

The Dawn of the Wireless Renaissance It's Time to Go Wireless!

Although we're constantly hearing about the miracle of wireless technology, we're merely at the dawn of the Wireless Renaissance. From Auckland New Zealand to Mt. Everest, Internet cafes and other wireless hot spots dot our increasingly interconnected globe (yes, there really is an Internet Café at a Mt. Everest base camp), but the best and most ingenious use of this breakthrough innovation is yet to come. For now, the wireless gold standard is 802.11g - the newest, fastest and most powerful 802.11 radio technology that broadens bandwidths to 54 Mbps within the 2.4 GHz band. Because of backward compatibility, older and slower 802.11b radio cards can interface directly with an 802.11g access point and vice versa at 11Mbps or lower, depending upon range.



We've come a long way, baby - just in the past couple of months. That's how rapidly the wireless net that will someday encompass the entire globe is morphing. Much quicker than we write these words, technicians are gleaming new ideas that will revolutionize the way we communicate. From Marconi (the inventor of wireless communication back in the late 19th Century) to 802.11g - the sky is not the limit for how far we will take the wireless renaissance - it was merely a suggestion that we rejected long ago.

Rating the 802.11 Wireless Standards

In 1997, when the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard they called it 802.11. Because it could only support a maximum bandwidth of 2Mbps - far too slow for most of today's applications - ordinary 802.11 wireless products are no longer being manufactured. The next wireless incarnation was 802.11b, which supports bandwidths of up to 11Mbps, followed by the creation of 802.11g, which supports bandwidth up to 54 Mbps and signals in a regulated 5 GHz range. While 802.11g is the fastest wireless technology, is it the best for your home or business? Here is a brief synopsis of the three primary 802.11 standards:



1. 802.11b - This technology supports bandwidth up to 11Mbps, which is comparable to the speeds of traditional Ethernets. 802.11b uses the same 2.4GHz radio signaling as the original 802.11 standard. Because it is an unregulated frequency, 802.11b devices run the risk of incurring interference from appliances that use the same 2.4 GHz range, such as microwaves and cordless phones. However, if you install 802.11b devices out of range of other appliances, you can avoid the interference. Some manufacturers prefer using unregulated frequencies, such as 802.11b to lower their production costs. On the negative side, 802.11b is relatively slow and supports fewer simultaneous users.
2. 802.11a - IEEE created 802.11a at the same time it made 802.11b. 802.11a supports bandwidth up to 54 Mbps and signals in a regulated 5 GHz range. This higher frequency limits the range of 802.11a in comparison to 802.11b, and due to its higher cost it's used primarily in the business sector rather than in homes. 802.11a's higher frequency also causes its signals to have difficulty penetrating walls and other obstructions. Because they utilize different frequencies, 802.11a and 802.11b devices are incompatible with each other.
3. 802.11g - This technology supports up to 54 Mbps, uses the 2.4 GHz frequency and is backwards compatible with 802.11b devices. 802.11g supports more simultaneous users, offers the best signal range and is not easily obstructed. The disadvantages of 802.11g is higher cost and possible interference with appliances on the unregulated signal frequency.

The Evolution of 802.11 Wireless Technology

1997 - 802.11 - 2 MBps

1999 - 802.11a - 54 Mbps in regulated 5 GHz range. Pro: Fast access. Con: Limited range

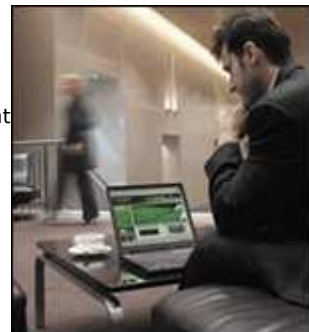
1999- 802.11b - 11Mbps in 2.4 GHz range

2002 - 802.11g - 54 Mbps in 2.4GHz range and is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa. Pro: Faster access and backwards compatibility. Con: Higher cost than 802.11b.

Why Connect?

According to International Data Corp. (IDC), about half of all U.S. households have a computer, and a much higher percentage of businesses use PCs. Tens of millions of these homes and businesses have more than one computer one. In fact, market research shows that current PC owners buy most of the new computers. This means that multi-computer households are becoming increasingly more common. If you are one of these multiple-PC owners, you have probably thought about how great it would be if your computers could talk to each other. With your computers connected, you could:

- Share a single printer between computers
- Share a single Internet connection
- Share files such as images, spreadsheets and documents



- Play games that allow multiple users at different computers

Here are the advantages of wireless networking:

It's fast (11 - 108Mbps).

It's reliable.

It has a long range (5,000 feet in open areas, 250 to 400 ft / 76 to 122 m in closed areas)

It's easily integrated into existing wired-Ethernet networks.

Virtually all 802.11g wireless networking products work with each other no matter what brand or model. Wireless offers Ethernet speeds without the wires. Access points vary greatly in cost, from about \$59.99 to \$1,400. Access points have an integrated Ethernet connection to connect to an existing wired-Ethernet network or routers provide connectivity to a high-speed data connection (DSL or cable modem). It also has an omni-directional antenna to receive the data transmitted by the wireless transceivers. Integrating PCs and Apple systems on the same network is also possible with the 802.11g standard. The majority of wireless network adapters used are in PCMCIA card form. But some manufacturers do offer USB adapters or PCI format cards. The cost per card ranges from \$39 to more than \$300. They are not typically sold in "do-it-yourself" kits. Instead, everything is a la carte, allowing customers to build a system that exactly meets their needs.

For businesses, the benefits of wireless technology are dramatic; we are not using hyperbole when we assure you that it will revolutionize your company. A wireless infrastructure makes it easier for you to adapt your office space as your company evolves. And the productivity gains you will reap dwarf the relatively inexpensive cost of setting up a wireless local area network (LAN). Here are the primary benefits your business will receive by going wireless:



- **Reduced Installation Costs** - It's less expensive to install wireless access points than wiring your office with Ethernet capabilities. Plus, you will not have to knock holes in walls to set up your network.
- **Flexibility** - If your company is growing rapidly and you need to constantly reorganize your space to accommodate ever-changing networking configurations, wireless networking provides rapid transition times, reduced down time and will not cost you as much as you would have to pay to rewire your office space. By setting up a network, you will be able to easily share devices, programs and technology with multiple computers. You can share peripheral devices, programs and technology to streamline your business and make it much more efficient.
- **Convenient Information Access and Increased Productivity** - Wireless delivers information access to anyone on your staff, from anywhere in your office. Most offices that have made the transition from wired networks to wireless systems have experienced remarkable increases in productivity.

It's Not as Complicated as You Think!

Most people think that networking your home or small office can be painful, with lots of wires, connections and other challenges. Plus, you have to make everything talk to each other. Don't fret, because it's not as much of a challenge as you might think. With most people using Microsoft Windows operating systems, networking has been built-in since Windows 3.11. Introduced in Windows 98, "Internet Connection Sharing" is a standard part of the operating system, allowing one computer to share an Internet connection with all computers on the home network. So, if you are running Windows, you can share files, printers and resources across your network without too much of a hassle. Following are 3 easy steps that will allow even a novice to setup a wireless network.

Wireless Networking Made Simple

3 Easy Set Up Steps Even the Novice Can Master

1. Plan Your System - Before you dive into the wireless world, make sure you know what lies ahead of you. Make a thorough analysis of your networking needs, what you need to accomplish, and what you expect to receive as a reasonable return on your investment. Assess your networking needs; determine how many workstations you'll need to connect and where you can best utilize them. Also, take an inventory of what upgrades you will have to make to your existing computer equipment and decide what equipment you will need to purchase. These are the types of devices required for your wireless network:

- **Wireless Access Point** - This is the "controller" of your wireless network. There are two types of access points - hardware access points and "integrated" access points. Hardware access points are used as an extension of an existing wired network. "Integrated" access points also provide the features of a router, and are connected to a high-speed connection (i.e.: DSL or cable modem). Access points generally can serve at least 50 users, so exceeding the connection limits is rarely an issue. Remember that when you are networking, your connection is shared with all active users. Having an 11, 22, 72, 108 Mbps network connection does not make your Internet connection "faster," however, it will allow faster data transmission between the users on the same wireless network. So, if you are planning on copying a bunch of files from your bedroom computer to the living room computer, or watching a video you recorded in your living room on your bedroom

computer, the data transfer speed is great. While surfing the Internet, you may see a decrease in access speed to the Internet if your son is downloading MP3s in his bedroom and you are trying to watch an online video. Your wireless connection speed will vary based upon your location (i.e. out by the pool vs. across the room from the access point), however proper placement of your access point can assist in providing the best service to all areas you intend on using a wireless connection. We carry a wide-range of wireless access points, including some which combine a multi-port wired hub so you can utilize one device for both your wired and wireless connections.

- **PCMCIA Wireless Adapter** - This is generally used for laptops. A PCMCIA card simply plugs into your notebook PC Card slot, and after configuration with the software provided with the card, will connect to any detected network. Some access points allow for configuration of security so only "allowed" cards are provided access. This will alleviate any problems if your neighbor decides to ride on your Internet service for free once they see you using the Internet out by your pool. Desktop PCs can also be connected to a wireless network by using an inexpensive PCMCIA-to-PCI adapter, which allow for fast, easy connection of a desktop PC through the use of an internal adapter card that the PCMCIA card slides into.
- **Compact Flash Wireless Network Adapters** - If you have a handheld device, which includes a CF Type II slot, you can connect it to your wireless network using a Compact Flash Wireless Network adapter.
- **USB Wireless Adapter** - Great for use with desktop PCs, a USB wireless adapter allows you to connect your system to the wireless network without installing any adapter cards or opening your PC whatsoever. These are a convenient and easy way to add wireless networking to an existing PC in your home. Additionally, based on user feedback, an external USB device has better reception than an internal PCMCIA card in the back of your computer, as you can move it around for the best reception.
- **"Wired" And "Wireless" Together** - "You can actually build a network comprised of Integrated access points, for both wired and wireless communications. Why would you want this? Well, let's say that you have the ability to run wire for the systems in your home. The cost is less per computer (an Ethernet NIC runs about \$10.00 and the cable anywhere from \$5-10) and you may have them easily accessible via cable. There are many mixed-mode devices, or "Gateways" available. For our full selection of Integrated Access Points. This device allows you to connect to a high-speed Internet connection (via the WAN port) and up to three wired devices (on the Ethernet ports) and up to 253 devices via the wireless access point built into the unit. This allows you to have standard desktops connecting with roaming notebooks and other devices where wiring is just not possible.

In summary, if you want to run a network in your home or office, it really isn't that tough! Pick the right parts to your network "puzzle" and get the best deal available. They'll work together and you'll make better use of ALL your resources

2. Setting Up Your System - Now that you have a plan in place that defines exactly what your equipment needs will be, how you will configure your network and what goals you expect to accomplish with wireless technology, it's time to set up your network. Before you take this step (don't worry, it's much easier than it seems), you must develop a good working understanding of the equipment involved in a wireless network. Wireless LAN equipment consists of wireless clients - the notebook computers, printers or handheld devices that can communicate over a wireless LAN - and access points, which are the points that accept the wireless radio signals and then connect the LANs. Your access point is the central communications point for your computers. These



Now it's time to build the wireless LAN! Again, don't panic - you will be amazed how simple it is. Here is what you have to do:

- Determine how many people will use your network; this will tell you how many access points you will need.
- Choose a central location for your LAN connection. If possible, this should be in an open environment to maximize your wireless range. Walls, cables, pipe, etc. within your existing environment can compromise your range.
- Configure your wireless network to work with your network.
- Test your installation before going live. With link test software you can find out what percent of your data is being sent correctly, how much time it takes to receive a response from the destination device, how the strength of the transmitted signal.
- Establish a protocol for managing your wireless LAN.

3. Implement security measures to protect the integrity of your wireless network - Remember, wireless communications transmit through the air rather than over a closed capable. Therefore, maintaining security over your system requires measures that are specific to wireless. Wireless security solutions include Media Access Control (MAC), WEP encryption and Traditional VPN (Virtual Private Network) securities controls. Following are brief summaries of these solutions:

Wireless Networking Guide

- MAC - Media Access Control restricts network access by unauthorized devices by assigning each network card a unique hardware identification number.
- WEP Encryption - A software algorithm that scrambles outgoing data and unscrambles it when it is received, maintaining its integrity while en route.
- Traditional VPN (Virtual Private Network) security controls - Allows users outside your system to gain access to your network. VPNs encrypt data prior to transmission over a wireless link, ensuring data security even if it is intercepted. VPNs are particularly critical when you are using a public hot spot.

Three simple steps - that's all it takes to join the wireless revolution - along with a relatively small investment in new technology that you will recoup many times with your exponentially improved efficiency and streamlined operation. We have the expertise, incomparable product line and unparalleled pricing to help you become experience all the advantages of benefits of wireless technology.

Choosing The Right Wi-Fi

Making Sense of the Wi-Fi Numbers and Letters

With three types of Wi-Fi "802.11" technology to choose from for wireless Internet access, and more on the way, which one is best for a new laptop? First there was 802.11b, the geeky name for the wireless technology which quickly made Wi-Fi a must-have for laptops. Next came versions 802.11g and 802.11a. And now, just when you've got Wi-Fi letters up to your eyeballs, yet another one is on its way. And another one, and some other ones. 802.11n is the newest generation of Wi-Fi technology, and although a unified 802.11n standard has yet to be finalized, some manufacturers are already selling equipment based on their own versions of "n" technology, which is more than twice as fast as 802.11g and 802.11a. But these "pre-N" products. But they're often twice as expensive as other Wi-Fi devices, so it might not be a wise investment since they may not be compatible with the eventual official standard. Meanwhile, back in the lab, engineers are working on another series of letters -- "e," "r," "s" and "t." And so it goes...

How to Choose Among the Wi-Fi Configurations

Actually, the decision isn't as tough as it seems, because no matter which Wi-Fi generation you choose, you'll be able to catch current wireless signals. That's because nearly all current Wi-Fi products are interoperable, and provides far more speed than most users need. So, even if your new laptop boards the slowest Wi-Fi incarnation, you won't really notice the difference. And slow, of course, is a relative term. It so happens that interoperability has been a major thrust of the industry group that coined the name Wi-Fi to describe the 802.11 family of wireless technologies. Nearly every Wi-Fi modem in a computer will talk to just about any Wi-Fi transmitter, at home or on the road, regardless of manufacturer. Furthermore, the next generations of the Wi-Fi standard, starting with 802.11n, may not hit the market until after 2006, so there's no reason to fret right away.

The Differences Among the Wi-Fi

The original "b" flavor of Wi-Fi can provide data speeds of up to 11 megabits per second (mbps). Actual data transmission is probably closer to half the maximum speed, but that's still several times faster than the broadband connections used by most homes and small businesses. The next version, 802.11g, allows speeds of up to 54 mbps, but is fully compatible with equipment based on 802.11b because they both use the same radio frequency, or wavelength, to transmit data over the airwaves. Once again, actual speeds are usually about half the maximum rate. While the third standard, 802.11a, is also billed at up to 54 mbps, it isn't compatible with either of the first two because its signal travels over a different wavelength. However, nearly all 802.11a products available to the general public are also equipped with 802.11g capability, so some level of connectivity is likely between devices with the latest Wi-Fi standard and those without it.

Nevertheless, it makes sense for most users to pay a little extra for 802.11g, but not necessarily 802.11a. In fact, most DSL and cable broadband connections aren't as fast as the slowest version of 802.11. As a result, few users can take full advantage of Wi-Fi's speed. But DSL and cable broadband providers are starting to boost the bandwidth they offer with little or no price increase, and some local phone companies are installing fiber-optic cables that will deliver lightning-fast connections. While 802.11a offers the same increase in speed as 802.11g, the advantage of 802.11a is that it operates at a wavelength that's less clogged by competing signals from other Wi-Fi users, microwave ovens and cordless phones. While most people don't encounter such interference, 802.11a could prove useful in densely populated environments such as an apartment building.

Turning Your Home into a Wi-Fi Network

Note: This article is intended as a guide only.

Please consult the instructions that accompany your networking products for additional information.

Step #1 - Before Starting

Creating a customized home Wi-Fi network is a great weekend project that you can accomplish with some patience and the proper tools. Before you dive into the wireless world, make sure you know what lies ahead of you. Make a thorough analysis of your networking needs, what you need to accomplish, and what you expect to receive as a

Wireless Networking Guide

reasonable return on your investment. Assess your networking needs; determine how many workstations you'll need to connect and where you can best utilize them. We recommend that you have the following equipment and information:

- A Wireless Router



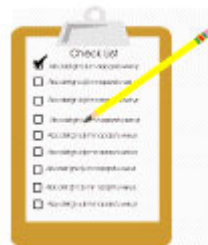
- Wireless adapters and/or a wireless-enabled system or laptop



- A broadband connection to the Internet (typically via cable or DSL modem)
- An Ethernet cable



- Pen and paper to write down current network settings, such as IP and MAC addresses



- The IP address assigned to your system by your ISP if you use a static IP address
- If you use DSL, the username and password assigned to you by your ISP
- The MAC address for all wireless network adapters

The core of any Wi-Fi network is a wireless router or gateway. For our demonstration, we are using the D-Link DI-624 AirPlus Xtreme G 802.11g router. The Airplus Xtreme G DI-624 delivers transfer rates up to 108Mbps in the 2.4GHz frequency and offers enhanced security to protect wireless communications. You'll also need a wireless adapter for each system that's connecting to the network. We installed two D-Link AirPlus Xtreme G 802.11g wireless adapters: a DWL-G650 PC Card adapter for a Windows 2000 notebook PC and a DWL-G520 PCI adapter for a secondary desktop running Windows XP Home Edition. Plus, the DWL-G650 and DWL-G520 also include a configuration utility to discover available wireless networks and create and save detailed connectivity profiles for those networks most often accessed.

The primary PC, connected to the router via Ethernet cable, was running Windows XP Professional.

Step #2 - Preparing for the Installation Job

Before you start your installation, you'll need to gather some essential information in order to set up your router correctly. You can get this information directly from your PC.

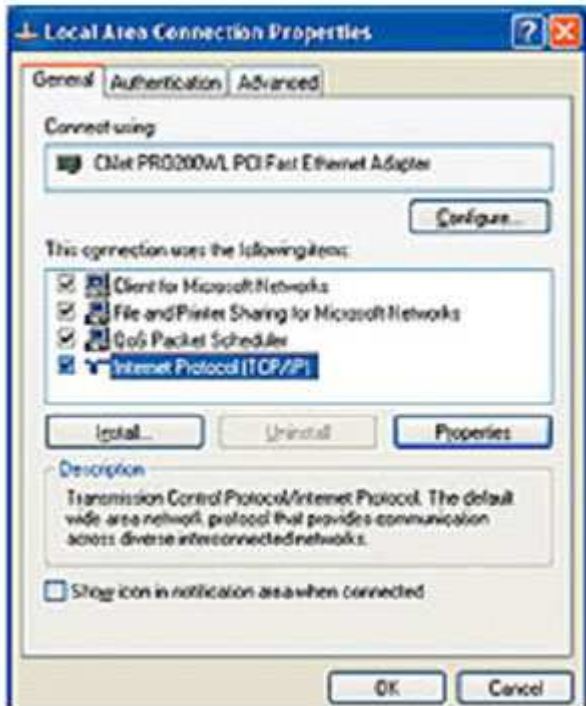
- Double-click the Network Connections icon within the control panel
- Right-click the icon for your PC's Ethernet adapter
- Choose Properties > Internet Protocol (TCP/IP) > Properties.

If "Use the following IP address" is highlighted, that means your Internet access uses a static IP address. Jot down the IP address, the subnet mask and the default gateway. Then click "Obtain an IP address automatically." Click OK to apply your changes and OK again to close the dialog.

If you have a DSL connection, you'll probably need the username and the password your system requires to connect to your ISP. If you don't know the values, try looking within the software your ISP provided. You may need to uninstall the PPPoE connection software that your ISP provided. To find out, check your router's documentation.

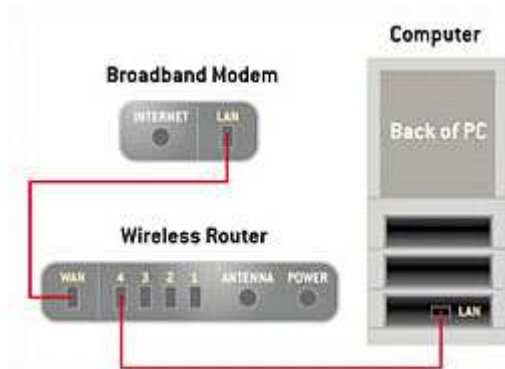
Now is also a good time to collect the MAC addresses of any wireless-network adapters you'll be installing. The MAC address should be printed on the Wi-Fi PC Card or the PCI adapter.





Step #3 - Installing the Wireless Router

Before you install the router, power down your PC and modem, then disconnect the Ethernet cable from your PC and connect it to your router's WAN port so that the Ethernet cable connects the modem to the router. Now, you'll need to string a second Ethernet cable between your PC's Ethernet port and one of the router's Ethernet ports.



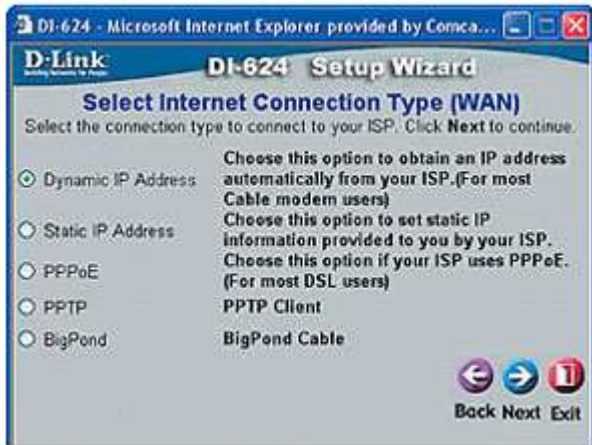
Connect your modem to the WAN port on the router and open your PC to an open Ethernet plug on the router.

Turn on the modem and wait until it connects. Plug in and power on the router and turn on your PC. When your system boots, open a browser window and try a few Web sites to test your Internet connection. If all seems to be working, go to the next step

Step #4 - Configuring the Router

Using the PC connected to the router, launch your browser. In the URL address field, enter the router-configuration IP

address provided in the documentation. For the D-Link KL-624, the IP address is 192.168.0.1. You will also need to enter the configuration-utility ID (usually admin) and the default password.



DSL users likely will have to choose a PPOeE Connection type.

Next, enter the information you collected in step 1 as instructed in your router's installation guide. If you jotted down an IP address in step 1, set the router to use a static IP address and enter the address and other information. If you're a DSL user, you'll likely need to choose a PPPoE Internet-connection type, then enter the username and password you selected to log on to your ISP. Leave other settings such as encryption and SSID at their defaults for now, exit your router's configuration routine, and check your Internet connection. If you still can't access any Web sites, check your router's documentation for troubleshooting advice and call the manufacturer for technical support, if necessary.

Step #5 - Installing the Wireless Adapters

If you're using the D-Link PC Card and PCI adapters, you must install the software from the CD before installing the wireless adapters (these adapters will connect wirelessly to the router). Next shut down your system, install the adapter and reboot. After Windows boots the Found New Hardware wizard should appear and begin the driver installation. Select "Install the software automatically" and click "Next." If you see a message warning you that the driver has not passed Windows logo testing, click "Continue Anyway."



Install a PCI card in each desktop system you want to connect to your network.

Note: If you have a notebook with built-in Wi-Fi you won't need the PC card adaptor.

Step#6 - Configuring the Wireless Systems

At this point, if you are unable to connect your wireless systems to the Internet you might have a couple of more steps to go before completing your wireless networking project. If you're using a Windows XP system try disabling the Windows wireless-configuration feature in order to establish a connection. This step is also necessary if you want to use the bundled utilities. To disable this feature, click the XP Networking icon (it looks like two computer monitors) in the system tray at the bottom right of your screen. When the Wireless Network Connection dialog appears, click the "Advanced" button and select the "Wireless Networks" tab. Uncheck "use Windows to configure my wireless network settings" and click "OK" to accept the change. Finally, reboot your system to bring the connection to life.



If your wireless systems won't connect to the Internet, try disabling Windows XP's wireless connection utility.

If you are using an operating system other than Windows XP, a simple reboot may be all that's necessary to get your Wi-Fi adapter running correctly after driver installation. However, if a simple reboot doesn't solve the problems, the next steps probably will.

Step #7 - Setting the Password

To secure your new Wi-Fi network, go to your wireless router's configuration utility again by entering its IP address in your browser. Using the router documentation or built-in help, if necessary, find the option that lets you change the default password. With the DI-624, this option is located within the Tools page. Apply the change, but leave the configuration routine open for the next step.



The Tools page in the DI-624's configuration utility allows you to change the router's password.

Step #8 - Setting the Service Set Identifier (SSID)

To put the finishing touches on securing your network, you must change its name. This is usually referred to as the Service Set Identifier (SSID). When using the DI-624, you can reach the SSID setting by clicking the Wireless button. Change the default SSID to anything you like. However, avoid entering values that a thief might guess such as your last name. Apply the change, but do not exit. Note: Your router may also allow you to disable DID broadcasting. This will keep your neighbors or potential intruders from seeing your wireless network among their Wi-Fi connection choices.



The Tools page in the DI-624's configuration utility allows you to change the router's password.

Enable Encryption

Now it's time to enable encryption. If your router and all of your wireless adapters support it, use Wi-Fi Protected Access (WPA) encryption with a pre-shared key. This provides more than adequate security for most home users. If your hardware doesn't support WPA, enable Wired Equivalent Privacy (WEP) encryption.

Most routers let you create WEP or WPA keys by entering a pass phrase. You'll likely need to enter the pass phrase twice for verification. Apply the changes without exiting.

Tip:

Don't use a pass phrase that's easy for an intruder to decipher. Mix it up; create one that's hard to guess, with a combination of numbers and letters.



For added security, choose WPA encryption over WEP if you have a choice.

Filter MAC addresses

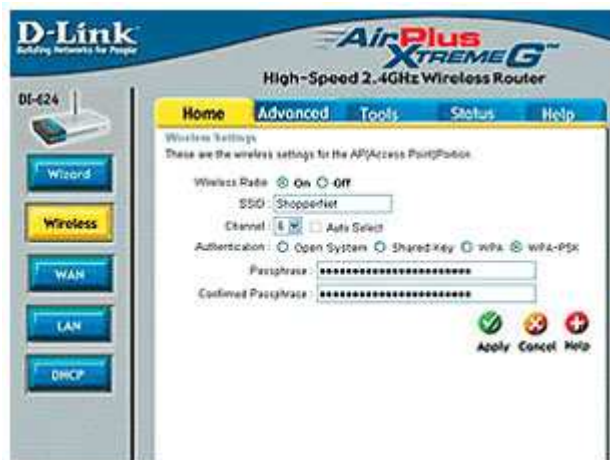
As a final security precaution, consider limiting access to network adapters with specific MAC addresses. To use MAC address filtering, you'll need to enable the feature in your router's configuration routine. Look for a filtering button or a menu option. Then enter the MAC addresses you recorded in step 3 for your Wi-Fi adapters. Apply the changes and exit the router's configuration utility.

Tip:

Most 802.11g routers come configured to work with both 802.11g and 802.11b clients. If you've purchased 802.11g devices for all of your wireless systems, choose an 802.11g-only mode to boost performance

Step #9 - Configuring, Part 2

If you've followed our instructions faithfully, your wireless systems will now be unable to connect to the router. To reestablish the connection, change the SSID within the wireless-configuration utility for each wireless adapter to match the value you entered for the router. You'll also need to enable the same type of encryption you enabled in the router and provide exactly the same pass phrase. After you apply the changes to each system, it should connect to the router and the Internet.



Enter the SSID and the encryption pass phrase into each system that you want to connect to your network.

Sharing Files and Printers with Your Wi-Fi Network

You can do more with a home wireless network than merely sharing your broadband connection. Installing a wireless network is also a great way to share files and printers. In order to share files and printers go to (in Windows XP) Control Panel > Network Connections and click "Set up a home or small office network." When asked for a connection method, choose "This computer connects to the Internet through another computer on my network or through a residential gateway."

Unless you're networking only Windows XP systems, choose "Create a network setup disk" when given the chance. This creates a floppy you can use to run the wizard on non-XP systems.

Now run the wizard on each additional system on your network. On non-XP systems, browse the floppy and run the file netsetup.exe. When configuring each system, assign each PC a different name but use the same workgroup name.

The Network Setup wizard automatically enables sharing on any printer connected to a PC during setup, but before you can use the printer from a networked PC, you'll need to install the printer driver on that system.

Each system configured with the Network Setup wizard should also have at least one shared folder given the name SharedDocs. To access these shared subdirectories within Windows XP, choose Start > My Network Places. You can easily set up additional subdirectories for sharing, but the more directories you share, the more you expose your drive in the event of a security breach.