



Product Overview

This chapter describes the Cisco Aironet Wireless LAN Adapters, also referred to as *client adapters*, and illustrates their role in a wireless network.

The following topics are covered in this section:

- Introduction to the Client Adapters, page 1-2
- Parts of the Client Adapter, page 1-3
- Security Features of the Client Adapter, page 1-5
- Network Configurations Using the Client Adapter, page 1-7
- Positioning Your Wireless Products, page 1-10

Introduction to the Client Adapters

The Cisco Aironet Wireless LAN Adapters, also referred to as *client adapters*, are radio modules that provide transparent wireless data communications between fixed, portable, or mobile devices and other wireless devices or a wired network infrastructure. The client adapters are fully compatible when used in devices supporting Plug-and-Play (PnP) technology.

The primary function of the client adapters is to transfer data packets transparently through the wireless infrastructure. The adapters operate similarly to a standard network product except that the cable is replaced with a radio connection. No special wireless networking functions are required, and all existing applications that operate over a network will operate using the adapters.

This document covers three types of client adapters:

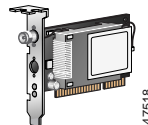
- **PC card client adapter** (also referred to as a *PC card*) – A PCMCIA card radio module that can be inserted into any device equipped with an *external* Type II or Type III PC card slot. Host devices can include laptops, notebook computers, personal digital assistants, and hand-held or portable devices.



- **LM card client adapter** (also referred to as an *LM card*) – A PCMCIA card radio module that can be inserted into any device equipped with an *internal* Type II or Type III PC card slot. Host devices usually include hand-held or portable devices.



- **PCI client adapter** – A client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop computer.



Refer to the “Radio Antenna” section on page 1-4 for antenna differences between these adapters.

Terminology

Throughout this document, the following terms are used:

- **client adapter** – Refers to all three types of adapters
- **PC card, LM card, or PCI client adapter** – Refers to only a specific adapter
- **workstation (or station)** – Refers to a computing device with an installed client adapter

Parts of the Client Adapter

The client adapter is composed of three major parts: a radio, a radio antenna, and two LEDs.

Radio

The client adapter contains a direct-sequence spread spectrum (DSSS) radio that operates in the 2.4-GHz license-free Industrial Scientific Medical (ISM) band. The radio transmits data over a half-duplex radio channel operating at up to 11 Mbps.

DSSS technology causes radio signals to be transmitted over a wide frequency range, using multiple frequencies simultaneously. The benefit of this technology is its ability to protect the data transmission from interference. For example, if a particular frequency encounters noise or interference or both, enough redundancy is built into the signal on other frequencies that the client adapter usually will still be successful in its transmission.

Radio Antenna

The type of antenna used depends on your client adapter:

- PC cards have an integrated, permanently attached diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by allowing the card to switch and sample between its two antenna ports in order to select the optimum port for receiving data packets. As a result, the card has a better chance of maintaining the radio frequency (RF) connection in areas of interference. The antenna is housed within the section of the card that hangs out of the PC card slot when the card is installed.
- LM cards are shipped without an antenna; however, an antenna can be connected through the card's external connector. If a snap-on antenna is used, it should be operated in diversity mode. Otherwise, the antenna mode used should correspond to the antenna port to which the antenna is connected.
- PCI client adapters are shipped with a 2-dBi dipole antenna that attaches to the adapter's antenna connector. However, other types of antennas may be used. PCI client adapters can be operated through the right antenna port only.



Note

Refer to the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for information on setting the client adapter's antenna mode.



Note

External antennas used in combination with a power setting resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are not allowed for use within the European community and other countries that have adopted the European R&TTE directive or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas in those countries, contact Cisco Corporate Compliance. See also the "Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC" section on page C-4.

LEDs

The client adapter has two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to Chapter 4 for an interpretation of the LED codes.

Security Features of the Client Adapter

The client adapter supports two principal security features to protect your data as it is transmitted through your wireless network: Wired Equivalent Privacy (WEP) keys and Extensible Authentication Protocol (EAP) or LEAP (also referred to as *EAP - Cisco Wireless*).

WEP Keys

WEP is an optional IEEE 802.11 feature that provides your client adapter and other devices on your wireless network with data confidentiality equivalent to that of a wired LAN. It involves packet-by-packet data encryption by the transmitting device and decryption by the receiving device.

Each device within your wireless network is assigned up to four encryption keys, called *WEP keys*, that encrypt data before it is transmitted. If a device receives a packet that is not encrypted with the appropriate key (as the *WEP keys* of all devices must match), the device discards the packet and never delivers it to the intended receiver.

For the client adapter, *WEP* is implemented through the client utilities. In Windows and Linux operating systems, the Client Encryption Manager (CEM) utility allows you to set *WEP keys*, and the Aironet Client Utility (ACU) is used to enable *WEP*. In the MacOS 9.x operating system, *WEP keys* are set and enabled in one utility.

**Note**

Refer to the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for instructions on setting *WEP keys* and enabling *WEP* for your specific operating system.

EAP and LEAP

EAP is an optional IEEE 802.1x security feature that is ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server, such as Cisco Secure ACS 2.6. The RADIUS server uses EAP to provide server-based authentication for clients.

Server-based authentication can be enabled for your client adapter in one of two ways:

- Through a host device and code built into its operating system (referred to as *EAP*)
- Through your client adapter's firmware and Cisco software (referred to as *LEAP*)

This method provides authentication service to client adapters whose host devices are not running an operating system with built-in EAP support. The term *LEAP* is used to distinguish authentication provided by the client firmware from authentication provided by a host and its operating system.

For Windows 95, 98, NT, 2000, or Me or future Windows operating systems, the Aironet Client Utility setup program, which installs the client utilities, is used to enable LEAP or EAP. After LEAP or EAP is enabled and the computer is rebooted, the client adapter authenticates to the RADIUS server using the username and password entered by the user at the network logon. See the "Installing the Client Utilities and Enabling LEAP or EAP" section on page 3-30 for instructions on using the Aironet Client Utility setup program to enable LEAP or EAP.

For Windows CE, Linux, and MacOS 9.x, LEAP is enabled through a particular screen in the client utilities. The username and password entered in this screen are used by the client adapter to authenticate to the RADIUS server. In Windows CE, you do not need to re-enter your username and password after your device is rebooted or your client adapter is ejected. In Linux and MacOS 9.x, the username and password need to be re-entered at the start of each new session. See the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for instructions on enabling LEAP through the client utilities.

When you enable EAP on your Access Points and LEAP or EAP on your client adapter, authentication to the network occurs in the following sequence:

1. The client adapter uses the username and password to start the authentication process.
2. The Access Point communicates with the EAP-compliant RADIUS server to authenticate the username and password.
3. If the username and password are valid, the RADIUS server and the client adapter negotiate a dynamic, session-based WEP key. The key, which is unique for the authenticated client, provides the client with secure network access.
4. The client and Access Point use the WEP key for all data transmissions during the session.

**Note**

Refer to the IEEE 802.11 Standard for more information on EAP 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

Network Configurations Using the Client Adapter

The client adapter can be used in a variety of network configurations. In some configurations, Access Points provide connections to your network or act as repeaters to increase wireless communication range. The maximum communication range is based on how you configure your wireless network.

This section describes and illustrates the following common network configurations:

- Ad hoc wireless local area network (LAN)
- Wireless infrastructure with workstations accessing a wired LAN

**Note**

For examples of more complex network configurations involving client adapters and Access Points, refer to the *Cisco Aironet Access Point Hardware Installation Guide*.

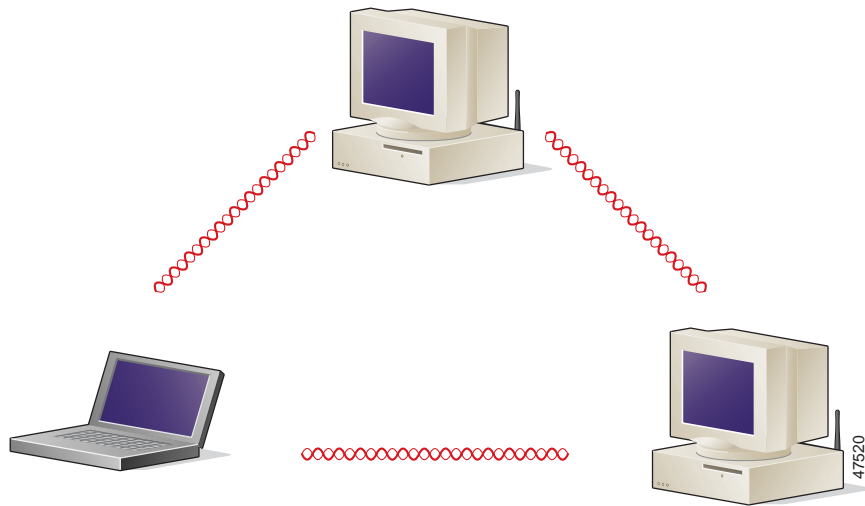
**Note**

Refer to the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for information on setting the client adapter's network mode.

Ad Hoc Wireless LAN

An ad hoc (or peer-to-peer) wireless LAN (see Figure 1-1) is the simplest wireless LAN configuration. In a wireless LAN using an ad hoc network configuration, all devices equipped with a client adapter can be linked together and communicate directly with each other.

Figure 1-1 Ad Hoc Wireless LAN

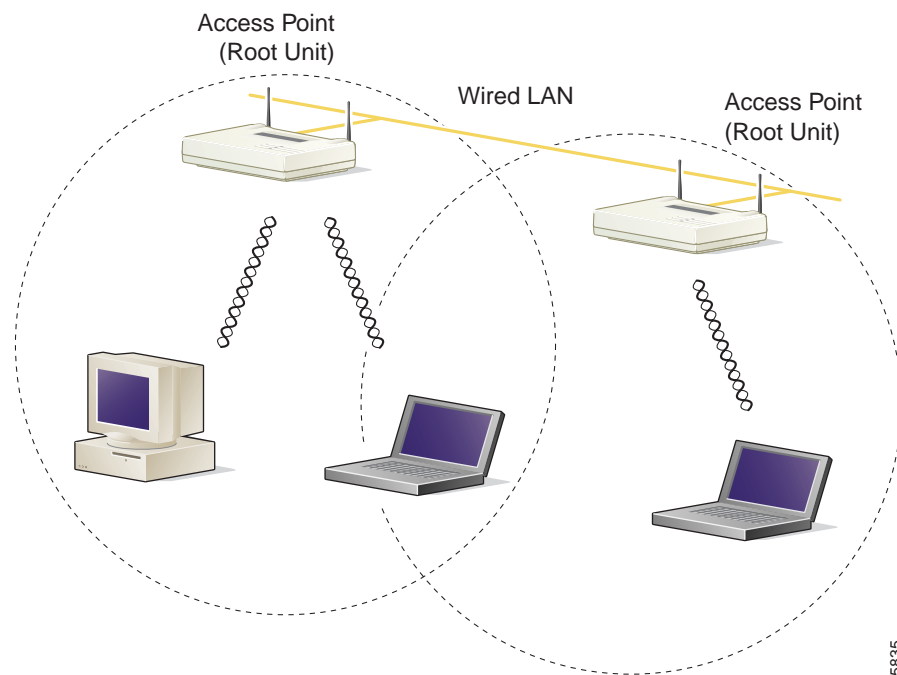


Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more Access Points on a LAN. Figure 1-2 shows a microcellular network with workstations accessing a wired LAN through several Access Points.

This configuration is useful with portable or mobile stations because it allows them to be directly connected to the wired network even while moving from one microcell domain to another. This process is transparent, and the connection to the file server or host is maintained without disruption. The mobile station stays connected to an Access Point as long as it can. However, once the transfer of data packets needs to be retried or beacons are missed, the station automatically searches for and associates to another Access Point. This process is referred to as *seamless roaming*.

Figure 1-2 *Wireless Infrastructure with Workstations Accessing a Wired LAN*



15835

Positioning Your Wireless Products

Determining the network location of your wireless products can be influenced by a number of factors. This section discusses those factors and provides guidelines and tools for achieving optimum placement.

The site survey and link test tools provided with the client utilities can help you to determine the best placement for Access Points and workstations within your wireless network. Refer to the *Cisco Aironet Wireless LAN Adapters Software Configuration Guide* for information on using these tools and to the *Cisco Aironet Access Point Hardware Installation Guide* for additional information on the placement of Access Points.

**Note**

The site survey and link test tools are not supported in the Linux operating system.

Site Survey

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Before installing the system, you should perform a site survey to determine the optimum utilization of networking components and to maximize range, coverage, and network performance.

Consider the following operating and environmental conditions when performing a site survey:

- **Data rates** – Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver threshold sensitivity occurs as the radio data increases.
- **Antenna type and placement** – Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- **Physical environment** – Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.

- **Obstructions** – A physical obstruction such as metal shelving or a steel pillar can hinder performance of the client adapter. Avoid locating the workstation in a location where there is a metal barrier between the sending and receiving antennas.
- **Building materials** – Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks. Metal or steel construction is a barrier to radio signals.

Link Test

The link test tool is used to determine RF coverage. The test results can help the installer to eliminate areas of low RF signal levels that can result in a loss of connection between the client adapter and the Access Point.

