

# How to Set Up a Wireless Network

In the relatively short time since the debut of wireless networking, incredible strides have been made in its ease-of-use, speed of transmission and security. Yet the range of products and “alphabet soup” jargon can seem daunting to new users.

If you are tired of a maze of cables and possibly tripping over them, it may be time for your small business to go wireless. On the following pages you can find out just how easy it is to set up a wireless network. With the wide range of wireless equipment and configurations available, you can deploy a wireless network on any budget, then scale as your business grows.

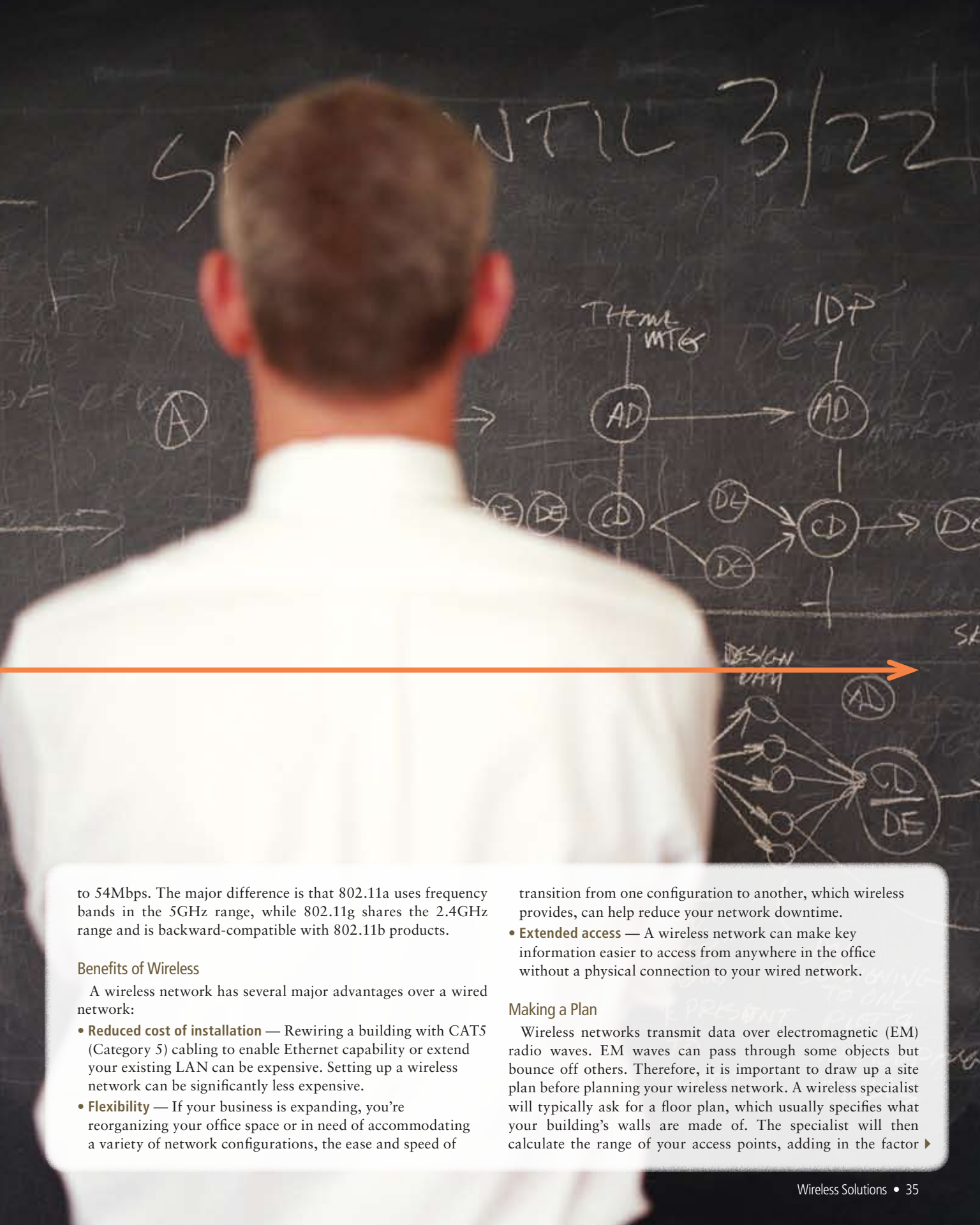
## Understanding Wireless

Wireless technology is any method of delivering data through the air, including radio, cellular, infrared and via satellite. The most commonly used wireless technology for business networks is called Wi-Fi (wireless fidelity) and is based on the technical specification of 802.11, developed by the Institute of Electrical

and Electronics Engineers (IEEE).

802.11 technology uses the radio frequency (RF) spectrum to transmit and receive data from one device to another without using wires. A radio transceiver is built into an access point, which negotiates a connection between the end user and the wired LAN (local area network), hooking the user up to the LAN in the same way a cable would. Understanding the basic science of radio waves is useful when designing your wireless network, allowing you to anticipate possible complications such as attenuation, channel spacing and signal-to-noise ratio.

The 802.11 family of specifications includes 802.11b, which uses the direct-sequence spread spectrum (DSSS) method of communication and provides 11Mbps transmissions in the 2.4GHz bandwidth. 802.11a and 802.11g specify orthogonal frequency division multiplexing (OFDM) and enable data rates up



to 54Mbps. The major difference is that 802.11a uses frequency bands in the 5GHz range, while 802.11g shares the 2.4GHz range and is backward-compatible with 802.11b products.

### Benefits of Wireless

A wireless network has several major advantages over a wired network:

- **Reduced cost of installation** — Rewiring a building with CAT5 (Category 5) cabling to enable Ethernet capability or extend your existing LAN can be expensive. Setting up a wireless network can be significantly less expensive.
- **Flexibility** — If your business is expanding, you're reorganizing your office space or in need of accommodating a variety of network configurations, the ease and speed of

transition from one configuration to another, which wireless provides, can help reduce your network downtime.

- **Extended access** — A wireless network can make key information easier to access from anywhere in the office without a physical connection to your wired network.

### Making a Plan

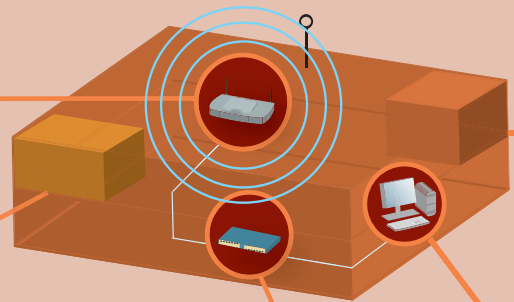
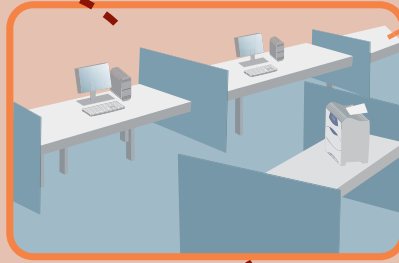
Wireless networks transmit data over electromagnetic (EM) radio waves. EM waves can pass through some objects but bounce off others. Therefore, it is important to draw up a site plan before planning your wireless network. A wireless specialist will typically ask for a floor plan, which usually specifies what your building's walls are made of. The specialist will then calculate the range of your access points, adding in the factor ▶

## Freedom From Wires

A wireless network allows you the freedom to roam from room to room, between floors, and throughout your building with ease, and allows for growth as your business grows.



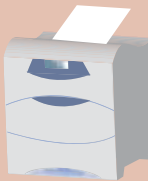
Allow your staff to have access to key information without being physically connected to the wired LAN.



Access Point

Switch/Router

Local Area Network



Print from print servers using wireless adapters.

of various antennas. These calculations will help formulate the critical aspects of your wireless implementation.

For more detailed help, a trained outside consultant can map out the area where your wireless network will be deployed and determine the appropriate number of access points and antennas. The consultant will typically review a building layout blueprint before coming in to map your specific network. They test thoroughly for access signal strength and throughput, making sure that each user will receive the appropriate network quality they need. A building's walls, floors and other obstacles, including people and distance, contribute to attenuation, or a reduction in signal strength during transmission.

The farther a computer is from an access point, the more the signal degrades, slowing the connection. Because of this, larger offices usually install several access points with overlapping ranges. In an environment free of obstructions, access points can be up to 300 feet apart. Otherwise, 50 feet is the normal maximum range. Antennas enhance the radio frequency coverage and/or extend the range of a wireless network. Point-to-point bridges provide wireless connection between two LANs.

The 2.4GHz frequency range used by wireless networks is also shared with equipment such as microwave ovens and some cordless telephones, which may cause additional interference. Interference from other transmissions contributes to the noise level, which should stay as low as possible. Comparing the radio signal strength to the noise level gives the signal-to-noise (S/N) ratio, which is one of the most telling numbers when evaluating the effectiveness of your wireless network.

Using specialized software and tools, your consultant can recommend any adjustments you need in a customized report. These efficient site planning and RF analysis tools enable the consultant to quickly determine your coverage model.

If your wireless implementation requires five or more access points, you should consider wireless management. Several manufacturers provide management for multiple access points. Whether you have Cisco, D-Link, Linksys or Proxim, existing software can handle management of heterogeneous wireless implementation.

Your plan should also account for security. If you are in a shared building, be aware of potential signal leakage. You may consider additional authentication methods to verify user identities or choose to include a VPN and encryption/authentication.

### Purchasing the Components

To create a wireless network, the three major components are access points, wireless-equipped client devices and a router or switch. To connect a wireless network to the Internet, you will need a broadband Internet connection, such as a partial or whole T-1 line or, for smaller offices, a DSL (Digital Subscriber Line) or cable connection.

Access points (APs) are key to connecting a wireless network because they transmit and receive the RF signals carrying the data. Access points may operate in a single frequency band, such as 802.11b, or in dual band to provide expanded access to all mobile users. For example, a Wireless A+G access point would provide service to anyone using 802.11a, 802.11b or 802.11g devices. An access point contains a radio transceiver, an antenna, communications and encryption software and an Ethernet port for a cable connection to a router or switch.

Many client devices — such as notebook PCs, handhelds, printers and others — have wireless functionality built right in. If a client device doesn't have a wireless adapter, it may easily be added with a wireless LAN card. A wireless LAN card is a PC card for a notebook computer; or a PCI adapter from manufacturers such as Cisco, Proxim, D-Link, Linksys, NETGEAR and 3Com; or a Universal Serial Bus (USB) adapter for a desktop computer. Printers and handhelds also use cards to enable wireless communications. The adapter functions as a network interface card (NIC), allowing the client to connect to the network through a wireless access point.

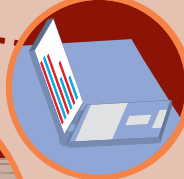
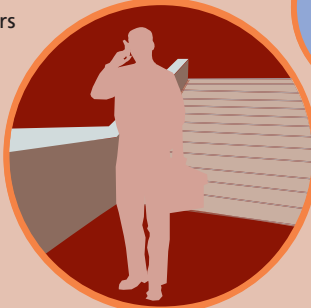
### Getting Connected

First, set up your access points at the place you determined in your plan. Connect the access points to your wired Ethernet router or switch. If you have a completely wireless network, connect to your Internet broadband modem or router. Power



Wireless capabilities make presentations easy with multimedia applications streaming from a notebook or PC. If the notebook or PC does not have built-in Wi-Fi support, a Wi-Fi adapter can be added.

Mobile wireless workers have the advantage of network access, anywhere or anytime, through high-speed Internet access at convenient public locations called hotspots.



## Steps to Your Wireless Solution

- 1 Connect your wireless access points to your switch or router.
- 2 Ensure all your computers are wireless-equipped.
- 3 Configure the SSID (Service Set Identifier) on your access points and computers to establish wireless connectivity.
- 4 Configure encryption keys and access codes to help protect your wireless network from unauthorized access.

over Ethernet (PoE) simplifies access point installation because it eliminates the need for power outlets.

Second, ensure that all of your computers and related equipment are equipped for wireless connectivity. For those that aren't, you can easily install an adapter card or USB adapter. Adapter cards slip into PCI slots on desktop computers or into PC slots on notebook computers, tablet PCs or handhelds.

Third, configure the SSID (Service Set Identifier) on your access points and on your computer; this helps distinguish wireless networks from each other. Access points are shipped with defaults set by the manufacturer. You need to change these defaults as an initial security measure. Reset your SSIDs with strong passwords made up of a mixture of letters and numbers. The documentation that comes with your access points and wireless cards will also provide details on how to set your SSIDs.

The final step is to complete all security configurations, starting with all the basic security built into your wireless devices. Then you can determine if you also want additional capabilities, like 802.11x user authentication. Read the documentation included with your access point to make sure that you have enabled all the options.

### Using Your Wireless Network

The goal of wireless networking is a transparent network connection for the end-user. Power users who chew up bandwidth with rich media applications may prefer a wired LAN connection. However, the majority of users will experience no appreciable quality-of-service issues.

Maintaining your wireless network security requires understanding the various and ongoing threats and the solutions created to address those threats. The following tactics can help:


- **MAC addressing:** MAC (media access control) addressing

allows you to control network access by identifying the unique hardware identification number assigned to each network device you approve. Your access point can be programmed to communicate only with approved MAC addresses, and it maintains the approved addresses in a password-protected table. Devices with unauthorized MAC addresses are denied access.

- **WPA encryption:** Configuring your encryption with WPA (Wi-Fi Protected Access) is similar to the previous standard, WEP (Wired Equivalent Privacy), but more secure. You supply a password, which will generate an initial key that you share with users for authentication. This leaves the actual encryption keys to be generated transparently. These keys are continually and automatically recycled, and so quickly that they can't be hacked using current technology.
- **VPN security:** Virtual private network (VPN) security devices, such as those produced by Cisco, SonicWALL and WatchGuard, provide a gateway through which your network traffic passes. This is especially useful for users who work from home or outside your building.

### Wireless Network Monitoring

To troubleshoot your wireless network, testers such as the Fluke Etherscope Network Assistant are available. It automatically scans all wireless LAN channels in the 2.4GHz and 5GHz bands to identify all detected networks, access points and clients.

Establishing a wireless network and wireless security policy can be the best strategy for eliminating ad hoc wireless networks and the security risks that follow them. Now is the time to discover how wireless networks offer affordable technology, low installation costs and inherent scalability — ideal for small businesses on a tight budget. 



Support your IT capabilities with wireless network technology services from CDW.