

© 2002. All rights reserved.
Black Box Corporation.

BLACK BOX[®]

NETWORK SERVICES

802.11: Wireless Networking

A white paper

1.0 Introduction

In the past decade, wireless has grown from an obscure and expensive curiosity into a practical and affordable networking technology. Today's most common wireless standard is 802.11b Ethernet, also called Wi-Fi (Wireless Fidelity). The 802.11b standard is fast enough to be practical and affordable enough for home networks. You can buy the components to set up a wireless network in nearly any store that sells computers.

The convenience of wireless is appealing—you don't have to deal with running cable, and you can move computers anywhere you want and still be connected to the network. Wireless is especially suited for use with laptop or notebook computers, offering users great freedom of movement. But enthusiasm for this new technology sometimes leads to the installation of a wireless network where a wired network would be more effective, economical, and secure. Wireless has shortcomings that make it ill suited for many networks. Yet its popularity and ongoing efforts to improve the technology make it a promising option in the future.

Here we examine current wireless networking technology and its appropriate uses—where wireless networks are suitable and where they are not the best solution. We'll also explain the basics of how a wireless network is designed and how it can be integrated with a traditional wired network.

2.0 A brief history of wireless

2.1 802.11—the first wireless Ethernet

The precursor to 802.11b, IEEE 802.11, was introduced in 1997. It was a beginning, but the standard had serious flaws. 802.11 supported speeds of only up to 2 Mbps. It supported two entirely different methods of encoding—Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)—leading to confusion and incompatibility between equipment. It also had problems dealing with collisions and with signals reflected back from surfaces such as walls. These defects were soon addressed, and in 1999, the IEEE 802.11b Ethernet standard arrived.

2.2 802.11b—wireless Ethernet refined

The 802.11b extension of the original 802.11 standard boosts wireless throughput from 2 Mbps all the way up to 11 Mbps. 802.11b can transmit up to 200 feet (61 m) under good conditions, although this distance may be reduced by the presence of obstacles such as walls.

The 802.11b upgrade dropped FHSS in favor of DSSS. DSSS has proven to be more reliable than FHSS, and settling on one method of encoding eliminates the problem of having a single standard that includes two kinds of equipment that aren't compatible with each other. 802.11b devices are compatible with older 802.11 DSSS devices, but they're not compatible with 802.11 FHSS devices. Also 802.11b differs from standard 802.3 and 802.5 wired Ethernet only at OSI Layers 1 and 2, it's interoperable with standard wired Ethernet. Because it's a real Ethernet standard and looks like Ethernet to your applications, 802.11b is perfectly compatible with both Microsoft® Windows® and Macintosh® OS, as well as more unusual operating systems such as Linux®. 802.11b is the most widely available wireless standard.

2.3 Up-and-coming wireless standards

2.3.1 802.11a

Only recently available, 802.11a uses a different band than 802.11b—the 5.8-GHz band called U-NII (Unlicensed National Information Infrastructure) in the United States. Because the U-NII band has a higher frequency and a larger bandwidth allotment than the 2.4-GHz band, the 802.11a standard theoretically achieves speeds of up to 54 Mbps.

2.3.2 802.11g

802.11g, on the other hand, is an extension of 802.11b and operates in the same 2.4-GHz band as 802.11b. It brings data rates up to 54 Mbps using OFDM (Orthogonal Frequency Division Multiplexing) technology. Because 802.11g is backward-compatible with 802.11b, an 802.11b device can interface directly with an 802.11g access point. You may even be able to upgrade some newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

2.3.3 Availability and usability of newer wireless technologies

802.11a and 802.11g technologies are still quite new to the market. They're more expensive and not as readily available as 802.11b. Also, because these newer wireless technologies have very limited ranges, you may find that you need more access points as compared to 802.11b.

3.0 Considerations before installing

Before deciding to install a wireless network, you should be familiar with wireless and know its strengths and weaknesses. One big advantage of wireless networking is flexibility. Because there are no wires connecting network components, a wireless network gives you the freedom to move your computer to wherever you want it and still be connected to the network. In addition, a wireless network can be easier to install than a wired network, because a properly installed wired network includes running cable, concealing the cable runs, and installing multiple wall outlets.

The disadvantages of wireless are less obvious. Today's wireless networks come with an inherent set of problems ranging from serious security gaps to mildly annoying interference from other devices. Knowing about these limitations is important when deciding which network is right for your use and your area. It's also helpful when following efforts to improve wireless technology, as this work will lead to better networks in the future.

3.1 Security

A primary concern when installing wireless is security. The rapid growth and popularity of wireless networks in both the commercial and residential market led to the use of wireless for many diverse applications, including the transmission of private information. The need for privacy was the impetus to develop wireless security protocols and continues to spur efforts to make wireless a more secure technology.

The current 802.11b Ethernet standard includes a security protocol called Wired Equivalent Privacy (WEP), which encrypts data packets well enough to keep out most eavesdroppers. WEP encrypts each 802.11 packet separately with an RSA RC4 cipher stream generated by a 64-bit RCA key. But several cryptanalysts have identified weaknesses in the RC4's key scheduling algorithm that make the network vulnerable to hackers. Software tools such as AirSnort have already been developed to enable hackers to crack WEP and gain access to wireless networks. These software tools are widely available on the Internet.

Making WEP's encryption system 100% secure is the goal of the 802.11 working group, which began redesigning WEP in August 2001 when it became clear that its underlying cryptography, RC4 algorithm, was unsound. Such efforts should improve the security of wireless networks in the future.

The biggest security problem with wireless technology is that wireless users often either do not activate WEP at all or fail to change the default passwords. When you fail to take these basic precautions, you leave your wireless network vulnerable to casual hacking.

Also, keep in mind that WEP is not the sole means available to protect your wireless network. Even if hackers obtain the WEP key, that doesn't mean they have complete access to information. Other security protocols exist at the higher network and transport layers. You should enable all available security protocols along with WEP.

3.2 Speed and reliability

802.11b claims a speed of 11 Mbps. A more realistic estimate of actual throughput is about 3.5 to 4.5 Mbps without WEP enabled and 2.5 to 3.5 Mbps with WEP enabled. Although WEP can slow your wireless network by 20 to 50%, it's important to keep network speed in perspective. Throughput in the 3.5-Mbps range is still much faster than your broadband Internet access. It's fast enough for most home applications, but is often inadequate for larger office applications, especially in workgroup situations such as in a design firm where a group of people regularly exchange large files.

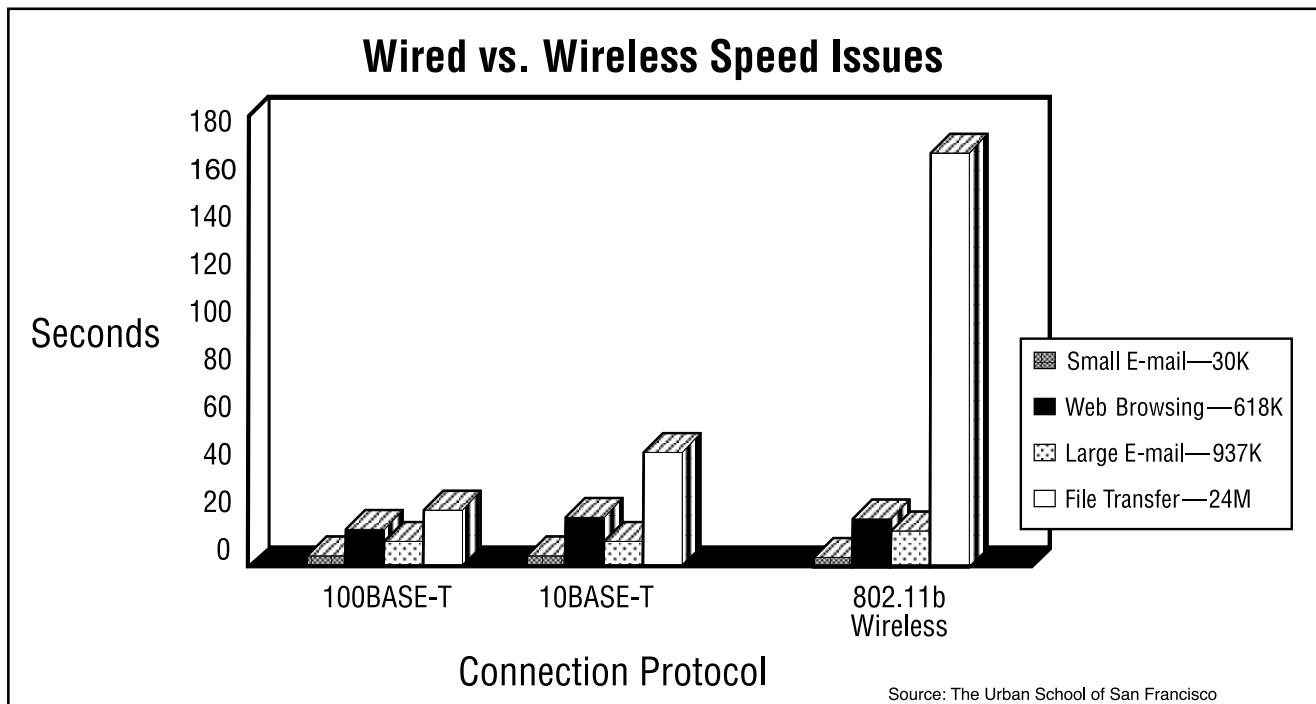
When considering a network, take a realistic look at your bandwidth requirements. If you have more than a few users, regularly transfer large files, or need lightning-fast network response, then wireless is not for you. But in a home environment, wireless can be more than adequate.

3.3 Environmental concerns

Environment can affect your wireless network, and your wireless network may affect electronic devices within your environment. Therefore, take a good look at the space where you intend to install your wireless network.

3.3.1 When your building gets in the way

When you set up your 802.11b network, chances are you won't get the network to operate effectively at more than a fraction of the promised 200 feet. This is because the distance given as the network range is the maximum distance accomplished in open space under ideal conditions.



Walls, desks, cubicles, and other large structural features can interfere with wireless transmission. The wireless network will compensate for some of this interference by dropping to a lower speed, but you're still likely to find that your transmission distance is shorter than anticipated.

Some buildings provide special obstacles to wireless transmission. For example, the solid stone walls, brick, or heavy coats of plaster on lathe in older, historic buildings can interfere with wireless transmission. For this reason, a wireless installation in an old building may require more access points than in a comparable modern building.

3.3.2 *Interference from other electronic devices*

The 2.4-GHz frequency used by 802.11b wireless is appealing for many wireless- and electronic-device manufacturers because the government doesn't require a license to use it. But no license also means there's no entity to coordinate use in this frequency. Interference from and with other 2.4-GHz devices can be a problem with wireless networking, especially in dense urban environments and apartment buildings.

Common devices that can interfere with or have interference caused by your wireless network include:

- Baby monitors
- Garage-door openers
- Cordless phones
- Microwave ovens
- A/V senders
- XM radio
- Energy-saving light bulbs
- Other wireless networks
- Many medical devices such as diathermy machines

Many of these devices, because they share the same 2.4-GHz spectrum, can noticeably degrade your wireless network's performance. A wireless network can also interfere with the performance of other devices operating in the 2.4-GHz spectrum. With devices such as portable phones, this doesn't matter much, but in the case of critical medical devices, a nearby wireless network can be literally life-threatening.

The problem of interference with nearby devices is extremely variable. One network will experience serious slowdowns in an environment that seems very similar to another wireless network that's operating perfectly. Most wireless vendors offer a software program that allows you to monitor the signal strength and connection speed. One way to test for interference is to place an Access Point in your home or business, insert a wireless card in your laptop, and then roam around to evaluate the strength of the signal. This exercise can reveal the areas for placing access points that offer the strongest signal and fastest connection.

Another way to minimize or eliminate interference is to simply remove or reposition the devices that cause it. Keep devices such as microwave ovens at least six feet from 802.11b access points.

3.4 *Ease of installation*

One of the reasons often given for choosing wireless over a traditional wired network is ease of installation. However, keep in mind that all Ethernet networks can be tricky to install. All networks—wired or wireless—require that you install and configure software and this process can be tricky for the novice user. The only thing that makes wireless networks easier to install than wired ones is that you don't have to run CAT5e cable.

3.5 *Compatibility*

Another consideration is whether a planned wireless installation is compatible with your existing network and with any network you may want to install in the future. 802.11b wireless Ethernet is compatible with wired Ethernet networks, with older 802.11 DSSS equipment, and with the newer 802.11g standard. But it is not compatible with older 802.11 FHSS devices and with 802.11a.

Something else to watch out for when considering compatibility is that some vendors—even though they are subject to 802.11b compatibility tests—will decide they have a better solution for speed or security and will build proprietary solutions into their wireless equipment. This means that although in theory *all* 802.11b devices work together—in actual practice they sometimes don't.

4.0 Deciding where to use wireless

4.1 *Appropriate applications for wireless networks*

Wireless is preferred for networks that are temporary, require flexibility, and in which high security is not needed. Some applications suitable for today's wireless networks are:

- Taking laptops to conference rooms for sharing information during training sessions or meetings.
- Quickly setting up temporary networks for temporary employees.
- Simplifying computer hookups for trade show booths. (Be aware, though, that wireless networks can interfere with each other at trade shows. You may want to make backup plans.)
- Connecting to advertising kiosks. Because the kiosks are wireless, you can move them at will. Security is not a major concern.
- Using notebook computers with bar-code readers for keeping track of warehouse inventory

and updating the inventory database in real time through a wireless link.

- A home network, depending on its location and your security needs. If no one lives or parks within 200 feet of your home network, for example, then wireless security concerns are minimal.

4.2 *Where you shouldn't use wireless*

4.2.1 *Networks that hold confidential data*

Any data that needs to be kept private should be kept off a wireless network. Until wireless attains the level of security offered by a wired network, don't use a wireless network to transmit:

- Credit-card numbers. Hackers will often go to a lot of trouble to get at this valuable information even in a highly-encrypted wireless network. Recently reported in the news was the story of a major electronics retailer that had credit-card numbers stolen from its wireless network by a hacker in the parking lot. Even in a home network, make a point of never ordering anything on-line by giving your credit-card number if you are on a wireless computer. Move to your desktop computer on the wired network for that.
- Sensitive financial data. This can be anything from your personal checking account to the inner workings of a major financial institution. In fact, financial institutions often use only fiber optic networks because fiber optics are far more secure than even copper wire.
- Anything you prefer to keep private. If you don't want your personal business known, don't risk broadcasting it over your wireless network.

5.0 **Installing a wireless network**

An 802.11b wireless network can operate in two modes: ad-hoc and infrastructure. In ad-hoc mode, your computers talk directly to each other and do not need an access point. In infrastructure mode, network traffic passes through a wireless access point. An infrastructure-mode wireless Ethernet segment can be easily added to a traditional wired network to make an integrated wired and wireless network.

5.1 *Installing an ad-hoc network*

Installing a simple ad-hoc network in a small area (such as in a home or small office) requires placing wireless network interface cards (NICs) in the PCs. They install just like any other NIC, but usually sport antennas that stick out of the computer's case like little ears. PC-card versions are available for laptop and notebook computers.

5.2 *Installing an infrastructure-mode network*

To install a larger network in infrastructure mode, both NICs and access points must be installed and configured. Placing access points to ensure proper coverage and performance can be tricky. For a smaller installation, simple trial and error will often find the best locations for access points. However, a large wireless network needs some organization. The best way to decide where to place access points is by performing a site survey. This is done by placing access points in various locations around the intended coverage area and recording signal strength and quality.

Network and power connections must also be considered. Often the best place for some access points is on the ceiling. While an access point can easily be mounted on the ceiling, most buildings do not have Ethernet and power connections on the ceiling. A partial solution to this problem is to run just an Ethernet connection to the access point but to use an access point that can be powered through the Ethernet cable. These access points get power from a device in the wiring closet that provides DC power over the unused wire pairs in the UTP Ethernet cable. This feature eliminates the need to run an AC power cable to the access point, making installation easier.

Access points and NICs must be configured after they're installed. Most vendors supply configuration tools with their wireless products, and some even provide for bulk configuration of access points on the same network. Access points can be configured via telnet, Web-based browsers, or SNMP; from a wireless station; or by using a serial console port built into the access point itself.

6.0 The integrated network solution

Wired and wireless networks each have different strengths—wired networks are faster and more secure; wireless is versatile and doesn't require cable runs. However, the ideal network might include both wireless and wired network segments combined into a single, integrated network. An integrated network enables you to take advantage of the flexibility of a wireless network while still retaining the higher security of a wired network for confidential data.

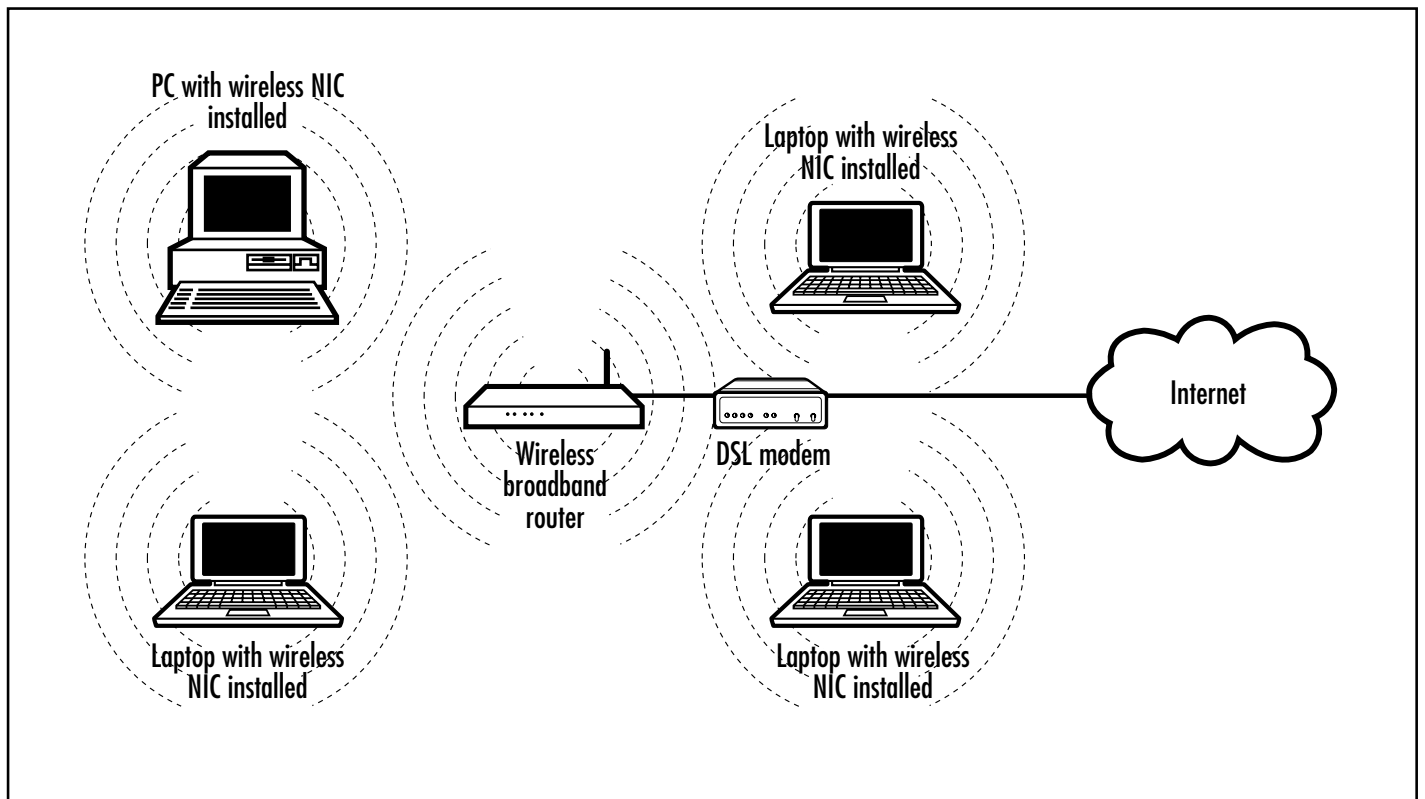
An Ethernet bridge makes this possible by keeping general network traffic off the wireless segment. An Ethernet bridge is a device that connects multiple network segments to create one homogeneous network but still keep one segment (or subnetwork) isolated from another. This division makes the network more efficient because each network segment keeps its traffic to itself. It also makes sure your wireless access points transmit only data going to wireless computers—data traveling on the wired network segment is not transmitted over the wireless network segment.

You do not have to buy a separate Ethernet bridge. An Ethernet switch has bridging capabilities, so installing a switch instead of a hub in your network ensures that each network device gets only that traffic intended for it. Higher-end wireless access points also have built-in bridging and keep wireless traffic separated from the rest of the network.

7.0 Network examples

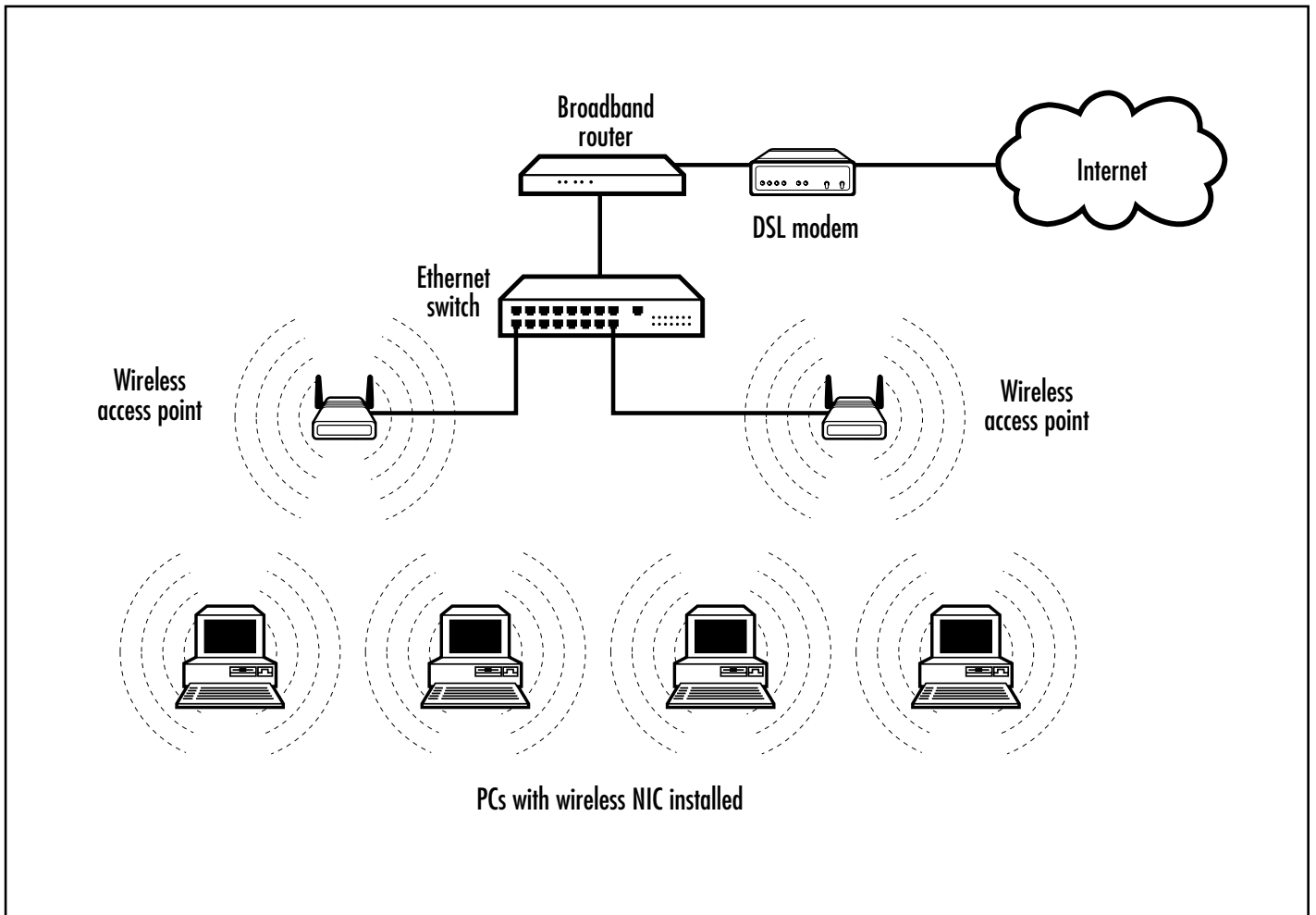
7.1 Ad-hoc wireless network

Ad-hoc wireless networks are an inexpensive and flexible option. An 802.11b network in the ad-hoc mode is entirely wireless. Each workstation relates on a peer-to-peer basis with other workstations. You can add a wireless broadband router to an ad-hoc network to provide Internet access to computers on the network. An ad-hoc network is suitable only for very small installations where security is not an issue.



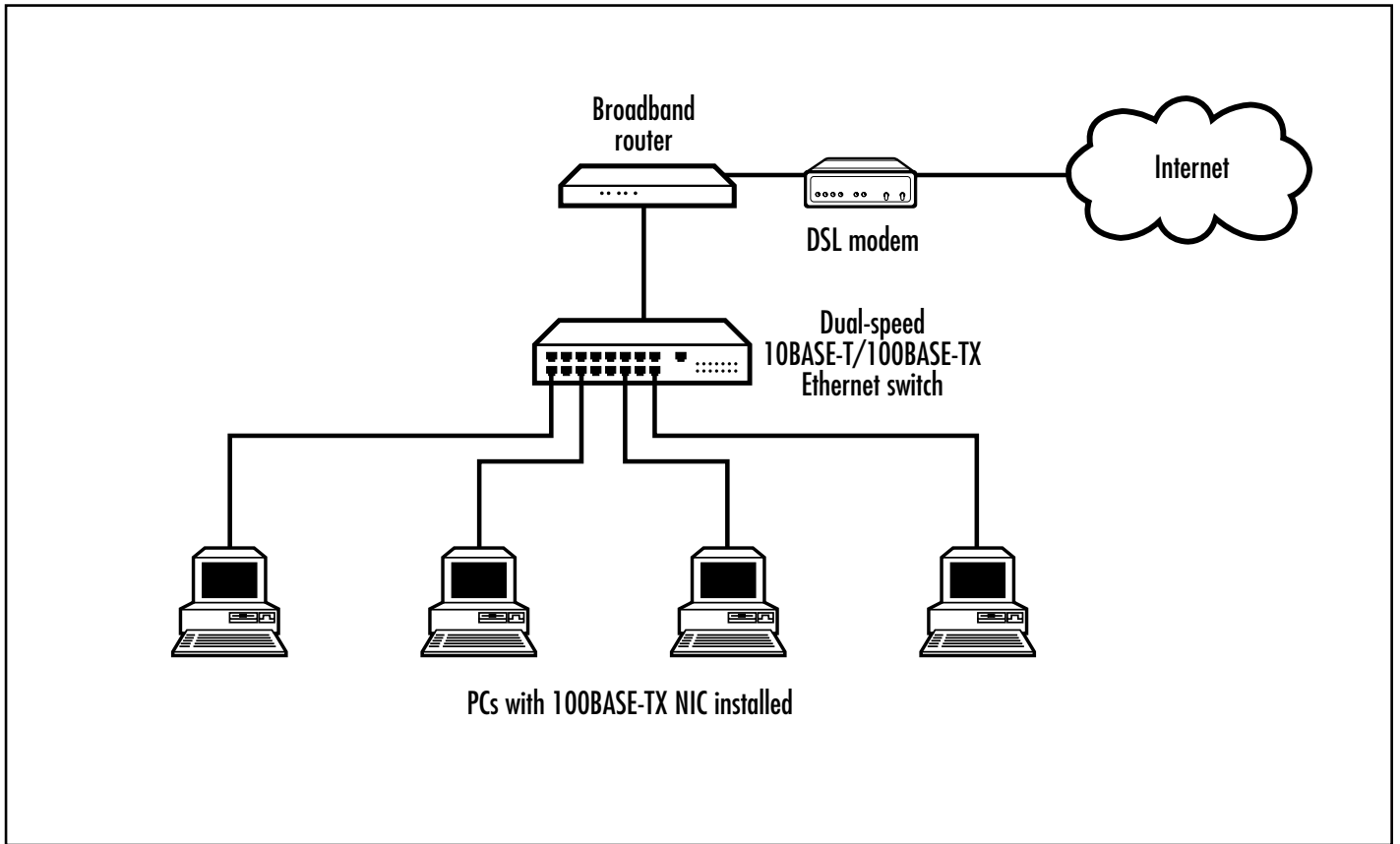
7.2 Infrastructure-mode wireless

For larger installations or for use in larger buildings, choose an infrastructure-mode wireless network. An 802.11b network in infrastructure mode depends on access points connected together. Each workstation communicates with an access point rather than directly with another workstation. Infrastructure mode is suitable for small-to-medium-sized wireless networks, but may not offer enough bandwidth for networks with heavy traffic. And, as with the ad-hoc network, security is still a concern.



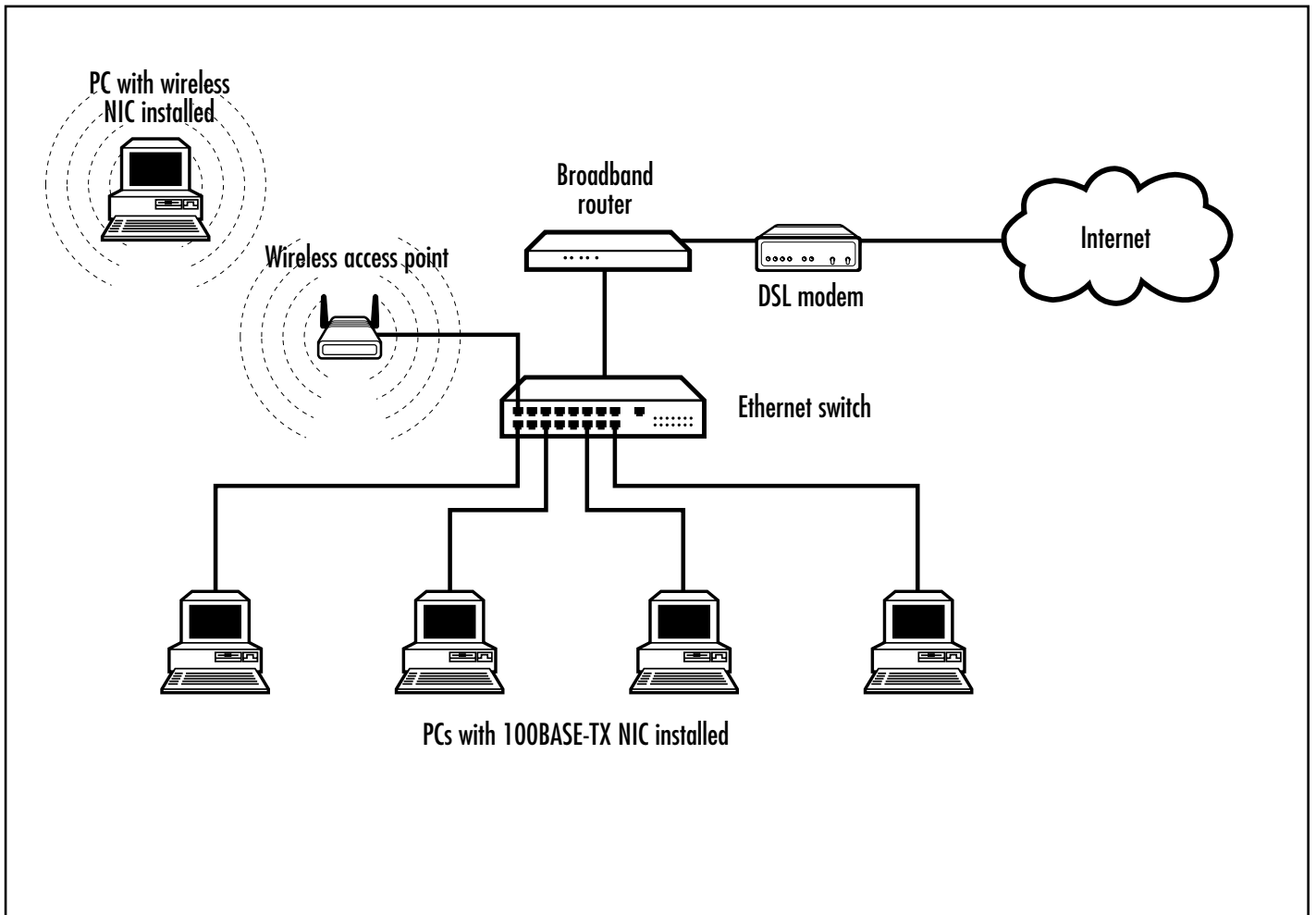
7.3 Wired network (10BASE-T or 100BASE-TX)

A wired network such as this 100BASE-TX network offers both high speed and security. It's easier to support large networks with many users on a wired network. However, a wired network lacks the flexibility of a wireless network—users must stay near a network connection and can't move their computers at will.



7.4 Integrated network

By adding a wireless access point to a wired network, you can build an integrated network that offers the freedom of wireless to some users, while maintaining the security of a wired network for others. Notice that this diagram includes an Ethernet switch rather than a hub. By choosing a switch over a hub, you ensure that each node receives only the traffic intended for it. Higher-end wireless access points include bridging capabilities, which serve to isolate the wireless segment in the same way a switch would. If you use one of these access points, traffic going to the wireless segment stays isolated from general network traffic even if you use a hub.



8.0 Conclusion

Planning your network up front can save a lot of expense and inconvenience later. Black Box recommends that you assess and list your network requirements before you decide what kind of network to use. Consider factors such as:

- Security requirements
- Bandwidth requirements
- Environmental factors that may interfere with wireless transmission
- Ease of installation
- Total number of network users
- Number of laptop users who will want wireless connections

802.11 wireless is a young technology that has come a long way since its inception, and considerable work is still necessary before this technology becomes a viable option upon which to base a big, multi-user network. You should evaluate your environment based on the above factors to determine the type of network that best fits their requirements. In some cases, an integrated network of both wired and wireless may be the best solution.

Whether you're interested in a commercial or residential application, and whether you're considering a wired, wireless, or integrated network, Black Box can provide. We'll supply the products and technical service required to plan, design, install, and maintain the network that's best for you.

Black Box is the world's largest technical services company dedicated to designing, building, and maintaining today's complicated network infrastructure systems. Black Box services clients of all sizes in 132 countries throughout the world.