



# CHAPTER 1

## Overview

---

The Cisco Aironet Cisco Aironet 1200 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* describes only the lightweight product.
- The term *access point* describes a product operating as an access point.
- The term *bridge* describes a product operating as a bridge.

## Autonomous Access Points

Cisco Aironet 1200 Series Access Points (models: AIR-AP1200, AIR-AP1210, AIR-AP1220B, AIR-AP1230B, AIR-AP1220A, AIR-AP-1230A, AIR-AP1231G, and AIR-AP1232AG) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, the 1200 series access point is a Wi-Fi certified, wireless LAN transceiver.

The 1200 series access point can contain two radios: a 2.4-GHz radio (IEEE 802.11b or IEEE 802.11g) in an internal mini-PCI slot and a 5-GHz radio module (IEEE 802.11a) in an external, modified cardbus slot. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios. You can configure the radios separately, using different settings on each radio.

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, 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 1200 Series Access Points (models: AIR-LAP1231G and AIR-LAP1232AG) combine mobility and flexibility with the enterprise-class features required by networking professionals. These access points are part of the Cisco Integrated Wireless Network Solution and require no manual configuration before they are mounted. The access point is automatically configured by a Cisco wireless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The access point contains two integrated radios: a 2.4-GHz radio (IEEE 802.11g) and a 5-GHz radio (IEEE 802.11a). Using a controller, you can configure the radios separately with different settings on each.

**Note**

---

The 1200 series lightweight does not support the 802.11b radio or the 802.11a RM20A radio module.

---

In the Cisco Centralized Wireless LAN architecture, access points operate in the lightweight mode (as opposed to autonomous mode). The access points associate to a controller. The controller manages the configuration, firmware, and control 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 access point an LWAPP join response allowing the access point to join the controller. When the access point is joined, the access point attempts to download new operating system software if the software 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 access point and controller by means of a secure key distribution, utilizing X.509 certificates on both the access point and controller.

This chapter provides information on the following topics:

- [Guidelines for Using 1200 Series Lightweight Access Points, page 1-3](#)
- [Hardware Features, page 1-3](#)
- [Network Examples with Autonomous Access Points, page 1-7](#)

# Guidelines for Using 1200 Series Lightweight Access Points

You should keep these guidelines in mind when you use a 1200 series lightweight access point:

- The access points can only communicate with Cisco 2006 series wireless LAN controllers or 4400 series controllers. Cisco 4100 series, Aireospace 4012 series, and Aireospace 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) 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 debug purposes (all configuration commands are disabled when connected to a controller).

## Hardware Features

This section describes access point features. Refer to [Appendix C, “Access Point Specifications,”](#) for a list of access point specifications.

Key hardware features of the 1200 series access point include:

- [Dual-Radio Operation, page 1-4](#)
- [LEDs, page 1-5](#)
- [Ethernet Port, page 1-5](#)
- [Console Port, page 1-6](#)
- [Power Sources, page 1-6](#)
- [UL 2043 Certification, page 1-6](#)
- [Anti-Theft Features, page 1-6](#)

## Dual-Radio Operation

The access point can be initially configured at the factory for single- or dual-radio operation. You can also upgrade an access point configured for single-radio operation to support dual-radio operation using a 5-GHz radio module or a 2.4-GHz mini-PCI radio card. The access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios.

The 1200 series access point supports these radios:

- 2.4-GHz IEEE 802.11b mini-PCI radio card: MP20B, hereafter called *802.11b radio*.




---

**Note** The lightweight access points do not support the MP20B 2.4-GHz IEEE 802.11b radio.

---

- 2.4-GHz 802.11g mini-PCI radio cards: MP21G or MP31G, hereafter called the *802.11g radio*.




---

**Note** The autonomous access points require Cisco IOS Release 12.2(13)JA or later

---

- 5-GHz 802.11a radio modules:

- AIR-RM20A-x-K9—802.11a radio module with integrated antenna, hereafter called the *RM20A radio module*.




---

**Note** The lightweight access points do not support the RM20A 5-GHz 802.11a radio module.

---

- AIR-RM21A-x-K9—802.11a radio module with integrated antenna, hereafter called the *RM21A radio module*.




---

**Note** The autonomous access points require Cisco IOS Release 12.3(2)JA or later.

---

- AIR-RM22A-x-K9—802.11a radio module with external RP-TNC antenna connectors, hereafter called the *RM22A radio module*.




---

**Note** The autonomous access points require Cisco IOS Release 12.3(2)JA or later.

---



**Note**

---

Cisco Aironet CB20A client radios can sometimes fail to associate to the RM21A or RM22A radio modules because the CB20A client radio does not support all the channels supported by the radio modules. The default channel setting for the RM21A or RM22A radio module, least congested, often results in the access point settling on one of these frequencies that the CB20A client radio does not support: channel 149 (5745 GHz), channel 153 (5765 GHz), channel 157 (5785 GHz), and channel 161 (5805 GHz). To avoid this problem, set the channel on the RM21A or RM22A radio module to one of the channels supported by the CB20A client radio. For additional information, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* or the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

---

The 2.4-GHz mini-PCI radio card connects to an internal mini-PCI slot. The 5-GHz radio module connects to the access point's modified card bus connector.

All 5-GHz radio modules incorporate an Unlicensed National Information Infrastructure (UNII) radio transceiver operating in the UNII 5-GHz frequency bands. The RM21A radio module contains dual integrated omnidirectional antennas and directional antennas for diversity operation. For autonomous access points, the 802.11g radio is called *Radio0* and the 802.11a radio is called *Radio1*.

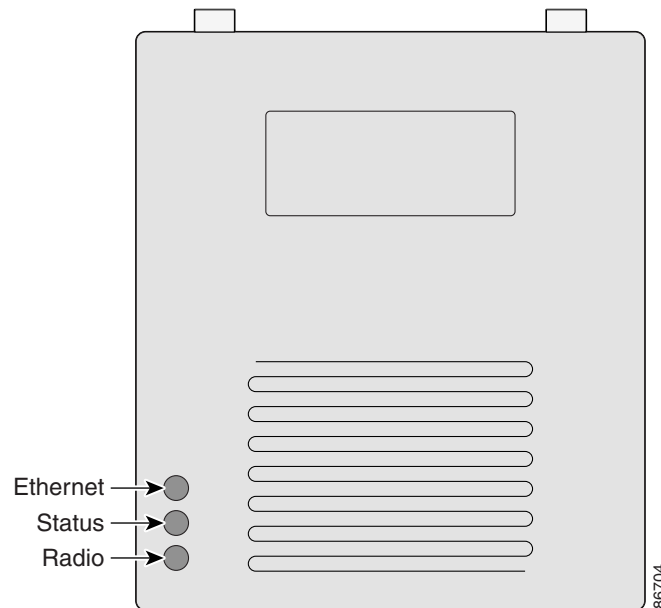
## LEDs

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. 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 1-1 shows the three status LEDs.

**Figure 1-1 Access Point LEDs**



## 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.

## Console Port

The serial console port can be used to monitor the access point power-up sequences using a terminal emulator program. 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.

## Power Sources

The access point 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 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 (AIR-PWRINJ-FIB or AIR-PWRINJ3)
  - A switch capable of providing inline power, such as Cisco Catalyst 3500XL, 3550, 4500, or 6500 switches
  - An inline power patch panel, such as the Cisco Catalyst Inline Power Patch Panel



---

**Note** The Catalyst 3550-24 PWR switch supports power for access points configured with both 2.4-GHz and 5-GHz radios. Other switches and patch panels might not provide enough power for both radios.

---

## UL 2043 Certification

The access point is encased in a durable metal case 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.

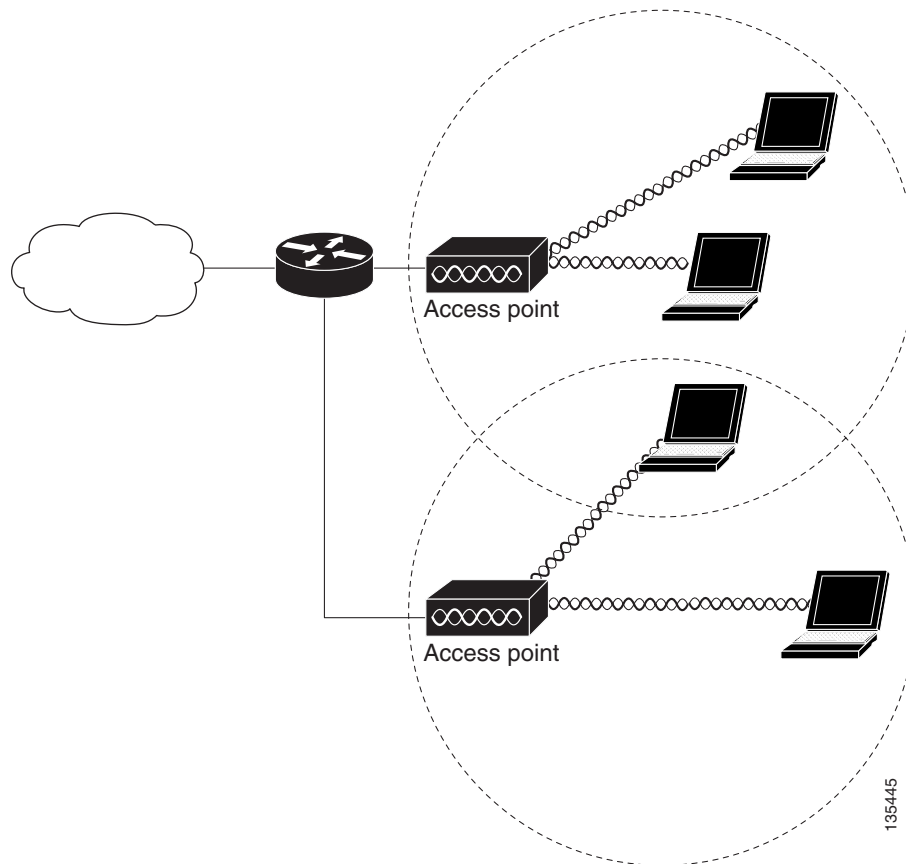
The autonomous 1200 series access point supports these operating wireless modes:

- 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 bridge—Connected to a wired LAN and supports non-root bridges and wireless clients.
- Non-root bridge—Not connected to a wired LAN, associates to a root bridge, supports wireless clients, and supports wired clients.

## Root Access Point 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 1-2](#) shows access points acting as root units on a wired LAN.

**Figure 1-2** Access Points as Root Units on a Wired LAN



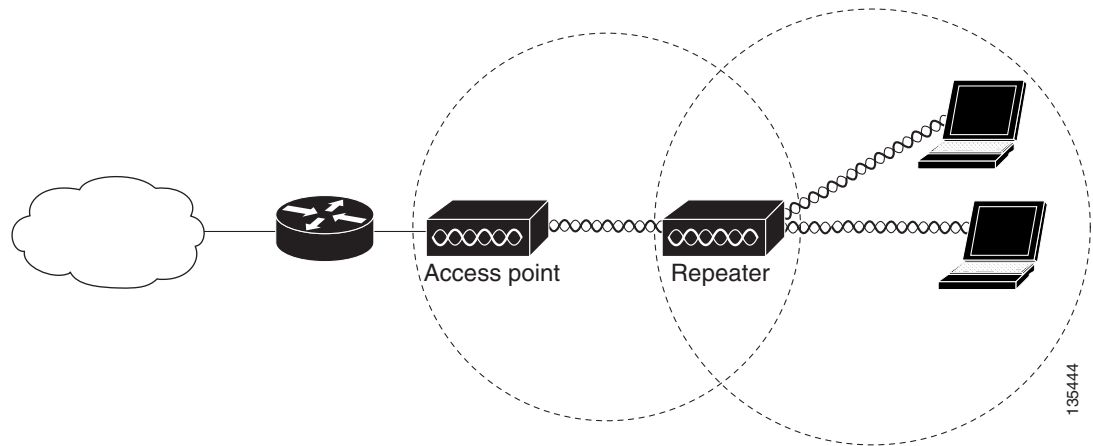
## Repeater Unit that Extends Wireless Range

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 1-3](#) 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.

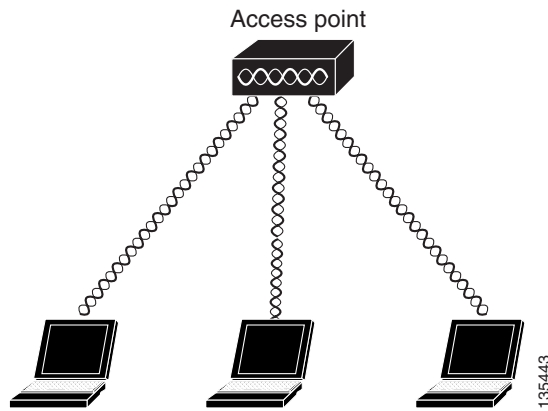
**Figure 1-3** Access Point as Repeater



## 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 1-4](#) shows an autonomous access point in an all-wireless network.

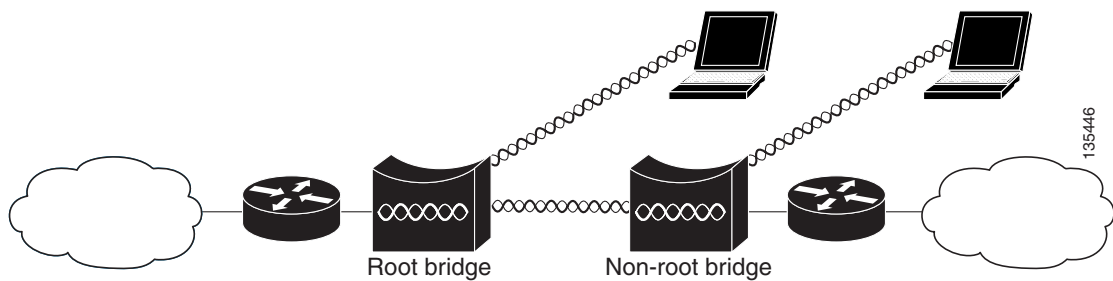
**Figure 1-4** Access Point as Central Unit in All-Wireless Network



## Bridge Network with Wireless Clients

The access point supports root bridge and non-root bridge roles used to interconnect a remote LAN to the main LAN (see [Figure 1-5](#)). The bridge units can also support wireless clients.

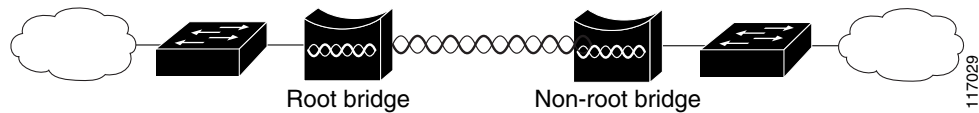
**Figure 1-5** Root Bridge and Non-root Bridge with Clients



## Point-to-Point Bridge Configuration

In a point-to-point bridge configuration, two bridges interconnect two LAN networks using a wireless communication link (see [Figure 1-6](#)). The bridge connected to the main LAN network is classified as a root bridge and the other bridge is classified as a non-root bridge.

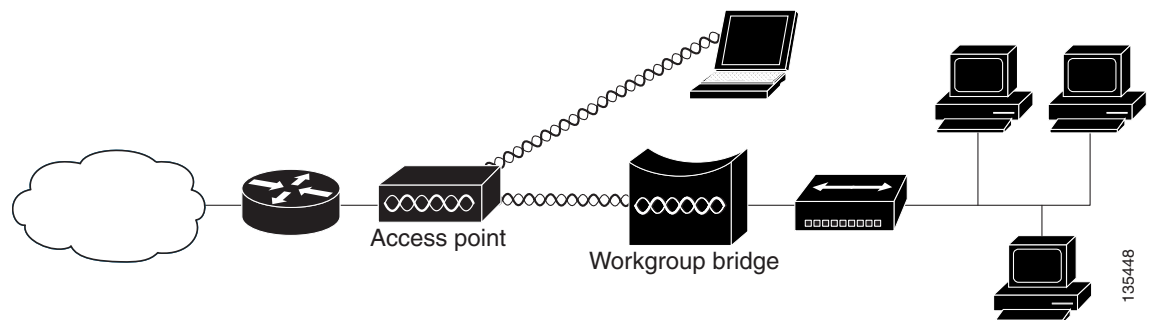
**Figure 1-6** Point-to-Point Bridge Configuration



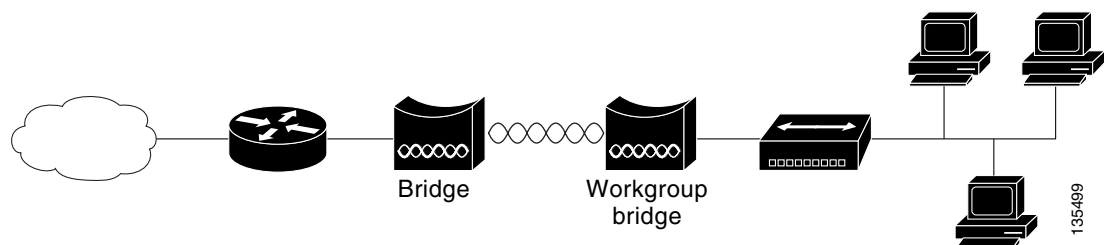
## Workgroup Bridge Network

The access point supports a workgroup bridge role to interconnect remote Ethernet workstations to the main LAN. The workgroup bridge can communicate with an access point (see [Figure 1-7](#)) or with a bridge (see [Figure 1-8](#)).

**Figure 1-7** Workgroup Bridge Communicating with an Access Point



**Figure 1-8** Workgroup Bridge Communicating with a Bridge



# 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.

This section illustrates a typical wireless network configuration containing lightweight access points and a Cisco Wireless LAN Controller (see [Figure 1-9](#)).

**Figure 1-9** Typical Lightweight Access Point Network Configuration Example

