 1: WLAN Architecture Comparison



For example, fat APs have to “talk among themselves” to determine how to handle changes to the network, such as which channel each should use when a new device comes online or what to do if an individual’s signal reaches two different APs. To talk among themselves, each AP has to support various communication and security protocols, such as IEEE 802.1X, PKIP, IPsec, and IAPP.

Alternatively, if these management and security functions are moved to a wireless switch, they are no longer needed on the individual APs. Instead, the switch can monitor and manage the activity across all of the APs, which not only lowers the cost of the APs, but also increases the wireless network’s speed, as one switch is handling what was previously negotiated across multiple APs. Instead of many fat APs, your wireless network now consists of many “Fit” APs and a wireless switch.

In addition, due to its centralized nature, a wireless switch can perform additional functions that Fat APs find difficult to do without getting fatter:

- Rogue protection: centralized switching is much more effective at countering a rogue threat (an unauthorized access point impersonating a legitimate AP) than a Fat AP approach, an issue that is discussed in more detail in the Security section of this paper below.
- Self-healing: there are currently three IEEE 802.11 channels in the 2.4 GHz spectrum. Overlapping APs cannot use the same

channel and maintain clear signals. With Fat APs, if a new AP joins the network, the APs all have to renegotiate which channel each will use. With a wireless switch, if the switch sees a new device, it first alerts an IT administrator to verify it is a legitimate device. Once verified, the switch allows the new AP into the network and automatically reassigns each AP’s channel.

- Site survey: today, site surveys are a manual process. A person wanders around a building, testing signal strength in different locations (called “sniffing”) to determine where to place the APs and what channels to use to get the best coverage. Then, he goes back to the management software and enters the configuration. If the environment changes, he must do it all again.

A wireless switch eliminates the need for this type of site survey. With a wireless switch, you can enter the building specifications and your performance requirements (throughput, speed, etc.) into software that comes with the switch. If APs are already installed, the switch will use them as sniffers to determine existing coverage. The software then runs the calculations and shows you where to put the APs. It can even provide a printable work plan that you can give to your installer. We’ll discuss the financial impact of this capability on WLAN deployment later in this paper.

A Fit AP = a Fit Wallet

How do the benefits of a Fit AP architecture translate into dollars and cents? That question was answered comprehensively by the people at Momenta Research in their April 2003 report “Wireless LAN Total Cost of Ownership Benchmark Study.”⁸ In that study, Momenta analyzed capital, support, redundancy, roaming support and scaling costs for 3 WLAN architectures: Thin AP-based, Fat AP-based, and Fit (or “Integrated” in the parlance of Momenta).

Table 1 summarizes the results of this TCO study, clearly demonstrating the considerable cost advantages provided by a Fit AP architecture under all deployment scenarios considered. Note that the Momenta study provided a range of potential TCO savings for each scenario (minimum and maximum). To emphasize the conservative nature of this discussion, we’ve chosen to present only the minimum potential savings in Table 1.

TABLE 1: TCO Comparison of Various WLAN Architectures

Number of WLAN Users (TCO Analysis Timeframe)	Minimum TCO Savings vs. Thin AP (IEEE 802.11a)	Minimum TCO Savings vs. Fat AP (IEEE 802.11a)	Minimum TCO Savings vs. Thin AP (IEEE 802.11b)	Minimum TCO Savings vs. Fat AP (IEEE 802.11b)
450 Users (1 year)	\$108,390	\$61,230	\$3,353	\$6,235
450 Users (3 years)	\$94,780	\$47,454	\$8,193	\$17,895
1,500 Users (1 year)	\$376,138	\$217,542	\$50,124	\$51,906
1,500 Users (3 years)	\$393,628	\$263,632	\$73,334	\$94,916
6,000 Users (1 year)	\$1,525,545	\$917,448	\$273,615	\$177,970
6,000 Users (3 years)	\$1,653,272	\$1,177,614	\$379,741	\$317,897

In addition, the Momenta report broke out the costs for providing WLAN redundancy, a critical requirement in environments such as hospitals. The TCO analysis showed that the cost advantage of a Fit AP approach to WLAN deployment was particularly prominent when the provision of redundancy was required. In short, and as illustrated in Table 2, it would

be roughly twice expensive to provide WLAN redundancy using either a Fat or Thin AP approach vs. a Fit AP-based architecture for an IEEE 802.11a, 450 user deployment over a one-year period.

TABLE 2: Redundancy Comparison of Various WLAN Architectures (450 users, 1 year TCO, IEEE 802.11a)

Costs	Minimum Cost (Thin AP)	Maximum Cost (Thin AP)	Minimum Cost (Fat AP)	Maximum Cost (Fat AP)	Minimum Cost (Fit AP)	Maximum Cost (Fit AP)
Capital	\$83,740	\$83,740	\$58,500	\$58,500	\$36,463	\$36,463
Support	\$13,102	\$17,443	\$15,612	\$20,604	\$3,101	\$4,082
Total	\$96,842	\$101,183	\$74,112	\$79,104	\$39,564	\$40,545

Better, Faster and Cheaper

Tables 1 and 2 unambiguously illustrate that a Fit AP architecture is the most cost-effective way to deploy a WLAN. What the table does not show, however, are some of the performance and functional benefits the Fit AP design provides that the Fat and Thin AP

approaches to WLAN design don’t. The first is the ability to seamlessly provide voice-over-IP (VoIP) benefits to your organization. Wireless VoIP benefits—financial and otherwise—are numerous and substantial, and are discussed in detail in other 3Com white papers.⁹

⁸ TCO summary data from that report can be obtained online at: <http://www.trapezenetworks.com/technology/market/TCO/TCO.pdf>

⁹ One quick example of VoIP-based productivity increases was provided by San Antonio Community Hospital: “With the current “fixed” desk phone and paging system, physicians, nurses and caseworkers lose valuable time because of missed calls and waiting for callbacks. Quicker access to physicians will allow nurses to move patients from critical care to ambulatory care in anticipation of discharge, freeing up needed beds for incoming patients from ER. With improved efficiencies, the hospital anticipates that patient-to-nurse ratios will increase 25%-30%.” See http://www.trapezenetworks.com/solutions/vertical/healthcare/casestudy/SACH/SACH_casestudy4.asp

In the context of our Fit AP conversation, it is important to recognize that VoIP deployment is much more effective, provides higher performance, and is easier to accomplish with a Fit AP architecture.

To provide VoIP over WLAN with acceptable performance, “fast-roaming” capability must be inherent in the system. That is, the AP to AP hand-off of a user (or more specifically, a phone call) must be seamless, and very fast, otherwise calls will be dropped.¹⁰

As mentioned previously, in a Fat AP architecture, the APs must negotiate with each other individually, with limited centralized control or input, to hand calls from one to another. This takes time, and extends the latency of data transfers, something very critical when that data is voice and obviously time-critical.

Meanwhile, the completely centralized functionality of a thin AP architecture requires additional time for non-AP encryption and SSID functions, slowing the exchange of users from AP to AP. Fit AP WLANs optimize the locations of these functions, minimizing data transfer latency, and thereby maximizing the performance of VoIP systems.

The second unique benefit of a Fit AP approach to WLAN design is an issue that has impeded the deployment of WLAN systems since their introduction: security.

Is that WLAN Secure?

Maybe it's Hollywood's fault. The obligatory scene in any cloak-and-dagger movie has the spy on his cell phone with the predictable instructions coming from headquarters on the other end of the phone: “Get to a landline and call me back.”; the message: mobile phones are just too easily compromised.

Hollywood or no Hollywood, the truth is that many businesses have serious concerns about wireless security and are therefore cautious about their deployment. Admittedly, first generation wireless products had security features that, as it turned out, were

fairly easily hacked. Since then, the design and architecture of WLANs, and therefore their security, have improved considerably, but early impressions still linger.

In fact, there's some evidence that the issue of security has increased as a WLAN deployment obstacle even as WLANs have grown in number. Indeed, a 2001 NOP World “Wireless LAN Benefit Study placed security as the 4th most popular answer to the “challenges of wireless LAN deployment” question (14%). That same study, updated 2 years later in 2003, reported that security was now the number one answer to that question with a respondent percentage in the mid 30s, double the 14% figure in 2001.¹¹

Indeed, the concerns of potential WLAN users are based on real threats. In the first half of 2003, organizations experienced an average of 38 attacks on their systems (wired and wireless LANs) per week.¹² Of course, few of these attacks are successful, but some are.

The 2004 CSI/FBI Computer Crime and Security Survey reports that 18% of the respondents to the survey experienced more than six successful outside attacks in the previous 12 months, and an additional 52% reported at least one or more successful attacks.¹³ That same survey reported the cost of successful virus attacks (as calculated by the survey respondents) to be over \$204,000 per company per year, not including the cost of service denial, theft, fraud and a number of other cost categories.

Similarly, a KPMG study in the UK put the cost of a single security breach at about \$110,000,¹⁴ while the UK's Corporate IT forum estimates each security incident to cost nearly \$175,000.¹⁵ (Some estimates of per incident security breaches appear exaggerated: a poll in the 2002 timeframe placed the average security breach cost at \$2,000,000 per incident.)¹⁶

Using the lowest of these estimates, Figure 2 illustrates the savings a more effective security system can provide by foiling attacks that may have otherwise penetrated the organization.

10 Fast roaming is also beneficial for data-only WLAN usage. A system that does not quickly hand-off users from AP to AP as they roam may drop them from the network, forcing them to re-register on the WLAN and re-authenticate.

11 “2003 Wireless LAN Benefits Study,” And “2001 Wireless LAN Benefits Study,” NOP World Technology

12 “Worms Spread Faster, Blended Threats Grow,” John Ledyden, October 1, 2003, The Register. http://www.theregister.co.uk/2003/10/01/worms_spread_faster_blended_threats/

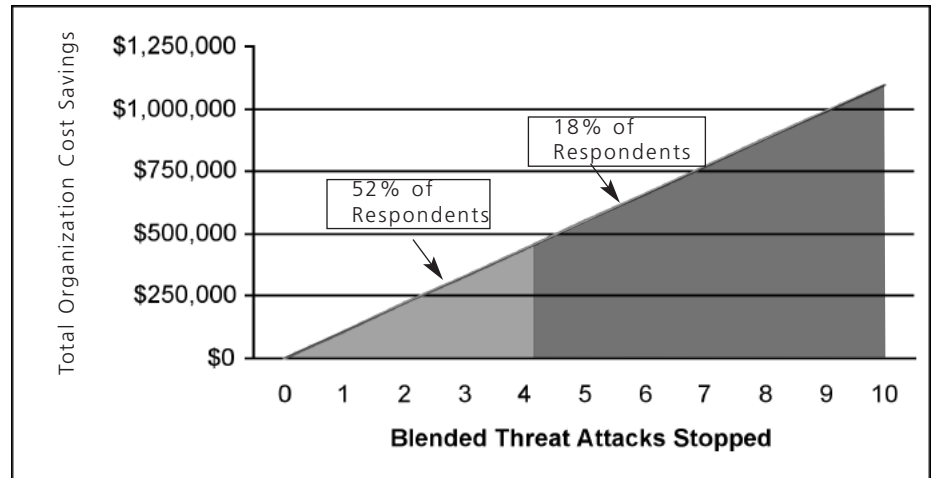
13 2004 CSI/FBI Computer Crime and Security Survey, page 8

14 “Cost of Each Security Breach – £77,000. IT Departments Struggling to Keep Up,” Andy McCue, vnunet.com, March 18, 2002. <http://www.networkitweek.co.uk/news/1130168>

15 “Can ROI be Measured for Security Implementations?” Fran Howarth, August 10, 2004 <http://www.it-director.com/article.php?articleid=12138>

16 “New Legislation Placing Increased Strain on Enterprise Security Programs,” December 18, 2002. http://www.systems-world.de/id/8319/CMEntries_ID/8268

FIGURE 2: Annual Cost Savings Resulting From Improved Security



Fit AP Architecture and Security

The two most common security problems in WLAN systems—rogues, or devices (often a laptop) posing as APs on your network, and unauthorized people connecting to the network¹⁷—can be more effectively controlled in a WLAN with Fit AP architecture.

The key to the security effectiveness of WLAN designs in today’s generation systems is centralized control, and optimizing the location of security functions. In 3Com’s system for example, the centralized switching architecture (WLAN Switch Manager Software) enables critical housekeeping functions that optimizes the performance and reliability of the WLAN on a day-to-day basis; for example:

- Coverage/Capacity “wizard” that defines geographic coverage and the number of users and desired bandwidth
- Centralized event viewer
- Unified management of images and configurations
- Configuration versioning:
 - Centralized upgrades and downgrades
 - Synchronize and rollback capabilities

That same centralized Switch Manager system is also integral to the optimization of security, particularly rogue detection. The Switch Manager, with its holistic view of the system, is perfectly positioned to:

- Detect the rogue
- Log the rogue for corrective action

- Manage & control the acceptable frequencies:
 - Reassign channels around the rogue to keep your network up and running
 - Detect other RF interference sources (microwave oven, cordless phones)

In contrast, Fat APs can compare their data to detect a rogue, but aside from detecting, they can’t take action to address the intruder. Since the 3Com Switch Manager monitors traffic across the network, it can see that an AP isn’t sending any traffic through the switch and therefore conclude it’s a rogue. Once detected, the switch can shut down the rogue’s port and prevent users from associating with it.

To prevent unauthorized access to the network, the second primary threat to WLAN security, the centralized switching architecture can be further utilized. By leveraging a pre-defined list of authenticated users (the “Active Directory in the parlance of the 3Com Switch Manager), the centralized WLAN switch can control who can and cannot access the network from the start. Further, multiple switches in the same system automatically synchronize with one another, so as new users are added, the process of Active Directory updating is automated.

Not all security functionality is accomplished by the centralized switch, however. To minimize the latency of the overall system (so as to accommodate real-time VoIP applications, for example), encryption is accomplished at the AP, yielding the primary distinction between a Fit AP and a Thin AP, which acts largely as a transmitter/receiver with little or no substantive processing capability.

¹⁷ When legitimate users associate with these rogues, or fake APs, it captures their information and then disassociates them from your network, taking the user information with it; unauthorized people connecting to the network demonstrates a lack of effective authentication.

Finally, not just any encryption is incorporated into the latest WLAN systems. Today's designs employ AES¹⁸ encryption, the most robust technology currently available to encrypt wireless data. Although a technical description of AES and its resulting efficacy is beyond the scope of this paper, the reader should note that AES technology was chosen by the US Government as the standard for the protection of secret information, through the "Top Secret" information level, quite a remarkable endorsement.

The combination of these design features mean that the newest WLAN architectures can now decrease the probability that one or more of those 38 attacks per week will be successful, and companies can realize the security cost savings illustrated in Figure 2.

Not Your Father's Site Planning Process

One of the biggest challenges in deploying a WLAN is also the first: determining how many APs will be required, and exactly where to put them. The answers to those questions depend on a host of factors including the size and layout of the building/campus, type of construction, number of WLAN users and their individual bandwidth requirements, among others.

The traditional approach to answering these questions is to conduct an RF site survey and WLAN layout. As discussed briefly above, the process includes testing various AP locations for interference, walking the site with equipment to detect various signal strengths, and a good deal of trial-and-error.

The good news for those considering new WLAN deployments is that this kind of approach to WLAN AP placement is now akin to "horse-and-buggy thinking."

The newest WLAN systems based on centralized switches and control include highly capable automated site planning software that takes the manual process and the associated "art" out of the AP location business.

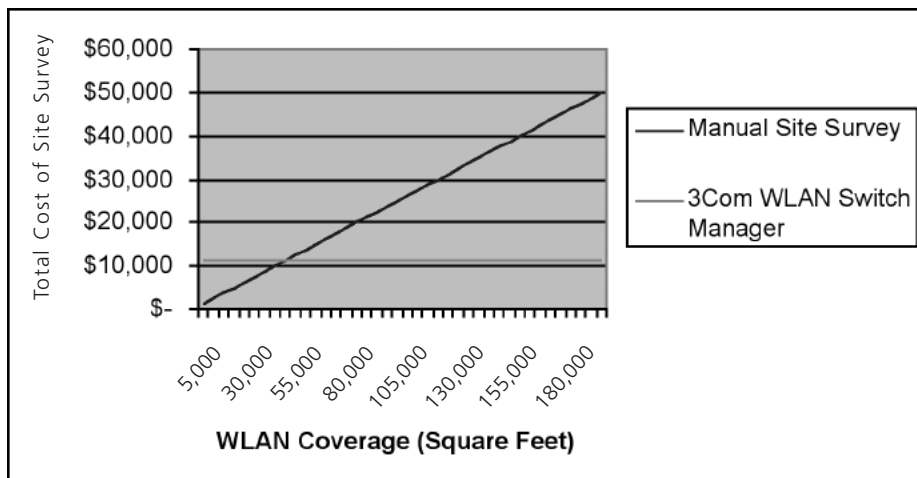
A perfect example of this new technology is 3Com's Wireless LAN Switch Manager. Although the Switch Manager provides critical post-deployment WLAN management functions, one its most valuable capabilities is the development of automated site plans.

The Switch Manager software simply requires AutoCad floor plans and a few other pieces of information as its primary inputs, and the software then generates a site plan indicating the number and location of required APs, saving substantial time and money. In fact, one estimate puts the cost to develop WLAN site surveys the old-fashioned way at \$5,000 per 20,000 square feet of WLAN coverage¹⁹.

Figure 3 uses that figure to provide a visual comparison of the costs associated with both methods of site survey completion.

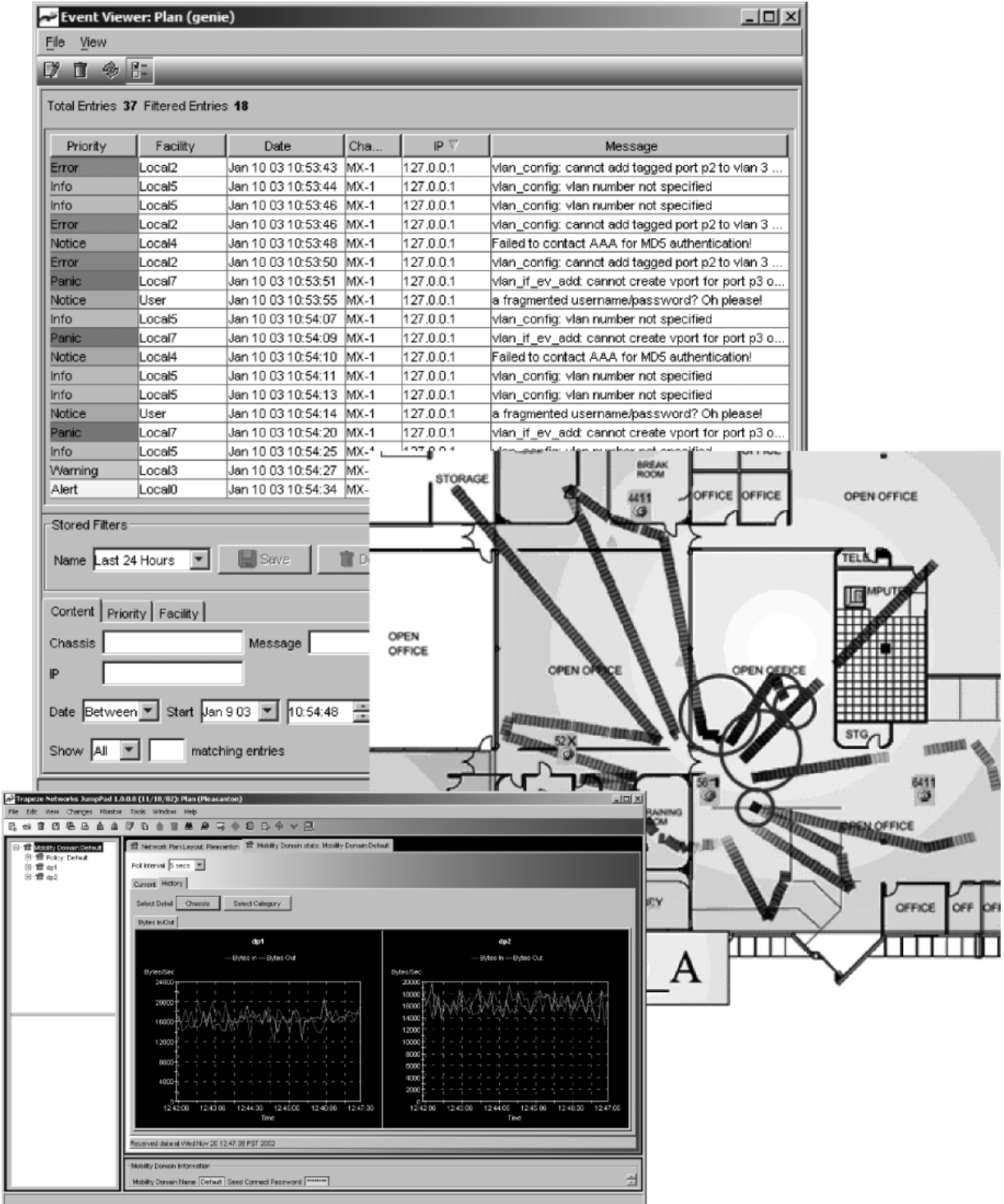
Figure 4 shows a sample site layout using the 3Com Wireless LAN Switch Manager software.

FIGURE 3: Comparison of Automated vs. Manual Site Survey Costs



18 Advanced Encryption Standard (AES). The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

FIGURE 4: Site Layout with the 3Com Wireless LAN Switch Manager



The total cost for 3Com's Wireless LAN Switch Manager includes the price for a starter kit (\$7,500) which includes the site planning software, and an additional \$4,000 for a \$100/hour professional to use the 3Com's Wireless LAN Switch Manager software to develop the site survey. As shown, especially for larger deployments, the automated Switch Manager approach is far superior, and this analysis ignores the post-deployment WLAN management functions included in the Switch Manager package that provide an on-going return on the investment.

Without question, the benefits of an automated site survey system were clearly evident to the previously-introduced San Antonio Community Hospital. When upgrading their first-generation system, the automated site survey system was used to lay out the AP grid. The reduced expense associated with the site planning software contributed a non-trivial portion of the substantial overall cost savings. When briefed about the site planning software, Irv Hoff, a manager at the facility, responded "this is too good to be true." However, after using it to plan and deploy his test system, and then San Antonio's production network in the ER, Hoff said, "One by one, we've confirmed every promise—it really works."²⁰

Out with the Old, but Not the Good

The best news about the next-generation WLAN technology discussed in detail previously is that the same benefits offered initially by WLAN systems are preserved by the newest designs:

- Improved employee productivity
- Substantially reduced building-to-building LAN bridging costs
- New LAN installation cost savings in existing buildings, particularly older ones

Each of these critical WLAN benefits is discussed in detail in the following sections.

Improving Productivity...With a Smile

In Germany this summer, managers at Siemens' Bocholt plant threatened to move their plant to Hungary to force their employees to work an additional 5 hours per week (from 35 hours to 40)²¹. Similarly, workers at a Bosch plant in France reluctantly agreed to work an additional hour per week (raising their weekly total to 36 hours) after their company threatened to move to the Czech Republic, and the European press predicts more such labor/management battles in the coming quarters²².

It would be fair to assume that most managers would like their employees to work more hours, but legal and practical restrictions render that wish an unrealistic goal. But wouldn't it be nice if employees not only worked an additional hour or more per day, but were happy to do so?

Believe it or not, wireless technology might just be able to make that utopia a reality for businesses, educational institutions, and healthcare facilities. Users of WLANs report, for example, the ability to answer email in a conference room while awaiting the start of a meeting, the ability to work from home while connected, the ability to quickly access files in a group work setting without having to walk back to their office to get it, or the ability to quickly access a website (e.g. a competitor's) during a strategy discussion.

All these seemingly small increases in work time add up to real productivity increases, and real dollars for the companies and institutions that employ WLANs.

Indeed, back in the fall of 2001, a study developed by market research firm NOP World reported WLAN technology enabled employees of surveyed companies to work an additional 70 minutes per day, while 87% of those same employees believed that the wireless LAN "improves their quality of life"²³. An updated, November 2003 version of that same study not only validated the 2001 findings, but showed an increase in the averaged daily work increase from 70 minutes per employee to 90 minutes²⁴.

20 http://www.trapezenetworks.com/solutions/vertical/healthcare/casestudy/SACH/SACH_casestudy3.asp

21 "Wake-Up Call for the 35-Hour Workers," Kate Connolly, NEWS.telegraph September 7, 2004. http://news.telegraph.co.uk/news/main.jhtml;sessionid=KOUTQGJ4LM1QFIQMFCM54AVCBQYJVC?xml=/news/2004/07/09/awork09.xml&secureRefresh=true&_requestid=74229

22 "Personal view: Work-life activists haven't put the long hours in on their homework," Ruth Lea, NEWS.telegraph. August 23, 2004. <http://news.telegraph.co.uk/money/main.jhtml?xml=/money/2004/08/23/ccpers23.xml&sSheet=/opinion/2004/08/23/ixopright.html>

23 "Wireless LAN Benefits Study," Fall 2001, NOP World http://www.intel.com/business/bss/infrastructure/wireless/roi/productivity_studies_cisco.pdf

24 "2003 Wireless LAN Benefits Study," November 2003. NOP World. http://www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf91f.pdf

Further, an April 2004 white paper developed by a completely different organization (MetaGroup) drew strikingly similar results, reporting that employees using laptops with wireless LAN connections averaged an additional six hours per week per employee when compared to those tethered to

conventional wired laptops, while over 50% of desktop users surveyed felt their job satisfaction would improve by “going mobile.” Table 3 presents the results of additional WLAN productivity studies showing results consistent with those discussed here.

TABLE 3: WLAN Productivity Study Summaries

Study	WLAN Productivity Increase Reported
Fall 2001NOP	70 minutes per day per employee
November 2003 NOP	90 minutes per day per employee
April 2004 MetaGroup	72 minutes per day per employee
August 2003 AllNet White Paper (quoting Sage)	96 minutes per day time savings per employee
August 2003 AllNet White Paper (quoting Mobileinfo.com)	15 to 30 minutes per day per employee

The conventional interpretation of improved productivity figures (or additional hours worked) suggests a simple multiplication of fully-loaded employee salaries with the additional time worked to generate the cost savings to the organization. The real world, however, doesn't work that way.

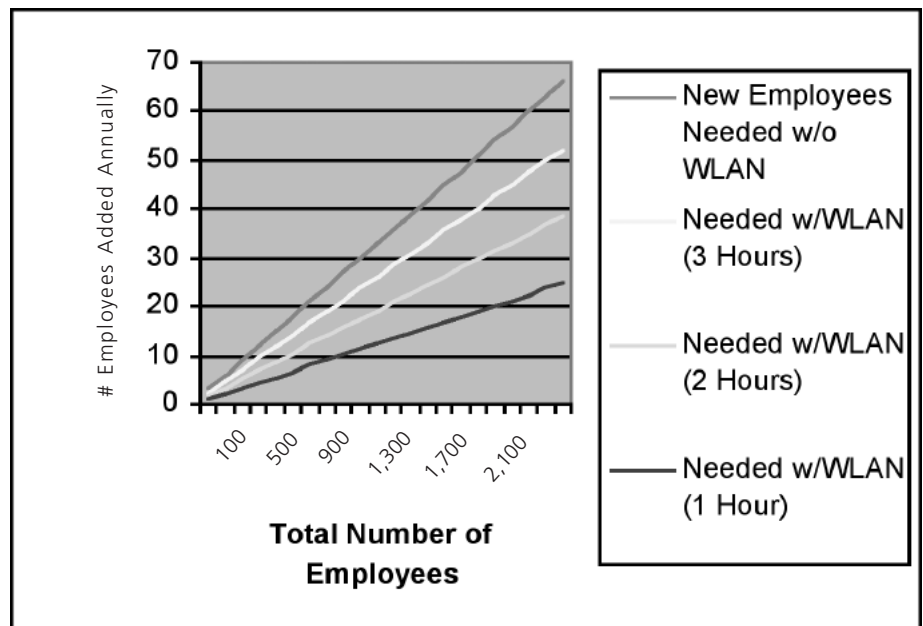
Especially in the case of a knowledge worker (as opposed to a factory or assembly worker), an additional 5 or 6 hours of work per week won't directly impact the company's bottom line. Their salary will remain the same; their work accuracy or quality may improve, but

the direct cost benefit will be much more nebulous. The cost savings will be realized when less people will be required to do the same amount of work.

This may result in better corporate efficiencies in the event of layoffs or downsizing, but a more optimistic analysis assumes the organization will grow, and improvements in per employee productivity will translate into fewer numbers of required new-hires.

Figure 5 illustrates this impact on long-term organizational growth and associated costs.

FIGURE 5: Potential New Hire Savings w/WLAN Deployment (Assumptions: 3% Company Growth; 25% WLAN Deployment)

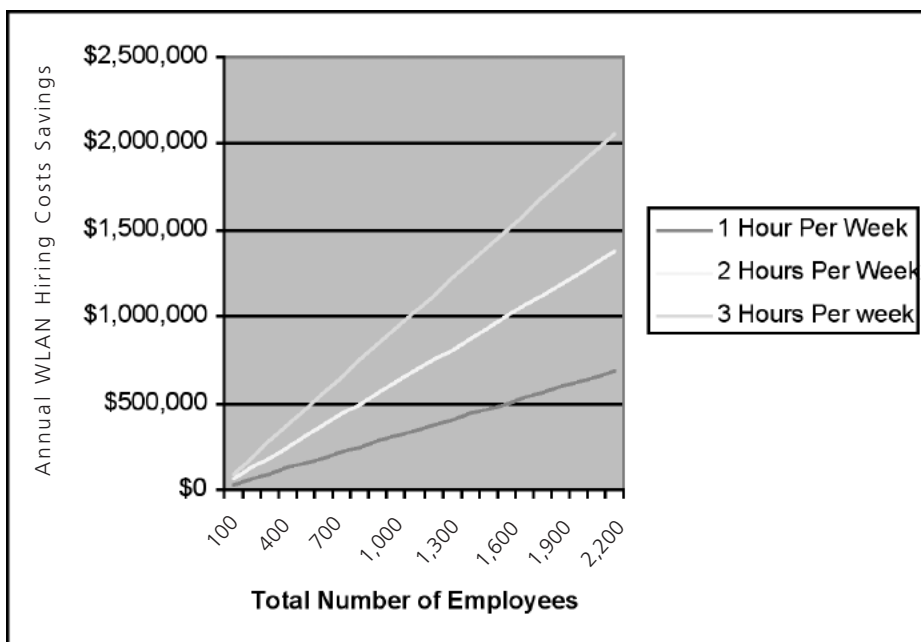


As shown, additional productivity can help absorb the increasing workload of a company growing at the approximate rate of national GDP expansion (assumed to be 3% in this analysis). The analysis assumes productivity growth to be less than that predicted by the studies summarized in Table 3 above (to enhance the conservatism of the analysis); results are shown for assumptions of 1-hour-

per-week additional work time, 2 hours, and 3 hours.

Figure 6 below financially quantifies this reduction in employee requirements, using the same assumptions as those employed in figure 5, but adding the average annual cost of a new employee at \$50,000.

FIGURE 6: Annual WLAN New Hire Cost Savings
 (Assumptions: 3% Annual Growth; 25% WLAN Deployment; Annual Cost of New Employee \$50,000)



In addition to productivity increases, mobile workers report improvements in accuracy, co-worker collaboration, and general morale as a result of improved work hours flexibility, and additional time spent with family. Clearly, all such benefits are real, substantial, and important to any organization. But the opposite side of the argument is that some employees may use the extra connection time to check their stock portfolios, the score of the ballgame, the latest update on the hot news story of the day, or even their daughter's soccer team statistics.

Thus, the actual cost benefit to the organization can be difficult to measure or predict in hard dollars, and the same is true for benefits like improved morale, flexibility, and even accuracy to some extent. We know they're real, but they can be very difficult to tag with a dollar figure.

Despite this, most WLAN studies agree that the positive financial impact of mobility is considerable, a finding epitomized by one WLAN survey concluding that "92% of respondents interviewed believe there is a definite economic and business benefit after installation."²⁶

In some industries, the productivity gains are more pronounced than others. That same report noted that in healthcare particularly: "The wireless LAN has shown to meet the technology and organizational needs of healthcare companies today by decreasing the length of hospital stay, speeding diagnostic and case analysis time turnaround, reducing hospital labor, procedural costs, documentation, and scheduling time."²⁷

26 "Wireless LAN ROI," <http://www.wlana.org/learn/roi.htm>

27 Ibid.

In addition to the San Antonio Community Hospital case study previously introduced, a recent survey of nurses at a European hospital further clarified the potential impact of WLAN systems on the productivity of healthcare workers. The results of that survey showed:

- Nurses spent an average of 6 minutes walking to a phone, paging other clinicians and specialists, and waiting for a response. They reported the frequency of this activity at approximately 5 times per shift. (Total: 30 minutes per shift)
- Nurses also spent approximately 5 minutes walking to the appropriate location to complete the process of ordering food, medicine or devices for patients. They found themselves accomplishing this about 10 times during a typical shift. (Total: 50 minutes per shift)

A WLAN with VoIP capability can substantially reduce this unproductive “walking” time by enabling nurses or clinicians to place orders in real time, or speak with their colleagues quickly without cumbersome paging systems. Although unproductive activities like those listed above cannot be completely eliminated, a reduction in the unproductive time devoted to just the two nursing activities mentioned here of just 25% will yield a WLAN payback period of approximately 6 months²⁸.

A Bridge Over High Trenching Costs

The good news for ROI-minded CIOs is that wireless LANs offer significant, and very quantifiable “hard” cost savings as well. One classic example is building-to-building bridging, or when an organization (business campus, school, university, hospital) expands its operation from one building to another, and wishes to extend its LAN to accommodate the new employees in the new building.

When confronted with this circumstance, IT managers traditionally chose from two options: 1) running cable to the new building, or 2) acquiring a separate T1/E1²⁹ line into the new building.

Running Cable to a New Building

This analysis will assume that the equipment on either end of the connection will remain the same for either bridging method. That is, the LAN architecture may call for a router on either or both ends, but that same router would be required irrespective of the bridging technique used. The second assumption employed in the analysis is that the bridging distance is short enough (i.e. campus environment) to exclude the requirement for fiber cable amplifiers, signal reshapers, and signal re-timers. Such optical amplification and signal conditioning equipment is required when tens of miles are being traversed³⁰, distances beyond the realm of a typical campus environment.

Thus, the comparison in this analysis focuses on the cost of a WLAN bridge with the cost of laying an optical fiber conduit between the buildings. As the cost for optical fiber trenching and installation varies by terrain, locality, and method, several estimates were gathered from different sources and are presented in Table 4. (As the estimates from multiple sources vary between \$2.00 and \$100 per foot, this analysis will assume conservative figures of \$3.00, \$5.00, and \$7.00 as indicated in figure 7.) Further, the cost of a WLAN bridge in this analysis was assumed to be approximately \$2,500, based on the use of 3Com’s Outdoor WLAN Bridge product, retailing for about \$1,000 per box (we’ve included an additional \$500 for incidental charges).

²⁸ Please contact your 3Com account representative for an ROI analysis of your specific circumstances, or the details of the analysis presented here.

²⁹ T1 lines offer a total data rate of 1.544 Mbps. E1, used predominantly in Europe provides 2.048 Mbps.

³⁰ An October 2003 Cisco “DWDM Networking Primer” presentation implied that a distance of 40 Km was traversable before optical signal conditioning was required. http://www.oar.net/presentations/cisco_systems_dwdm_primer_oct03.ppt

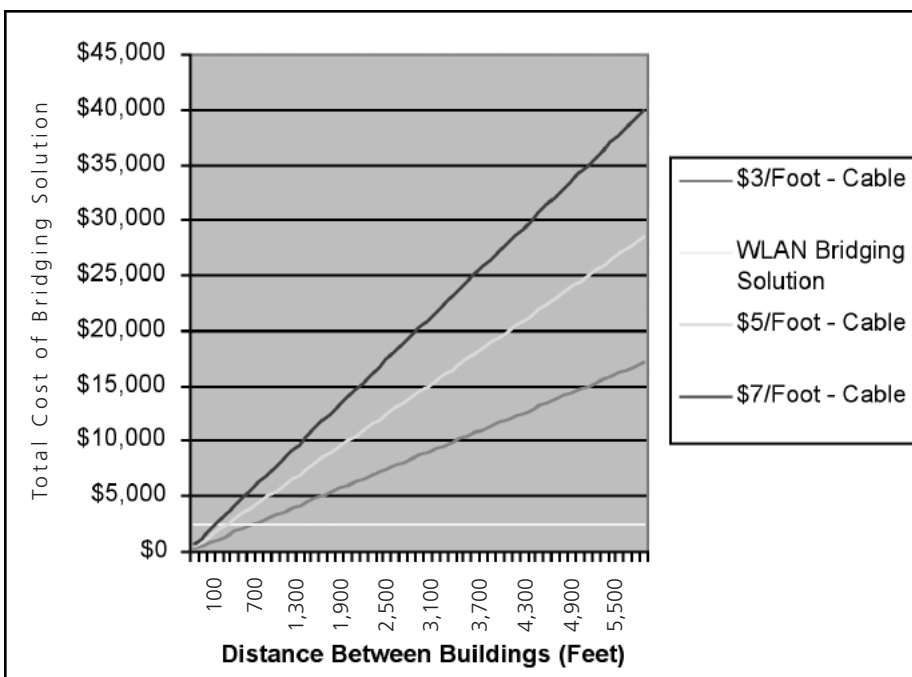
TABLE 4: Various Estimates for Cable Trenching Costs

Source	Estimated Cost per Foot
"The Price of Laying Fiber" ³¹	\$3.03 (rural areas)
	\$15.15
	\$35.00
	\$94.70 (city business district)
	\$2.00 - \$6.00
"DWDM Networking Primer" ³²	\$4.50 - \$27.27
"Performance Evaluation of CHART" ³³	\$10.00 (vendor quote)
	\$56.12 (SHA ³⁴ estimate)
	\$15.00 (vendor quote)
	\$12.31 (FCC industry analysis)
	\$30.00 (SHA estimate)
	\$100.00 (consultant estimate)

Figure 7 presents the results of the analysis as the distance between the bridged buildings increases. Note that the analysis assumes that the new building is a permanent facility, excluding scenarios, for example, in which a high school or university adds temporary classrooms for overflow students, or a hospital employs a temporary structure while renovations are underway in their main facility, all situations what would unequivocally benefit from a WLAN approach.

Further, legal and regulatory costs associated with obtaining permits, rights-of-way, or overcoming other hurdles necessary to conduct trenching operations are excluded, as they are quite often difficult to quantify. Despite the use of conservative assumptions and the exclusion of these other costs from the discussion, figure 7 clearly illustrates that the WLAN business case (vs. cable bridging) is very compelling for all but the shortest bridges.

FIGURE 7: Cost Comparison Between Wireless and Conventional Cabling Building-to-Building Bridging



31 "The Price of Laying Fiber. Members of the ISP-CLEC list discuss various benchmark prices-per-mile for laying fiber optic cable," ISP-Planet, http://www.isp-planet.com/business/fiber_price_bol.html

32 October 2003 Cisco "DWDM Networking Primer" presentation, http://www.oar.net/presentations/cisco_systems_dwdm_primer_oct03.ppt

33 "Performance Evaluation of CHART – an Incident Management Program, 1997, Final Report, Dr. Gang-Len Chang and Jean Yves Point-Du-Jour. <http://64.233.167.104/search?q=cache:4GV73NGxxYAJ:www.chart.state.md.us/downloads/readingroom/telecomStudy/Sec4/s4b.doc+site:www.chart.state.md.us+CHART+network+md+SHA+4.2&hl=en&start=1>

34 State Highway Administration (SHA)

Acquiring a Separate T1/E1 Line

The second option for organizations adding buildings to their operations is to run separate data access pipes (i.e. T1/E1 lines) into the new building. The result is a recurring monthly fee for a relatively low bandwidth option. T1 monthly access charges vary from about \$500 to \$1,200 per month³⁵ depending on location, while the European E1 rates average about \$850 per month³⁶.

Given the cost of a WLAN bridge in the \$2,500 range, the business case for a WLAN bridge versus a new T1/E1 line is not difficult to develop, as illustrated in Table 5. Note that the T1/E1 solution not only provides substantially less bandwidth than the WLAN's capacity, it

also in no way provides seamless connection to the corporate LAN for the employees in the new building.

From economic and operational perspectives, the WLAN approach is the clear winner.

The reader should note that WLAN building bridges can experience signal loss in poor weather circumstances, an issue of no significance for a cabled bridge. Attenuation studies have shown, however, that state-of-the-art WLANs, operating in the 2.4 GHz spectrum, show very little poor weather attenuation for line-of-sight bridges spanning fewer than 3 Km.

TABLE 5: New T1/E1 Bridge Solution vs. WLAN

Time from Minimum Deployment (months)	T1 Accumulated Costs ³⁷	E1 Accumulated Costs ³⁸	WLAN Accumulated Costs
6	\$3,300	\$5,100	\$2,500
12	\$6,600	\$10,200	\$2,500
18	\$9,900	\$15,300	\$2,500
24	\$13,200	\$20,400	\$2,500
30	\$16,500	\$25,500	\$2,500

Turning Wired LAN's Inside Out

The previous analysis presented a compelling business case for wireless inter-building bridges versus alternative options. In the case of a campus extension, the next decision confronting the cost-minded IT manager is what method to use to wire the "new" building.

Unlike the building-to-building bridging decision, whether to hardwire or install a wireless LAN in a new facility is somewhat less straightforward, and depends on the specific characteristics of the new building.

First, we'll establish a baseline capital cost per user for a WLAN installation, and to do so we'll use the previously-discussed 2003 Momenta Research report "Wireless LAN Total Cost of Ownership Benchmark Study: TCO Summary Data"³⁹. That study estimated the total capital cost per user for a WLAN implementation to be \$115, \$101, and \$96 for 450, 1500, and 6000-user WLAN deployments

respectively (the analysis assumed a "Fit AP" architecture, the best-case cost approach for WLAN deployment, as we've previously established). Note that those hypothetical estimates are consistent with the 1997 WLAN implementation case study at Hofstra University we discussed previously which reported a \$12,000 total installation cost for a 120-user LAN (\$100/user)⁴⁰.

The best-case scenario for a wired LAN approach is new construction. Wiring a building during its construction is clearly much less expensive than doing so afterward, and a reasonable estimate for that wiring effort is about \$25/drop⁴¹, an estimate derived from a residential/multiple dwelling deployment; to be fair, it is likely that a commercial deployment with higher user/square foot density would be even lower. Thus, from a pure installation cost perspective, a conventional wired LAN presents a strong business case relative to WLAN if the building can be wired during its construction at the optimum time.

35 T1 Shopper Website, <http://t1shopper.com/us/>

36 "Utilizing the Inherent Advantages of Lower Frequency Bands for Advanced Communications Systems," Joe Nordgaard, June 26, 2003, http://www.cdg.org/technology/3g/cdma450/files/Joe_Norgaard.pdf

37 An \$550/month T1 cost was assumed

38 An \$850/month E1 cost was assumed.

39 <http://www.trapezenetworks.com/technology/market/TCO/TCO.pdf>

40 http://www.mobileinfo.com/Wireless_LANs/business_case.htm

41 <http://www.one-economy.com/products-services/access-toolkit2-2.asp>

For existing, unwired buildings, the economic story changes considerably. Thanks to the University of Texas, an estimate of cabling costs for existing buildings is unnecessary; the University’s IT department posts the amounts it charges for cabling installations for all buildings on its campus based on not only category, but the actual building itself.

The bottom line is that for the oldest buildings on campus (what the University terms “Category C” buildings with “hard (solid) walls & Structural (open) ceilings”), the minimum cost to hardwire the building is \$150 per user (for more than 100 drops; the cost for less than ten drops is over \$250 per drop). On other end of the difficulty spectrum is a “Category D” building (“hollow walls & lay-in ceilings”). The minimum cost per drop in a Category D building is \$74 (over 100 drops), while the price per drop is \$119 in a “D” building for less than 10 users.

According to the University’s policy:

“Quotations include cable installation at published prices, plus any additional labor or materials required to satisfactorily complete the installation. Quotations reflect present knowledge of existing conditions. Unforeseen conditions, such as the need for asbestos abatement, or overcoming previously unknown construction obstacles, can significantly affect project costs and timeline estimates.”

Some of these “unforeseen conditions” were encountered by some of the Universities responding to a WLAN survey previously introduced:

“Wireless LANs were being used to help students be more mobile and the schools to reduce network costs and connect remote locations to central buildings and servers. In the university environment providing a wired connection was extremely expensive, especially when it involved historical buildings—running cable through ceilings and walls was cost-intensive. Running wire through ceilings and walls in buildings at one site was going to potentially disturb asbestos insulation, forcing a removal process estimated to cost over \$90,000.”

Thus, the estimated costs to wire the buildings reflect best-case scenarios, and actual costs are likely to be higher. Even assuming these wiring costs are maintainable and realistic, the business case for a WLAN is still highly compelling for older existing buildings, and potentially competitive for existing newer construction buildings when wiring installation risk is considered. The costs discussed here are summarized in Table 6.

TABLE 6: Comparison of Wired to Wireless Costs

Scenario Deployment	Wired LAN Installation Cost /User	Wireless LAN Total Cost/User
New construction	\$25	\$115
Existing modern construction	\$74	\$115
Existing older construction	\$150	\$115

Prime Time for a Change

Recognizing a good idea which is here to stay is easy: the first version of the product is greeted with enthusiasm as it fills a need or offers a grand new convenience. That initial enthusiasm is dampened, however, when the new product's first version inevitably turns out to be clumsy or riddled with flaws. Bad ideas die under those conditions, but the good ones see their bugs worked out, with new versions not only solving that problem, but further improving the product with better performance.

The first WLANs were expensive, security nightmares, and very difficult to deploy, but the market could foresee that the concept of mobility was a winner, if only it could be brought effectively to fruition. In 2004, the concept is still a winner: productivity improvements attributable to wireless mobility are still largely unchallenged, and installing access points in lieu of pulling cables is still an easy decision.

The difference is that the newest generation of Fit AP-based WLANs has worked out many of the bugs, improved security, and rendered WLANs not only cost competitive, but more cost effective than wired approaches in all but the most obscure circumstances. As these pages have discussed, WLANs are still a good idea, and now they're ready for prime time.

"WLANs: The Next-Generation Business Case" is one of a number of 3Com white papers discussing ROI and other important issues confronting decision-makers in organizations. This paper was researched by and developed with Phormion Sales Tools, Inc., www.phormion.com.



3Com Corporation, Corporate Headquarters, 350 Campus Drive, Marlborough, MA 01752-3064

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

The information contained in this document represents the current view of 3Com Corporation on the issues discussed as of the date of publication. Because 3Com must respond to changing market conditions, this paper should not be interpreted to be a commitment on the part of 3Com, and 3Com cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only; 3Com makes no warranties, express or implied, in this document.

Copyright © 2004 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. 503142-001 10/04