



7 CRITICAL MISTAKES TO AVOID WHEN YOU'RE SETTING UP A WIRELESS NETWORK.

A BRIEF HOW-TO GUIDE
FOR TODAY'S BUSINESS
AND TECHNOLOGY
DECISION-MAKERS.



THE FUTURE OF WIRELESS IS NOW. AND IT'S MOVING FAST

Picture this: As one of your salespeople waits at the gate in an airport, she's able to securely gain access to your network—and instantly get important price and performance data that enables her to close a sale.

Or...when one of your customer service reps is working from home because his child is sick, he's able to securely connect to your network for vital information that answers a client's urgent question.

In both of these cases—and in countless others across the business world today—a wireless network is being used to increase employee mobility and productivity, enhance corporate responsiveness, and add to the bottom line.

It's why corporate management and end users are discovering they no longer need to rely exclusively on wired technology—and are instead connecting via a Wireless Local Area Network (WLAN). They're gaining access from inside the office, home, and on the road—without the costs or physical constraints of cabling. And they're doing it via desktops, laptops, printers, PDAs and other devices—an increasing number of which now come with embedded 802.11 WLAN technology.

Quite simply, the corporate WLAN is changing the way we work—revolutionizing it, in fact. As business and technology decision-makers look to the future, they are seeing that wireless technology is a key strategic component for improving employee performance, serving customers, and growing their businesses.

HOW MUCH CAN YOUR COMPANY BENEFIT? JUST LOOK AT THE FIGURES.

The numbers tell an impressive story. According to a recent study completed by NOP World Technology¹, the implementation of wireless technology can enable you to:

*** Increase worker productivity by 27%.**

On average, end users who use wireless are able to stay connected to the corporate network for 3.5 additional hours per day. This freedom and mobility has proven to be a huge boon to productivity.

*** Save almost 80 minutes per employee per day.**

By giving your end users the ability to access your network from home—or from the road via hot spots in airport lounges, coffee shops and hotels—you enable them to save an enormous amount of time.

*** Save almost \$14,000 per employee per year.**

That's what the increase in productivity and savings in time add up to. It's a staggering figure—but it's being attained by many businesses today. Better yet, according to the trends, as an organization rolls out wireless technology to an increased number of users, the savings per employee increases simultaneously. In fact, the savings per employee is roughly double what it was only two years ago.

¹ 2003 Wireless LAN Benefits Study, Conducted by NOP World Technology on Behalf of Cisco Systems, November 2003.

IT PAYS TO PROCEED CAREFULLY—FOLLOWING A FEW SIMPLE STEPS.

What's the best wireless configuration for your business? And the most cost-effective? Who in your organization should be the first to use the technology? Where do you place your access points? What hardware should you use?



**...she's able to
securely gain
access to your
network...**

*...certain
“do’s” and
“don’ts” have
emerged.*

In asking these questions—and in answering them—it’s fair to state that certain ways of bringing wireless technology into your organization are more effective than others. In fact, during the past several years, as more and more businesses have begun to adopt and roll-out wireless technology, certain “do’s” and “don’ts” have emerged. Based on these findings, we have put together several common-sense guidelines to help you through the establishment and implementation of your wireless network. By following this series of steps, you can avoid some of the more frequent mistakes that are made when businesses “go wireless”—and instead, proceed in a manner that’s as seamless, efficient and cost-effective as possible.

Of course, it’s also true that no two businesses or set of circumstances are alike. So while we encourage you to heed these recommendations, we also encourage you to speak to an expert who can help you assess the specifics of your organization’s needs.

#1: DON’T MOVE FORWARD WITHOUT A CLEAR WIRELESS PLAN.

The benefits of setting up a wireless network are compelling—so compelling, in fact, that certain organizations have rushed headlong into the implementation process, without proper planning and network design.

The lesson to be learned from their experiences is that you need to carefully map out your wireless strategy and tactics—then move forward with a plan that still provides you with enough flexibility to change as circumstances change. First and foremost, in creating your wireless plan, you must:

- Determine network applications
- Set security policies for wireless and wired—for the office, at home, or on the road
- Establish coverage and capacity requirements
- Ascertain your number of users and the nature of your user population
- Identify types of client devices
- Pinpoint environmental and structural obstacles that can create interference during transmissions
- Select vendors and equipment

It’s important to note that this is a fluid process. As your plan evolves—and you move from your early iterations to a final blueprint—you will need to ensure that your plan gives you adequate room for maneuver.

Of course, in doing so, you may wish to consult with wireless experts who have extensive experience helping organizations establish a wireless network. In which case, please see page 7 once you have finished reviewing the seven steps outlined in this booklet.

#2: DON’T SHORT-CHANGE YOUR USER BASE WHEN YOU’RE ESTABLISHING YOUR USAGE AREA.

All too often, when upper management and corporate IT departments undertake a wireless program, they focus primarily on *where* they need to implement a solution, but not on *who* they need to serve. In other words, they take a site survey to delineate a proposed coverage area, but do not conduct a proper audit of precisely who will be accessing the wireless network and what applications they may be using.

This flaw in the planning process may be one reason that a recent NOP World Technology² study found that many IT professionals seriously underestimate the number of their company's users who are working via the wireless network. As a result, when organizations miscalculate the size and/or density of their user population (not simply in terms of current users, but also future users), they run the risk of not installing enough access points and not scaling adequately to the needs of a growing user base.

As a rule of thumb, you should have between 10-15 users per access point, assuming that the primary applications they're using are web and e-mail based. You will need a greater number of access points for a specific area if your users are using data-heavy applications such as voice and video.

² 2003 Wireless LAN Benefits Study. Conducted by NOP World Technology on Behalf of Cisco Systems, November 2003.

#3: DON'T ASSUME THAT ENTERPRISE-GRADE WIRELESS HAS SECURITY PROBLEMS.

If you're like many business and technology decision-makers, you may have heard that wireless presents you with some formidable security challenges. In fact, at the present time, security is the number one concern of business people who are contemplating the implementation of a wireless network.

The good news is that these challenges are in no way prohibitive. That's because decisive improvements have been made in security for enterprise-grade wireless networks—in contrast to retail “home user” wireless products, which can still present users with security issues.

Quite simply...Security concerns should never prevent you from adopting wireless technology and enjoying substantial gains in employee productivity and corporate efficiency. That's because security measures now exist—and can be put in place—that ensure secure operations across your wireless enterprise.

Implementing a proper security solution really consists of two parts: First, you must realistically assess and analyze the security risks that you face. And secondly, you must select the method of protection that guarantees you secure operations. Of course, it's important to note that a proactive security policy must not only be set, but must also be turned on.

Understand the risks. In terms of security risks, one of the greatest threats you face may come from not knowing how many of your users are already wireless. For example, if users bring laptops from home into the workplace, the laptops may have an embedded wireless chip that is turned on by default. Even if the users are hard wired into your network—and aren't taking advantage of their machines' wireless capabilities—a hacker could still connect to them via wireless and “piggy back” onto your wired network. So even if you don't currently have a wireless network in place, you can still be subject to a wireless attack. (And keep in mind, it's not only laptops you need to be concerned with—it's printers, PDA's and all sorts of other devices with embedded wireless.)

Given this reality, it's no wonder that even organizations that rely exclusively on wired connections are developing strategies to deal with wireless security threats. In fact, certain organizations that have established a policy of not implementing wireless as a business tool—certain financial institutions come to mind—are still deploying wireless for the express purpose of detecting other wireless threats. The lesson to be learned: No matter how much or how little you plan on making wireless part of your future, you still need a wireless security strategy.

Implement a solution: From a micro perspective, the best way to prevent “piggy back” attacks is to ensure that your IT department knows what's on your network. This can be accomplished with a hardware audit that determines the number and location of wireless radios on your network, including non-authorized, non-IT deployed radios.



...you should have between 10-15 users per access point...

*...superior
security for
wireless is
here...*

From a macro perspective, it's fair to state that you have multiple security solutions to choose from. Are you best served by a standards-based solution, or a non-standards-based solution? What about your choice of authentication and encryption solutions—both of which are now encompassed in wireless LAN security mechanisms? Working with a security expert (see page 7), you can select and implement the solution that makes the most sense for your particular needs.

For example, over the past few years, organizations have relied on a series of built-in 802.11b standards—including Wired Equivalent Privacy (WEP), Media Access Control (MAC) and service set identifier (SSID). WEP, the common currency in WLAN security protocol, is now relatively easy for hackers to breach. In contrast, a new security standard, Wi-Fi Protected Access (WPA) is much more difficult to breach—exceedingly difficult, in fact—thanks, in large part, to the fact that it rotates the encryption key. Furthermore, an even more ironclad security protocol—Advanced Encryption Standard (AES)—is under development and will soon be available to protect the enterprise.

The bottom line: Superior security for wireless is here—and even better security is on the way. The security challenge has been met, head-on, and should not be an impediment to the adoption of wireless.

#4: DON'T ASSUME THAT WIRELESS IS A REPLACEMENT FOR WIRED.

There's unlimited potential in wireless technology. From a financial perspective alone, you just have to look at the savings per employee (see page 2), and the savings of not having to run cable to every desktop or re-cabling when changes are made to the network.

But, attractive as wireless is, you may not want to view it as a replacement for the wired network you have in place. By and large, wireless is intended to *augment* the robust capabilities of your wired infrastructure, not send it into early retirement. You want wireless *on top* of wired, not *instead* of it.

After all, it's still to your advantage to have switch ports on your users' desktops—giving them the fullest range of functionality. And there's the simple matter of throughput—whereas a wireless network offers connection speeds of 11Mb/s or 54Mb/s shared, a wired network offers 100Mb/s or 1000Mb/s switched connection speeds.

However, having said this, we should hasten to add that no rule is absolute. In certain industries—in certain circumstances—wireless can be used as a total replacement for wired. In a manufacturing warehouse, for example, where it's too expensive to run cable, a 100% wireless solution may be appropriate and necessary. Or, for a small business in a temporary location, an all-wireless network may be the solution of choice.

#5: DON'T IMPLEMENT A PARTIAL DEPLOYMENT WITHOUT PLANS FOR A WIDER ROLLOUT.

It's all too easy to say, "We want to provide wireless access in the lobby and conference rooms only." Or, "we want only such-and-such a department to have wireless access." While these types of solutions may seem less expensive in the short term, they may not be the most prudent decisions in terms of long-range impact on your business.



*...you can
save...by
deploying all
at once.*

The fact is, wireless is a viral technology that spreads like wildfire. The more certain workers use it, the more other workers in your company will want to use it. If you foresee just your sales force “going wireless,” for example, you may be surprised at how quickly marketing and manufacturing will demand to go wireless as well. And it won't be long before your suppliers, contractors, and other mobile workers request guest networking access.

It may therefore be wise to plan on a wide rollout as opposed to a narrow one. That's what many companies are doing as they plan an architecture that is globally scalable to multiple buildings and offices worldwide. Or, if you still believe it's best to limit the coverage area and/or eligible user groups, you will at least want to have plans for a broader rollout in your back pocket.

As you'll see, you can save a considerable amount of money by deploying all at once. By covering your entire building or campus as opposed to a few common areas—or by extending wireless to the bulk of your organization as opposed to a few select users—you place yourself ahead of the technology curve and implement a far-sighted solution that positions you well for the years ahead.

#6: DON'T UNDERESTIMATE THE EFFECT THAT WIRELESS WILL HAVE ON YOUR BUSINESS.

The workplace is changing. The idea that work is an activity, not a place, is becoming more widespread. Increasingly, workers are telecommuting. Users of laptops are expecting to have the ability to roam and to collaborate effectively with co-workers via a wireless connection. Users of wireless IP/Telephony products are experiencing a seismic shift in how they conduct business—for example, when mobile workers run applications like softphone on their laptops to enhance their IP communications. Developers of new wireless products are finding an eager business marketplace that is ready to adopt their new technologies.

Quite simply, over the next few years, everything that *can* benefit from being wireless-enabled *will* benefit from being wireless-enabled. We will be living in a wireless world—and today's early adapters will be joined by mainstream (and Main Street) business people in utilizing wireless to the fullest extent of its capabilities. Several sectors are currently leading the way: Manufacturing. Education. Healthcare. Retail. Government. And virtually every other sector of the economy is following suit. We're seeing the introduction of wireless technology into virtually every aspect of our lives: Wireless RFID tags will soon replace bar codes in the consumer and business-to-business markets...and even the waiting rooms of doctor's offices are now being given wireless access, so patients can work while they wait.

Given this reality, you will want to find a wireless vendor—indeed, a wireless partner—who has the foresight, longevity and stability to help you upgrade seamlessly to new technologies as they are introduced.

#7: DON'T PICK THE WRONG VENDOR.

One of the most common mistakes in wireless planning and implementation—and one of the most avoidable—is picking the wrong vendor to help you put your wireless solution in place. Typically, this error occurs when business and technology decision-makers are looking for best-of-breed solutions—and, in their zeal, find themselves turning increasingly to niche players without fully considering all of the features and benefits of the products offered or the necessity of seamlessly integrating wired and wireless technology. Furthermore, careful consideration needs to be given to not only initial capital expenditure costs for equipment, but longer term operating expenses.

For example, doesn't it make sense to consider your wireless network an extension of your wired network—and build on the strong wired infrastructure that's already in place, as opposed to trying to replace it? (see page 5) And as a result, wouldn't it be advantageous if you found a vendor who enabled you to integrate your wireless access points directly with your existing switches, as opposed to installing an entirely separate set of switches for your wireless operation? Wouldn't you want to ensure the vendor provides a complete wireless solution that includes not only clients and access points, but also security and management?

The fact is, it's a smart solution to have a single, unified wired/wireless infrastructure—with one operating system, and ubiquitous tools for not only managing switchports, but wireless ports as well. This type of integrated solution is superior to a niche solution, since it will provide you with extensive cost-savings, robust functionality and operational efficiencies for years to come. More importantly, it will allow you to provide your end users with all the benefits of wireless, while reducing the total cost of ownership and simplifying the IT department's tasks.

You will want to be sure to find a vendor who will deliver all of these advantages to you—a vendor like Cisco.

TURN TO CISCO—THE WIRELESS LEADER.

To ensure that your wireless initiative moves forward in the most efficient and successful manner possible, you'll want to rely on the experts at Cisco Systems. We have many proven deployments of WLANs worldwide, and we continue to innovate for the future. We know how to integrate your wireless network with your wired network. And we've got the experience and know-how to help you through the entire process—from planning and surveying through implementation and maintenance.

Quite simply, at Cisco, we offer you the infrastructure, intelligent services, applications and devices that enable you to implement the wireless network that's ideal for your needs. In fact, statistically speaking, we're the world's #1 provider of WLAN infrastructure—and lead the industry in delivering secure, manageable, enterprise-class solutions.

And not only are we the market leader, we're the people's choice. According to a recent Heavy Reading Survey³, buyers and users of wireless products rate us #1 in many wireless product categories for performance, quality/reliability and service/support.

³ Heavy Reading, Volume 1, Number 8, December 2003, Wireless LAN Market Perception Study.

Rely On Cisco For Superior WLAN Products.

With Cisco's Aironet® Series of WLAN solutions, you're assured of seamless integration into an existing network as a wireless overlay, or of easy implementation as a freestanding all-wireless network. In both cases, you'll increase mobility and productivity dramatically—with a product set that sets the enterprise standard for high performance, security, manageability and reliability.

As you'd expect, Cisco products support IEEE 802.11a/b/g technologies—and offer a complete line of in-building and building-to-building WLAN solutions that include access points, WLAN client adapters, bridges, antennas and accessories, along with security and management platforms. Additionally, the Cisco Aironet Series is a key component of the Cisco Structured Wireless-Aware Network—an innovative, comprehensive Cisco IOS Software-based solution for deploying, operating and managing your wireless network.

This is what Cisco can offer you. This is the power of the network. NOW.

*...we're the
world's #1
provider
of WLAN
infrastructure*

FOR MORE INFORMATION...

**SIMPLY CALL CISCO AT
1-866-282-8329.**

We'll be glad to provide you with additional details on how to avoid critical mistakes in your wireless implementation process. We'll also tell you how Cisco can provide you with a full range of wireless solutions that help you in the here and now—and far into the future. Naturally, your inquiry places you under no obligation whatsoever.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia
Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece
Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico
Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004, Cisco Systems. All rights reserved. CCIP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0208R)

Printed in the U.S.A.