Can going wireless really be simple?

Five Steps to Deploying a Wireless LAN

Yes.

Adding wireless connectivity to your LAN takes only five steps.

Just start with mobile PCs and build on the network you already have.

Wireless now, step by step.

The best way to add wireless connectivity is to start small and plan with an eye toward expansion.

Reach first for those employees who use notebooks now, for they will benefit most from wireless access.

Get started today.

1. Establish a pilot that will test and confirm how wireless can work within your business campus and needs.
2. Tie in Internet access and a robust data security system.
3. Install wireless access points, and equip notebook PCs for wireless use (e.g., provide PC cards or upgrade to PCs with integrated wireless connectivity built in).
4. Train and turn your participants loose with their wireless notebook PCs.
5. After the pilot, build on what you learn to broaden your wireless LAN (WLAN) to cover other areas and users.

1. Plan your pilot.

Define scope, participants, zones, metrics, and training.

Choose suitable usage models.

Successful wireless implementations apply usage models that make sense in the business environment.

Popular sites for wireless LAN projects include executive offices, sales offices, operational facilities, and new buildings.

Define which kinds of wireless usage you're trying to capture at each location.

Decide on participants.

It's vital to obtain a good sampling from each location in which you plan to install wireless. Plan for 100 to 500 participants, depending on the pilot's scope, your campus size, and user base.

Include coverage for various job classifications, employee segments, and departments—all of whom will derive a different value from wireless.

Encourage executives or senior management to join the effort, and include nay-sayers as well as evangelists. Senior manager buy-in is a contributor to a pilot's success.

You may want to offer to pay for the PC upgrades, rather than bill departments who participate. The cost of equipping users with wireless-enabled PCs can deter some groups from joining a pilot.

Once you define the pilot, allow at least two months to prepare it, and two to three months to run it.

Inventory the notebook PCs.

Inventory the mobile PCs that participants use, to determine which will need wireless cards (e.g., PCMCIA cards) to communicate with access points.

A start-up wireless pilot will be less expensive and will yield higher initial value if you work with employees who already use notebook PCs extensively.

However, a pilot also presents a good opportunity to begin equipping participants with notebook PCs that have integrated wireless network support.

Determine what the pilot should measure.

Measuring the outcome of a wireless pilot is vital to moving ahead to a broader network. You need far more than a handful of evangelists extolling its virtues: you must build your ROI model so you know exactly what you're dealing with.

At the very start, lay out how you'll measure the production value index. Start with a baseline measurement of costs before the pilot, and plan how to measure and report productivity and ROI metrics afterward. Someone from Human Resources may be a valuable contributor to your team for this aspect.

Only your company knows what ROI model works best for you. Success metrics might include productivity hours reclaimed, adoption rates, increases or decreases in revenue and costs, or how well people understand and use the WLAN.

Would the users complain if you wanted to take it down after the pilot? If so, wireless is very likely to succeed for you on a broader scale.

Another approach would be to ask how the participants foresee using wireless day to day before the pilot begins, then create metrics and surveys to reveal how they actually used and benefited from wireless.

Intangible benefits should also be measured, such as a user's sense of convenience, job satisfaction, increase in perceived productivity, and better life/work balance.

And don't forget plans to measure the success of your security. Arrange to have your technical support teams try hacking into the wireless system, then get feedback.

To increase the amount of user feedback, consider providing incentives for participation and reporting. And keep in mind that early adopters are often very enthusiastic, so numbers may be slightly inflated—another good reason to include nay-sayers in the pilot.

Employees with access to their files and tools during team meetings are significantly more productive.

Define wireless zones.

Map the wireless zones that participants will use (conference rooms, common areas, cafeterias, offices, operational areas, etc.), and determine the LAN wiring you have in those areas. Access point hardware is hard-wired to the LAN. Work closely with your facilities team to incorporate wireless technology in ways that will minimize rework as the WLAN expands.

If your campus has several buildings, you'll get the full benefit only after you outfit the whole vicinity. Until then, you'll greatly improve the pilot by spreading wireless over a good-sized representative area—don't just sample it on a single floor, as this constrains the mobility value of wireless.

As you define zones, make sure you can support the whole wireless network well. A larger pilot is a better test of usability and productivity, but you need the resources to support it.

Plan access points for adequate coverage. 802.11b access points have a range of about 300 feet (about 100 meters). Installations should overlap the ranges to ensure a seamless hand-off for roaming employees. (Have your representative area surveyed for best coverage results.)

How many people per access point?

The number of simultaneous users that an access point can support depends mostly on the amount of data traffic at the time (heavy vs. light downloads and uploads).

Bandwidth is shared among users on a WLAN as with wired network connections. Network performance, as gauged by the number of simultaneous users, hinges on the combined computing activity.

For example, in 802.11b, each hardware access point has up to 11 Mbps through-put. This capacity is adequate for:

- 50 nominal users who are mostly idle and check an occasional text based e-mail
- 25 mainstream users who use a lot of e-mail and download or upload moderately sized files
- 10 to 20 power users who are constantly on the network and deal with large files

To increase capacity, more access points may be added, which gives users more opportunity to enter a network.

Networks are optimized when the access points are set to different channels. For instance, a company may place three 802.11b access points (with a range of up to 100 meters each) in three adjacent offices, with each unit set to a different channel.

In theory, many users could then "share" up to 33 Mbps total capacity (although no single user would ever have throughput faster than 11 Mbps). In reality, clients associate with the access point with which they share the strongest signal, so the bandwidth may not be dispersed evenly among users.

When considering placement, higher is better, and open areas work better than smaller spaces. Look for physical limitations that might interfere with wireless radio signals. Just as for cordless phones, building objects and concentrations of people can affect a WLAN's coverage.

Each access point can accommodate from 10 to 50 users at once, depending on data traffic (see sidebar). Having multiple access points will extend the number of users the WLAN can support.

Establish a training program.

The success of a pilot often pivots on how well participants and your Help Desk personnel are trained, and whether your support group can respond quickly to requests for help.

This includes training your first, second, third, and even fourth levels of support to make sure they know how to use wireless and troubleshoot it.

Start early to document how users should get started, how to use the system, and how to obtain support.

Prepare trainers and FAQs for deployment, and train your IT and technical support teams thoroughly in the new technology. Plan to have roving trainers during the first two weeks of the pilot, so they can help users through tricky spots.

To guarantee 100 percent training participation, consider a deployment process in which pilot participants cannot receive their wireless hardware without getting usage instructions at the same time.

First impressions can make or break the success of the pilot.

Well-planned WLAN coverage means people can work effectively anywhere they choose.

2. Secure your network.
Apply multiple layers of data security and monitor regularly.

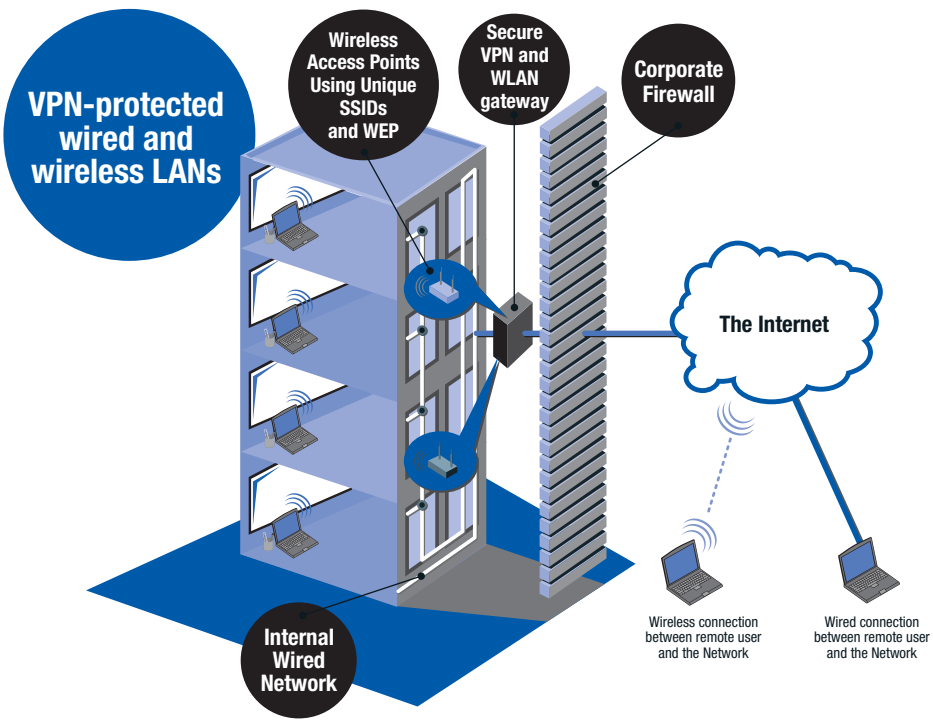
Authenticate and encrypt—then do it again.

A wireless network can be effectively secured with the right steps, attention, and diligence.

Existing virtual private networking (VPN) for remote access can make the leap much easier: just apply the same system and security protection to wireless.

But don't rely on just one form of WLAN security—create multiple layers to thwart both casual and determined hackers (see sidebar).

Whatever measures you take, set up everything correctly. Improper implementation and enforcement of the security technology are the leading causes of security violations.



Other guidelines that have proven useful.

- Evaluate your corporate LAN security policies to determine how to extend them to wireless.
- Don't use default settings for any security technology.
- Set up a client firewall with VPN as an extra layer of defense around notebook (remote) PCs.
- Evaluate exterior security perimeters to sniff out passers-by who are using access points.
- Seek to standardize on a single vendor when possible.
- Provide ample employee training about password management.
- Have the ability to revoke access quickly when needed.
- Establish an IT group dedicated to security matters, and have outside consultants test and review security measures.

Stay current.

Evaluate and adopt the most powerful wireless standards as appropriate when they become available.

For greater detail on VPN and a wireless LAN, see Intel's white paper, "Wireless 802.11 Security in a Corporate Environment," available at www.intel.com/ebusiness/wireless.

Protecting your WLAN.

Malicious or not, intruders into your WLAN are never welcome. Here are some guidelines for protecting against unwanted access to your WLAN.

- **Change the default wireless network IDs (SSIDs) immediately after installing access points, disable automatic SSID broadcasting, and change SSIDs regularly, if possible.**
- **Enable (but don't depend only on) the WEP (Wired Equivalent Privacy) protocol on your 802.11b system. Give it your own WEP key instead of the default, and set up WEP keys to generate by session or by user.**
- **Authenticate wireless users by employing the same RADIUS (Remote Authentication Dial-In User Service) servers you use to authenticate remote users.**
- **Install virtual private networking (VPN) for a secure end-to-end tunnel between user and network.**
- **Combine wireless and wired security policies to simplify implementation and maintenance (such as assigning an employee the same user ID and password for access to the WLAN or LAN).**
- **Pay attention to the product feature details of the 802.11b equipment you choose for your WLAN. Security capabilities may vary, even if a device carries the WiFi label.**
- **Regularly scan your WLAN for rogue networks set up by non-technical staff, and establish formal policies for approved installations.**

Adapted from "Channel Viewpoint: Top 10 wireless security tips" by Bruce Comeau, Business Networking Specialist at 3Com, for the eChannelLine site.

3. Install the equipment.
Equip the workplace, workers, and IT pilot team.

Purchase and install access point devices.

Most access point hardware provides similar features. Pick the top providers, especially those that will provide solid product support.

If your wireless network is to be international, make sure the access point product is available worldwide, can support wireless frequencies that vary from country to country, and can be secured and supported wherever users go.

You may want to consider purchasing dual-band access points, which support both 802.11a and b. Even if you deploy 802.11b, you can take advantage of the features and greater throughput of 802.11a when it becomes more widely available.

Choose access point units that offer interchangeable antenna options (e.g., omni-directional and directional antennas). These accommodate different spaces so you can fine-tune reception for optimal reach.

Access point units need electricity. Larger installations do best using power over existing Ethernet/Cat-5 cabling to avoid expensive retrofitting of electrical wiring. Make sure the units you buy support Power over Ethernet.

Allocate multiple channels for different floors and access points. Carefully planned channels can be used to direct certain people to certain access points, in effect providing a second WLAN that only specific users can access.

Install switches to route traffic from access points to the de-militarized zone in only one direction.

Use RADIUS servers for secondary authentication.

Provide wireless adapters to mobile participants.

Create auto-installers to install all the WLAN drivers, VPN software, etc. in participants' notebook PCs.

Install network interface cards (NICs), or provide users with notebook PCs that have integrated wireless connectivity.

Make sure to quality-test the drivers and software in the notebook PCs as an integrated solution set (not only as individual units) before you deploy the pilot.

Prepare for training, support, and measurement.

Set up the IT systems that you established in previous steps for training, security, technical support, and measuring.

4. Deploy the pilot.
Support and adjust the live system.

Train participants.

Following the training program you set up earlier, make it easy and mandatory for users to get training on their new systems—preferably at the same time they receive their wireless-enabled notebook PCs.

Set appropriate user expectations for support and how they should request it. Then train them to actually call, report, and get help.

Go live.

Check in as you go.

Get user feedback from the very start. This can be even more important than technical feedback.

Consider an informal system in which IT personnel roam the wireless zones for on-the-spot input from users. You might also schedule interviews or drop-in lunch meetings to gather comments and reactions.

Collect intermediate metrics for ROI reporting, and address technical issues as needed during the pilot.

Maintain security vigilance.

Closely monitor the WLAN access and be prepared to react quickly to seal security leaks or handle other problems.

Ask your best technical support members to try to hack into the system or interfere with its functioning. Document the results and, if necessary, immediately act to re-secure the network.

Feedback from users during deployment ensures the pilot's success and helps with future planning.

5. Repeat to expand.
Assess the pilot and widen the wireless net.

Evaluate pilot results.

Gather and report findings and ROI values. Review ways to improve systems to meet needs that the pilot didn't address, such as additional access points or smoother setup or support for users.

Report the findings to stakeholders to get buy-off for broader deployments.

Provide outcomes to all your pilot users, as well—they need to know what became of their efforts to help.

Repeat the process to broaden the wireless reach.

With an eye to the larger organization, return to step 1 and reassess the questions and decisions you made for the pilot in light of scaling the WLAN to include more zones.

Decide whether to deploy wireless across the entire network, or to expand it selectively to serve the next level of mobile-user needs. Also remember that wireless can be used at home and on the road with public hot spots, which could continue to increase the value of wireless to your business.

When you're ready, repeat steps 2 to 5 to broaden the WLAN, being sure to consider the cost and ROI of equipping additional users with notebook PCs.

Standardize security access across the site no matter how large the WLAN gets, so users won't run into lockout problems as they roam.

For more information, visit us on the Web at www.intel.com/ebusiness/wireless

0902/JM/RC/CG/10K/PDF Order Number: 251636-001