

# How To: Wireless Network Encryption

by Lee Bennett, [lbennett@atpm.com](mailto:lbennett@atpm.com)

## Setting Up Wireless Network Encryption Between a Macintosh and a Non-Apple Transmitter

So, you've decided (as I did last month) to dive into wireless networking, frequently referred to as wireless fidelity or Wi-Fi. I confess, hearing about half-price Apple AirPort cards on sale at a few (and I do mean a *few*) Circuit City stores was the clincher for me. My initial plan was not to spend money on a transmitter to go wireless at home, but rather to make use of my office's Wi-Fi network when I occasionally brought my laptop with me. It didn't take more than a few times of doing this before I just had to have a transmitter of my own!

### AirPort Base Station or Non-Apple Transmitter?

I could spend a couple of paragraphs arguing the pros and cons of buying and using a third-party transmitter instead of the Apple Base Station, but this article is about the encryption, so I'll be brief. A third-party transmitter with a built-in multi-port switched router will usually suit your current and future needs better than the Apple Base Station, and cost half as much. Read more about this in *Macworld's* April 2002 [Base Station review](#). Also, be sure to choose a device that is configured via a local Web interface and not by Wintel software.

**Linksys** is one such brand, and happens to be the brand I bought.

*Important Note:* At first, you'll have to physically connect an Ethernet cable from your computer to the transmitter in order to access its setup screens. This is one of the few drawbacks of using a third-party device; the Base Station software supplied with all new Macs will

immediately communicate with a Base Station, meaning you can configure it to access the Internet without ever physically connecting your computer.

## Providing Free Broadband Without Even Trying

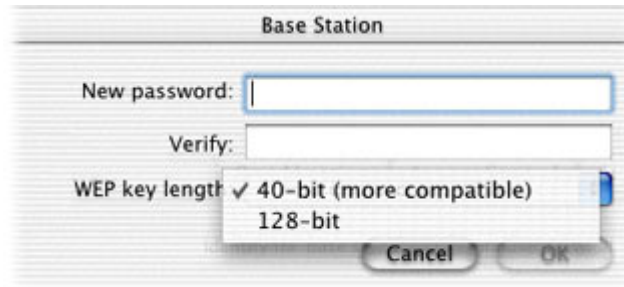
At this point, we'll assume you're happily (and wirelessly) surfing the Net. I bet you weren't surfing quite so happily however when you stumbled upon the [knowledge from the \*New York Times\*](#) that there are people out there who run around sniffing out unencrypted Wi-Fi networks and posting their existence to [Wi-Fi databases](#) so that they, or anyone else, can camp within range of those transmitters. Voilà! Free wireless broadband! If you want to [comment](#) on the ethics and legalities of this, be my guest. I'm not touching that one, but I do want to prevent people from using *my* bandwidth. As fodder for such a debate, here's a quote from the aforementioned *Times* article:

Those who use cable theft as an analogy point to federal law, which prohibits anyone from receiving communications offered over a cable system unless authorized by the cable operator.

But how the law will apply to Wi-Fi technology has not yet been tested. Some legal experts say using stray Wi-Fi signals is like trespassing. Others say the burden of securing the network may lie with its owner, as it does with satellite broadcasters. It is not a crime to tune in to unscrambled satellite programs, but it is illegal to crack the encryption of scrambled broadcasts.

## Encryption: AirPort Base Station vs. Other Devices

With Apple's Base Station, encryption is easily accomplished by setting a passphrase and using that phrase each time your computer's AirPort card goes to work (or letting your Keychain handle the passphrase for you). An algorithm converts the passphrase into a series of hexadecimal digits to make up a key.



### Assigning an Apple Base Station Password

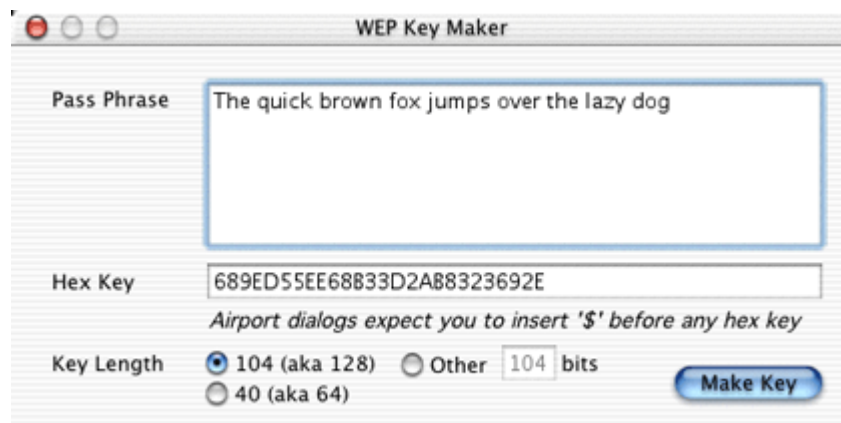
The process is essentially the same for non-Apple computers and transmitters where a protocol known as Wired Equivalent Privacy (WEP) is used. Technically, Apple's process is also called WEP, although Apple doesn't seem to use the term as freely as others. Regardless of what you call it, Apple's algorithm for generating a key from the passphrase is different from the algorithm used by most other transmitters. Consequently, if you use "The quick brown fox jumps over the lazy dog" as a passphrase on a non-Apple transmitter, using the exact same phrase on your Mac will not get you connected. To solve this, you must use an actual key to decrypt the connection instead of a passphrase. There are free utilities to generate hexadecimal keys from passphrases, such as [WEP Key Maker](#). This allows you to memorize a phrase instead of a long hexadecimal key.

At this point, I find myself asking, "Why use a utility? Why not simply type a passphrase in the transmitter's WEP configuration screen, let it generate the key, then copy that key to use on the Macintosh?" By way of a response, when I experimented with the *exact same* passphrase typed into WEP Key Maker and my Linksys transmitter, they generated different keys. So much for that theory.

So now I'm asking myself, "Why not just make up a random 10-digit (for 64-bit) or 26-digit (for 128-bit) hexadecimal code, type it into the transmitter's key field, then also type it in as the password (and save it to the Keychain) when AirPort attempts to connect?" My answer quickly spawned from the unsuccessful experiment from the first question. If it were that easy, someone probably wouldn't have bothered to write the WEP utility, and since I finally got my encrypted wireless connection running, I'm not going to mess around with it! If you know something about this, by all means, [tell us about it](#).

## Encryption Steps

So, unless someone identifies a way to decrypt the connection without using the utility, here's what you need to do. First, launch the WEP utility and type a passphrase into the space provided. Choose between 64-bit or 128-bit encryption, then click the Make Key button. Highlight and copy the Hex Key, and you're done with the WEP utility.



Generating a Hex Key with WEP Key Maker

Open the configuration screen of your transmitter and go to the WEP settings. Remember, you'll have to be physically connected with an Ethernet cable for this step, or using another computer that is physically connected. Ignore the field where you would type a passphrase. Select the same level of encryption that you chose in the WEP utility and paste the key into the WEP Key field. If you see multiple key fields, use the first one and make sure it's selected. Confirm that encrypted connections are enabled, then save/apply your settings. You're now done with the transmitter configuration page.

Finally (assuming your network settings are correct—probably simply set for DHCP), turn on your Mac's AirPort connection and select the name of the network you want to use. This name is defined in your transmitter's setup screens and is probably labeled ESSID. You should then be asked for a password, where there'll be an option to add the password to your Keychain. Use the same hex key for the password, except prefixed by a \$ symbol. The dollar sign apparently tells your Mac to not generate a key from what you type since you're manually entering the key itself. Note that you will not likely be able to paste the hex key from your clipboard into the password field. If not, just

paste it into a text window where you can see both it and the AirPort password field, and type it in manually.



Remember to precede the WEP key with a dollar sign, and consider using your Keychain so you won't have to type this in again.

## One Last Consideration

As a postscript to all of this, allow me to share one other tidbit that I learned while gathering information for this article. I was informed that using encryption will cut the bandwidth of your wireless connection by roughly half. At first, I thought, "That's impossible. I'm using encryption and I get the same speeds as when I still ran an Ethernet cable." But then I realized that broadband bandwidth (generally between 512 Kbps and 2 Mbps) is vastly slower than the throughput Wi-Fi transmitters are capable of (usually around 11 Mbps under ideal conditions). So, if you're only using Wi-Fi for Internet access, this slowdown won't affect you in the least. However, if you intend to transfer large chunks of data between local computers over a Wi-Fi network, you may want to consider an alternate form of security.



*Copyright © 2002 Lee Bennett, [lbennett@atpm.com](mailto:lbennett@atpm.com).*

<http://www.atpm.com/8.04/wifi.shtml>