2004-11-01

Install Your Own Wireless Network

William G. Heninger
heninger@byu.edu

Craig J. Lindstrom

Bryce H. Peterson

Marshall B. Romney

Original Publication Citation

Install your own wireless network, Journal of Accountancy Volume 198, Issue 5, Pages 51-57, American Institute of Certified Public Accountants, Jersey City, NJ, 11, 24.

JOURNAL OF ACCOUNTANCY

TECHNOLOGY WORKSHOP

Install Your Own Wireless Network

Access your computer, printer and peripherals without cables.

BY BRYCE H. PETERSON, WILLIAM G. HENINGER, CRAIG J. LINDSTROM AND MARSHALL B. ROMNEY

NOVEMBER 2004

Key to Instructions
To help readers follow the instructions in this article, we used two different typefaces:
■ **Boldface type** is used to identify the names of icons, agendas and URLs.
■ Sans serif type indicates the names of files and the names of commands and instructions users should type into the computer.


ould you like to access the Internet, your printer and your other computers, including laptops, without stringing wires throughout your office or home? The solution is a wireless local area network (WLAN) and we'll tell you how easy it is to install one yourself at a nominal cost.

WLANs replace conventional wires with devices called wireless access points that plug into any electrical wall socket. WLAN hardware contains miniature transmitters and antennae that send and receive radio signals to and from your computers and other peripherals.

In order to determine how many access points you will need and where they should be placed, sketch the layout of your home or office. Consumer-grade access points have an average effective indoor range of up to 150 feet, though thick concrete walls, metal wall studs and appliances can reduce that range. A small office may need just one access point, which can cost as little as $70. Powerful commercial devices, which provide coverage of extended areas, either indoor or outdoor, cost as much as several thousand dollars.

You also will need to install in each computer, printer and peripheral a wireless network interface card (NIC), which contains a transmitter and antenna to send and receive signals from an access point. Wireless NICs cost from $40 to several hundred dollars. A $40 model is adequate for a home or small office WLAN.

SELECT THE STANDARD

When you shop for wireless equipment, you will be asked which of three industry WLAN industry standards you plan to employ —802.11b, 802.11a or 802.11g. All wireless equipment uses one or more of these standard specifications. The 802.11b designation was the first to be deployed and is the most widely used. The "a" standard was introduced next but is not widely used because it isn't compatible with "b" devices. The "g" standard is the newest and the most versatile; it's compatible with both "a" and "b" (see " ABGs of WLAN ").

The ABGs of WLAN
There are three WLAN specifications: 802.11b, 802.11a and 802.11g. Therefore, it is important to make sure your hardware is compatible.

You need to check the letter following 802.11—that is, *b* , *a* or *g* . The "b" designation came first and is the most widely used standard. The "a" standard was next. However, it is not widely used, primarily because of its incompatibility with "b" devices.

In 2003 the "g" standard was introduced, and it is "backward-compatible" with "b" but not "a." The "g" has an effective indoor range of about 150 feet and almost five times the transmission output of a "b" and costs only a few dollars more—clearly a wise choice for a small office WLAN.

The "g" standard not only sends digital music as effectively as "b," but it also sends video and increases the rate of file

transfers (text, graphics and digital photographs) over the wireless network. The 802.11g is capable of operating faster than most high-speed Internet connections. As a result don't expect to see any increase when using "g."

For our example, we will use equipment designed for the "g" standard, a Linksys Wireless Access Point Router, which costs about $70, and two Ethernet cables, costing about $5 each.

Configuring the WLAN takes no more than an hour or so. Follow along with us as we provide the steps.

The Linksys does multiple tasks. As a wireless access point it creates the connection to your network. Its four ports also let you connect wired devices. And as a router it allows the office network (wireless and wired) to share a high-speed cable or DSL Internet connection; a dial-up connection is not recommended because it is too slow.

Since the Linksys provides both wired and wireless local area network (LAN) access, you also can plug a desktop computer into it for a wired connection.

Even though our example is hardware-specific, the guidance we present can be followed with slight modifications when using other brands.

LOAD LAPTOPS

We will prepare laptop wireless equipment first.

Step 1. Many new laptops come with a NIC already installed. If your laptop lacks it, you will need to install one by following the instructions provided by the vendor. Usually you can slide the credit-card-sized NIC into the laptop's PC-card slot. You'll also have to load the wireless software, which will be provided on a CD-ROM with the NIC, onto the laptop.

Step 2. Plug one end of the first Ethernet cable into the network port on the desktop PC. You usually can find the slot on the back of the computer (it looks like an oversize telephone jack).

Step 3. Plug the other end into any one of the four ports labeled LAN on the wireless access point router (see exhibit 1 , below). Nearly all new desktop computers have built-in network ports. If yours is more than a few years old and doesn't have them, you may need to install an Ethernet 10/100 NIC into one of the expansion slots.

Exhibit 1

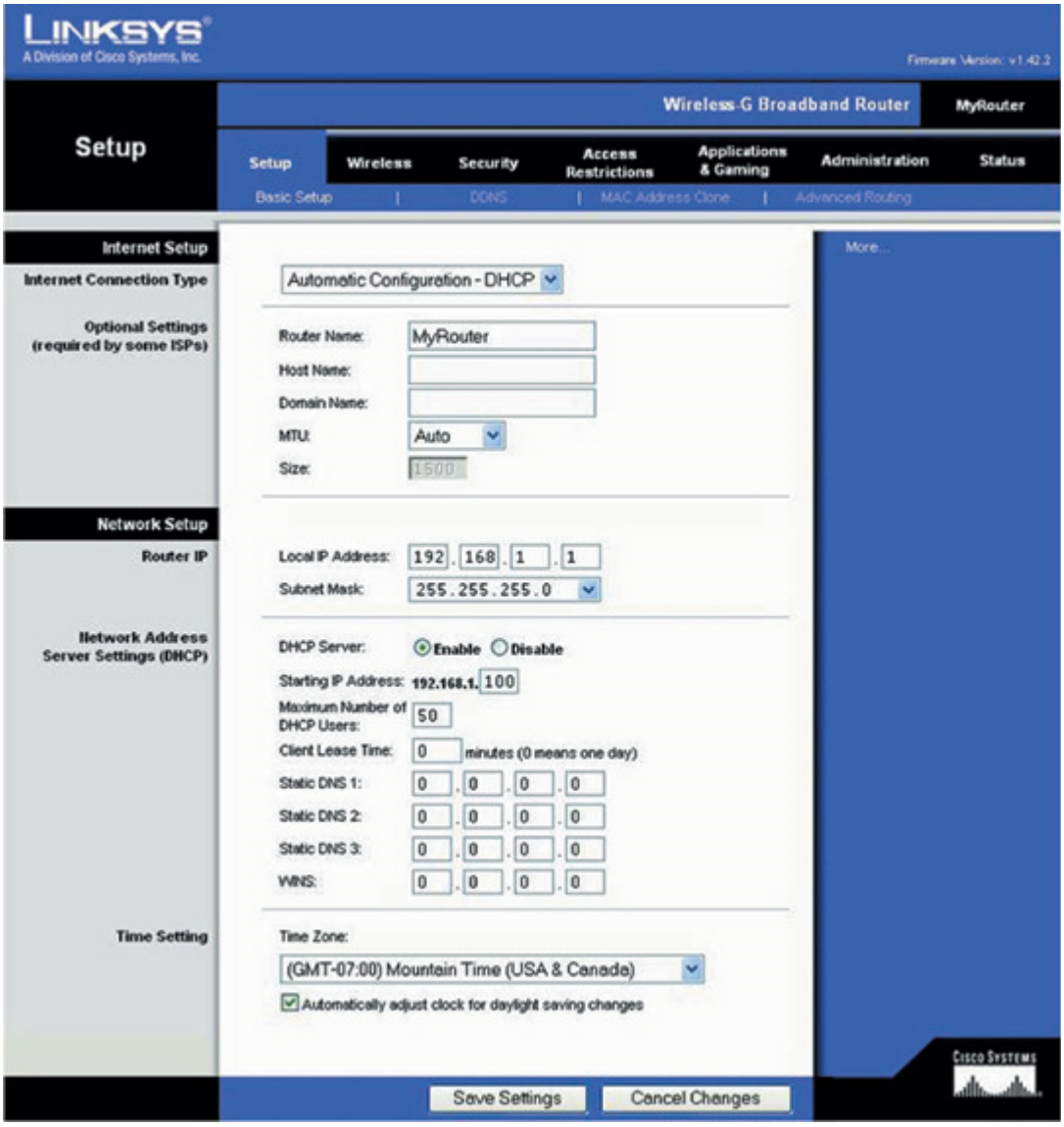
Step 4. To allow multiple wired and wireless users to access your high-speed Internet connection simultaneously, plug one end of the second Ethernet cable into your DSL or cable modem and the other end into the Internet port on the access point router. Be sure to review the policies of your Internet service provider (ISP) to determine the maximum number of concurrent users allowed on your Internet connection.

Step 5. Plug in the access point router, wait a few minutes and then turn on the PC and laptop. To verify connectivity between the PC and the access point router, check to be sure the tiny light-emitting diode lights are illuminated; they're usually situated on the network port on the back of your desktop PC. If they aren't illuminated, you probably failed to connect the desktop PC to the access point router or to turn on the computer or access point router.

The laptop now is configured. Next we prepare the network devices, which need two pieces of information to communicate: an Internet protocol (IP) address on the network (four sets of numbers) and a subnet mask. Some network devices are configured automatically, but doing it manually is not difficult, although, as you'll see, it involves many steps.

Step 6. Start with the access point router; in this case it's the Linksys. To access the configuration interface, fire up the PC's Web browser and type in the address bar 192.168.1.1 —the default LAN IP address for the Linksys. If you're using an alternative brand, follow the documentation. You will be prompted for a username and password. Since the Linksys has no default username, leave this field blank. Type the password, admin , click on **OK** and a **Setup Configuration Screen** will appear (see exhibit 2).

Exhibit 2



Step 7. The screen has several parameters and each must be configured:

■ **Internet Connection Type.** This is the type of configuration you want for your wide area network (WAN) port. If you are using a high-speed Internet connection and have not leased a fixed or static IP address from your ISP, leave this field at "Automatic Configuration-DHCP." Your ISP will automatically supply the access point's WAN interface with an IP address and other configuration parameters.

If you have leased a static IP address, ask your ISP for the WAN IP address, the subnet mask, the default gateway and domain name system (DNS) servers' IP addresses. Select Static IP and enter that information.

■ **Router Name.** Pick an identifier of your choosing.

■ **Host Name.** Call the ISP's customer support line to determine whether you need a Host Name. If not, leave this field blank.

■ **Domain Name.** Leave it blank.

■ **MTU.** This specifies the largest packet that can be retrieved from the Internet. Leave this setting at **AUTO** .

■ **Local IP Address.** Leave the default IP address unchanged unless you have a sound understanding of IP addressing.

■ **Subnet Mask.** If you left the IP address unchanged, leave the subnet mask unchanged at **255.255.255.0** .

■ **DHCP Server.** Leave this setting at **Enabled** .

■ **Starting IP Address.** We suggest using the default **Starting IP Address** .

■ **Maximum Number of DHCP Users.** This shows the maximum number of computers the DHCP server should assign addresses to. The default for Linksys is 50, but the maximum is 253. You may change it to accommodate the number of computers accessing your network.

■ **Client Lease Time.** We recommend using the default **Client Lease Time** .

■ **Static DNS 1–3.** The domain name system is the method the Internet uses to translate Web site names into IP addresses. You can enter up to three here if you know the IP addresses, or your ISP will provide one for you. Otherwise, leave these fields at **0** and your computers will use your ISP's DNS servers.

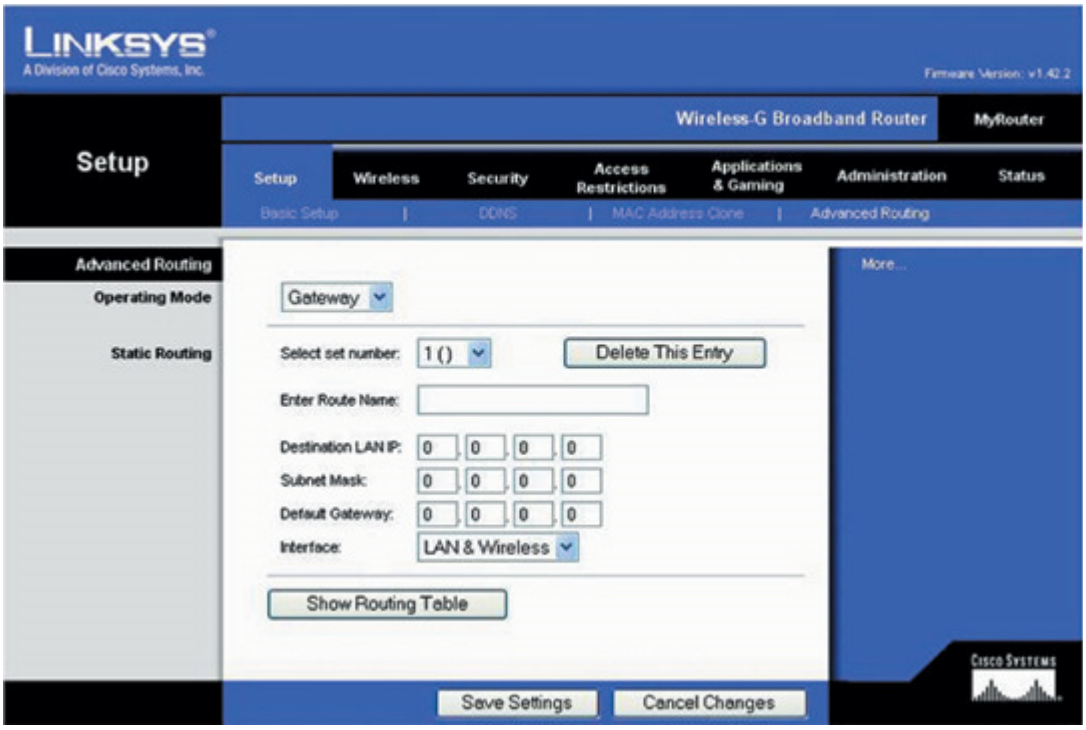
■ **WINS.** If you are using a Windows Internet naming service (a small office or home probably would not), then fill in its IP address; otherwise leave the fields at **0** .

■ **Time Zone.** Set your time zone.

Step 8. When completed, the setup screen should resemble exhibit 2 , above. After you've entered the appropriate data in all of the required fields, click on **Save Settings** at the bottom of the screen.

Step 9. Then click on the **Advanced Routing** subtab in the upper right-hand portion of the setup screen. This generates a screen (exhibit 3) that allows you to enable network address translation (NAT) so that your laptop can communicate on the Internet using the access point router's public IP address.

Exhibit 3



Your wireless access point router will substitute its public IP address for your laptop's private IP address. Select **Gateway** as the **Operating Mode** and you will not need to enter any **Static Routing** information. Click on **Save Settings** .

Step 10. Next, click on the **Wireless** tab at the top of your screen (exhibit 4) to set the basic wireless settings and security features.

Exhibit 4

The screen has four parameters:

■ **Wireless Network Mode.** This identifies the networking standards available to your network. Leave this field at **Mixed** so that both 802.11g and 802.11b devices can communicate with your wireless router. If you have only “g” devices, selecting **802.11g** may provide slightly better performance than setting it at **Mixed** .

■ **Wireless Network Name (SSID).** The initials SSID stand for service set identifier, the public identifier for your access point. Wireless workstations use the SSID to find and connect to your WLAN. You can keep the default SSID at **linksys** or change it to another value such as your name. This name will pop up in the taskbar in Windows XP when your client computer senses the presence of an access point.

■ **Wireless Channel.** This is the specific communications channel your access point will use to broadcast its radio signals. Use the default channel **6-2.437GHz** .

■ **Wireless SSID Broadcast.** This determines whether your access point will broadcast the SSID. Check the **Enable** radio button.

Step 11. Next, click on the **Wireless Security** submenu tab at the top of the screen to open the screen shown in exhibit 5 . The screen has several parameters that must be set. They are

■ **Security Mode.** Set it at **WEP** (wired equivalent privacy), the most basic standard security mode, or if you are content with no security, select **Disable** .

■ **Default Transmit Key.** Leave the default key setting at **1** .

■ **WEP Encryption.** Choose between the 64- and the 128-bit encryption key. We suggest using the more secure **128-bit** key.

■ **Passphrase.** Select a random set of characters of your choosing used to create a random WEP key. We used cpa .

■ **Keys 1–4.** Select any of four keys generated from the encryption algorithm. You can choose one (we chose **Key 1** for our example) and enter it in the wireless NIC configuration settings for each device. See the installation instructions provided by your NIC vendor on how to enter your WEP key on each device.

Exhibit 5

Step 12. We will now create a password and configure the administration settings for the wireless access point router. To do that, click on the **Administration** tab so your screen looks like exhibit 6 .

Exhibit 6

In the two fields provided, create a password and re-enter it to confirm. Keep the password in a safe place; if you forget it, you must reset the router by pressing and holding the **RESET** button on the back for 10 seconds, which will change all of your settings back to their factory default settings.

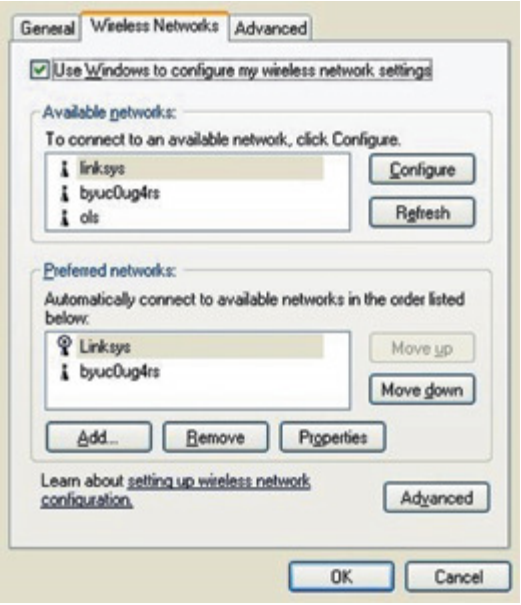
- For increased security, leave **Remote Management** at **Disabled** .
- Leave **UPnP** (Universal Plug and Play) services enabled.

Finally, click on **Save Settings** .

Your wireless access point now is configured and you can close the Web browser.

Step 13. Finally, you have to configure your laptop to join the network. Go to the laptop's **Control panel** (**Start** , **Settings** , **Control Panel**) and click on the **Network Connections** icon. Then right-click on your wireless NIC's icon and select **Properties** to open the **Wireless Network Connection Properties** screen (exhibit 7).

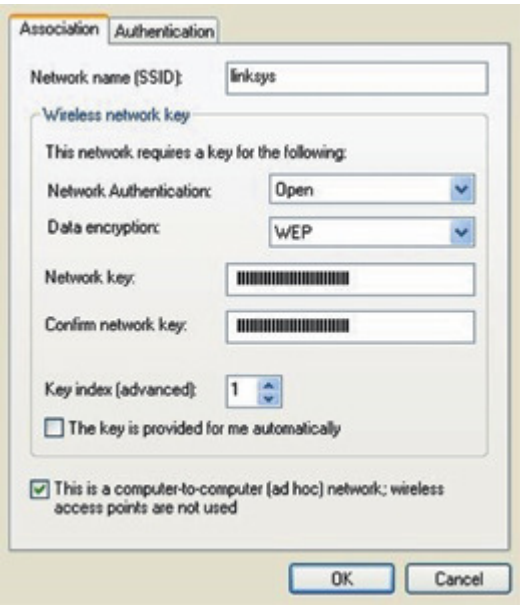
Exhibit 7



Choose **Wireless Networks** to configure your NIC, which tells your laptop which wireless network to connect to. If there are no other access points within range of your laptop, you will see only your access point's SSID listed. If there are multiple access points within range (for example, your next-door neighbor's WLAN), you will need to select your network (in this case it's Linksys) in the **Available networks** window.

If you enabled WEP on your wireless access point router, you'll need to configure a WEP key on your laptop by selecting your network (**Linksys** , in our example) in the **Available networks** window and clicking on **Configure** to produce the Wireless Network Properties window (exhibit 8).

Exhibit 8



Step 14. Click on **Association** to configure your security parameters as shown in exhibit 8 and select **Open** in the **Network Authentication** box. Since we are using **WEP** , select WEP in the **Data encryption box** and uncheck the **The key is provided for me automatically** box. Enter your WEP key in the **Network key** and **Confirm network key** boxes. This key was generated in the access point configuration (see exhibit 5). Since we are using **Key 1** in this example, we will leave the **Key index** (**advanced**) field at **1.** If you selected one of the other three keys, change the **Key index** field accordingly. Finally, click on **OK** to return to the **Wireless Network Connection Properties** screen (exhibit 7). Make sure your network is first in the **Preferred Networks** list (the lower box in exhibit 7) and then click on **OK** . Because you have enabled your wireless access point to act as a DHCP server, you will not need to configure any other network properties. Your laptop now is configured.

To test your WLAN, access the Internet from your laptop and walk around in your transmission range. You now can enjoy the convenience and flexibility of wireless networking in your office or home. ■

BRYCE H. PETERSON, master's in information systems management (MISM), is an associate in the risk advisory services practice at KPMG LLP in Phoenix. His e-mail address is bpeterson@kpmg.com . WILLIAM G. HENINGER, CPA, PhD, is an assistant professor at Brigham Young University, Provo, Utah. His e-mail address is bill_heninger@byu.edu . CRAIG J. LINDSTROM, MS, Microsoft Certified Systems Engineer + Internet (MCSE+I), Cisco Certified Network Associate (CCNA), is an assistant professor at Brigham Young University. His e-mail address is craig_lindstrom@byu.edu . MARSHALL B. ROMNEY, CPA, CFE, PhD, is the John and Nancy Hardy Professor of accounting and information systems at Brigham Young University. His e-mail address is mbr@byu.edu .

Is Someone Eavesdropping on You?

B efore installing your wireless network, here's a question you must ask: Is my wireless network safe from eavesdroppers?

If you don't build security into the system, practically anyone passing by with a portable computer and an inexpensive wireless network card can not only read your e-mails, but also can dip into your stored data files and pluck out anything at will.

In 2002 a wireless security firm conducted drive-by tests in Atlanta, Chicago and San Francisco. Armed with a wireless-equipped laptop, staffers drove the downtown streets of those cities and found that of the 1,136 WLANs detected, they could easily tap into 57% of them because they had no protection at all. A similar test in Spokane, Washington, found 70% of the 650 detected networks were vulnerable to eavesdropping because they, too, lacked secure configurations.

The message is clear: Don't operate a WLAN without security.

Why are wireless networks more vulnerable than wired networks? The feature that makes them convenient—easy access via over-the-air radio links—is the same feature that makes them vulnerable. A data thief need only be within range of the wireless data transmitter (access point or wireless card) to intercept network transmissions. Controlling network transmissions on conventional wired networks is much easier because the transmissions are limited to the physical wires conducting them.

Since a wireless system cannot block anyone from picking up its broadcast signal, the obvious protection is encryption—that is, encode the information so it cannot be understood by an eavesdropper. Until recently, the available solutions were not very effective, but engineers have developed enhanced security standards. The most recent standard is called Wi-Fi Protected Access (WPA). It not only requires stronger encryption keys and techniques than previous standards, but additional user authentication, too. More details about WPA can be found at www.wifialliance.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf .

WPA-compliant devices now are widely available commercially and they are quickly replacing WEP as the default security standard. Most new access points support WPA as well as WEP. Many existing access points may be upgraded to support WPA via a simple software update. Check with your wireless access point router's vendor for update availability. All you have to do is download the new WPA-compliant software from your wireless vendor and you'll be protected.

On the Horizon

The future of wireless security will be determined, in large part, by the anticipated release of the next standard, 802.11i, which will include, among other things, an even stronger encryption algorithm called advanced encryption standard (AES). AES, which has yet to be breached, is used by U.S. government agencies.

Even though the "i" standard will provide enhanced security for wireless networking, the costs of this new technology may be a barrier for some small CPA offices. However, as the technology is more widely adopted, even small offices will be able to afford it.