9. The *Basic Settings* screen will appear next. Enter a descriptive name in the *Device Name* field. Create a password that will control access to the Access Point's Web-based Utility and Setup Wizard.

   If your network router will automatically assign an IP address to the Access Point, then select **Automatic-DHCP**.

   If you want to assign a static or fixed IP address to the Access Point, then select **Static IP**. Enter the IP Address, Subnet Mask, and Default Gateway settings. If you are not sure what changes you should make, then keep the default values.

   Then, click the **Next** button to continue or **Back** to return to the previous page.

   Device Name - Enter a descriptive name for the Access Point.

   Password - Enter a password that will control access to the Utility and Setup Wizard.

   IP Address - This IP address must be unique to your network. (The default IP address is **192.168.1.245**.)

   Subnet Mask - The Access Point's Subnet Mask must be the same as the subnet mask of your Ethernet network.

   Default Gateway - Enter the IP address of your network gateway (usually your router).

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

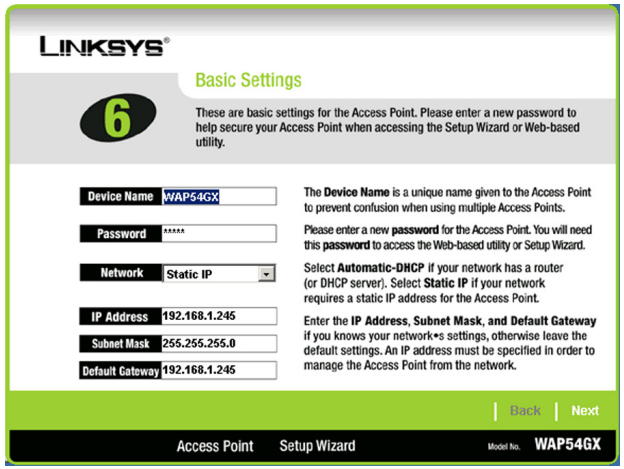

Figure 5-8: Basic Settings Screen

Configuring the Access Point's Wireless Settings

1. The Setup Wizard will ask you to enter the SSID, Channel, and Network Mode settings for your wireless network.

   SSID - Enter the name of your wireless network. The SSID must be identical for all devices in the network. The default setting is **linksys** (all lowercase).

   Channel - Select the operating channel for your wireless network. All of your wireless devices will use this channel to communicate.

   Network Mode - Select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed Mode**. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-Only**. If you want to disable your wireless network, select **Disable**.

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

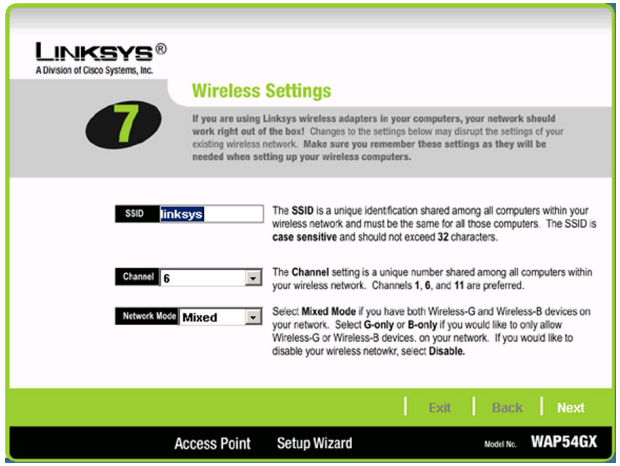

Figure 5-9: Wireless Settings Screen

2. Select the level of security you want to use: **WEP** or **WPA/WPA2 Personal**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. Click the **Next** button and proceed to step 3. If you do not want to use any wireless security method, select **Disabled** and then click the **Next** button. Proceed to step 4..

   If you want to use WPA-Enterprise, it is available through the Access Point's Web-based Utility. Select **Disabled**. Click the **Next** button and proceed to step 4. After you complete the Setup Wizard, refer to the Wireless Security tab in "Chapter 6: Configuring the Wireless-G Access Point with SRX."

3. Proceed to the appropriate section for your security method.

WEP

WEP (64-Bit)

To use 64-bit WEP encryption, select **WEP (64-bit)**. Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It 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. Valid hexadecimal characters are "0" to "9" and "A" to "F".

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

WEP (128-Bit)

To use 128-bit WEP encryption, select **WEP (128-bit)**. Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It 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 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

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

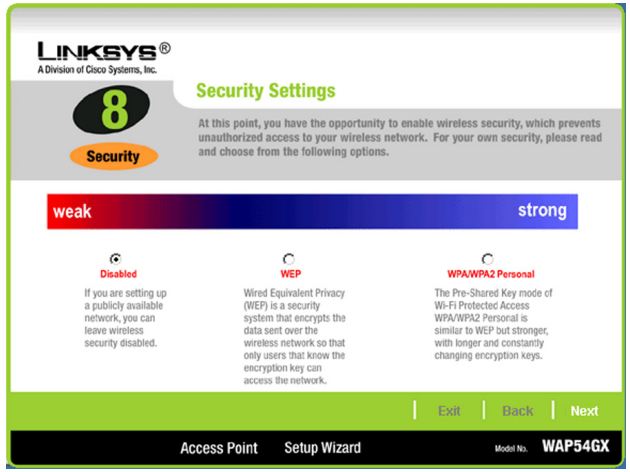

Figure 5-10: Security Settings Screen

Figure 5-11: WEP Settings Screen

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

encryption: *encoding data transmitted in a network.*

WPA/WPA2 Personal

WPA Personal

To use WPA Personal security, select **WPA Personal** from the *Security* drop-down menu. 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 8-32 characters in length.

Encryption - Select **TKIP** or **AES** from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 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 5-12: WPA Personal Settings Screen

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.*

WPA2 Personal

To use WPA2 Personal security, select **WPA2 Personal** from the *Security* drop-down menu. WPA2 Personal uses AES encryption with dynamic keys. Enter a Passphrase that is 8-32 characters in length.

Encryption - The default for WPA2 Personal, **AES**, is automatically selected.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 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 5-13: WPA2 Personal Settings Screen

WPA2 Mixed Mode

To use WPA2 Mixed Mode security, select **WPA2 Mixed Mode** from the *Security* drop-down menu. WPA2 Mixed Mode uses TKIP and AES for encryption. Enter a Passphrase that is 8-32 characters in length.

Encryption - The default for WPA2 Personal, **TKIP +AES**, is automatically selected.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 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 5-14: WPA2 Mixed Mode Settings Screen

4. The Setup Wizard will ask you to review your settings before it saves them. Click the **Yes** button if you are satisfied with your settings, or click the **No** button if you do not want to save your new settings.

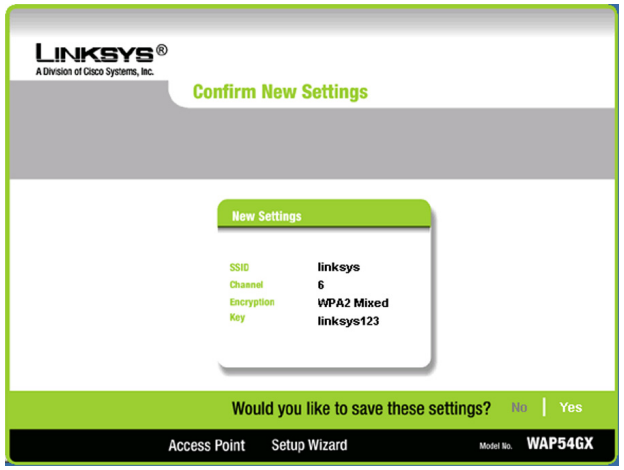

Figure 5-15: Confirm New Settings Screen

5. The *Congratulations* screen will appear. Click the **Online Registration** button to register the Access Point, or click the **Exit** button to exit the Setup Wizard.

Congratulations! The installation of the Wireless-G Access Point with SRX is complete.

If you want to make advanced configuration changes, proceed to "Chapter 6: Configuring the Wireless-G Access Point with SRX."

Figure 5-16: Congratulations Screen

Chapter 6: Configuring the Wireless-G Access Point with SRX

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 *Network 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's 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 four main tabs: Setup, Wireless, Administration, and Status. Additional screens will be available from most of the main tabs.

Setup

Enter the network and AP mode settings for the Access Point.

- *Network Setup*. Enter the settings for the Access Point and your Internet connection on this screen.
- *AP Mode*. Set up how the Access Point will work with other access points in your network.

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, SSID, and other basic settings on this screen.
- *Wireless Security*. Use this screen to configure the Access Point's wireless security settings.
- *Wireless MAC Filter*. From this screen, you can allow access to your wireless network by MAC address.
- *Advanced Wireless Settings*. Configure the Access Point's more advanced wireless settings.

Administration

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

- *Management*. This screen allows you to customize the password settings, as well as back up or restore the Access Point's configuration file.
- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Defaults*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.

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

Status

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

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

Accessing the Utility

To access the Web-based Utility of the Access Point, launch Internet Explorer or Netscape Navigator. In the *Address* field, enter the Access Point's default IP address, **192.168.1.245**, or the IP address you entered during the Setup Wizard. (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.

The login 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 - Network Setup Tab

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

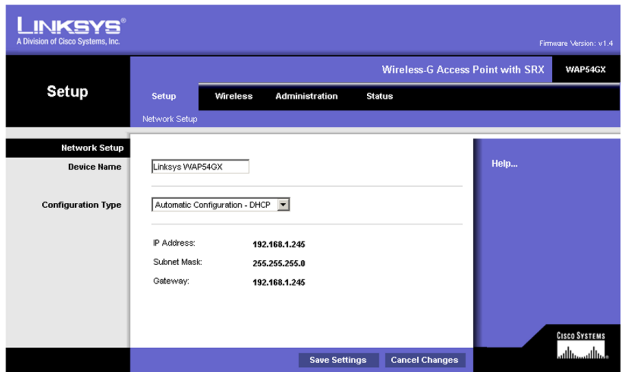

Figure 6-2: Setup - Automatic Configuration - DHCP Screen

Network Setup

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.

Configuration Type

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

The Access Point's IP Address, Subnet Mask, and Default Gateway address are displayed here.

Select **Static IP** 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.

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.

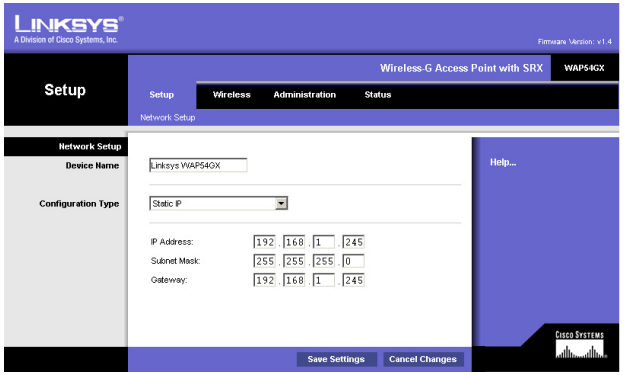

Figure 6-3: Setup - Static IP Screen

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.

Figure 6-4: Wireless - Basic Wireless Settings Screen

Basic Wireless Settings

Configure the Access Point using the available settings.

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. To disable wireless performance, select **Disabled**.

Network Name (SSID). Enter the name of the Access Point's wireless network.

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

SSID Broadcast. This feature allows the 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 SSID to all wireless devices in range. Click **Disabled** to increase network security and block the SSID from being seen on networked PCs.

The Wireless - Wireless Security Tab

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

Wireless Security

Security Mode. Select the security method you want to use, **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed**, **WPA-Enterprise**, **RADIUS**, or **WEP**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is a stronger version of WPA. 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 **Disabled**.

WPA-Personal

Encryption. 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**.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. 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.

WPA2-Personal

Encryption. **AES** is automatically selected as the encryption method.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. 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.

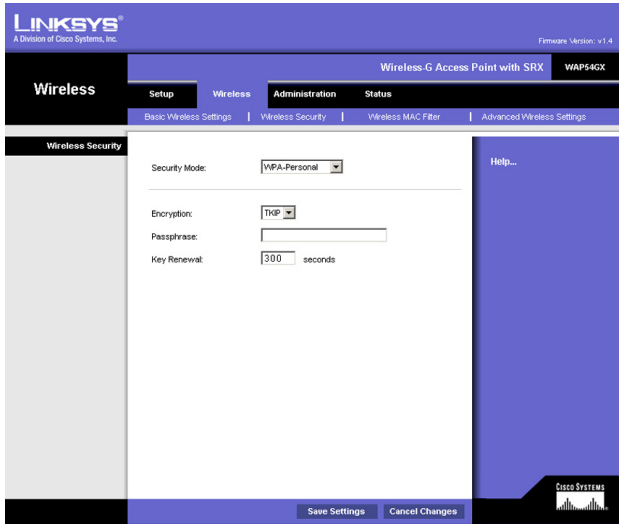

Figure 6-5: Wireless - Wireless Security (WPA-Personal) Screen

encryption: *encoding data transmitted in a network.*

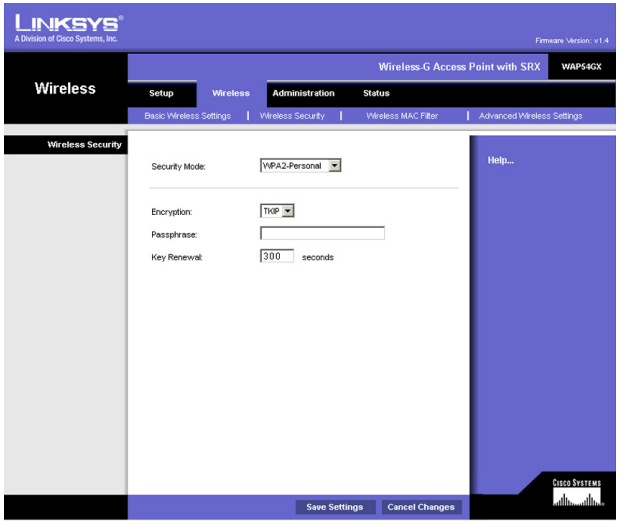

Figure 6-6: Wireless Security - WPA2-Personal Screen

WPA2-Mixed

Encryption. **TKIP + AES** is automatically selected so both methods can be used.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. 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.

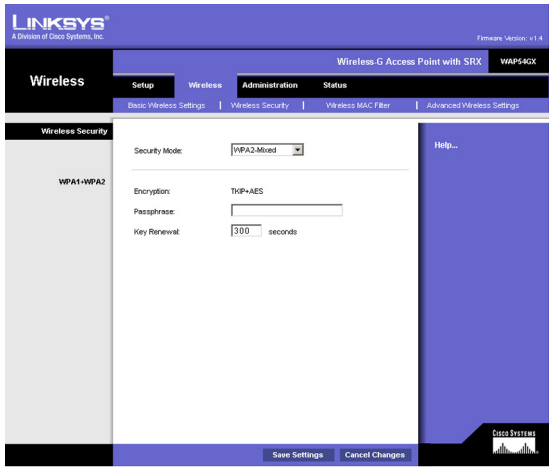

Figure 6-7: Wireless Security - WPA2-Mixed Screen

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.)

Encryption. 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. Enter the RADIUS server's IP address.

RADIUS 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. 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.

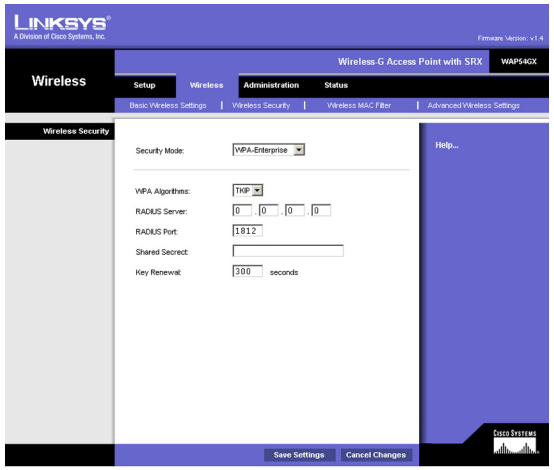

Figure 6-8: Wireless Security - WPA-Enterprise Screen

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.)

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

RADIUS 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.

Encryption. Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **104/128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, 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.

TX Key. Select which Key to use for data transmissions.

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.

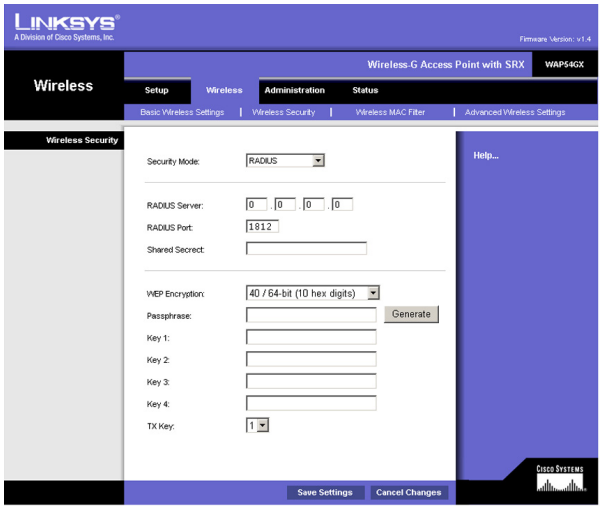

Figure 6-9: Wireless Security - RADIUS Screen

WEP

Encryption. Select a level of WEP encryption, **40/64 bits (10 hex digits)** or 104/**128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, 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.

TX Key. Select which Key to use for data transmissions.

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.

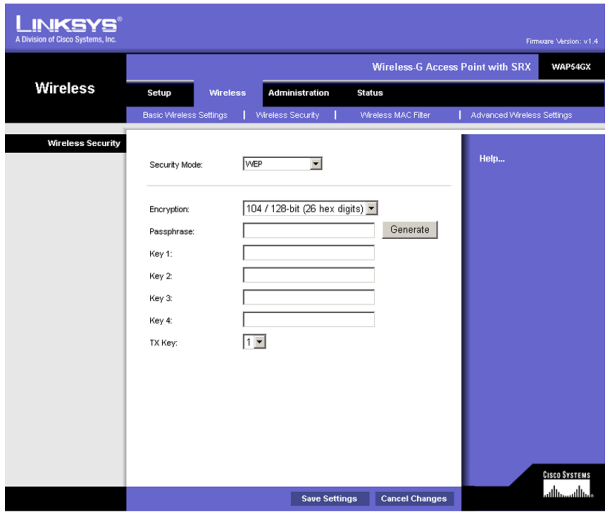

Figure 6-10: Wireless Security - WEP Screen

The Wireless - Wireless MAC Filter Tab

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

Wireless MAC Filter

Access Restriction

If you want to allow access to your wireless network, select **Enable**. Then, click **Permit PCs listed below to access the wireless network**.

MAC 1-50. Enter the MAC addresses of the computers whose access you want to allow. To see a list of MAC addresses for wireless computers or clients, click the **Wireless Client Table** button.

The *Wireless Client List* screen will list MAC addresses for your wireless devices. Click the **Refresh** button to get the most up-to-date information. To add a specific computer to the Mac Address Filter List, click the **Save to MAC Filter** button and then the **Add** button. Click the **Close** button to return to the *Wireless MAC Address Filter* screen.

Click the **Clear** button if you want to delete a MAC addresses you have entered.

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.

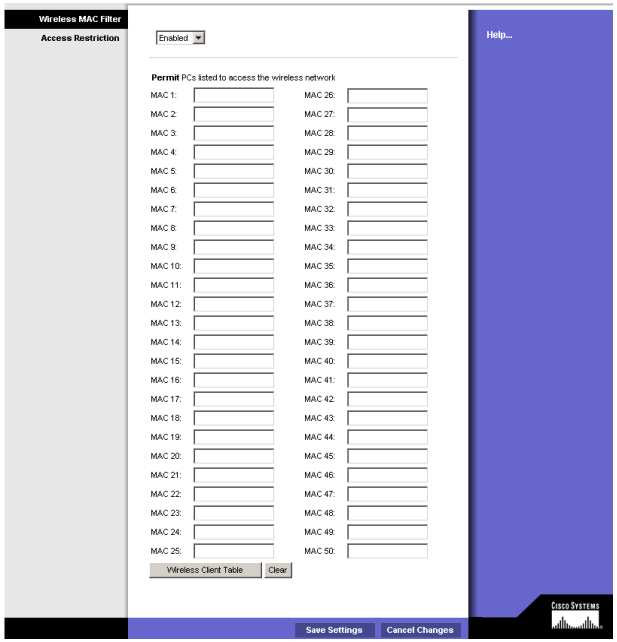

Figure 6-11: Wireless - Wireless MAC Filter Screen

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

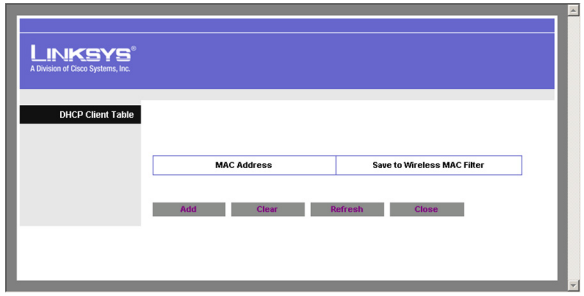

Figure 6-12: Wireless - Wireless Client Table

The Wireless - Advanced Wireless Settings Tab

This screen allows you to configure the advanced settings for the Access Point. In most cases, these settings do not need to be changed.

Advanced Wireless

You can change the data transmission and output power settings for the Access Point.

Authentication Type. Select the authentication method you want the Access Point to use, **Shared Key, Open System, or Auto**. 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. In most cases, keep the default, **Open System**, otherwise use **Auto**.

CTS Protection Mode. The CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance. Select **Enable** if you want to permanently enable this feature, or keep the default, **Disable**, if you want to permanently disable this feature. In most cases, CTS Protection Mode should remain disabled, unless the Wireless-G products are experiencing severe problems trying to transmit to the Access Point in an environment with heavy 802.11b traffic.

ACK Mode. This setting prioritizes QoS for users who also have ACK Mode enabled. Users with Immediate ACK (the default setting) will experience reliable connectivity for normal network use. Burst ACK is faster but less reliable and may also affect long-range wireless performance. The No ACK setting disables the ACK feature. Clients utilizing ACK must have their wireless adapter on the same setting as the Router. This is normally used in a multicast broadcast like video. Do not use this unless you are an advanced user.

Transmission Rates. The range is from 1 to 108Mbps. 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, **Auto** (Default), to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client.

Preamble Type. The preamble defines the length of the CRC block for communication between the Access Point and the roaming Network Card. (High network traffic areas should use the shorter preamble type.) Select the appropriate preamble type, **Long Preamble (default)** or **Short Preamble**.

Network Density. This setting is a reflection of the Access Point's range. Setting the density to **Low** provides you with a greater range. Setting the density to **High** gives you a lower range. The default setting is Low.

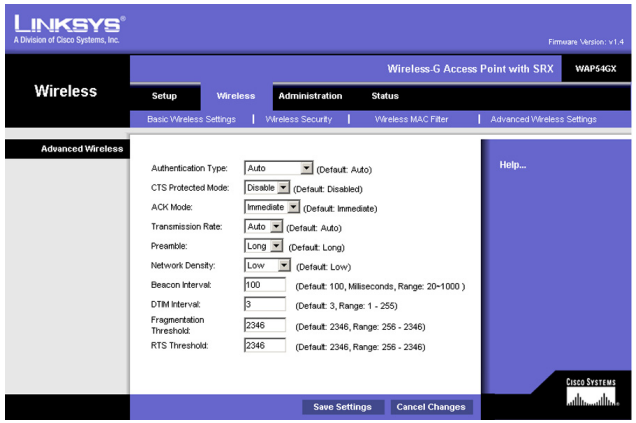

Figure 6-13: Wireless - Advanced Wireless Settings Screen

***cts** (clear-to-send): a signal sent by a wireless device, signifying that it is ready to receive data.*

Beacon Interval. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless networks service area, the Access Point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

packet: *a unit of data sent over a network.*

beacon internal: *data transmitted on your wireless network that keeps the network synchronized.*

DTIM Interval. This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.

dtim *(delivery traffic indication message): a message included in data packets that can increase wireless efficiency.*

Fragmentation Threshold. This specifies the maximum size a data packet can be before splitting and creating a new packet. It should remain at its default setting of **2346**. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

fragmentation: *breaking a packet into smaller units when transmitting over a network.*

RTS Threshold. This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications are recommended.

rts *(request to send): a networking method of coordinating large packets through the RTS Threshold setting.*

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.