Overview

The Cisco Aironet Cisco Aironet 1100 Series Access Point series access point is available in autonomous and lightweight configurations. The autonomous access points can support standalone network configurations with all configuration settings maintained within the access points. The lightweight access points operate in conjunction with a Cisco wireless LAN controller with all configuration information maintained within the controller.

Product Terminology

The following terms refer to the autonomous and lightweight products:

- The term *access point* describes both autonomous and lightweight products.
- The term *autonomous access point* describes only the autonomous product.
- The term *lightweight access point* describs only the lightweight product.
- The term *access point* describes the product when configured to operate as an access point.
- The term *bridge* describes the product when configured to operate as a bridge.

Autonomous Access Points

The autonomous access point (models: AIR-AP1120B or AIR-AP1121G) (model: AIR-AP1252) supports a management system based on Cisco IOS software. The 1100 series is a Wi-Fi certified, wireless LAN transceiver and uses a single mini-PCI radio (IEEE 802.11b-compliant or IEEE 802.11g-compliant).

The access point serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless access to the network.

You can configure and monitor the access point using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Lightweight Access Points

The Cisco Aironet 1100 Series Lightweight Access Point (AIR-LAP1121G) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before being mounted. The lightweight access point is automatically configured by a Cisco wireless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The lightweight access point contains one integrated radio: a 2.4-GHz radio (IEEE 802.11g). Using a controller, you can configure the radio settings.

In the Cisco Centralized Wireless LAN architecture, access points operate in the lightweight mode (as opposed to autonomous mode). The lightweight access points associate to a controller. The controller manages the configuration, firmware, and controls transactions such as 802.1x authentication. In addition, all wireless traffic is tunneled through the controller.

LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run-time operations. LWAPP also defines the tunneling mechanism for data traffic.

In an LWAPP environment, a lightweight access point discovers a controller by using LWAPP discovery mechanisms and then sends it an LWAPP join request. The controller sends the lightweight access point an LWAPP join response allowing the access point to join the controller. When the access point is joined, the access point downloads its software if the versions on the access point and controller do not match. After an access point joins a controller, you can reassign it to any controller on your network.

LWAPP secures the control communication between the lightweight access point and controller by means of a secure key distribution, using X.509 certificates on both the access point and controller.

This chapter provides information on the following topics:

Hardware Features

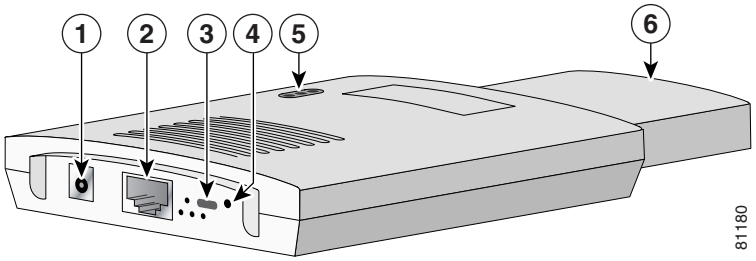
This section describes the access point features. Refer to Appendix C, "Access Point Specifications," for a list of access point specifications.

Key hardware features of the 1100 series access point include:

- Single Radio Operation, page 1-3
- Ethernet Port, page 1-3
- LEDs, page 1-4
- Power Sources, page 1-4
- UL 2043 Certification, page 1-5
- Anti-Theft Features, page 1-5

Figure 1-1 shows the location of some of the hardware features of the access point.

Figure 1-1 Access Point Layout and Connectors



1	48-VDC power port	**4**	Mode button
2	Ethernet port (RJ-45)	**5**	Status LEDs
3	Cable lock slot	**6**	Antenna

Single Radio Operation

The access point contains a 2.4-GHz radio (IEEE 802.11b-compliant or IEEE 802.11g-compliant) in a mini-PCI slot and two 2.2-dBi dipole integrated antennas. You can perform a field upgrade to the mini-PCI radio and antennas to support new radio technologies, such as the 2.4-GHz IEEE 802.11g-compliant radio.

Ethernet Port

The auto-sensing Ethernet port accepts an RJ-45 connector, linking the access point to your 10BASE-T or 100BASE-T Ethernet LAN. The access point can receive power through the Ethernet cable from a power injector, switch, or power patch panel. The Ethernet MAC address is printed on the label on the back of the access point.

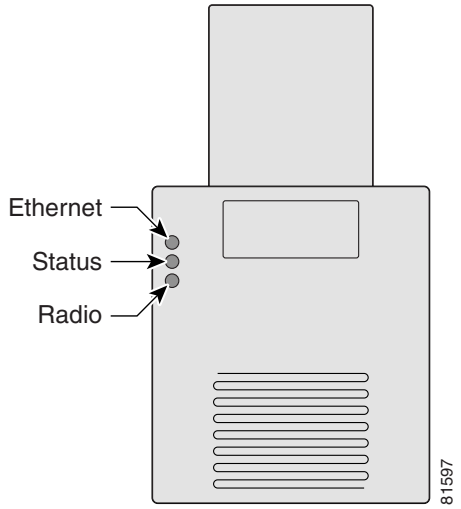
LEDs

The three LEDs on the top of the access point report Ethernet activity, association status, and radio activity.

- The Ethernet LED signals Ethernet traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED signals wireless traffic over the radio interface. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point radio.

Figure 1-2 shows the three status LEDs.

Figure 1-2 Access Point LEDs



Power Sources

The access point draws up to 4.9W of DC power and can receive power from an external power module or through inline power using the Ethernet cable. Using inline power, you do not need to run a separate power cord to the access point. The access point supports the following power sources:

- Power supply (input 100–240 VAC, 50–60 Hz, output 48 VDC, 0.2A minimum)
- Inline power from:
  - Cisco Aironet Power Injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=)
  - A switch capable of providing inline power, such as the Cisco Catalyst 3500XL, 3550, 4000, or 6500
  - An inline power patch panel, such as the Cisco Catalyst Inline Power Patch Panel

UL 2043 Certification

The access point is encased in a durable plastic enclosure having adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(c) of the NEC, and with Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.

Anti-Theft Features

There are two methods of securing the access point to help prevent theft:

- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, such as those used on laptop computers.
- Security hasp—When you mount the access point on a wall or ceiling using the mounting bracket and the security hasp, you can lock the access point to the bracket with a padlock. Compatible padlocks are Master Lock models 120T and 121T or equivalent.

Network Examples with Autonomous Access Points

This section describes the autonomous access point's role in three common wireless network configurations. The autonomous access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

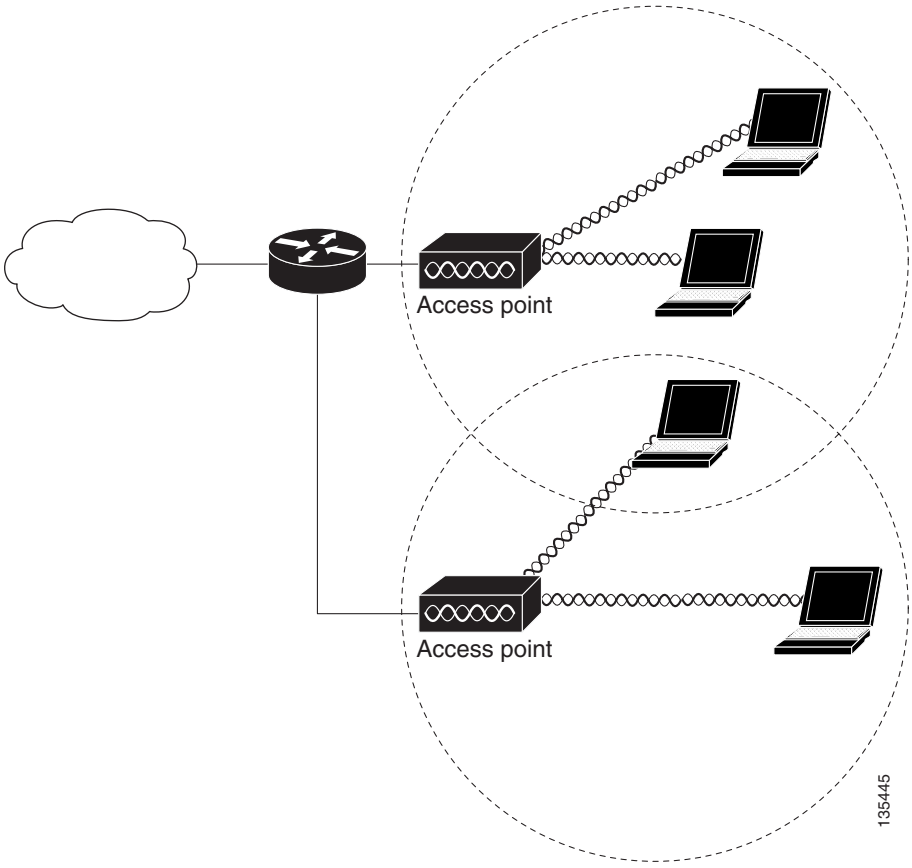
The autonomous 1100 series access point supports these operating wireless modes:

- Root access point—Connected to a wired LAN and supports wireless clients.
- Repeater access point—Not connected to a wired LAN, associates to a root access point, and supports wireless clients
- Workgroup bridge—Not connected to a wired LAN, associates to a root access point or bridge, and supports wired network devices.

Root Unit on a Wired LAN

An autonomous access point connected directly to a wired LAN provides a connection point for wireless users. If more than one autonomous access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-3 shows access points acting as root units on a wired LAN.

Figure 1-3 Access Points as Root Units on a Wired LAN

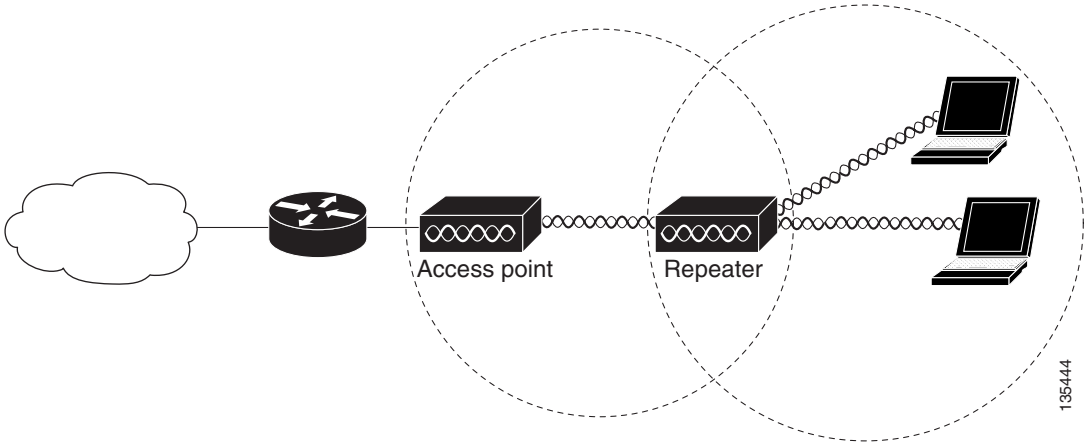


Repeater Unit that Extends Wireless Range

An autonomous access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-4 shows an autonomous access point acting as a repeater. Consult the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting up an access point as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

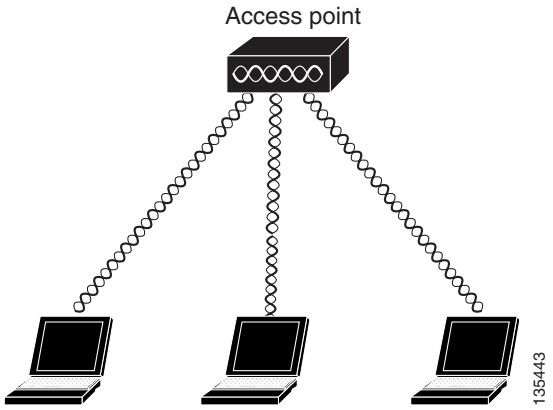
Figure 1-4 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an autonomous access point acts as a stand-alone root unit. The autonomous access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-5 shows an autonomous access point in an all-wireless network.

Figure 1-5 Access Point as Central Unit in All-Wireless Network

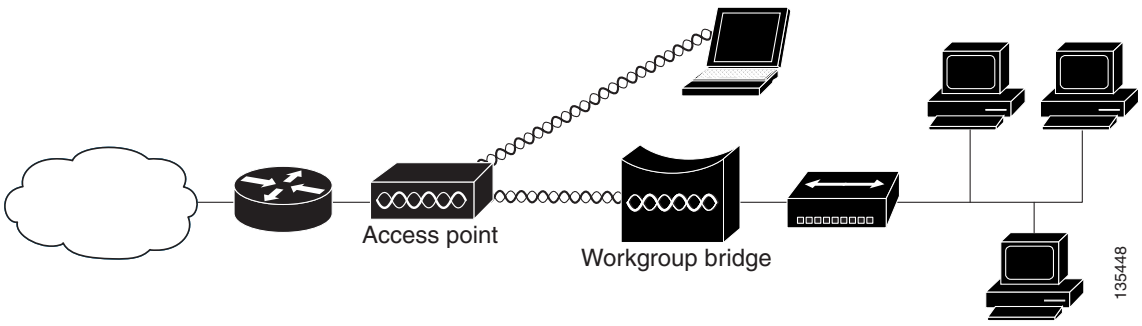


Workgroup Bridge Configuration

When configured in the workgroup bridge mode, the autonomous unit provides a wireless connection for remote wired devices to a Cisco Aironet access point or to a Cisco Aironet bridge.

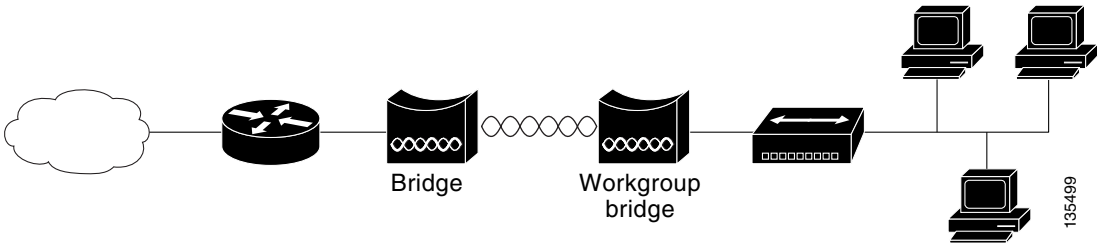
In Figure 1-6, the unit is configured in workgroup bridge mode and is associated to a Cisco Aironet access point as a wireless client device. This configuration allows the Ethernet-enabled devices to pass Ethernet traffic to and from the main LAN using the workgroup bridge.

Figure 1-6 Workgroup Bridge Configuration 1



In Figure 1-7, the autonomous unit is configured in workgroup bridge mode and is associated to a Cisco Aironet root bridge as a wireless bridge device. This configuration allows the Ethernet-enabled devices pass Ethernet traffic to and from the main LAN using the workgroup bridge. The main advantage of this configuration is that the wireless communication link can be over a longer distance than an access point supports. Typically, an access point can communicate over approximately a 1-mile range; however, the bridge-to-bridge wireless link can communicate over approximately a 21-mile range.

Figure 1-7 Workgroup Bridge Configuration 2



Network Example with Lightweight Access Points

The lightweight access points support Layer 3 network operation. Lightweight access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

Figure 1-8 illustrates a typical Layer 3 network configuration containing lightweight access points.

Figure 1-8 Typical Layer 3 Network Configuration Example