11. The *Wireless Security Settings* screen will appear next. From this screen, you can set the level of security you desire for each of your three networks.

    First, select the wireless network you want to configure, **Main SSID**, **SSID1**, or **SSID2**.

    Then select from **WEP (64-Bit)**, **WEP (128-Bit)**, and **WPA-Personal**, and follow the appropriate instructions below. If you want to use WPA-Enterprise, then select **Disabled** from the *Security* drop-down menu. (You will have to use the Web-based Utility to set up WPA-Enterprise or RADIUS; for more information, refer to "Chapter 6: Configuring the Wireless-G Access Point with Power Over Ethernet.")

    After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

    For more information on wireless security, refer to "Appendix B: Wireless Security."

    - WEP (64-Bit) or WEP (128-Bit). Enter the Passphrase for your network. If want to manually enter the WEP key, then leave the *Passphrase* field blank and enter the WEP key in the *Key 1* field. The WEP key can consist of the letters "A" through "F" and the numbers "0" through "9" and should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

      After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

Figure 5-10: Wireless Security Settings - WEP Screen

wep *(wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.*

bit: *a binary digit.*

wpa *(wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.*

passphrase: *used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.*

- WPA-Personal. With WPA-Personal, you will use TKIP or AES for encryption with dynamic keys. Then enter a Pre-Shared Key of 8-63 characters.

  After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

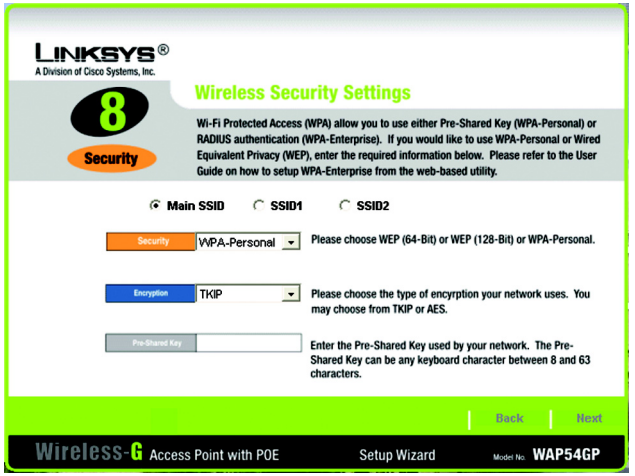

Figure 5-11: Wireless Security Settings - WPA-Personal Screen

tkip *(temporal key integrity protocol): a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.*

12. The *Wireless Power Management* screen will appear. You can adjust the power output of the Access Point to get the appropriate coverage for your wireless network. Select the setting appropriate for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**. Click the **Next** button to continue or **Back** to return to the previous page.

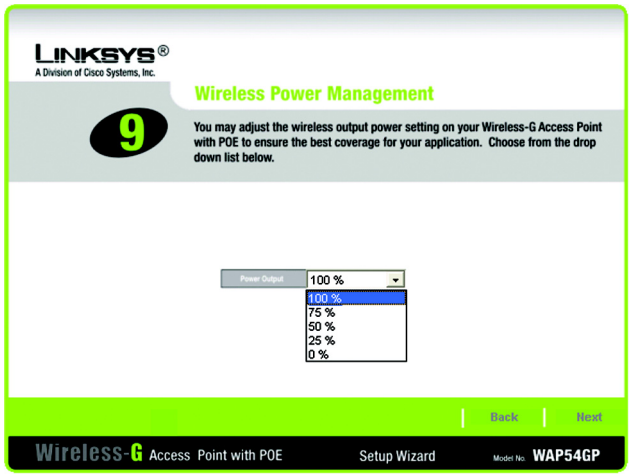

Figure 5-12: Wireless Power Management Screen

13. On the *Confirmation* screen, make sure your new settings for the Main SSID are correct. Click the **SSID1** and **SSID2** radio buttons to view their settings. To save your new settings, click the **Yes** button. If you do not want to save your changes, then click the **No** button.

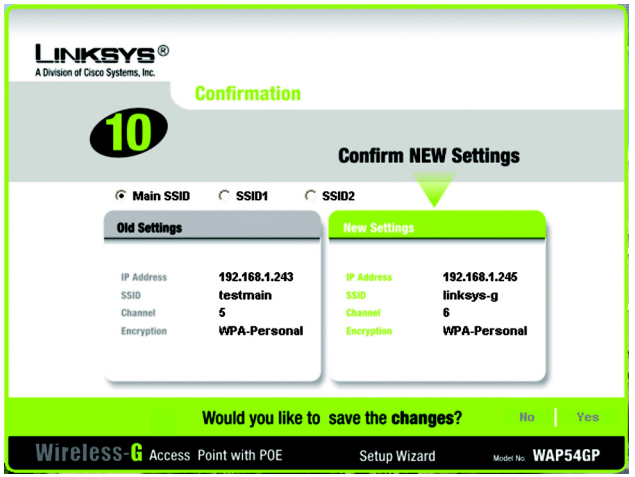

Figure 5-13: Confirmation Screen

14. At this point, the configuration performed with the Setup Wizard is complete. To configure any other Access Points in your network, you can run this Setup Wizard again.

    Click the **Online Registration** button to register the Access Point, or click the **Exit** button to exit the Setup Wizard.

For more advanced configuration, you can go to "Chapter 6: Configuring the Wireless-G Access Point with Power Over Ethernet."

Figure 5-14: Congratulations Screen

Chapter 6: Configuring the Wireless-G Access Point with Power Over Ethernet

Overview

The Access Point has been designed to be functional right out of the box, with the default settings in the Setup Wizard. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the Web-based Utility. This chapter explains how to use the Utility.

The Utility can be accessed via Microsoft Internet Explorer or Netscape Navigator through use of a computer that is networked with the Access Point.

For a basic network setup, most users only have to use the following screens of the Utility:

- Setup
  On the *Setup* screen, enter your basic network settings here.
- Management
  Click the **Administration** tab and then select the **Management** screen. The Access Point's default password is **admin**. To secure the Access Point, change the AP Password from its default.

HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.

tcp/ip: *a set of instructions PCs use to communicate over a network.*

browser: *an application that provides a way to look at and interact with all the information on the World Wide Web.*

NOTE: The Access Point is designed to function properly after using the Setup Wizard. This chapter is provided solely for those who wish to perform more advanced configuration or monitoring.

Navigating the Utility

There are five main tabs: Setup, Wireless, AP Mode, Administration, and Status. Additional screens will be available from most of the main tabs.

Setup

Enter the settings for the Access Point and your Internet connection on this screen.

Wireless

You will use the Wireless tabs to enter a variety of wireless settings for the Access Point.

- *Basic Wireless Settings*. Enter the network mode, Virtual Local Area Network (VLAN) settings, SSIDs, and other settings on this screen.

- *Wireless Security*. Use this screen to configure the Access Point's security settings.
- *Wireless Network Access*. From this screen, you can permit or block access to your wireless network.
- *Advanced Wireless Settings*. Use this screen to configure the Access Point's more advanced wireless settings.

AP Mode

Use this screen to configure how the Access Point will work with other access points in your network.

Administration

You will use the Administration tabs to manage the Access Point.

- *Management*. This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings.
- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Default*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.
- *Language Upgrade*. On this screen, change the language of the Access Point's Web-based Utility.
- *Reboot*. Use this screen to reboot the Access Point.
- *Config Management*. You can back up the configuration file for the Access Point, as well as save the backup configuration file to the Access Point.

snmp: *the standard e-mail protocol on the Internet.*

firmware: *the programming code that runs a networking device.*

Status

You will be able to view status information for your local network, wireless networks, and network performance.

- *Local Network*. This screen will display current information on the Access Point and its local network.
- *Wireless*. This screen will display current information on the Access Point and its wireless networks.
- *System Performance*. This screen will display current information on the Access Point and its data transmissions.

Accessing the Utility

To access the Web-based Utility of the Access Point, launch Internet Explorer or Netscape Navigator, and enter the Access Point's default IP address, **192.168.1.245**, in the *Address* field. Press the **Enter** key.

Open your web browser and type the IP address you entered in the Setup Wizard. (The default IP address is **192.168.1.245**.) (Should you need to learn what IP address the Access Point presently uses, run the Setup Wizard again. It will scan the Access Point and give you its IP address.) Press the **Enter** key and the following screen will appear. Enter **admin** in the *User Name* field. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

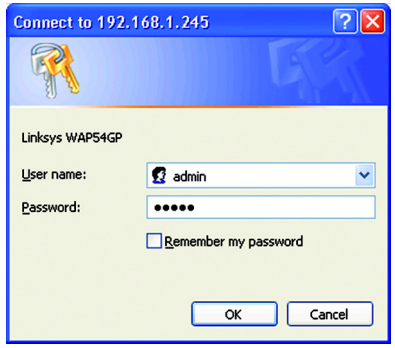

Figure 6-1: Login Screen

The Setup Tab

The first screen that appears is the *Setup* screen. This allows you to change the Access Point's general settings.

Setup

Enter the Host and Device Names for the Access Point.

Host Name. You may assign any Host Name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network.

Device Name. You may assign any Device Name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network.

Network Setup

The selections under this heading allow you to configure the Access Point's IP setting(s).

IP Settings

Select **Automatic Configuration - DHCP** if your network router will assign an IP address to the Access Point.

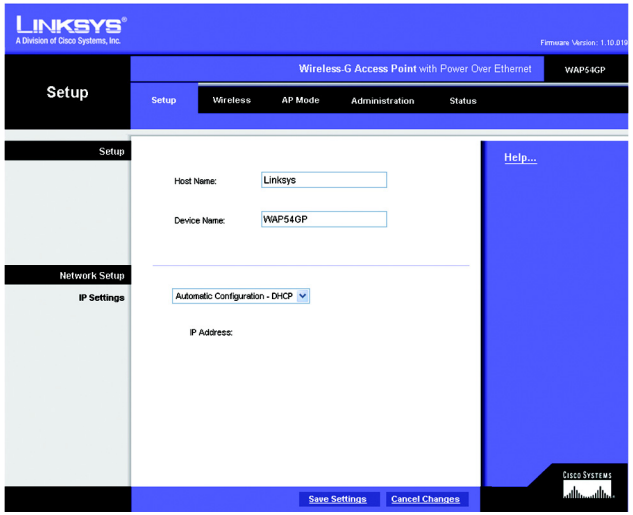

Figure 6-2: Setup - Automatic Configuration - DHCP Screen

Select **Static IP Address** if you want to assign a static or fixed IP address to the Access Point. Then complete the following:

- **IP Address**. The IP address must be unique to your network. We suggest you use the default IP address of **192.168.1.245**.
- **Subnet Mask**. The Subnet Mask must be the same as that set on your Ethernet network.
- **Default Gateway**. Enter the IP address of your network's gateway. The gateway is the device that enables communication between your computers and the Internet. In most cases, your router acts as your gateway.
- **Primary and Secondary DNS**. Enter the IP address of your Domain Name System (DNS) server. This information should be provided by your ISP. You should enter at least one DNS address.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

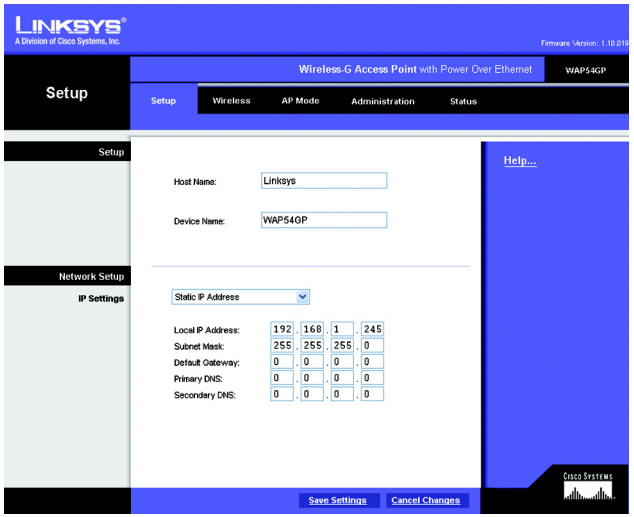

Figure 6-3: Setup - Static IP Address Screen

static ip address: *a fixed address assigned to a computer or device that is connected to a network.*

The Wireless - Basic Wireless Settings Tab

Change the wireless network settings on this screen. The Access Point can connect to up to eight wireless networks at the same time.

Figure 6-4: Wireless - Basic Wireless Settings Screen

Wireless Network

Configure the Access Point using the available settings. You can enter and save more than one configuration for the Access Point because the Access Point can work with a primary wireless network and up to seven Virtual Local Area Networks (VLANs).

NOTE: To use the Access Point's VLAN features, you must have a managed switch.

Wireless Network Mode. Select **Mixed** and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed will be reduced. Select **G-Only** for maximum speed with Wireless-G products only. The final selection, **B-Only**, allows only Wireless-B products on the network. You can also disable wireless performance if you select **Disabled**.

VLAN Trunk. Select **Enabled** if you want to use the Access Point's VLAN features.

Priority. Select **Enabled** if you want to use the Access Point's capability to assign VLAN priorities. Select **Disabled** if you want to disable the Access Point's capability to assign VLAN priorities.

Main SSID. Enter settings for the Access Point's primary wireless network.

Virtual SSID1-7. You can enter settings for up to seven virtual wireless networks.

SSID Name. The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in each wireless network.

VLAN ID. Enter the ID number you want to assign to this VLAN. Make sure at least one of these matches the Access Point VLAN ID entered on this screen.

Priority. You can assign VLAN priority to each wireless network, **Low**, **Medium**, or **High**.

TX Rate Limitation. The default setting is **54 Mbps**. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can keep the default setting, **54 Mbps**, to have the Access Point enable the Auto-

Fallback feature. Auto-Fallback will automatically negotiate the best possible connection speed between the Access Point and a wireless device.

Access Point VLAN ID. Enter the VLAN ID of the Access Point. Make sure this matches at least one of the VLAN IDs listed in the aforementioned table.

NOTE: You must use the Access Point VLAN ID for one of your wireless networks in order to maintain access to the Access Point's Web-based Utility.

Wireless Channel. Select the appropriate channel from the list provided; this will be the channel that all of your wireless devices will use.

Wireless SSID Broadcast. This feature allows the main SSID to be broadcast by the Access Point. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software and gain unauthorized access to your main network. Click **Enabled** to broadcast the main SSID to all wireless devices in range. Click **Disabled** to increase network security and block the main SSID from being seen on networked PCs.

NOTE: Only the main SSID of the Access Point can be broadcast. The Access Point cannot broadcast any of its Virtual SSIDs.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

The Wireless - Wireless Security Tab

Change the Access Point's wireless security settings on this screen.

Wireless Security

Enter the security settings for each SSID of the Access Point.

Select SSID. Select the SSID whose security settings you want to configure.

Security Mode. Select the security method you want to use, **WPA-Personal**, **WPA-Enterprise**, **RADIUS**, or **WEP**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below. For detailed instructions on configuring wireless security for the Access Point, turn to "Appendix B: Wireless Security." To disable such security, select **Disable**.

WPA-Personal

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

WPA Algorithms. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.

WPA Shared Key. Enter a WPA Shared Key of 8-32 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

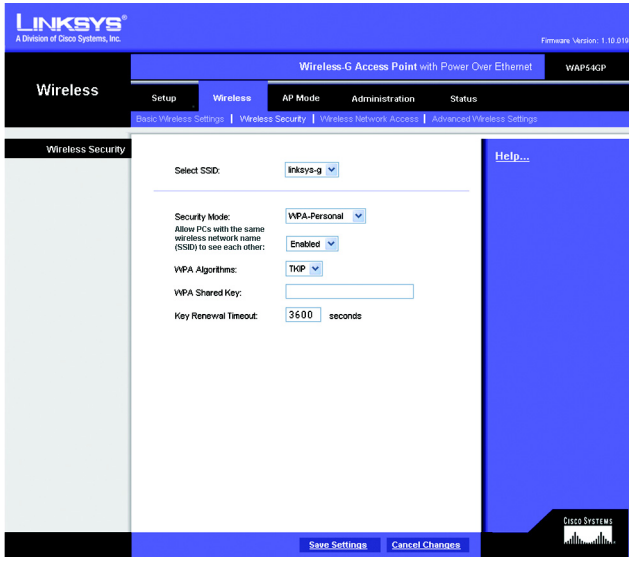

Figure 6-5: Wireless - Wireless Security (WPA-Personal) Screen

encryption: *encoding data transmitted in a network.*

WPA-Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Access Point.)

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

RADIUS Server IP Address. Enter the RADIUS server's IP address.

WPA Algorithms. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.

RADIUS Server Port. Enter the port number used by the RADIUS server.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

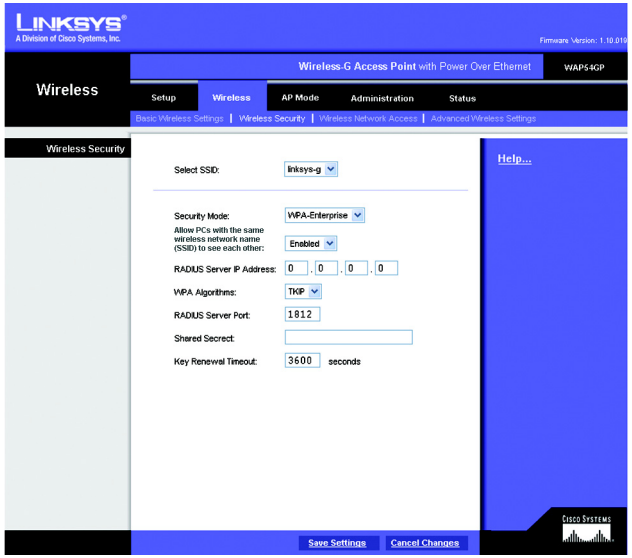

Figure 6-6: Wireless Security - WPA-Enterprise Screen

radius: *a protocol that uses an authentication server to control network access.*

server: *any computer whose function in a network is to provide user access to files, printing, communications, and other services.*

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Access Point.)

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Default Transmit Key. Select a Default Transmit Key (choose which Key to use).

WEP Encryption. Select a level of WEP encryption, **64 bits (10 hex digits)** or **128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, then enter the Passphrase and click the **Generate** key.

Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

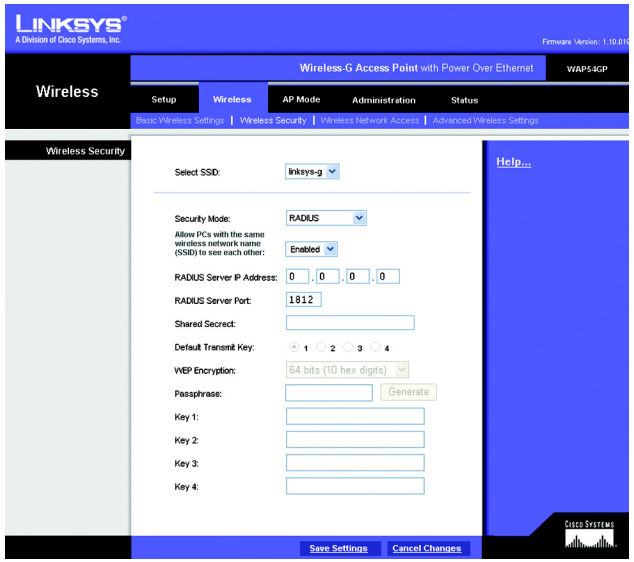

Figure 6-7: Wireless Security - RADIUS Screen

WEP

Authentication Type. Select the authentication method you want the Access Point to use, **Shared Key** or **Open System**. Shared Key is when both the sender and the recipient share a WEP key for authentication. Open System is when the sender and the recipient do not share a WEP key for authentication. All devices on your network must use the same authentication type.

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

Default Transmit Key. Select a Default Transmit Key (choose which Key to use).

WEP Encryption. Select a level of WEP encryption, **64 bits (10 hex digits)** or **128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, then enter the Passphrase and click the **Generate** key.

Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

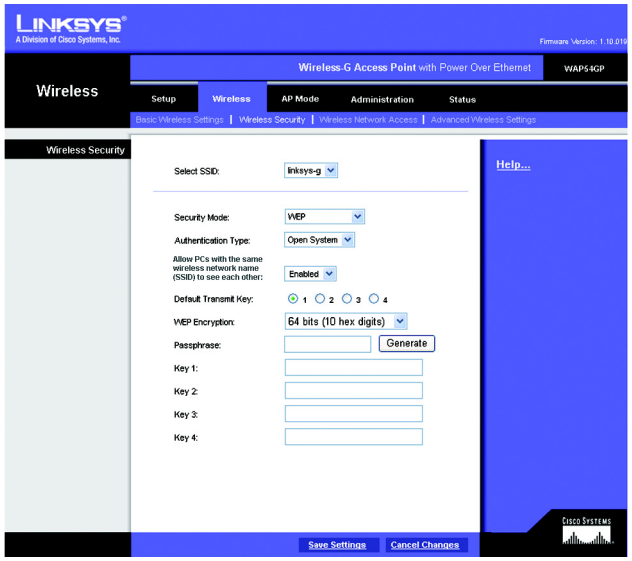

Figure 6-8: Wireless Security - WEP Screen

The Wireless - Wireless Network Access Tab

This screen allows you to permit or block wireless access for computers with specific MAC addresses.

Wireless Network Access

You can allow or block access for the MAC addresses you have entered.

Access List. To permit access, click **Permit to access**. To deny access, click **Prevent from accessing**. If you do not wish to filter users by MAC address, select **Disabled**.

MAC 1-20. Enter the MAC addresses of the computers whose access you want to control.

Select MAC Address from Networked Computers. If you want to select a MAC address from a list, click this button. The MAC addresses for your computers will be automatically displayed. Click the checkboxes of the MAC addresses you want to add to your access list. Change these settings as described here and click **Apply** to apply your changes. Click **Refresh** to retrieve the latest MAC addresses. Click **Close** to close this screen and return to the *Wireless Network Access* screen.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

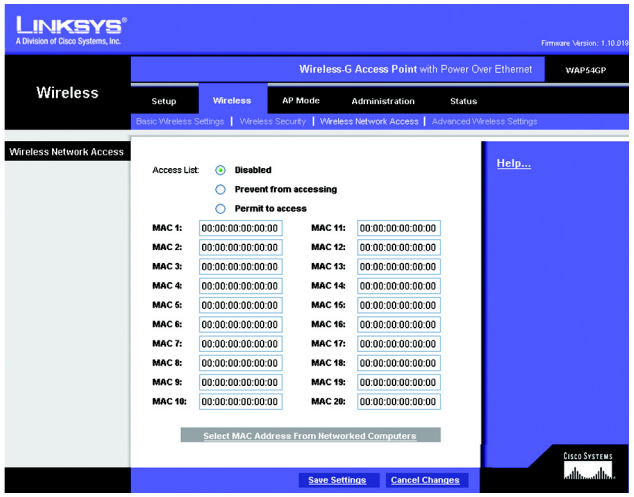

Figure 6-9: Wireless - Wireless Network Access Screen

mac address: *the unique address that a manufacturer assigns to each networking device.*

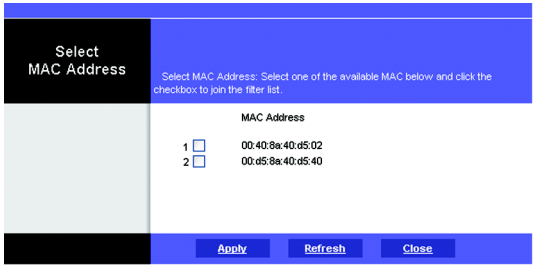

Figure 6-10: Select MAC Address Screen