CHAPTER 1

Overview

The Cisco Aironet 1130AG 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

Cisco Aironet 1130AG Series Access Point (models: AIR-AP1131AG and AIR-AP1131G) supports a management system based on Cisco IOS software. The 1130AG series access point is a Wi-Fi certified, wireless LAN transceiver. The 1131AG access point uses dual integrated radios (IEEE 802.11g and IEEE-802.11a). The 1131G access point uses a single integrated radio (IEEE 802.11g).

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 uninterrupted 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 1130AG Series Access Point (models: AIR-LAP1131AG and AIR-LAP1131G) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before they are 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 1131AG access point contains two integrated radios: a 2.4-GHz radio (IEEE 802.11g) and a 5-GHz radio (IEEE 801.11a). The lightweight 1131G 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:

Guidelines for Using 1130AG Series Lightweight Access Points

You should keep these guidelines in mind when you use a 1130AG series lightweight access point:

- The access points can communicate only with 2006 or 4400 series controllers. Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because they lack the memory required to support access points running Cisco IOS software.
- The access points do not support Wireless Domain Services (WDS). The access points communicate only with controllers and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support eight BSSIDs per radio and a total of eight wireless LANs per access point. When a lightweight access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- The access points do not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debuging purposes (all configuration commands are disabled after connecting to a controller).

Hardware Features

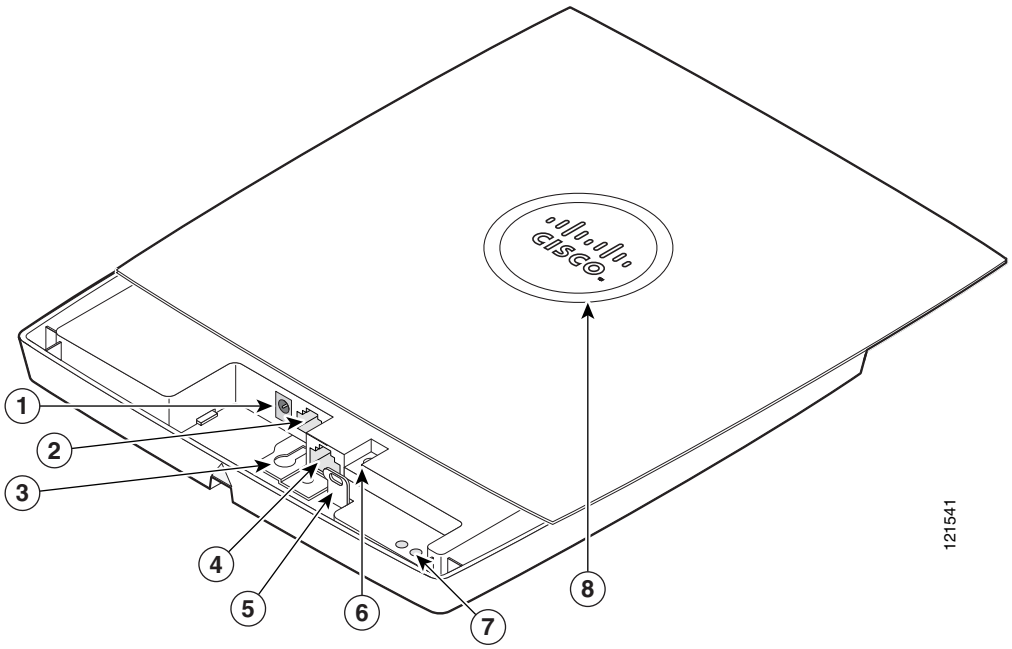
Key hardware features of the access point include:

- Dual-radio operation (see page 1-4)
- Ethernet port (see page 1-4)
- Console port (see page 1-4)
- LEDs, (see page 1-4)
- Multiple power sources (see page 1-5)
- UL 2043 certification (see page 1-5)
- Anti-theft features (see page 1-6)

Refer to Appendix C, "Access Point Specifications," for a list of access point specifications.

Figure 1-1 shows the access point hardware features.

Figure 1-1 Access Point Hardware Features



1	48-VDC power port	**5**	Padlock post
2	Ethernet port (RJ-45)	**6**	Mode button
3	Keyhole slot	**7**	Ethernet (E) and radio (R) LEDs
4	Console port (RJ-45)	**8**	Status LED

Single or Dual-Radio Operation

The 1131AG access point supports simultaneous radio operation using a 2.4-GHz 802.11g radio and a 5-GHz 802.11a radio. The 1131G access point supports a single 2.4-GHz 802.11g radio. Each radio uses dual-diversity integrated antennas.

The 5-GHz radio incorporates an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands. The 802.11g radio is called *Radio0* and the 802.11a radio is called *Radio1*.

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 (refer to the "Locating the Product Serial Number" section on page xiii). The port is located in a cable bay area that is hidden by the closed top cover (see Figure 1-1).

Note Do not attempt to connect a cable with a protective boot to the access point Ethernet port. Because of limited space in the connection area, booted connectors might not fit.

Console Port

The serial console port can be used to monitor the access point power-up sequences using a terminal emulator program. The port is located in a cable bay area that is hidden by the top cover (see Figure 1-1). Use an RJ-45 to DB-9 serial cable to connect your computer's COM port to the access point's serial console port. (Refer to Appendix E, "Console Cable Pinouts," for a description of the console port pinouts.) Assign the following port settings to a terminal emulator to open the management system pages: 9600 baud, 8 data bits, No parity, 1 stop bit, and no flow control.

Note Do not attempt to connect a cable with a protective boot to the access point console port. Because of limited space in the connection area, booted connectors might not fit.

LEDs

The access point has three LEDs to indicate Ethernet activity, radio activity, and status indications (see Figure 1-1). For additional information, refer to the "Troubleshooting Autonomous Access Points" section on page 3-1 or the "Troubleshooting Lightweight Access Points" section on page 4-1.

- The Status LED provides general operating status and error indications (top cover closed).
- The Ethernet LED is located in the cable bay area under the access point top cover. This LED signals Ethernet traffic on the wired Ethernet LAN and provides Ethernet error indications.
- The Radio LED is located in the cable bay area under the access point top cover. This LED signals that wireless packets are being transmitted or received over the radio interface and provides radio error indications.

Note The access point cover must be closed to view the Status LED but the cover must be open to view the Ethernet and the Radio LEDs.

Power Sources

The access point can receive power from an external power module or from inline power using the Ethernet cable. The access point supports the IEEE 802.3af inline power standard and Cisco CDP Power Negotiation. Using inline power, you do not need to run a power cord to the access point because power is supplied over the Ethernet cable.

Warning **This product must be connected to a Power over Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.** Statement 353

Caution Be careful when handling the access point; the bottom plate might be hot.

The access point supports the following power sources:

- Power module
- Inline power:
  - Cisco Aironet Power Injector (AIR-PWRINJ3 or AIR-PWRINJ-FIB)
  - An inline power capable switch, such as the Cisco Catalyst 3550 PWR XL, 3560-48PS, 3570-48PS, 4500 with 802.3AF PoE module, or the 6500 with 802.3AF PoE module
  - Other inline power switches supporting the IEEE 802.3af inline power standard

Note Some switches and patch panels might not provide enough power to operate the access point when configured with both 2.4-GHz and 5-GHz radios. At power-up, if the access point is unable to determine that the power source can supply sufficient power, the access point automatically deactivates both radios to prevent an over-current condition. The access point also activates a Status LED low power error indication (refer to the "Low Power Condition for Autonomous Access Points" section on page 3-6 or the "Low Power Condition for Lightweight Access Points" section on page 4-6).

UL 2043 Certification

The access point has 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; the AIR-PWRINJ3 power injector and the power module are not tested to UL 2043 and should not be placed in a building's environmental air space, such as above suspended ceilings.

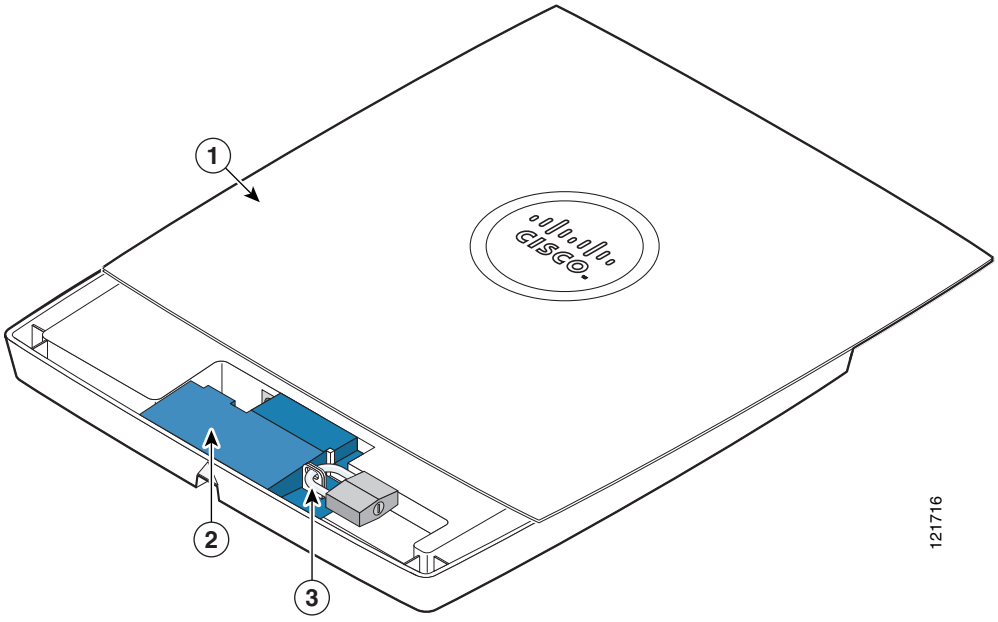
Anti-Theft Features

There are three methods of securing the access point:

- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, like those used on laptop computers (refer to the "Using a Security Cable" section on page 2-18).
- Security hasp adapter—When you mount the access point on a wall or ceiling using the mounting plate and the security hasp adapter, you can lock the access point to the plate with a padlock (see Figure 1-2). Compatible padlocks are Master Lock models 120T and 121T or equivalent.

Note The security hasp adapter covers the cable bay area (including the power port, Ethernet port, console port, and the mode button) to prevent the installation or removal of the cables or the activation of the mode button.

Figure 1-2 Access Point with Security Hasp Adapter



1	Access point cover in open position	**3**	Security padlock
2	Security hasp adapter		

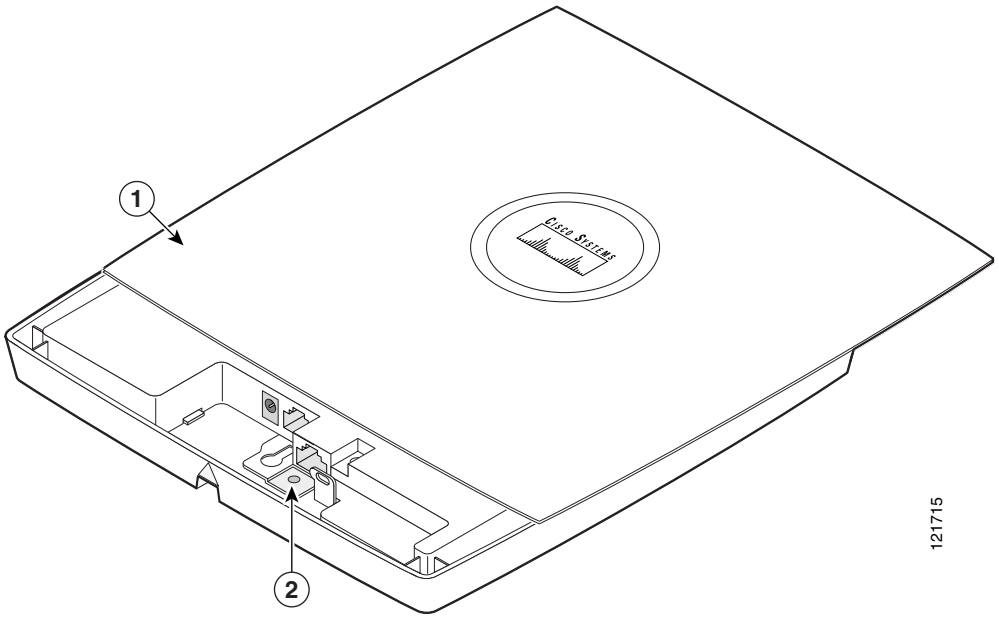
- Security screw—The access point contains a security screw hole (see Figure 1-3) that can be used to secure the access point to the mounting plate.
  - When the supplied #8 Philips head screw is used, the access point is prevented from accidently detaching from the mounting plate in vertical and over-head mounting positions.

Note The supplied #8 Philips head screw provides minimal anti-theft protection.

– When a tamper-resistant head screw (user supplied) is used, access to the mounting screws that attach the mounting plate is greatly restricted.

Note The use of a tamper-resistant head screw does not restrict access to the access point cables or the mode button.

Figure 1-3 Access Point Security Screw Hole



1	Access point cover in open position	2	Security screw hole

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 or workgroup bridge roles require a specific configurationsetting.

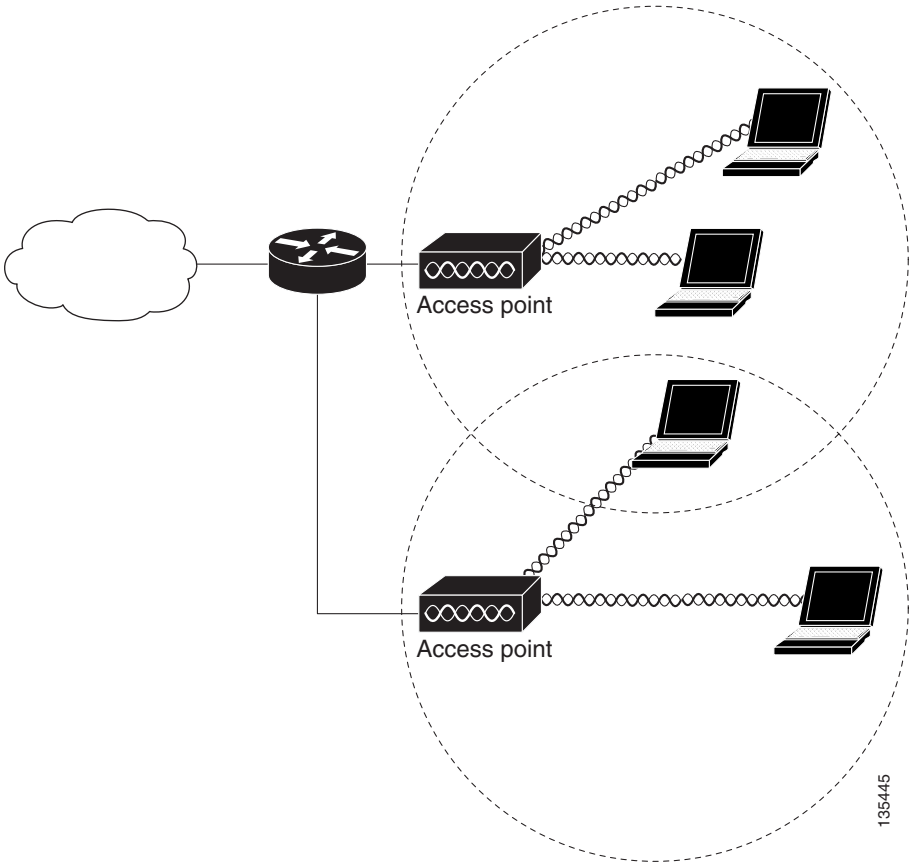
The autonomous 1130AG series access point supports these operating wireless modes:

- 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 1-4 shows access points acting as root units on a wired LAN.

Figure 1-4 Access Points as Root Units on a Wired LAN

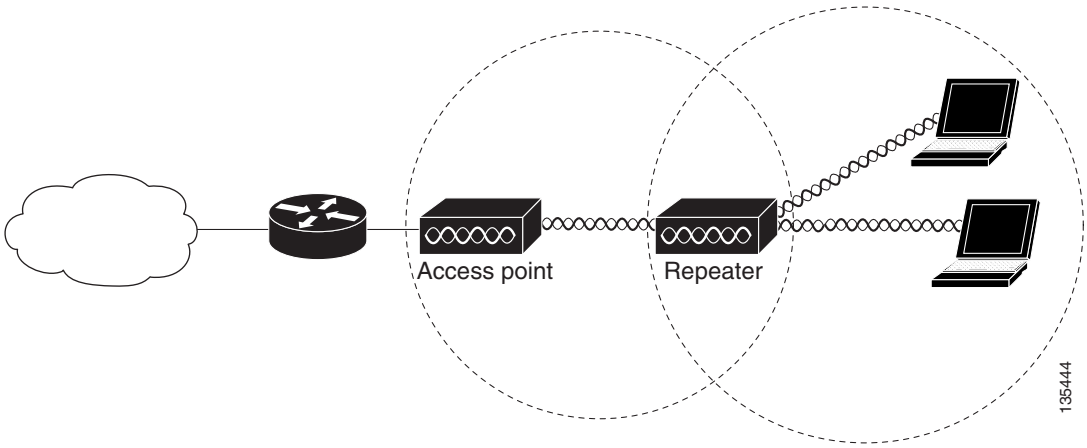


Repeater Unit that Extends Wireless Range

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 1-5 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.

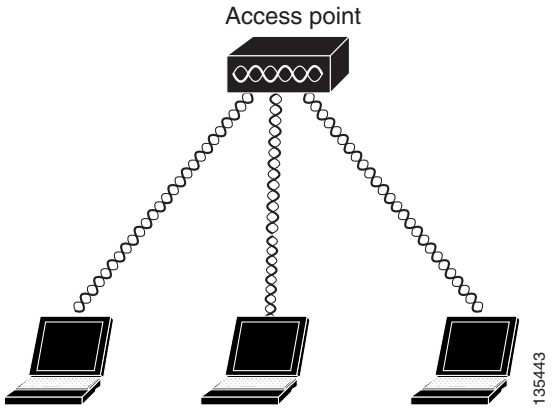
Figure 1-5 Access Point as Repeater



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 1-6 shows an autonomous access point in an all-wireless network.

Figure 1-6 Access Point as Central Unit in All-Wireless Network

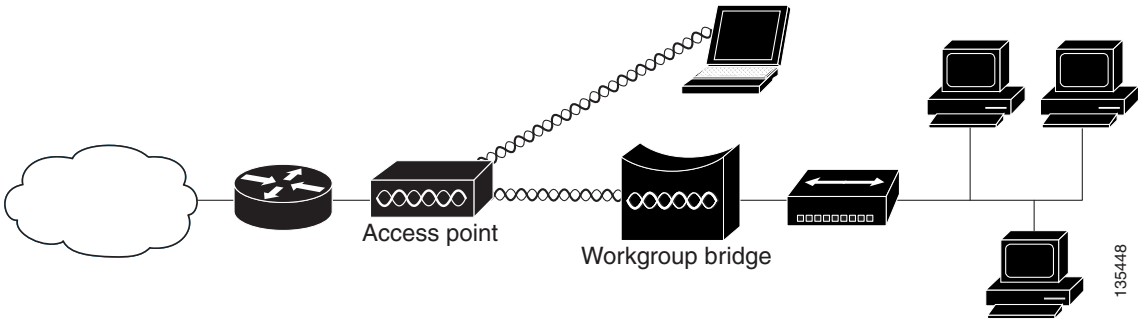


Workgroup Bridge Configuration

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.

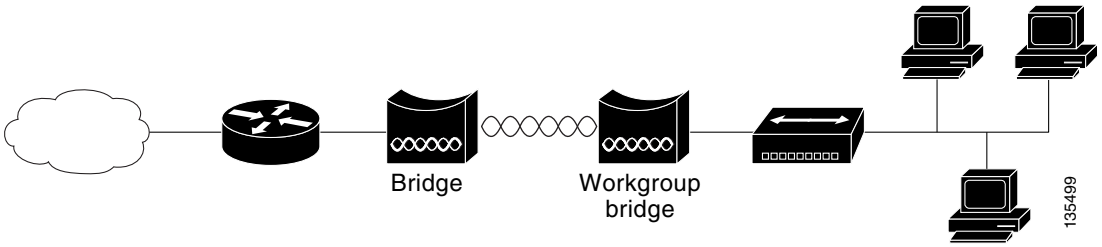
In Figure 1-7, the unit is configured in workgroup bridge mode and is associated to a Cisco Aironet access point as a wireless client device. This configuration allows the Ethernet-enabled devices to pass Ethernet traffic to and from the main LAN using the workgroup bridge.

Figure 1-7 Workgroup Bridge Configuration 1



In Figure 1-8, 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 1-8 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 1-9 illustrates a typical network configuration containing lightweight access points.

Figure 1-9 Typical Lightweight Access Point Network Configuration Example