The Wireless Networking Starter Kit, 2nd Edition Excerpt

Hi there!

You have in your virtual hands Chapter 17, *Setting up a Gateway*, from the second edition of *The Wireless Networking Starter Kit*. We've made this excerpt available as another tool in your kit for deciding whether this book is for you.

Read the chapter for a sense of how we approach topics. The book has 34 chapters and three appendixes covering a wide range of wireless topics, focused on Wi-Fi, but extending to Bluetooth, cellular, and other topics.

You can purchase the book in either print or electronic form by following the link at left for the best prices and the quickest delivery, including free shipping within the United States.

We hope you enjoy this excerpt.

—Adam C. Engst and Glenn Fleishman, November 2003

17

Setting up a Gateway

Most wireless gateways have a lot in common despite minor cosmetic and organizational differences in their interfaces. In this chapter, we look at three popular gateways: the Linksys EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch (model number BEFW11S4), the Linksys WRT54G Wireless-G Broadband Router, and Apple's AirPort Extreme Base Station. For each one, we'll provide two sets of instructions, one for a simple, open wireless network and another for a more secure wireless network.

(((•))) **NOTE**

Linksys makes several EtherFast models, but when we say EtherFast in this chapter, we mean specifically the BEFW11S4. The Web-based interfaces of the other models look much the same. A newer version, the WRT54G, supports 802.11g networking, and we also cover its differences in this chapter.

If you use a gateway from another manufacturer, the instructions should be relatively similar; also see **Table 17.1** at the end of this chapter for a comprehensive listing of standard settings.

Linksys BEFW11S4

The Linksys EtherFast Wireless AP + Cable/DSL Router w/4-Port Switch (BEFW11S4) was one of the most popular 802.11b gateways sold for many months, making it a good example of access points that use a Web-based interface. Web-based interfaces used by other gateways all rely on the same set of information.

$((\bullet))$ **NOTE**

The newer 802.11g-based Linksys WRT54G has an almost identical configuration. We cover its differences in the next section.

To connect via the EtherFast's Web-based interface, your computer must be on the private 192.168.1.0 network; see the sidebar, "Configuring Your Computer to Perform Initial Setup," to set your computer up properly. The EtherFast is set to be at the IP address 192.168.1.1 out of the box, and its default password is admin (no user name is necessary).

Configuring Your Computer to Perform Initial Setup

To configure an access point with a built-in Web server that has its default IP address on a private network (usually the 192.168.1.0 network), you must set your computer's networking options so it's on the same network. You typically make this initial connection over an Ethernet cable connecting the computer and the gateway, not wirelessly, though you can perform all subsequent configuration via the wireless connection.

To configure Windows XP:

1. Open Control Panel, open Network Connections, and open the Local Area Connection device corresponding to your Ethernet adapter.

2. Click Properties in the General tab.

3. Select Internet Protocol (TCP/IP) and click Properties.

4. To avoid disturbing an existing connection, select the Alternate Configuration tab.

5. Select the User Configuration radio button.

6. Set the IP address to 192.168.1.49, subnet mask to 255.255.255.0, and gateway to 192.168.1.1. You may leave the other fields blank (**Figure 17.1**).

7. Click OK.

To configure Mac OS X:

1. Open the Network preferences pane, and choose Network Port Configurations from the Show pop-up menu.

2. Click the New button, select Built-In Ethernet, and enter Private Configuration as the name.

3. Make sure the box next to Private Configuration is checked, and select Private Configuration from the Show menu.

4. In the TCP/IP tab, set the IP address to 192.168.1.49, subnet mask to 255.255.255.0, and gateway to 192.168.1.1 (**Figure 17.2**). You may leave the other fields blank.

5. Click Apply Now.

You can later disable or delete these network configurations if you desire.

Figure 17.1
Configuring
Windows XP to
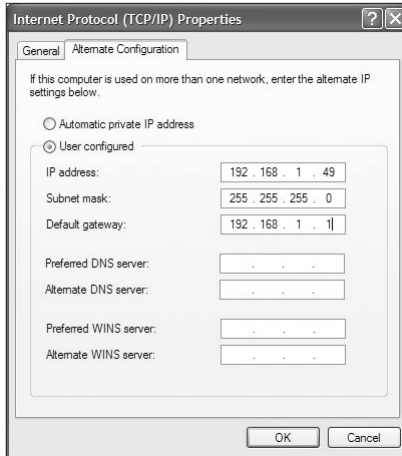connect to a
gateway for the first
time.

Figure 17.2
Configuring Mac
OS X to connect to
a gateway for the
first time.

Simple Setup

Follow these instructions to set up a simple wireless network that shares your cable- or DSL-based Internet connection.

1. Once you've configured your computer appropriately, open a Web browser and in the Address field, type 192.168.1.1, and then press Enter.

    Your browser connects to the EtherFast's built-in Web server and presents you with a password dialog.

2. Enter admin as the password (you can leave the user name field blank), and press Enter again to convince the EtherFast that you are indeed allowed to configure the gateway.

    The EtherFast presents the Setup tab.

TIP

If you have the same model of EtherFast that we're configuring here, but its interface looks quite different, visit Linksys's Web site and see if there's a newer version of the firmware. As you can see, we're using version 1.42.7, from April 23, 2002, but earlier versions looked different.

3. Change the SSID field from "linksys" to whatever you want to name your network.

4. From the WAN Connection Type pop-up menu at the bottom of the screen, choose the appropriate connection type. In most cases, it will be Obtain an IP Automatically (which means your ISP assigns you a dynamic IP address) or Static IP (which means your ISP has given you a set IP address that never changes). Other options include PPPoE, RAS, and PPTP (**Figure 17.3**).

Figure 17.3
Configuring basic settings in the EtherFast's Setup tab.

5. Click the Apply button, and when the EtherFast reports "Settings are successful" click the Continue button.

6. Click the Password link at the top of the screen to switch to the Password tab (**Figure 17.4**).

7. Enter your desired password in both Router Password text fields.

8. Click the Apply button, and when the EtherFast reports "Settings are successful" click the Continue button.

Figure 17.4
Changing the EtherFast's default password.

TIP

Although the EtherFast defaults to not allowing anyone outside of your local private network to manage the gateway, even if they have the password, you should still change the default password in the Password tab to prevent someone from connecting via a wireless connection and messing with your settings. If this were to happen, your only recourse would be to reset the EtherFast to its factory defaults and reconfigure it.

9. Verify that you can connect to the wireless network and out to the Internet. You may wish to reset your computer to use DHCP to do this.

That's it—you should have a working wireless network that shares your Internet connection and assigns IP addresses via DHCP.

Secure Network Setup

If you want your wireless network to be more secure, you must configure some additional settings:

1. Perform the instructions in "Simple Setup," and make sure everything works properly before enabling security settings.

2. In the Setup tab, change Allow Broadcast SSID to Associate to No. That closes your network so passersby won't automatically see it listed with available networks.

3. Set WEP to Mandatory, and click Continue next to the WEP options.

The EtherFast displays the WEP Key Setting window.

4. Choose either 64Bit or 128Bit from the first pop-up menu. 128Bit is slightly more secure, assuming all your equipment supports it, but requires that you enter a much longer WEP key each time you want to connect.

5. Either enter a passphrase and click the Generate button, or enter WEP keys manually. The advantage of the passphrase is that the keys are more random; the disadvantage of the passphrase is that random keys are much harder to remember and type (**Figure 17.5**).

Figure 17.5
Configuring basic settings in the EtherFast's Setup tab.

To creat a new WEP key, either enter a passphrase and press the generate button, or enter the key elements into the table below.

64Bit

Passphrase: SniffThis!   Generate

Key 1: 332D381E8A   Clear
Key 2: 5A5FE5C24C
Key 3: F903E1C25C
Key 4: C80A26DC88

Default TX Key: 1

Apply   Undo

6. Click Apply to save your WEP key settings, and click Continue when the EtherFast reports "Settings are successful."

7. Back in the Setup tab, click the Apply button, and when the EtherFast reports "Settings are successful" click the Continue button.

8. Verify that you can still connect to your network, which requires that you enter the network name manually, along with the WEP key that you entered.

TIP

If you screw something up and can't connect, remember that you can always reset the EtherFast to its factory defaults by pressing the reset switch on the back for 3 to 5 seconds. You should then close the network and verify that you can connect, and then enable WEP and verify that you can connect again.

Other Interesting Controls

The EtherFast's manual is good and rich with detail, but let's discuss a few of the more interesting things you can do with the EtherFast that may not be obvious initially.

• In the Password tab, you can reset the EtherFast to its factory defaults, which may be easier than holding down the reset button for a few seconds, depending on where you've positioned the EtherFast.

- In the Status tab, you can check on the EtherFast's IP setup, which is useful if you're troubleshooting a connection problem with your ISP.

- In the DHCP tab, you can not only enable, disable, and configure DHCP settings, you can also check to see what computers the EtherFast has assigned IP addresses to by clicking the DHCP Clients Table button. This could help you determine if outsiders are using your network. Remember that the number of addresses you set here doesn't affect how many client computers the EtherFast can actually handle at the same time.

((•)) **NOTE**

Because the EtherFast routes the whole local network out to the Internet whether or not addresses are assigned by DHCP, you can also set static IP addresses on the local network below the starting address you define. For instance, if you start DHCP at address 192.168.1.100, you could assign static addresses to machines that use port forwarding or other features requiring a fixed address to 192.168.1.2 through 192.168.1.99. Adam always does this so he can easily connect to all the computers on his local network by IP address.

- Click the orange Advanced button to switch to a different set of tabs where you can configure more advanced settings.

- Most people aren't likely to want to use the EtherFast's filters to prevent computers on a network from getting out via certain points, but it might be useful for preventing an addicted teenager from playing games for too many hours each day.

- If you want to make Internet services on a local machine available to computers on the Internet, you have two choices. You can enter that computer's IP address in the DMZ Host tab, which exposes all ports on that computer to the Internet, or you can make specific ports available in the Forwarding tab (**Figure 17.6**). Here we've forwarded traffic for port 80 (which is the Web) to the computer at 192.168.1.11, which is running a Web server. The Port Triggering button lets you set triggers for gaming.

- If your ISP allows only one specific MAC address to connect, you can have the EtherFast use that MAC address in the MAC Addr. Clone tab.

Linksys WRT54G

The Linksys WRT54G, as we noted at the start of this chapter, is nearly identical in configuration to its earlier cousin, the BEFW11S4. We wanted to highlight a few differences, though, which relate to its more advanced features.

Figure 17.6
Configuring port
forwarding for the
EtherFast.

Security Options

In the Setup tab, selecting the Enable radio button next to Wireless Security and
then clicking Edit Security Settings lets you choose more modern encryption
options (**Figure 17.7**).

Figure 17.7
Security settings.

*The encryption and
authentication options
(above) for the WRT54G.*

The encryption options available from the Security Mode pop-up menu now
extend way beyond WEP. They include:

- **WPA Pre-Shared Key.** The most likely option you would choose is WPA
  Pre-Shared Key, which lets you employ the strongest and simplest form
  of encryption available. (We discuss it in depth in Chapter 26, *Securing
  Data in Transit.*) When using WPA Pre-Shared Key, choose TKIP from
  the WPA, the most compatible key used with WPA, and enter a key of 8
  to 26 characters, including punctuation, spaces, and numbers. The group
  key renewal feature isn't well explained: it's unclear whether it improves
  security at all.

- **WPA RADIUS.** This option enables you to use WPA with a back-end authentication server (see Chapter 22, *Small Office Wi-Fi Networking*).

- **RADIUS.** You can select RADIUS for WEP encryption with an authentication server (again, see Chapter 22, *Small Office Wi-Fi Networking*).

- **WEP.** Use old, broken WEP with this option.

Advanced Wireless

Click the Advanced tab at the upper right of the WRT54G's Web configuration screen, and then click the Advanced Wireless tab to set options that tune your high-speed performance (**Figure 17.8**).

Figure 17.8
Advanced Wireless options.
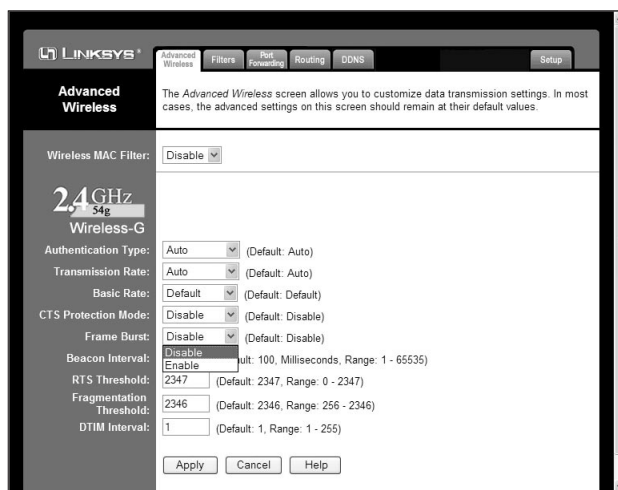
The options that are most important when running an 802.11g-based network include:

- **Transmission Rate.** Use this pop-up menu to lock a speed on your network. Choosing a value other than Auto prevents some remote devices from connecting at all. For instance, if you set a value of 12 Mbps or higher, 802.11b adapters can't connect.

- **Frame Burst.** Enabling this option can improve throughput enormously on 802.11b/g and 802.11g networks. (See "802.11e: Quality of Service" in Chapter 4, *Other Wireless Standards*, for more details on frame or packet bursting.) Frame bursting is entirely compatible with other adapters: even those that don't offer frame bursting as a feature can still interpret frames that have been rewritten (or burst).

Dynamic DNS

The Linksys WRT54G supports dynamic DNS, so you can map a human-readable domain name to the dynamic IP address assigned to your computer by your ISP (see Chapter 16, *Buying a Wireless Gateway*). Click the Advanced tab at the upper right and then select the DDNS tab to access the dynamic DNS features (**Figure 17.9**). You can choose one of two providers, DynDNS.org or TZO.com.

Figure 17.9
Dynamic DNS options.

AirPort Extreme Base Station

Apple's AirPort Extreme Base Station is a joy to configure—its settings are clearly labeled and have distinct purposes, and it provides a dedicated piece of Macintosh software, the AirPort Admin Utility, instead of a Web interface. (If you don't have a Mac, you have several other options; see the sidebar.)

Configuring without an AirPort Card or Macintosh

If you lack a Macintosh, a Mac with an AirPort card, or a Mac running a new enough Mac OS to run the Airport Admin Utility, you can still use one of two tools to configure an AirPort or AirPort Extreme Base Station:

- A Java-based configuration program that runs on several platforms. Download it from `http://edge.mcs.drexel.edu/GICL/people/sevy/airport/`.

- Apple's unsupported AirPort Extreme Admin Utility for Windows. Download it from `http://docs.info.apple.com/article` `.html?artnum=120226`. This utility supports only the AirPort Extreme Base Station and the newer snow AirPort Base Station, not the original graphite AirPort Base Station. At this writing, it's not just unsupported, it's also a beta version.

Of course, you can always do what Windows users did before these utilities appeared: invite a friend with an iBook or PowerBook over to dinner. Once you've configured a base station, you usually don't need to use Apple's Admin Utility again.

(((•))) **NOTE**

You cannot configure an AirPort Extreme Base Station if your Mac runs Mac OS 9 or earlier.

(((•))) **NOTE**

Many of the settings discussed in this section—except for WDS and the 802.11g choices—are identical for the older graphite and snow AirPort Base Stations that support only 802.11b.

(((•))) **NOTE**

Often after installing an AirPort software update, the next time you connect to your AirPort Base Station, the AirPort Admin Utility will prompt you to update the unit's firmware. Before updating firmware, it's a good idea to save the unit's configuration just in case the upgrade erases any of your settings.

Simple Setup

AirPort Admin Utility hides most settings from you on your first connection, presenting you with just the critical settings you need to set up a straightforward Wi-Fi network.

1. Open AirPort Admin Utility (likely located in the Utilities folder inside your Applications folder).

2. In the Select Base Station window you see any AirPort or AirPort Extreme Base Stations on the local network; selecting one displays additional details about it (**Figure 17.10**). To connect to a base station, double-click it. You must also enter its password if it's not already stored in the system Keychain.

Figure 17.10 Connecting to local base stations.
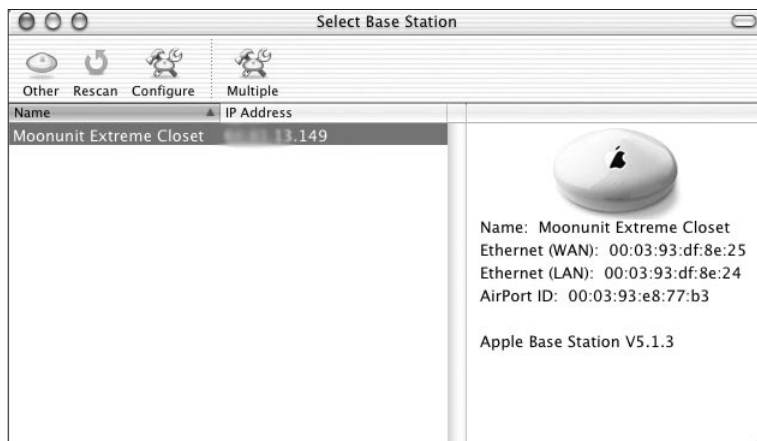
> ### TIP
> *If your base station doesn't appear in the list but has a static IP address, you can connect to it by clicking Other and entering the IP address and password in the connection dialog that appears. You can also configure base stations over the Internet this way.*

> ### TIP
> *The default password for a new base station is* `public` *(all lowercase).*

3. AirPort Admin Utility shows the Show Summary tab by default (**Figure 17.11**). Click the Name and Password button.

Figure 17.11
Summary tab's
display.

4. In the Name and Password screen, enter a name in the Base Station Name field that identifies this base station uniquely, and then click Change Password and set the password necessary to access the base station (**Figure 17.12**).

5. Rename the network by entering a new name in the Wireless Network Name field, which is the SSID for this device.

> ### TIP
> *If you have multiple base stations connected to your Ethernet network and want to enable roaming among them, make sure to use the same network name for all of them.*

6. Click the Internet Connection button.

Figure 17.12
Setting the base
station's name and
password.
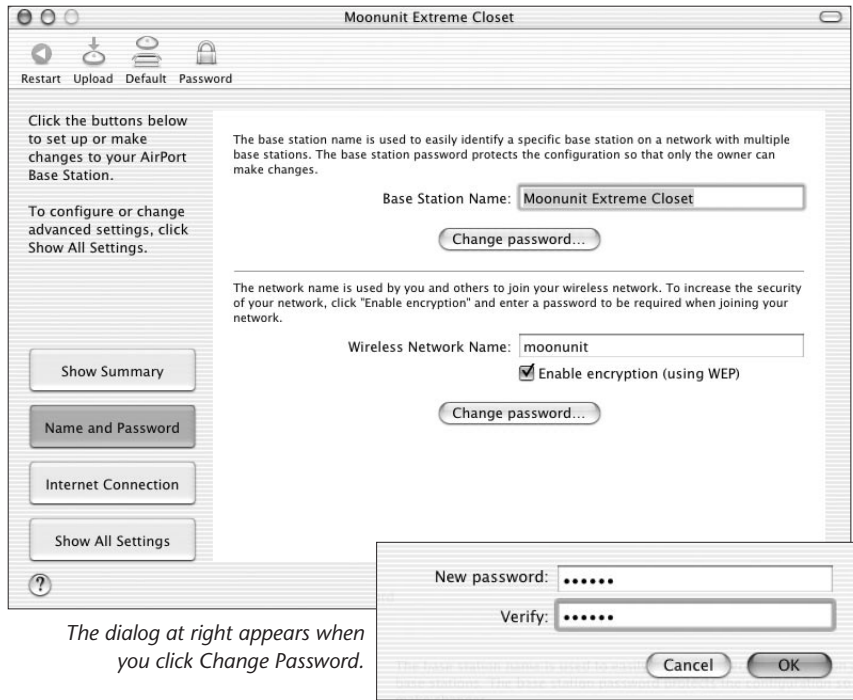
*The dialog at right appears when
you click Change Password.*

7. In the Internet Connection screen, enter the settings necessary to connect
your base station to the Internet as outlined in the list below (**Figure
17.13**).

Figure 17.13
Configuring your
Internet connection.
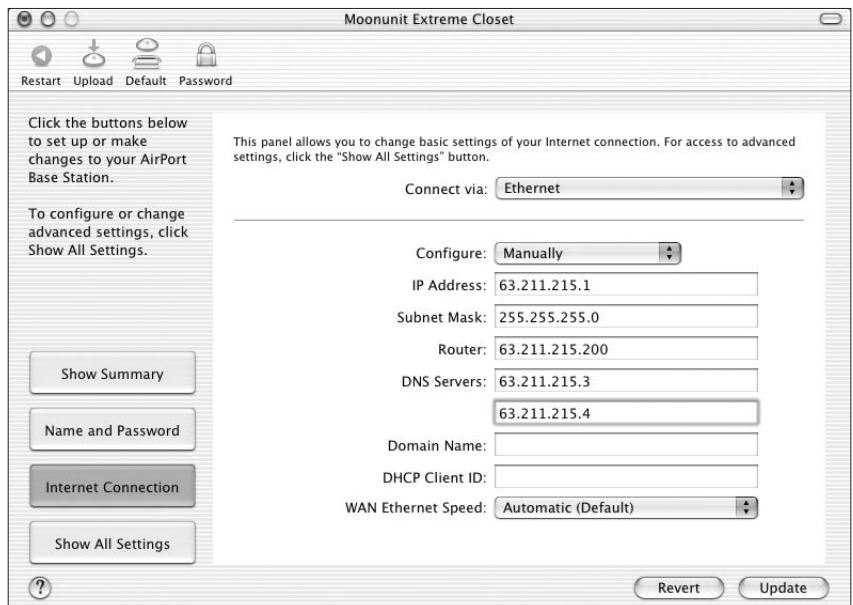
- For DSL and cable modem Internet connections, choose Ethernet from the Connect Via pop-up menu, and choose DHCP from the Configure pop-up menu. If your ISP requires that you use a DHCP Client ID, enter it in the DHCP Client ID field (this setting is often essential to making a connection work).

- Some broadband services require that you log in using PPP over Ethernet. If that's true of your ISP, choose PPP over Ethernet (PPPoE) from the Connect Via pop-up menu, and enter your account name and password (**Figure 17.14**).

- For dial-up Internet connections, choose the Modem setting that's available, and enter your ISP's dial-in information.

Figure 17.14
Setting up PPP over
Ethernet.
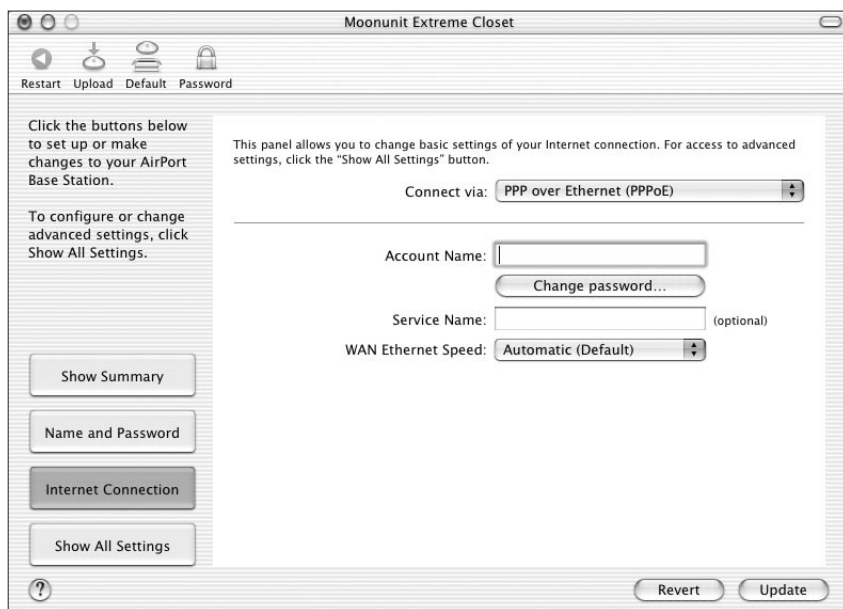
8. Click Update.

   The base station should reboot and connect to the Internet.

Secure Network Setup

If you want to turn on WEP encryption, which we recommend, follow steps 1 to 5 in the previous section, and in the Name and Password tab perform the following steps:

1. Check Enable Encryption (Using WEP), and click the Change Password button.

2. Enter the WEP password as text and from the WEP Key Length pop-up menu, choose 40-bit or 128-bit (**Figure 17.15**). Stick with 128-bit WEP unless you have older devices that can handle only 40-bit WEP.

Figure 17.15
Entering the
WEP password
and choosing
encryption depth.

3. Continue by following steps 6, 7, and 8 in the previous section.

((•)) **NOTE**

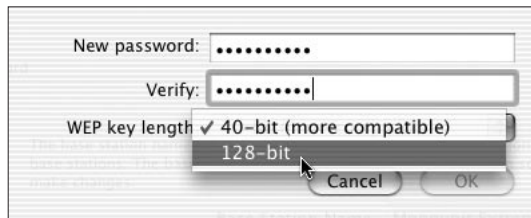*According to a statement that Apple made in June 2003, Apple will add WPA (Wi-Fi Protected Access) as an option by the end of 2003. Check our site for updates.*

Advanced Controls

The basic controls to set up a network are just the tip of the iceberg with Apple's AirPort Admin Utility. After you've connected to a base station, click the Show All Settings button in the main screen, and the full set of tabs and details appear in their full glory. Some of these are repeated from our instructions above, but they appear typically with more detail here.

((•)) **NOTE**

After making any changes, click the Update button at the bottom of the window to save your changes and reboot the base station with the new settings. Click Revert to abandon changes and go back to the previously loaded configuration.

AirPort Tab

The AirPort tab contains basic information about the AirPort Base Station, including details such as the name of the unit (used to identify it in the AirPort Admin Utility's Select Base Station window), and optional details such as the contact person and location (**Figure 17.16**). You can set the administrative password by clicking Change Password.

Click the WAN Privacy button to set a few obscure items that affect how visible the base station is on the Internet and local network (**Figure 17.17**).

- SNMP (Simple Network Management Protocol) allows network management software to monitor the base station's performance.

Figure 17.16
Naming and
locating the base
station.
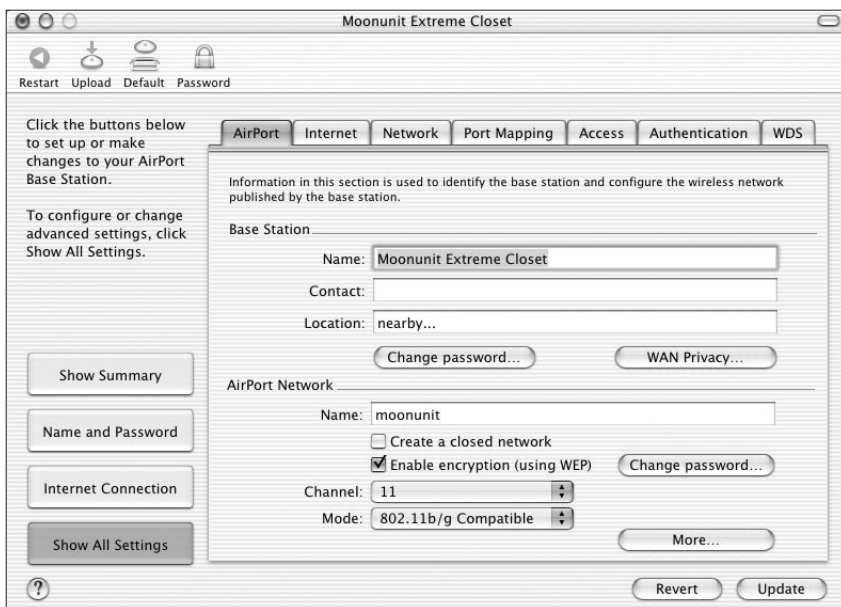
Figure 17.17
Setting WAN
privacy options.
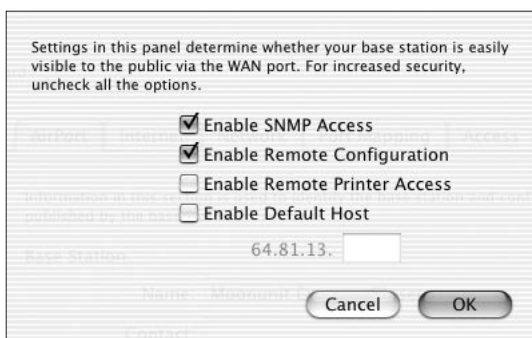
- Remote Configuration is dangerous: when enabled, anyone on the Internet can try to connect to your base station (otherwise, it's possible to connect to the base station only from your local network).

- Enabling remote printer access allows people outside your local network to print to a USB printer connected to the base station.

- We were unable to find documentation on Enable Default Host at Apple's site or elsewhere!

TIP
If you select Enable Remote Configuration, make sure to change the default password!

The AirPort tab lets you set the basic access point settings (**Figure 17.16**, above). The Name is your network name (as opposed to the base station's name). Checking Create a Closed Network prevents the base station from broadcasting its name, and thus hides the network from casual users.

Check Enable Encryption (Using WEP) to turn on WEP encryption, and click the Change Password button to configure your WEP key. See step 2 under "Secure Network Setup," earlier.

TIP

If you want PCs or non-AirPort-equipped Macs to connect after you set a WEP password, choose Equivalent Network Password from the Base Station menu to retrieve your WEP key in hexadecimal, suitable for entering into other wireless client software.

Choose a channel from the Channel pop-up menu. Make sure that if there are multiple base stations within range, you choose non-overlapping channels. (See Chapter 2, *Wireless Standards*, for details on selecting a channel.)

The Mode pop-up menu lets you exclude either 802.11b or 802.11g clients from your network, although most of the time you want to allow mixed 802.11b/g networking by choosing 802.11b/g Compatible.

Click the More button to set a few radio settings that may seem esoteric but can be surprisingly helpful in many situations (**Figure 17.18**).

Figure 17.18
Setting radio options.

Settings in this panel can reduce the range of your base station and should generally not be modified without good reason.

The multicast rate may be increased to improve the performance of certain types of network activity. This increase in performance will reduce wireless range.

Multicast rate: 1

Interference robustness should be enabled when you are in an environment with other 2.4Ghz devices that may be interfering with your network. Devices that can interfere include certain wireless telephones, television repeaters, or microwave ovens.

☐ Enable interference robustness

The transmitter power may be reduced to limit the wireless range of this base station. This can be useful in areas where many base stations are in close proximity to each other.

Transmitter Power:
10%   50%   100%

Cancel   OK

- Multicast sets the lowest threshold for connection, which can prevent more-distant computers with weak signal strength from associating with the AirPort Base Station. You can speed up a network but reduce the effective network range by raising the threshold above 1 Mbps.

- Check Enable Interference Robustness if your network appears to have problems with competing networks or other sources of interference like a 2.4 GHz cordless phone or nearby microwave oven.

- Reducing Transmitter Power from 100 percent reduces the range of the base station, but also decreases the likelihood of interference with adjacent Wi-Fi access points.

Internet Tab

In the Internet tab, you set the options for connecting your base station to an ISP (**Figure 17.19**). The Connect Using menu allows you to choose the network method, such as Ethernet, PPPoE, Modem, or AOL. If you use a cable or DSL modem without PPPoE, choose Ethernet.

Figure 17.19
Configuring your
base station to
connect to your ISP
with Connect Using
options inset.
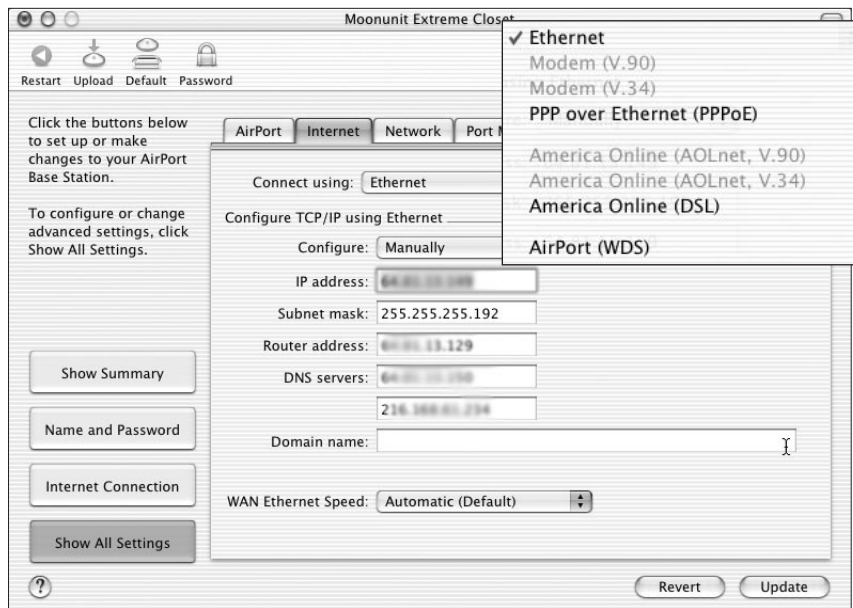
The settings you enter here are identical to what you would use when connecting to your ISP from a single computer, so refer to the information provided by your ISP for the details.

The AirPort (WDS) item in the Connect Using pop-up menu enables you to bridge multiple base stations to extend a network wirelessly. See Chapter 20, *Bridging Wireless Networks*, for detailed instructions on using WDS (Wireless Distribution System).

Network Tab

The Network tab offers a variety of interrelated options that together provide network services like DHCP and NAT. Contextual help at the bottom of the window explains each setting as you select it.

Checking Distribute IP Addresses turns DHCP service on, which tells the AirPort Base Station's DHCP server to offer IP addresses to all the computers that connect to it. You have two choices for how addresses are shared: using DHCP and NAT or using a range of IP addresses with just DHCP.

If your ISP provides you with multiple static IP addresses to use for computers connected to your AirPort Extreme Base Station, you can choose Share a Range of IP Addresses (Using Only DHCP) and enter your IP address range (**Figure 17.20**).

You should select Share a Single IP Address (Using DHCP and NAT) if your Internet connection provides you with only a single IP address, which is probably the most common situation (**Figure 17.21**). Apple suggests, in its pop-up menu ranges, three well-known, non-routable, private address ranges. However, you can also choose your own from the Other menu.

Figure 17.20
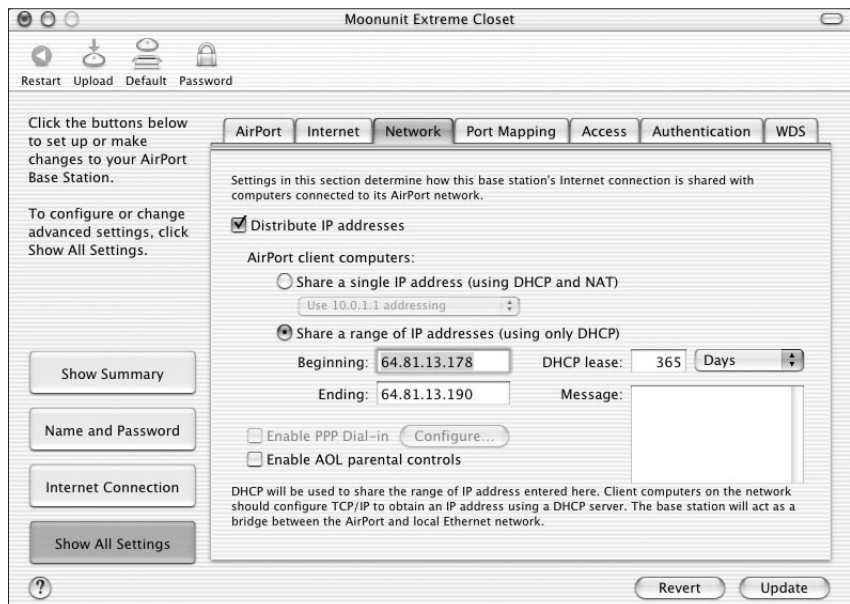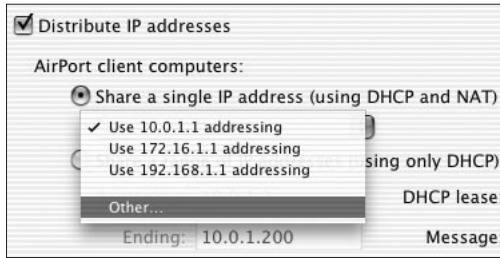Configuring your base station to share a single IP address.

Figure 17.21
Configuring your
base station to
share a range of IP
addresses.

You can set the length of time a DHCP number can be used by one of your client computers. If you have more computers that might want to connect than available IP addresses, set the DHCP lease time low to avoid tying them all up. If you have more than enough IP addresses to share out to your regular users, then you can set the DHCP lease time high so each individual user is likely to keep the same IP address for a while.

Checking Enable PPP Dial-in lets you turn an AirPort Extreme Base Station into an Internet modem bridge, so you can connect to your local network while you're traveling. Click Configure and a dialog lets you set access parameters (**Figure 17.22**).

Figure 17.22
Enabling dial-in
access for an AirPort
Extreme Base
Station.
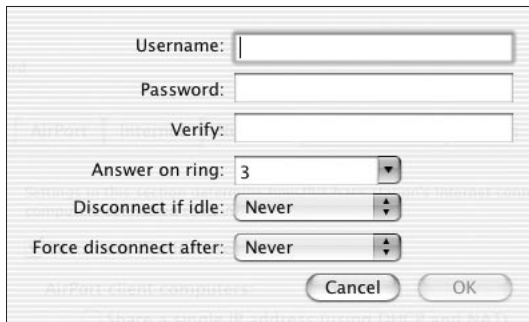
Lastly, the Enable AOL Parental Controls checkbox works in conjunction with dialing into AOL or using AOL Broadband, and it lets parents enforce policies within the base station.

Port Mapping and Access Tabs

The options in the Port Mapping tab let you map outside ports to computers on your wireless network that you want to be accessible from the Internet. We talk about port mapping in Chapter 16, *Buying a Wireless Gateway.* The Access tab offers options for controlling which unique wireless devices can connect to the base station; for more about controlling access by MAC address, see Chapter 25, *Preventing Access to Your Network.*

Authentication

The Authentication tab provides settings for configuring your base station to communicate with an authentication server to handle user logins. Users must have client software on their computers that enables them to enter their credentials when prompted; the base station hands these credentials off to a RADIUS or other authentication server, and then allows users to connect only if the authentication server confirms their identity.

Unless you're in an office or corporate environment, you can ignore this tab. (See Chapter 22, *Small Office Wi-Fi Networking*, for details on authentication servers.)

WDS Tab

We explain WDS and the WDS tab in Chapter 20, *Bridging Wireless Networks*.

Common Gateway Settings

To configure any access point, you must enter a few pieces of information. Although this may seem intimidating, most gateways ship with a default configuration or pick up some settings appropriately once you've made the necessary connections. Other settings you determine when planning your network, by referring to the documentation from your ISP, or talking to a network-savvy friend or colleague. **Table 17.1** outlines common settings, alternate names, and the type of information you'd enter for each.

Connecting to a Base Station without an AirPort Card

PC users and Mac users with older equipment may face the task of trying to connect to an AirPort or AirPort Extreme Base Station without having access to Apple's AirPort client software. That's usually not a problem, since connecting to one of these base stations is much like connecting to any other access point. The one difference is in determining the WEP key used to encrypt communications.

If WEP is enabled on the base station, you must use Apple's AirPort Admin Utility to obtain the non-AirPort WEP key.

1. Launch AirPort Admin Utility.

2. Connect to your base station.

3. In the list of icons at the top of the window, click Password, or choose Equivalent Network Password from the Base Station menu.

If you don't have a Mac that can run the AirPort Admin Utility, try the two tools noted in the sidebar, "Configuring without an AirPort Card or Macintosh." WPA might complicate this option; visit our Web site for updates.

Table 17.1

Common Configuration Settings for Gateways

Setting	What It Might Also Be Called	Explanation	Example Settings and Values
SSID (Service Set Identifier)	Network name, ESSID (Extended SSID for networks with two or more access points)	Clients connect to Wi-Fi networks by name. For networks with multiple access points, all should be named identically.	moonunit
Access point name	Base station name, unit name	Some configuration software uses this name to distinguish among available access points.	Bobmarley
IP address	WAN IP address	The gateway's external IP address. With most ISPs, your gateway picks this address up via DHCP, although you can also enter it manually. (You won't see this or the next three settings with PPPoE.)	24.6.5.130
Gateway		The IP address of the Internet router to which your gateway connects. Again, DHCP usually provides this automatically.	24.6.5.1
Subnet mask		The subnet mask defines the size of the local network. DHCP provides this in most cases; otherwise ask your ISP.	255.255.255.0
DNS servers	Name servers	DNS servers are necessary mainly if the gateway acts as a DHCP server, so the DNS addresses can be passed on to the client computers. Your ISP's DHCP usually provides DNS server information.	24.6.15.100 24.6.15.22
Local IP address	LAN IP address	The gateway's address on your internal network.	192.168.1.1
Channel		802.11b has 14 channels, only certain of which are allowed for use depending on the country you're in; to avoid signal overlap, choose among channels 1, 6, or 11 for adjacent access points in dense networks.	6
Closed network	Hidden network, turn off beaconing	Hides the network name from casual browsers.	

PPPoE	PPP over Ethernet	Used to login to an Internet account, most often with cable modems.	Username: tristane Password: 98fink1e!
DHCP client		Turn on the DHCP client if your gateway needs to identify itself to acquire its IP address from a DHCP server.	DHCP Client ID: SWBELL001
DHCP server		A DHCP server provides IP addresses to client computers on your network. Some gateways let you pick the range of addresses to use and the length of time a DHCP lease lasts.	192.168.1.1– 192.168.1.150 Lease time: 1 day
NAT	Network Address Translation, private address server	NAT is often built into the DHCP server option rather than broken out separately.	
Firewall	Filtering	Restricts traffic from or to specific services or IP addresses.	Ban all traffic from network 36.44.0.0.
Port forwarding	Port mapping, punch-through	Redirects incoming requests to a specific service to a port on a specific machine.	Inbound port 80 on the gateway connects to port 8127 on machine 192.168.1.53.
DMZ	Virtual server	Allows a single machine to appear as though it, instead of the gateway, is directly accessible from the Internet.	
Trigger		Enables compatibility with games that need to accept incoming traffic on ranges of ports.	When a local computer connects out via port 3307, open inbound ports 4000–5000 to that machine.
WEP	Encryption, security, network password	Allows up to four keys to be used to encrypt all traffic passing between adapters and the access point.	F71A82FF0D
WPA	WPA-PSK, WPA passphrase	Uses a new encryption method that relies on a passphrase to generate robust keys automatically.	Inky, dinky, foo.
Antenna diversity		Units with more than one antenna can have one antenna set to receive and the other to transmit, or both to overlap these functions.	

Setting	What It Might Also Be Called	Explanation	Example Settings and Values
Transmit speed	Tx speed, compatibility	For full compatibility with 802.11b, gateways must handle lower speeds; turning this off in smaller, close-range networks can improve overall network performance.	
802.11b/g		Newer gateways with 802.11g support may work in a g-only mode, mixed mode, and/or b-only mode.	g only
Admin password		All gateways let you secure the configuration by setting a password.	ish234#kab
Clone MAC address	Rewrite MAC address	Lets you change the unique Ethernet address on the access point to match, for instance, a registered address of another machine that an ISP allows onto its network.	08:23:1c:55:F4:0D
Firmware	Upgrade software	Not a setting, but a control that typically lets you select a firmware upgrade file to upload to the gateway, after which the gateway reboots.	
Modem settings		Enter the ISP's phone number, and often an alternate, along with user name and password information.	Number: 123-4567 Username: tristane Password: 98fink1e!
Dynamic DNS	DDNS	Choose a service, like DynDNS.org, from a pop-up menu and enter your account details to have your gateway's IP number matched to a host name, even when the IP number changes.	User name: stinkelfuss Password: 98finkle! Host Name: shoe.leather.com
WDS	Wireless Distribution System	Choose other access points with which this gateway exchanges data wirelessly, and other settings to make a gateway a master in a WDS network.	MAC address: 03: 08:3F:AC:EE:66