



CHAPTER 2

Wireless Device Overview

Wireless devices (commonly configured as *access points*) 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. When configured as an access point, the wireless device 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 can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

With a management system based on Cisco IOS software, wireless devices are Wi-Fi CERTIFIED™, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

Software Modes

The access point is shipped with an autonomous image and a recovery image on the access point's flash. The default mode is autonomous; however, the access point can be upgraded to operate in Cisco Unified Wireless mode.

Each mode is described below:

- **Autonomous mode**—Supports standalone network configurations, where all configuration settings are maintained locally on the wireless device. Each autonomous device can load its starting configuration independently and still operate in a cohesive fashion on the network.
- **Cisco Unified Wireless mode**—Operates in conjunction with a Cisco Unified Wireless LAN controller, where all configuration information is maintained within the controller. In the Cisco Unified Wireless LAN architecture, wireless devices operate in the lightweight mode using Lightweight Access Point Protocol (LWAPP), as opposed to autonomous mode. The lightweight access point, or wireless device, has no configuration until it associates to a controller. The configuration on the wireless device can be modified by the controller only when the networking is up and running. The controller manages the wireless device configuration, firmware, and control transactions such as 802.1x authentication. All wireless traffic is tunneled through the controller.

For more information about this network architecture design, see *Why Migrate to a Cisco Unified Wireless Network?* on Cisco.com.

Management Options

The wireless device runs its own version of Cisco IOS software that is separate from the Cisco IOS software operating on the router. You can configure and monitor the access point with several different tools:

- Cisco IOS software CLI
- Simple Network Management Protocol (SNMP)
- Web-browser interface:
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

**Note**

The web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98, 2000, and XP platforms and with Netscape version 7.0 on Windows 98, 2000, XP, and Solaris platforms.

**Note**

Avoid using the CLI and the web-browser tools concurrently to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface may display an inaccurate interpretation of the configuration. This inappropriate display of information does not necessarily mean the wireless device is misconfigured.

Use the **interface dot11radio** global configuration CLI command to place the wireless device into the radio configuration mode.

Network Configuration Examples

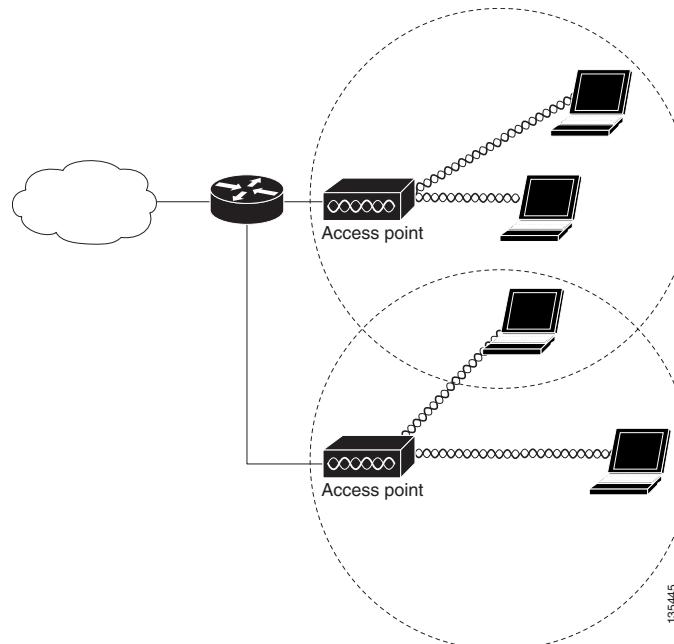
Set up the access point role in any of these common wireless network configurations. The access point default configuration can either be as a root unit connected to a wired LAN or as a central unit in an all-wireless network. Access points can also be configured as bridges and workgroup bridges. These roles require specific configurations, as defined in the following examples.

- [Root Access Point, page 2-3](#)
- [Central Unit in an All-Wireless Network, page 2-4](#)

Root Access Point

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one 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 2-1](#) shows access points acting as root units on a wired LAN.

Figure 2-1 Access Point as Root Unit on a Wired LAN



Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The 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 2-2](#) shows an access point in an all-wireless network.

Figure 2-2 Access Point as Central Unit in All-Wireless Network

