The Profiles Tab

The Profiles screen lets you save different configuration profiles for different network setups. You can also import or export profiles. The default profile holds the initial configuration saved when you ran the Setup Wizard.

Profile - Name of the connection profile.

SSID - The wireless network's unique name, as set in the connection profile.

Profile Information

Wireless Mode - The mode of the wireless network currently in use.

Transfer Rate - The data transfer rate of the current connection. (In Auto mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)

Channel - The channel to which the wireless network devices are set.

Security - The status of the security feature.

Authentication - The authentication setting for the network.

Connect - To connect to a wireless network using a specific profile, select the profile, and click the **Connect** button.

New - Click the New button to create a new profile. See the next section, "Creating a New Profile," for detailed instructions.

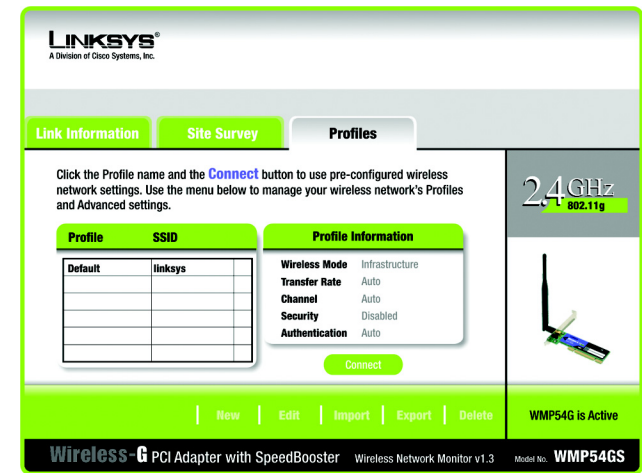**Edit** - Select a profile, and click the **Edit** button to change an existing profile.

Figure 5-9: The Profiles Tab

Import - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file and click the **Open** button.
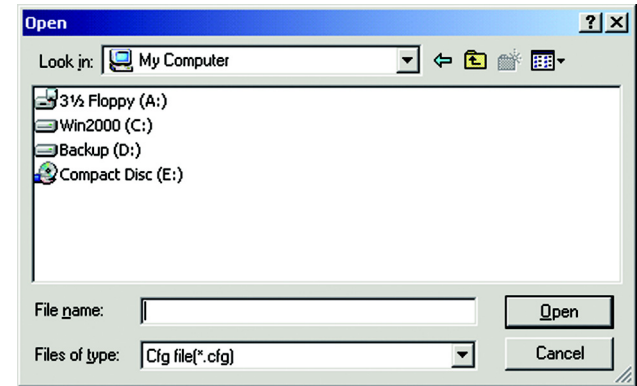

Figure 5-10: Importing a Profile

Export - To save the profile(s) in a different location, click the **Export** button. Direct Windows to the appropriate folder and click the **OK** button.
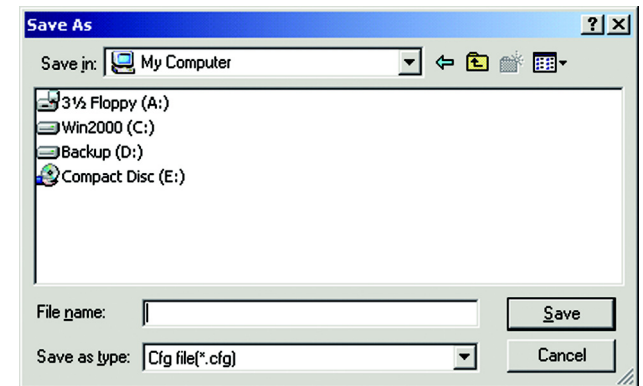

Figure 5-11: Exporting a Profile

Delete - Click the **Delete** button to delete a profile.

Creating a New Profile

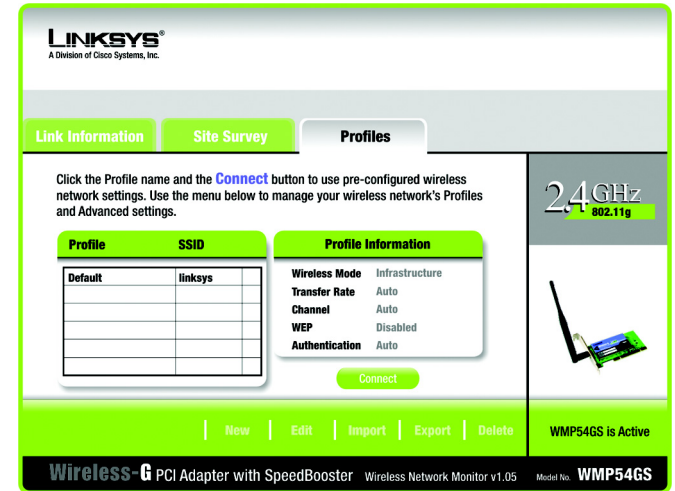1. On the *Profiles* tab, click the **New** button to create a new profile.

Figure 5-12: The Profiles Tab

2. When the Create connection profile screen appears, enter a name for the new profile. Click **OK** to save the profile name or click **Cancel** to return to the previous screen.

Figure 5-13: Create Connection Profile

3. Enter your network's settings on the *Network Settings* screen, which appears next.

    If your network has a DHCP server (or Router), click the radio button next to **Obtain an IP address automatically (DHCP)** and click the **Next** button to continue.

    If your network does not have a DHCP server (or router), click the radio button next to **Specify the IP address.** Enter an **IP Address, Subnet Mask, Default Gateway,** and **DNS** appropriate for your network. Enter each address in this format: xxx.xxx.xxx.xxx (the x's represent the numbers that make up each address). You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, then leave these fields alone.

    IP Address - This IP Address must be unique to your network.
    Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.
    Default Gateway - Enter the IP address of your network's Gateway here.
    DNS - Enter the DNS addresses of your network here.

    Click the **Next** button to continue or the **Cancel** button to return to the previous screen.

Figure 5-14: Profiles - Network Settings

4. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point, and continue to Step 6. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Click the **Next** button to continue or the **Back** button to return to the previous screen.

    SSID - The SSID is the unique wireless network name shared among all devices in your wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which can be any keyboard character.
    Infrastructure Mode - This mode allows wireless and wired networks to communicate through a wireless router or access point. Continue to Step 6 if selecting this mode.
    Ad-Hoc Mode - This mode allows wireless-equipped computers to communicate directly with each other. No access point or wireless router is used.

Figure 5-15: Profiles - Wireless Mode

5. The *Ad-Hoc Mode Settings* screen, for those who chose an Ad-hoc network, will appear next. Select the correct operating channel for your network from the Channel drop-down menu. Then, select the Network Mode from the drop-down menu. Click the **Next** button to continue or click the **Back** button to change any settings.

    Channel - The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, leave the default channel.
    Network Mode - Select Mixed Mode, and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed will be reduced. Select G-Only Mode for maximum speed, but no Wireless-B users will be allowed on the network.
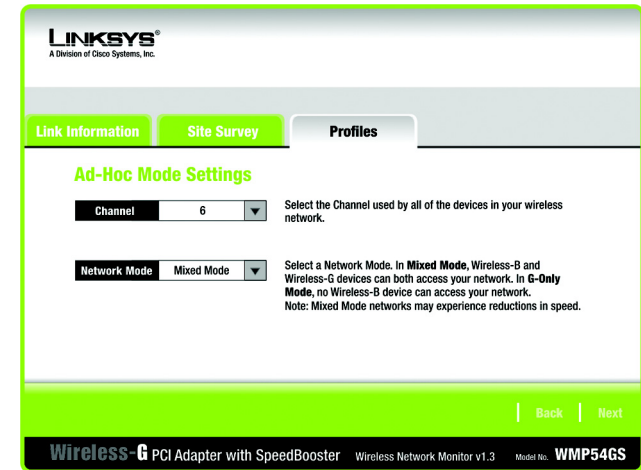

Figure 5-16: Profiles - Ad-Hoc Mode Settings

6. Select the method of security that is used on your wireless network: **WEP**, **WPA-Personal**, **WPA2-Personal**, **WPA-Enterprise**, or **RADIUS**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA is a stronger security method than WEP. WPA2 is a newer and stronger version of WPA. RADIUS stands for Remote Authentication Dial-In User Service. WPA-Enterprise and RADIUS use a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen. For more information about the information on this screen, you can also click the **Help** button.

    If you don't want to use encryption, select **Disabled** and then click the **Next** button to continue. Proceed to Step 9.

7. Proceed to the appropriate section for your security method: WEP, WPA-Personal, WPA2-Personal, WPA-Enterprise, or RADIUS.
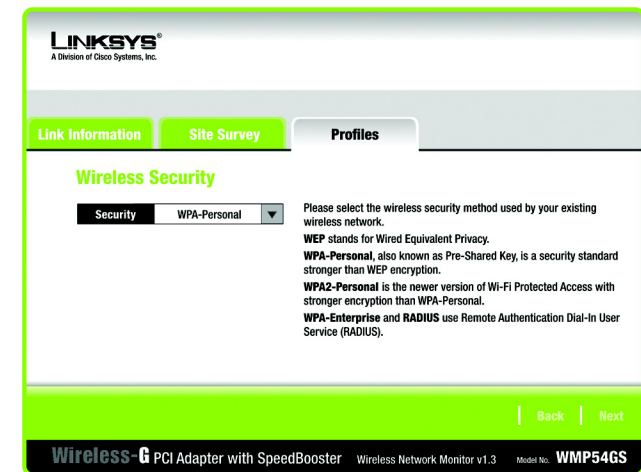

Figure 5-17: Profiles - Wireless Security

WEP

WEP - Select **64-bit** or **128-bit** encryption from the drop-down menu.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select **TKIP** or **AES** for encryption. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-18: Profiles - Wireless Security - WEP

Figure 5-19: Profiles - Wireless Security - WPA Personal

WPA2 Personal

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-20: Profiles - Wireless Security - WPA2 Personal

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

Figure 5-21: Profiles - Wireless Security - WPA Enterprise - EAP-TLS

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel, **EAP-MSCHAP v2** or **Generic Token Card**. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the Next button to continue or the **Back** button to return to the previous screen.

Figure 5-22: Profiles - Wireless Security - WPA Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the Next button to continue or the **Back** button to return to the previous screen.

Figure 5-23: Profiles - Wireless Security - RADIUS - EAP-TLS