CHAPTER 4

Security Features

This chapter describes the security features of your client adapter and provides instructions for enabling security.

The following topics are covered in this section:

Overview of Security Features

When you use your client adapter with the Mac OS operating system, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of Wired Equivalent Privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the LEAP authentication process. The information in the sections below can help you to decide which type of WEP keys you want to use. Dynamic WEP keys with LEAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits in length. The 128-bit WEP keys contain more characters than the 40-bit keys and, therefore, offer a greater level of security.

Message integrity check (MIC) is a security protection feature supported by your client adapter in conjunction with an access point (see the "MIC" section on page 4-4).

Static WEP Keys

Each device (or profile) within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys must match in all devices that are to communicate with each other), the device discards the packet.

For the Mac OS X, the Static WEP keys are write-only and stored in an encrypted format (for security reasons) in your Macintosh; therefore, you cannot read them back. When the driver loads and reads the client adapter's parameters, it also finds the static WEP keys, decrypts them, and stores them in volatile memory on the client adapter. The WEP keys in the client adapter are temporary and they are lost when power to the adapter is removed or the Macintosh is rebooted. Although the keys in the client adapter are temporary, you do not need to re-enter them when you restore power or reboot because the keys are stored in your Macintosh.

For the Mac OS 9.x, the Static WEP keys can be permanently or temporarily stored in your client adapter. If the keys are temporarily stored in volatile memory, the keys will be lost when power is removed from your client adapter.

The client utility allows you to enable or disable static WEP and to add or change keys.

Dynamic WEP Keys with EAP

The new standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE), is called *802.1X for 802.11*, or simply *802.1X*. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

The use of an 802.1X authentication type, which is supported by the client and the authentication server, causes the following to occur:

- After associating to the access point, the client does not gain access to the network until mutual authentication between the client and the authentication server is successful.
- The client and authentication server derive the same dynamic WEP key.
- The authentication server sends the dynamic WEP key to the access point.
- For the length of a session, or time period, the access point and the client use the dynamic WEP key to encrypt and decrypt all unicast packets that travel between the access point and the client.

A Cisco Aironet client adapter running on the Mac OS operating system supports the following 802.1X authentication type:

- EAP-Cisco Wireless (or LEAP)

EAP-Cisco Wireless or LEAP

Support for EAP-Cisco Wireless or LEAP is provided in a Cisco Aironet client adapter's firmware and the Cisco software that supports it. The RADIUS servers that support LEAP include Cisco Secure ACS version 2.6 and above and Cisco Access Registrar version 1.7 and above.

LEAP is enabled or disabled using the client utility. When LEAP is enabled, the client adapter uses your LEAP username and password to perform mutual authentication with the RADIUS server through the access point. The username and password are stored in the client adapter's volatile memory; therefore, they are temporary and need to be re-entered whenever the radio is turned off, the client adapter is removed, or the Macintosh is powered down.

Note In Mac OS 9.x, when your computer is rebooted, a pop-up message appears to inform you that you must use the client utility to enter your LEAP username and password.

Note In Mac OS X, when your computer is rebooted, the Wireless Network Login screen appears and prompts you to enter your LEAP username and password.

When you enable Network-EAP on your access point and LEAP on your client adapter, authentication to the network occurs in the following sequence:

a. The client adapter associates to an access point and begins the authentication process.

Note The client adapter does not gain access to the network until the mutual authentication with the authentication server is successful.

b. Communicating through the access point, the client adapter and the authentication server complete a mutual authentication process, with the password being the shared secret for authentication. The password is never transmitted during the process.

c. If mutual authentication is successful, the client adapter and the authentication server derive a dynamic, session-based WEP key that is unique.

d. The authentication server transmits the key to the access point using a secure channel on the wired LAN.

e. For the length of a session, or a time period, the access point and the client adapter use this key to encrypt or decrypt all unicast packets that travel between them.

Note Refer to the IEEE 802.11 Standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm

MIC

Your client adapter, in conjunction with a Cisco Aironet Access Point, supports message integrity check (MIC) to protect against bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. Client adapters using driver version 1.0.3 and firmware version 4.25.2x or greater support MIC; however, MIC can be used only if it is enabled on the access point.

Note If the access point is using MIC, your client adapter's driver and firmware must support MIC; otherwise, the client cannot associate. MIC operation on your client adapter is automatic when the feature is enabled on the access point.

Security Options for Mac OS 9.x

Configuring WEP Keys

The client utility allows you to create a new WEP key or use an existing key.

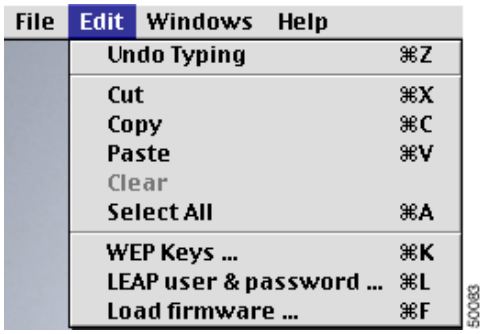
Note Entering a WEP key does not enable WEP.

Entering a New WEP Key

Follow the instructions below to enter a new WEP key for your client adapter. If you wish to select an existing WEP key, go to the "Selecting an Existing WEP Key" section on page 4-8.

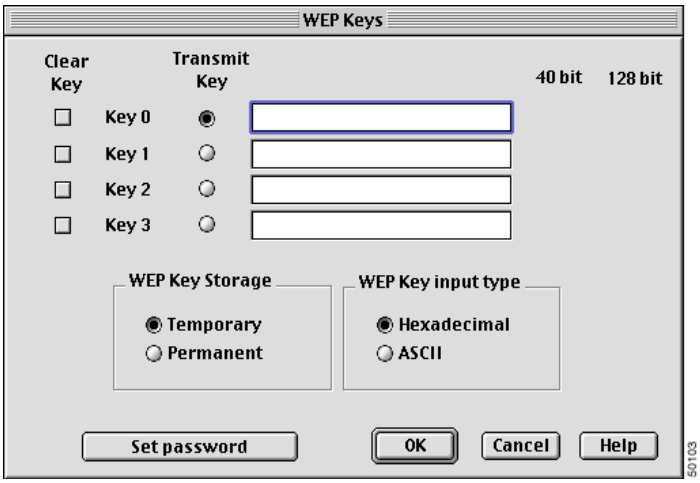
Step 1 Select **WEP Keys** from the Edit pull-down menu (see Figure 4-1).

Figure 4-1 Edit Pull-Down Menu



The WEP Keys screen (see Figure 4-2) allows you to create up to four WEP keys.

Figure 4-2 WEP Keys Screen



Step 2 Under WEP Key input type, select whether the WEP keys are entered in hexadecimal characters (0-9, A-F, and a-f) or ASCII text.

Step 3 Decide on a WEP key and enter it in the blank field for the key you are creating. Follow the guidelines below to create a new WEP key:

- Your client adapter's WEP key must match the WEP key used by the access point or clients with which you are planning to communicate.
- When setting more than one WEP key, the WEP keys must be assigned to the same WEP key numbers for all devices.
- WEP keys can be comprised of ASCII text or hexadecimal characters, depending on the option you selected in Step 2.
- WEP keys must contain the following number of characters:
  - 13 characters for 128-bit WEP keys using ASCII input
  - 26 characters for 128-bit WEP keys using hexadecimal input
  - 5 characters for 40-bit WEP keys using ASCII input
  - 10 characters for 40-bit WEP keys using hexadecimal input

Note Any key that is entered with more than 10 characters is padded by the client adapter to 26 characters to create a 128-bit key.

Note After you create a WEP key, you can delete it by selecting the Clear Key check box to the left of the key.

Step 4 Click **Transmit Key** next to the key you just created to indicate that this is the key you want to use to transmit packets.

Step 5 Click **Permanent** under WEP Key Storage to allow your client adapter to retain this WEP key even when power to the adapter is removed or the computer in which it is installed is rebooted.

If you select **Temporary**, the WEP key is lost when power is removed from your client adapter or when the adapter is reset.

Step 6 If you want the WEP Keys screen to be password protected, click the **Set Password** button. The Set Password screen (see Figure 4-3) appears.

Figure 4-3 Set Password Screen

Follow these steps to password protect the WEP keys:

a. Enter a password in the Password field.

Note Passwords are case sensitive and must contain at least eight characters.

b. Re-enter the password in the Verify Password field.

c. Click **OK** to set the password protection.

Note The next time you attempt to enter the WEP Keys screen you will be prompted to enter the correct password. After you enter the screen, the password can be changed using the Change Password button. If you leave the fields blank in the Change Password screen, the password is cleared.

Step 7 When you have completed the entry of the WEP keys, click **OK**

To enable WEP, follow the instructions in the "Enabling WEP" section on page 4-9.

Selecting an Existing WEP Key

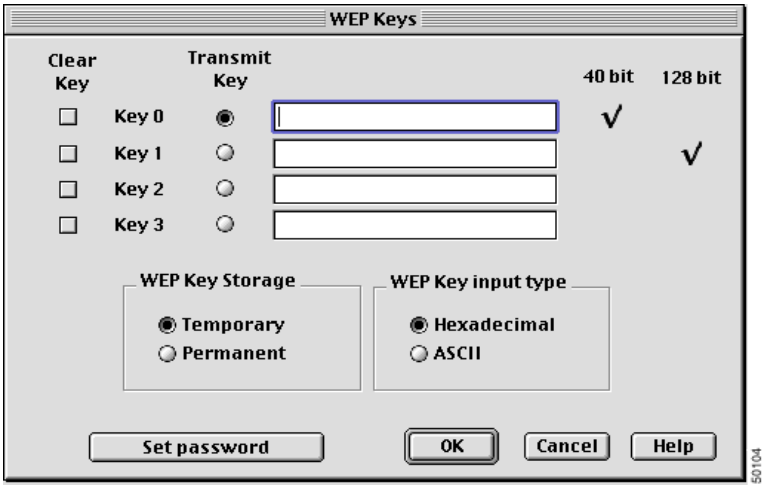
If you want an existing WEP key to be used with your client adapter, follow the instructions below.

Step 1 Select **WEP Keys** from the Edit pull-down menu (see Figure 4-1).

Step 2 Enter the correct password and click **OK**.

Step 3 The WEP Keys screen appears (see Figure 4-4).

Figure 4-4 WEP Keys Screen



A checkmark appears in the 40-bit or 128-bit column for all existing WEP keys.

Note To protect WEP key security, the codes for existing WEP keys do not appear on the screen.

Step 4 Click **Transmit Key** next to the key you want to use to transmit packets.

Step 5 Click **OK**.

To enable WEP, follow the instructions in the "Enabling WEP" section on page 4-16.

Enabling WEP

The client utility provides several screens that allow you to enable WEP for an office network or a home network.

For an Office Network

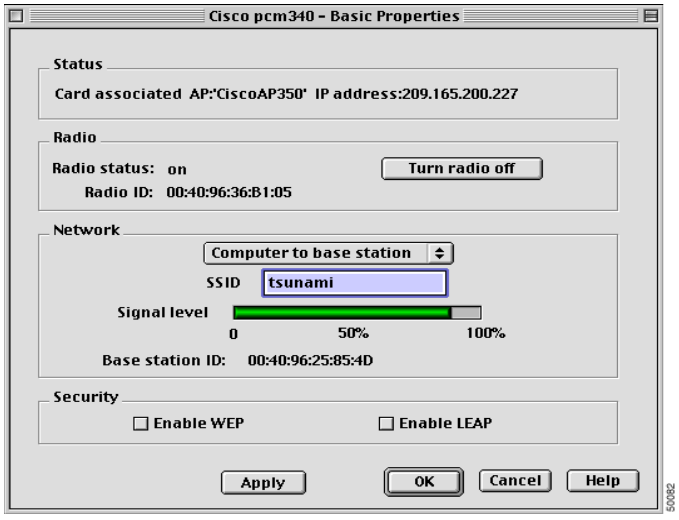
After you have created or selected a WEP key, follow the steps below to enable WEP.

Step 1 Open one of the following screens:

a. Basic Properties screen (see Figure 4-6) by selecting **Basic Properties** from the File pull-down menu (see Figure 4-5).

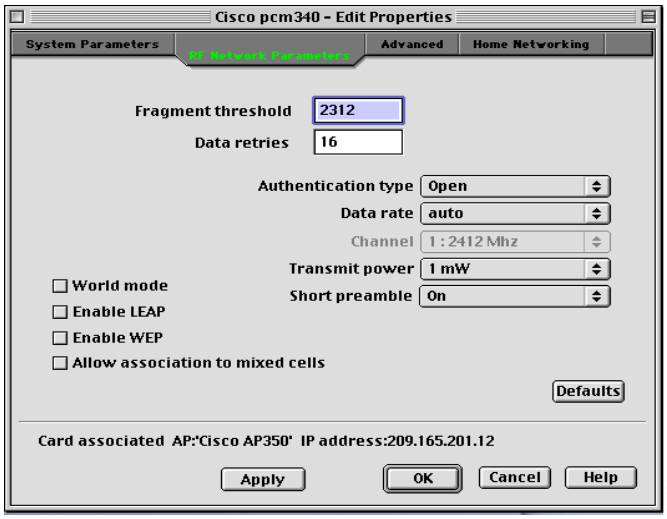
Figure 4-5 File Pull-Down Menu

Figure 4-6 Basic Properties Screen



b. RF Network Parameters screen (see Figure 4-7) by selecting **Edit Properties** from the File pull-down menu (see Figure 4-5) and click the **RF Network Parameters** tab.

Figure 4-7 RF Network Parameters Screen



Step 2 Select the **Enable WEP** check box in the Basic Properties screen or RF Network Parameters screen.

Note You can disable WEP at any time by deselecting the Enable WEP check box.

Step 3 Click **Apply**.

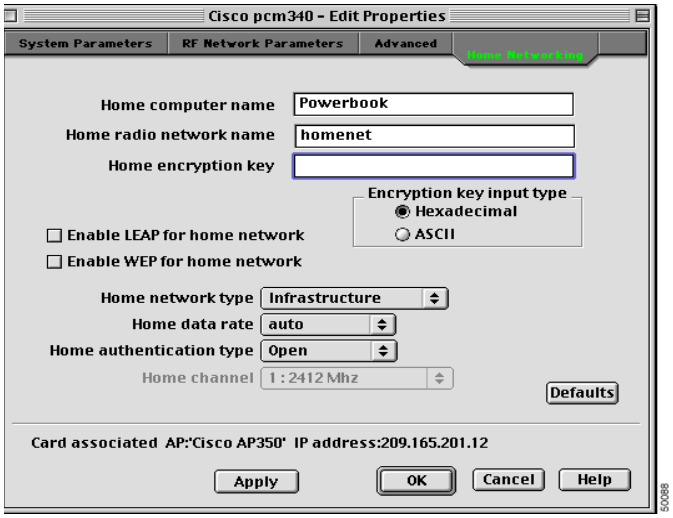
To enable LEAP, refer to the "LEAP" section on page 4-12.

For a Home Network

After you have created or selected a WEP key, follow the steps below to enable WEP.

Step 1 Open the Home Networking screen (see Figure 4-8) by selecting **Edit Properties** from the File pull-down menu (see Figure 4-5) and clicking the **Home Networking** tab.

Figure 4-8 Home Networking Screen



Step 2 Select the **Enable WEP for Home Network** check box in the Home Networking screen.

Note You can disable WEP at any time by deselecting the Enable WEP for home network check box.

Step 3 Click **Apply**.

To enable LEAP, refer to the "LEAP" section on page 4-12.

LEAP

Follow the instructions below to enable LEAP for your client adapter.

Step 1 Select **LEAP User & Password** from the Edit pull-down menu (see Figure 4-1 on page 4-5). The Set LEAP Username and Password screen appears (see Figure 4-9).

Figure 4-9 Set LEAP Username and Password Screen

Step 2 Enter your LEAP username in the Username field.

Note If you work in an environment with multiple domains and want your login domain to be passed to the RADIUS server along with your username, you must append the domain name to your username; for example: *domain\username*. Check with your network administrator.

Step 3 Enter a LEAP password in the Password field.

Step 4 Click **OK**.

Step 5 Select the **Enable LEAP** check box on one of the following screens:

- For the office network use one of the following screens:
  - Basic Properties screen (see Figure 4-6).
  - RF Network Parameters screen (see Figure 4-7).
- For the home network use the Home Networking screen (see Figure 4-8).

After LEAP is enabled, your client adapter authenticates to the RADIUS server using your LEAP username and password and receives a session-based WEP key.

Note When you enable LEAP, the Enable WEP check box is automatically checked. This indicates that dynamic, session based WEP is active. You do not have to enter a static WEP key.

Note You can disable LEAP at any time by deselecting the Enable LEAP check box, but to enable LEAP again, you will have to reenter your LEAP username and password.

Verifying Installation

To verify that you have properly installed the appropriate driver and client utilities, perform one of the following:

- Double-click the **pcm3x0PPC** icon in the Cisco pcm3x0 folder to open the pcm3x0PPC client utility. If the installation was successful, the top of the Basic Properties screen indicates that your client adapter is associated to an access point and provides its IP address.

Note If your installation was unsuccessful or you experienced problems during or after driver installation, refer to Chapter 8 for troubleshooting tips.

Security Options for Mac OS X

Configuring WEP Keys

The client utility allows you to enable or disable WEP and to create new WEP keys or use an existing key.

Note Entering a WEP key does not enable WEP.

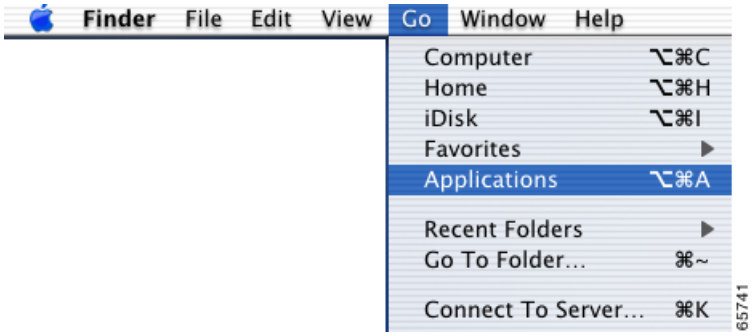
Entering a New WEP Key

Follow the instructions below to enter a new WEP key for your client adapter. If you wish to select an existing WEP key, go to the "Selecting an Existing WEP Key" section on page 4-15.

Step 1 If the client utility is not active on your desktop perform the following steps:

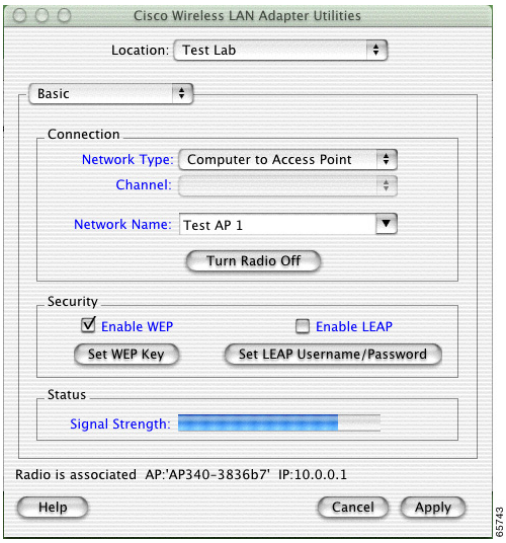
a. From the Finder menu bar on the top of the screen, select **Go** and click **Applications** (see Figure 4-10). The applications screen appears.

Figure 4-10 Finder Menu Bar



b. Double-click the **Aironet Client Utility** icon. The client utility screen appears, and the computer searches for the client adapter radio. After the radio is found, the basic properties screen appears (see Figure 4-11).

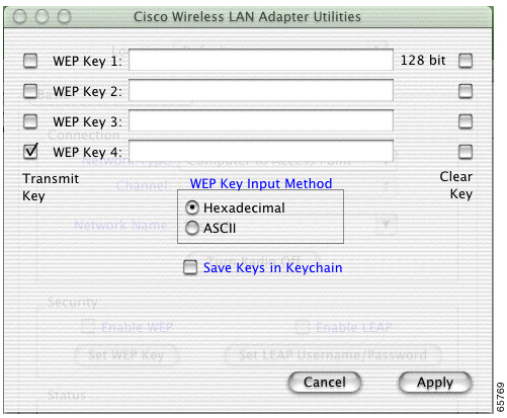
Figure 4-11 Client Utility Basic Properties Screen



Step 2 On the Client Utility Basic Properties screen, click **Set WEP Key** (see Figure 4-11). The WEP key screen appears (see Figure 4-12).

The WEP key screen allows you to create up to four WEP keys.

Figure 4-12 WEP Key Screen



Step 3 Under WEP Key Input Method, select whether the WEP keys are entered in hexadecimal characters (0-9, A-F, and a-f) or ASCII text.

Step 4 Decide on a WEP key and enter it in the blank field for the key you are creating. Follow the guidelines below to create a new WEP key:

- Your client adapter's WEP key must match the WEP key used by the access point or clients with which you are planning to communicate.
- When setting more than one WEP key, the WEP keys must be assigned to the same WEP key numbers (1 to 4) for all devices.
- WEP keys can be comprised of ASCII text or hexadecimal characters, depending on the option you selected in Step 3.
- WEP keys must contain the following number of characters
  - For 128-bit ASCII WEP keys, use 13 ASCII characters
  - For 128-bit hexadecimal WEP keys, use 26 hexadecimal characters
  - For 40-bit ASCII WEP keys, use 5 ASCII characters
  - For 40-bit hexadecimal WEP keys, use 10 hexadecimal characters

Note You must enter the number of characters shown above because the client utility does not fill the WEP key with zeros or nulls. The client utility also uses the number of characters entered to determine 40-bit or 128-bit WEP keys.

Step 5 Click **Transmit Key** next to the key you want to use to transmit packets.

Note Only one WEP key can be selected as the Transmit Key.

Note You can delete an existing WEP key by selecting the Clear Key check box to the right of the key.

Step 6 Click **Apply** when you have finished entering WEP keys**.**

To enable WEP, follow the instructions in the "Enabling WEP" section on page 4-16.

Selecting an Existing WEP Key

If you want an existing WEP key to be used with your client adapter, follow the instructions below.

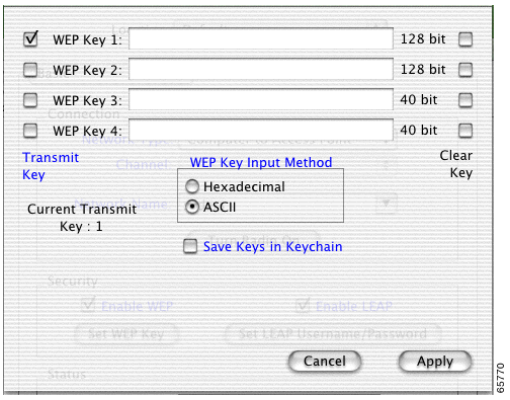
Step 1 If the client utility is not active on your desktop perform the following steps:

a. From the Finder menu bar on the top of the screen, select **Go** and click **Applications** (see Figure 4-10). The Applications window appears.

b. Double-click the **Aironet Client Utility** icon. The client utility screen appears, and the computer searches for the client adapter radio. After the radio is found, the basic properties screen appears.

Step 2 On the Client Utility Basic Properties screen, click **Set WEP Key** (see Figure 4-11). The WEP key screen appears (see Figure 4-13).

Figure 4-13 WEP Keys Screen



The WEP key size identifies all existing WEP keys; for example: 128 bit or 40 bit.

Note To protect WEP key security, the existing WEP keys do not appear on the screen.

Step 3 Click **Transmit Key** next to the key you want to use to transmit packets.

Note You can delete a WEP key by selecting the Clear Key check box to the right of the key.

Step 4 Click **Apply**.

Enabling WEP

The client utility allows you to enable or disable WEP.

Step 1 If the client utility is not active on your desktop perform the following steps:

a. From the Finder menu bar on the top of the screen, select **Go** and click **Applications** (see Figure 4-10). The Applications window appears.

b. Double-click the **Aironet Client Utility** icon. The client utility screen appears, and the computer searches for the client adapter radio. After the radio is found, the basic properties screen appears.

Step 2 On the Client Utility Basic Properties screen (see Figure 4-11), you can enable WEP by clicking the **Enable WEP** check box.

Note You can disable WEP at any time by deselecting the Enable WEP check box.

Step 3 Click **Apply**.

LEAP

The client utility allows you to enable or disable LEAP and to set your LEAP username and password.

Note You must enter your LEAP username and password each time you power-up your Macintosh, reinsert your client adapter, or turn-on the radio.

Step 1 If the client utility is not active on your desktop perform the following steps:

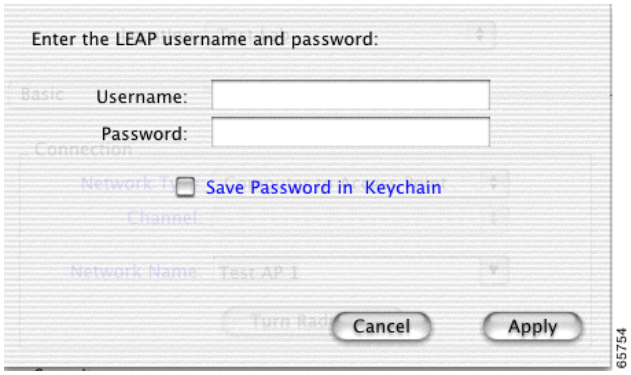
a. From the Finder menu bar on the top of the screen, select **Go** and click **Applications** (see Figure 4-10). The applications screen appears.

b. Double-click the **Aironet Client Utility** icon. The client utility screen appears, and the computer searches for the client adapter radio. After the radio is found, the basic properties screen appears.

Step 2 On the Client Utility Basic Properties screen, you can enable LEAP by clicking the **Enable LEAP** check box (see Figure 4-11).

Step 3 On the Client Utility Basic Properties screen, click **Set LEAP Username/Password** and the LEAP username and password screen appears (see Figure 4-14).

Figure 4-14 LEAP Username and Password Screen



Step 4 Type your LEAP username in the **Username** field.

Note If you work in an environment with multiple domains and want your login domain to be passed to the RADIUS server along with your username, you must append the domain name to your username; for example: domain\username.

Step 5 Type your LEAP password in the **Password** field.

Step 6 Click **Save Password in Keychain**, if you want to save your LEAP username and password in your Macintosh keychain. When saved, your LEAP password is stored (in an encrypted format) and will be automatically entered into the password field.

Step 7 Click **Apply** when you have finished entering your username and password.

After LEAP is enabled, your client adapter authenticates to the RADIUS server using your LEAP username and password and receives a session-based WEP key.

Note When you enable LEAP, the Enable WEP check box is automatically checked. This indicates that dynamic, session based WEP is active. You do not have to enter a static WEP key.

Note You can disable LEAP at any time by deselecting the Enable LEAP check box, but to enable LEAP again, you will have to reenter your LEAP username and password.

Verifying Installation

To verify that you have properly installed the driver and client utility, perform the following:

Step 1 From the Finder menu bar, click **Go** and select **Applications**. The applications screen appears.

Step 2 Double-click the **Aironet Client Utility** icon. The client utility screen appears.

If the installation was successful, the client utility successfully detects the client adapter radio and your client adapter associates to an access point and provides its IP address (check the bottom of the client utility basic properties screen).

Note If your installation was unsuccessful or you experienced problems during or after driver installation, refer to Chapter 9, “Troubleshooting.”