Installing, Troubleshooting, and Repairing Wireless Networks

Jim Aspinwall

McGraw-Hill
New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

Cataloging-in-Publication Data is on file with the Library of Congress

1 2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7 6 5 4 3

P/N 141071-6
PART OF
ISBN 0-07-141070-8

The sponsoring editor for this book was Judy Bass and the production supervisor was Sherri Souffrance. It was set in Century Schoolbook by Patricia Wallenburg.

Printed and bound by RR Donnelley.

This book was printed on recycled, acid-free paper containing a minimum of 50% recycled, de-inked fiber.

CHAPTER 2

Wireless Network Criteria and Expectations

There are generally three well-known types or deployments of wireless networks:

- The simple local area network (LAN) that you would find at home or in a small office
- A campus or neighborhood LAN that you would find emanating from a home or central location to cover roughly a square mile or less—often called a *hotspot*, where wireless activity may be available
- A metropolitan area network covering several square miles, from which several mobile and portable users benefit

These are typically point-to-multipoint installations where one or many access points together are used to distribute a single network to multiple client systems. Lesser known, but equally useful and beneficial, are point-to-point relay systems to interconnect different networks or facilities.

Each of these types of networks may be associated with one of the following types of services:

- Personal/private use by an individual or family
- Publicly shared use by those known and familiar to the host/provider of the network
- Private network use to serve a business and its employees
- Subscription-based networks or Internet service providers (ISPs) available to anyone paying to obtain the service as you would obtain dial-up, digital subscriber line (DSL), or cable Internet access

Similar to the subscription services that make wide area access available to the general public are several growing efforts to deploy free wireless Internet services to the public in different communities—Seattle and San Francisco being among them.

The U.S. government sees wireless services as a way to solve the "last mile" problems of spreading high-speed Internet access to the general public, especially in areas where cable TV and phone service providers have not or will not deploy cable or DSL services to their subscribers because they will not recover the high costs of these services with relatively few subscribers.

Most of the issues with all of these types of wireless networks are about the same—how much signal can you get how far away, what is

in the path of the signal, and how can you make the signal better? What typically differs is the type of equipment used, as well as how it is installed, configured, secured, and maintained. There will also be cost differences in the equipment and type of installation. External antennas and cabling cost extra. Mounting an antenna at home is free, but putting an access point or a wireless relay/bridge system atop a building will usually incur monthly fees.

Performance—What To Expect

The success of any network, any project for that matter, is based on expectations, perceptions, specifications, and factors, and of course actual performance—that is, does it work?

Chances are, a reasonable/feasible, properly designed and implemented wireless networking system will work flawlessly for you. So the first steps are to define and understand reasonable/feasible and properly designed, and implemented in this context.

Reasonable and feasible have both an economic and a practical aspect. The economics of wireless networking are discussed in the next section, but expect a 30–40 percent savings versus conventional wired networks. The practical aspects, including design, implementation, and maintenance have to consider several physical, logistical, and administrative aspects. Consider the following a basic reality check and checklist for your implementation:

- Do you need wireless technology?
  - Is this a permanent or temporary installation?
  - Are you unable to freely or practically access areas to string cables?
  - Are you prevented by lease, contract, or policy from running wires?
  - Will you always have control over the security and access to your cabling?
  - Do you currently have a wired network?
  - Is there an aesthetic reason to go wireless?
  - Do you need a temporary peer-to-peer setup?
  - Do you travel and need or want more than dial-up connection speeds?

- Is the site wireless-friendly?
  - Are there sources of interference that cannot be eliminated?
  - Will a wireless network system interfere with other devices?
  - Do technical or security policies preclude broadcasting your network traffic through a wireless system?
  - Does the structure facilitate wireless technology with little or no metallic obstruction?
- Can you use wireless technology?
  - What distances are you hoping to cover?
  - Do you have a line-of-sight path to all systems?
  - What data throughput speeds do you need?
  - Can you adequately secure your data over a wireless connection? Do you care?
  - Are all of your systems wireless capable—current or recent hardware, operating systems, and applications?
  - Will some of your systems still need to be wired (older technology)?
- Who will design, install, and maintain your wireless system?
  - Do you or your vendor understand and have experience doing wireless?
  - Do you or your vendor have access to analytical equipment or software tools to survey your site as part of the design phase and to troubleshoot implementation problems?
  - Will there be enough skilled resources to administer your network?
- Can you afford wireless?
  - In the simplest forms of wireless implementation, as an alternative or replacement for a wired LAN, wireless networking has significant cost advantages over wires. If you need to cover greater distances or bend around corners to get between systems, you will need intermediate sites and equipment. This topic is covered in "The Cost of Wireless" section in this chapter.

As you can see, creating a wireless network can be more involved than a jaunt to the local computer store or on-line shop, grabbing a few wireless cards and access points, and plugging things in—they just might not work. Many of these issues are covered in depth in the following sections and in subsequent chapters.

Do You Need Wireless Technology?

Those who cannot or will not run wires—apartment dwellers or those restricted by office lease or the physical structure itself from running cables across easements, civil boundaries, etc.—are obvious candidates for using wireless networking.

Shared office facilities, where tenants may share a common telephone/network equipment and cabling room, are also good candidates for wireless—to reduce the risks of bandwidth or data theft, tampering, or encountering old or inadequate wiring.

When using temporary office space, as for a campaign headquarters, charity event/race/marathon, emergency operations center, or field post, or while awaiting the completion of a permanent office, certainly do not waste the time and money involved in deploying a wired LAN infrastructure.

Wireless is ideal for travelers and commuters who need to stay connected to corporate or personal communications and can find a location at many large airports, urban cafés, public libraries, and some college campuses having wireless services. Free and subscription-based wireless services are being deployed more and more. Unfortunately, you may have to maintain subscriptions to many service providers in order to be able to connect, as well as be familiar with the many different wireless network connection parameters and subscription log-on methods to get and stay connected.

Using wireless network adapters is ideal for setting up a quick peer-to-peer network between friends, much as you might use the infrared connection features of personal digital assistants (PDAs) to beam information back and forth.

Is the Site Wireless-Friendly?

The issue of other devices and wireless services interfering with your wireless network can be the biggest barrier to a successful implementation. There are both technical and social engineering means of determining if wireless networking might work.

The first technical method is to simply acquire one access point and one client wireless network card, preferably on a laptop personal computer (PC), and set up a simple wireless connection to an existing network. Walk around with the laptop and try to use the network

in as many places of interest as possible. Many of the client-side adapters include signal strength monitoring software so that you can see how strong and reliable your wireless connection will be. If you approach a piece of equipment that interferes with the wireless signal, your received signal strength will probably drop below acceptable levels and you will lose your connection to the network.

Loss of connection may be intermittent, rather than based on a specific location or simply proximity to other equipment, and this may be an indication that another wireless service or an appliance that affects your signal is in use nearby. Pay attention to this when microwave ovens and special equipment may be in use more often than at other times. Of course, interference from the microwave oven in the company cafeteria is a great excuse to stop working, take a break, and get away from the computer.

More technical, often preferred, and hyped by many wireless networking consultants is a complete radio frequency (RF) site survey performed with a spectrum analyzer—a highly technical piece of test equipment that can see details of both large and small portions of RF spectrum—identifying, qualifying, and quantifying the types of signals it receives. In some cases, the analyzer can also tell you what type of signal is being received, if it is not obvious by the visual display and characteristics of the spectrum. Unless the received signal can be demodulated to reveal the information within, and that information contains the identity of who is responsible for the transmission, it may be impossible to tell who is generating that signal. Moving the spectrum analyzer's antenna closer to or farther from different areas, or using a directional antenna, can tell you proximity or locate the transmitting device.

A spectrum analysis may not be conclusive evidence as to whether the site will accommodate wireless networking, because 802.11a and 802.11b use sophisticated modulation and signal processing techniques, a signal may get through 100 percent of the time even in the presence of interference. You will only know by trying it.

Conversely, unless a spectrum analyzer is present and monitoring the right portion of the RF spectrum for several days, a typical 1–2 hour "quick check" of a site may miss very significant interference that could render your network useless for several minutes or hours. Similarly, a clean, interference-free site today could become cluttered with new interference as other networks, appliances, or services come online nearby.

To enhance your confidence in your site's ability to accommodate wireless, do a little walk-around/talk-around investigation, and not just before you install your system. Do so frequently to help determine if nearby building tenants, new occupants, or other sources of interference are about to be introduced into your environment.

Can You Use Wireless Technology?

One of the most common questions about wireless is, How far will it go? As with most answers about technical things, it depends. 802.11b was designed with native, unmodified, unenhanced devices to extend the length of a 10BaseT Ethernet wire by 300 meters. This equals 985 feet, about a city block, or 0.18 miles. Unobstructed, unimpeded with line-of-sight, 802.11b will do just that and probably more. But who is going to hold their laptops above their heads or mount an access point itself on a rooftop to communicate digitally?

In most real-world cases, two native 802.11a devices will do well to clear 100 feet before the signals fade or are reflected too much to make a reliable connection. You may be able to add external antennas to your wireless equipment, overcome obstructions, and generally improve near-field penetration or increase range.

If you simply need to improve straight distance range, look for a directional antenna, or a pair of them, to provide approximately 8, 12, or 16 dB of signal gain. These may provide up to 10–12 miles of range between devices—not bad if you want to walk around a city park with a directional antenna attached to your laptop, attracting the attention of others.

To get this kind of range, one of the devices needs to be mounted high above surrounding terrain and buildings—which means finding space at a commercial radio site or a friend's house atop a hill or high-rise building. (I would be keenly interested to know if anyone successfully builds a solar-powered access or relay point and hides it in a tree someplace just to prove that wireless can be free and everywhere.)

If that meager 100 feet of coverage around your office bothers you, or you cannot seem to stay connected to the LAN during critical presentations in the conference room, then installing an omnidirectional antenna with 3–6 dB of gain will add penetration.

Remember, the primary intent of wireless is to get you off the 10BaseT CAT 5 cable tether. Stretching that invisible nonwire to cover

neighborhoods and vast metropolitan areas involves just a little engineering and significant financial investment, which will be covered in later chapters. At this point, keep in mind that you are trying to get what amounts to a beam of light, or a reflection thereof, through an obstructed maze in a fog bank—and you will have a little better understanding of what you are up against with some wireless systems.

When you start trying to use wireless beyond the desktop, the issues of interfering with other devices and wireless services, as well as any security or policy issues that may preclude or prohibit the use of wireless, may or may not be obvious.

As a potentially interfering party, you should be mindful of other services. It would not be a good thing to discover that your wireless equipment interfered with medical diagnostic equipment, aircraft or military systems, or otherwise violated the Federal Communications Commission (FCC) rules by making an amateur radio system unusable. Doctors or medical technicians may not be able to discern, locate, or identify a source of interference with their instruments, but technical people such as amateur radio operators, who generally associate with engineers at various levels, can muster considerable resources to pinpoint interfering equipment.

If interference is not an issue, then certainly where you choose to apply wireless networking may be an issue. Radio signals will reflect off metal surfaces, but will not bend around corners. Unless you can establish a precise reflector, you cannot count on your signal getting around, much less through, metal reinforced walls, metal doors, elevators, dense plumbing, electrical wiring, or similar often hidden obstructions. One of the most common and troublesome hidden obstructions you can encounter is the wire screening used as a support for stucco and concrete construction materials. Another is aluminum siding. These are especially troublesome if you are trying to use your wireless gear between your inside home office and your patio or the neighbor's home. Those who live in wood or vinyl sided structures are better off in this regard. Metal screening and siding, as well as dense metal framing and plumbing or electrical tubing, will block and reflect wireless signals.

Look around you now and consider how many metallic objects are near you. Then walk around and consider how many more objects are between all the places where you would put wireless equipment. Consider everything from your computer monitor and case, file cabinet, recipe box, mini-blinds, window frames and screens, toaster, microwave

oven, coffee maker, range vent hood, oven, cooktop, refrigerator, pots and pans, canisters, soup cans, a roll of aluminum foil, door knobs, hinges, faucet handles, VCR, DVD player, TV set, lamp bases, cubicle walls, and towel dispensers, down to your gold pen and favorite metal travel mug. Inside your walls are electrical wires, conduit, gas, water and vent pipes, metal framing pieces, and hundreds of screws or nails. Each of these is a possible point of reflection for a radio signal. The tiniest objects may be the most significant, as a 2.4 GHz wireless signal wave is only a couple of inches long—matching almost perfectly with a common construction nail. Your signal may also be absorbed by natural objects—trees, plants, leaves, and moist earth.

Blocked or absorbed wireless signals simply mean that the received signal will be weaker than desired, making your network unreliable. Reflected wireless signals, even when you have a line-of-sight path between the transmitter and receiver, can cancel out or jumble the desired signal, making it unusable. It is also possible, especially in nonline-of-sight conditions, for the reflected signals to be stronger than the original signal. Think of a blocked wireless signal like dense fog decreasing visibility and light levels. Think of reflected wireless signals like a mirror ball with light dancing in different directions. You do not see the original light source, just the reflections, which may be decorative, but not very useful to light an object.

You may expect out-of-the-box 802.11b wireless equipment to reach a few hundred feet, 100–300 feet being the typical advertised range. Because 802.11a equipment uses higher frequencies, it is typically limited to 50–100 feet without additional antennas.

Distance and overall obstruction/reflection density are significant technical influences on the success of a wireless network. Distance can be overcome with the use of external antennas (if your device provides such a connection), repeating or network bridging stations to extend the network, and additional access points to distribute the wireless network farther or into difficult to reach places. Neighborhood, campus, and metro area networks require the use of higher elevations at one end to overcome obstructions and improve line-of-sight path opportunities, as well as higher gain antennas and transmitter signal amplifiers to extend their range. Obviously, the more equipment you have to deploy to make the network work, the more expensive it will be.

If interference, signal blocking, or reflections are not of concern, you may have other sources of interference keeping you from deploy-

ing wireless networking—company or other policy being one of them, as well as the risk of signal and, thus, data theft being the other. Without very tight directional antenna patterns, it is possible to receive almost any wireless signal if you can get close enough to it. Most of the time, highly directional antennas are used only to extend a wireless signal between two fixed points, or a mobile user with a directional antenna and a fixed point with a nondirectional antenna. They are generally too large, inconvenient, and expensive to use for each and every client workstation.

A large retail chain store—a computer store selling wireless equipment no less—experienced someone receiving signals from its checkout systems and intercepting the data, including customer information and credit card numbers. The unknown assailant did not hack into the network, but merely listened to and stored what was heard. Wireless networking enthusiasts entertain themselves by driving and even walking around towns and campuses sniffing out wireless network signals—often finding hundreds of different wireless networks in operation within urban downtown areas. Wireless signals essentially cannot be contained. Like a smoker trying to sneak a puff in the restroom, a tell-tale whiff can be detected.

Knowing that wireless signals can be picked up by anyone, as if they had plugged into your wired LAN systems, means that you should probably provide some form of additional security for your data. Then, if someone does get your data, it will be unreadable or useless to them. While 802.11a and 802.11b do provide encryption (WEP) for the data placed on wireless networks, it is a very weak security measure that can be cracked within a few minutes by anyone with the AirSnort program running on a Linux-based computer. The answer to the weakness of the WEP feature is to use additional virtual private network (VPN) software to restrict access to the network and encrypt the data you place onto and take from the wireless network—so that even if someone gets your data, he needs to have the same VPN software and access codes to be able to use it. VPN software is a must among roving corporate users accessing the company network from the variety of dial-up, DSL, cable, and wireless Internet access methods available.

Certainly in very secure environments, from military posts to private research facilities, security experts do not trust any data leaving the immediate area, however well encrypted it may appear to be.

Who Will Design, Install, and Maintain Your Wireless System?

With the plethora of wireless products available in computer stores, it may appear as easy to install and implement a wireless network as it is to replace a computer mouse. Indeed, some products, especially all-in-one client network cards and access point kits, make the process very easy. But as you get further into the subject matter and start to expand the network with products from different companies and use different software, you will find nuances in firmware used in the network equipment, differences in terminology for the same items, different software, and occasionally different channel changing capabilities for different products.

Your best bet is to select a reputable, qualified vendor who can give you references to other customers, who will use high-quality equipment from major manufacturers for dependability and consistency, and who will intentionally design and implement your network for a bit of overcoverage to ensure reliability. The vendor you select should be able to accommodate different types of PCs and operating systems, work with different types of wired-network equipment and your servers, and most importantly, be attentive to your business and users' needs.

Your vendor should be willing and able to do a site survey before, during, and occasionally after your installation to ensure reliability and spot potential problems before and as they occur. The survey process should characterize the building structure to assess obstructions and reflections, and assess the environment for potential sources of interference, as well as interference your network may cause.

Implementation should consider security, vulnerability, and installing measures in addition to WEP. Ongoing maintenance should include changing security codes as employees come and go, just as you would change passwords to e-mail and network servers. You can enhance network security somewhat by using access point equipment that allows you to limit wireless access to only the specific wireless client cards you specify in the access point configuration. To do this, use their media access control (MAC) address—a unique number that identifies each and every network connection. Combining 128-bit WEP encryption between wireless equipment, MAC address control of which equipment can connect to an access point,

and a secure VPN application between clients and networks is about as much as you can do to secure your network.

As part of your vendor selection process, you will also consider the cost of implementing your wireless system—pitting one vendor against the other and the cost of wireless versus wired.

The Cost of Wireless

Adding wireless to or using it as your home network might be more expensive than a few cables and conventional network adapters and a hub—a novelty or luxury. But going wireless at a workplace or places where construction or other issues make installing wires prohibitive may be the only way to go.

Let's compare the costs of installing wired and wireless networks in a typical small- to medium-sized office with 50 people/computers, even without considering whether or not cabling can be installed because of physical constraints.

TABLE 2.1

Cost Comparison Between Wired and Wireless Networks for 50 Systems

Equipment and Labor	Wired Network Cost	Wired Totals	Wireless Network Cost	Wireless Totals
Network Card (50)	$100	$5,000	$100	$5,000
Jacks and Cable Installation (50)	$50	$2,500	0	0
Patch Panels (3)	$400	$1,200	0	0
Patch Cables (100)	$5	$500	0	0
Hub/Switch (2–3)	$400	$1,200	0	0
Access Points (2)	0	0	$400	$800
Workstation Setup (1 hour)	$50	$2,500	$50	$2,500
Total		$12,900		$8,300
Difference				$4,600 less

The simple comparison in Table 2.1 shows you come out way ahead in cost savings when you go with a wireless network solution upon initial installation. With the money you save, you can expand your network by 50 percent for free versus a wired infrastructure. Long-term savings are also cumulative in that you do not have to do as much maintenance when users or systems move from one location to another—no patch cable changes at each end and far fewer bumps on the head from crawling under desks.

The initial and long-term savings could easily pay for VPN software to secure the network if needed. There is also long-term convenience to users, who can move about freely with laptops and take their data with them into conference rooms, meetings, and presentations without worrying about network cables or transferring files to another system or a server and retrieving them on another system later.

Multiply the savings by 2, 10, 20, or 100 times for larger scale implementations and the savings begin to add up to some significant money—enough that your CEO and CFO could be so impressed you could move up closer to CTO, if that is where you are headed.

LAN implementations are not the only place significant savings are apparent by going wireless. Consider simply connecting two nearby office buildings together when your company expands, typically done by running the equivalent of a T-1 carrier circuit or fiber optic thread through an underground trench. The permits and cost of trenching alone are almost prohibitive—well into thousands of dollars of heavy machinery work. Add a couple thousand dollars for burial cable or fiber and about a thousand for interconnect equipment at each end. Compare trenching with about a thousand dollars worth of wireless equipment for both ends and there is no comparison—you are going wireless. In some cases, you may even be able to interconnect directly with a branch office a few miles away via wireless—something that would cost a couple thousand dollars for a Frame Relay or T-1 circuit installation and a recurring monthly cost of $1200 per month. Wired is obviously very expensive.

There are unseen costs of wireless—depending on what your vendor may charge for site surveys, interference checks and remedies, determining reflection and absorption that may affect signals, additional access points to improve coverage, and recurring security maintenance—but they may not be an issue at all in a clean environment and could be absorbed in the overall cost savings versus wired networking.

Summary

If the cost advantages of wireless networking excite you, then things are looking up. Certainly for a small, modest wireless LAN, the cost savings are obvious. Larger networks with more client systems may require different and more costly access point equipment. If your network spans a larger area than one access point or antenna scheme can cover, you will have to work out the design and costs of creating a contiguous, multi-access-point network. We still have a lot of work to do in considering network design, equipment selection, installation and setup time, and eventually performance tweaking. Before you can design, install, and set up a wireless network, you need to know a bit more about the various equipment and configuration options—from access points to antennas, cabling to client software—and that is covered in Chapters 3, 4, and 5.