



Overview

Cisco Aironet Access Points (hereafter called *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. With a management system based on Cisco IOS software, Cisco Aironet 350, 1100, and 1200 series access points are Wi-Fi certified, 802.11b-compliant, 802.11g-compliant, and 802.11a-compliant wireless LAN transceivers.

The 350 series access point, which can be upgraded to run Cisco IOS software, uses a single, 802.11b, 2.4-GHz mini-PCI radio. The 1100 series access point uses a single, 802.11b, 2.4-GHz mini-PCI radio that can be upgraded to an 802.11g, 2.4-GHz radio. The 1200 series access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The 1200 series 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.

Access points serve 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).

This chapter provides information on the following topics:

- [Features, page 1-2](#)
- [Management Options, page 1-3](#)
- [Roaming Client Devices, page 1-4](#)
- [Network Configuration Examples, page 1-4](#)

Features

Access points running Cisco IOS software offer these software features:

- **World mode**—Use this feature to communicate the access point's regulatory setting information, including maximum transmit power and available channels, to world mode-enabled clients. Clients using world mode can be used in countries with different regulatory settings and automatically conform to local regulations. World mode is supported only on the 2.4-GHz radio.
- **Repeater mode**—Configure the access point as a wireless repeater to extend the coverage area of your wireless network.
- **Standby mode**—Configure the access point as a standby unit that monitors another access point and assumes its role in the network if the monitored access point fails.
- **Multiple SSIDs**—Create up to 16 SSIDs on your access point and assign any combination of these settings to each SSID:
 - Broadcast SSID mode for guests on your network
 - Client authentication methods
 - Maximum number of client associations
 - VLAN identifier
 - Proxy Mobile IP
 - RADIUS accounting list identifier
 - A separate SSID for infrastructure devices such as repeaters and workgroup bridges
- **VLANs**—Assign VLANs to the SSIDs on your access point (one VLAN per SSID) to differentiate policies and services among users.
- **QoS**—Use this feature to support quality of service for prioritizing traffic from the Ethernet to the access point. The access point also supports the voice-prioritization schemes used by 802.11b wireless phones such as Spectralink's Netlink™ and Symbol's Netvision™.
- **Proxy Mobile IP**—Use this feature to configure the access point to provide proxy Mobile IP service for clients that do not have mobile IP software installed.
- **RADIUS Accounting**—Enable accounting on the access point to send accounting data about wireless client devices to a RADIUS server on your network.
- **TACACS+ administrator authentication**—Enable TACACS+ for server-based, detailed accounting information and flexible administrative control over authentication and authorization processes. It provides secure, centralized validation of administrators attempting to gain access to your access point.
- **Enhanced security**—Enable three advanced security features to protect against sophisticated attacks on your wireless network's WEP keys: Message Integrity Check (MIC), WEP key hashing, and broadcast WEP key rotation.
- **Enhanced authentication services**—Set up repeater access points to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater, it authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

- **Wi-Fi Protected Access (WPA)**—Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.
- **Fast secured roaming using Cisco Centralized Key Management (CCKM)**—Using CCKM, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
- **Access point as backup or stand-alone authentication server**—You can configure an access point to act as a local RADIUS server to provide authentication service for small wireless LANs without a RADIUS server or to provide backup authentication service in case of a WAN link or a server failure. The access point can authenticate LEAP-enabled wireless client devices and allow them to join your network.
- **Rogue access point detection**—Access points running Cisco IOS Release 12.2(11)JA work together with LEAP-enabled client devices running firmware version 5.02.17 or later to detect rogue access points on your wireless LAN. The access point records a message in the system log when a client device discovers and reports an access point on the wireless LAN that fails to authenticate the client using LEAP. When the client successfully authenticates through another access point, it reports the access point that failed LEAP as a potential rogue device.
- **Client ARP caching**—To reduce traffic on the wireless LAN, you can configure access points running Cisco IOS Release 12.2(13)JA to reply to ARP queries on behalf of associated client devices. In previous releases, the access point forwards ARP queries to all associated client devices, and the specified client responds with its MAC address. When the access point maintains an ARP cache, however, it responds to ARP queries on behalf of the client device and does not forward the queries through its radio port.
- **CCKM voice clients and WPA clients on the same VLAN**—Access points running Cisco IOS Release 12.2(13)JA allow both 802.11b CCKM voice clients and 802.11b WPA clients on the same VLAN.
- **WISPr RADIUS attributes**—The Wi-Fi Alliance's WISPr *Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document lists RADIUS attributes that access points must send with RADIUS accounting and authentication requests. You can configure access points running Cisco IOS Release 12.2(13)JA to include these attributes in all RADIUS accounting and authentication requests.
- **Support for 802.11g radios**—Cisco IOS Release 12.2(13)JA supports the 802.11g, 2.4-GHz mini-PCI radio. You can upgrade the 802.11b, 2.4-GHz radio in 1100 and 1200 series access points with an 802.11g, 2.4-GHz radio.

Management Options

You can use the access point management system through the following interfaces:

- The Cisco IOS command-line interface (CLI), which you use through a Telnet session. Most of the examples in this manual are taken from the CLI. [Chapter 4, “Using the Command-Line Interface,”](#) provides a detailed description of the CLI.
- A web-browser interface, which you use through a web browser. [Chapter 3, “Using the Web-Browser Interface,”](#) provides a detailed description of the web-browser interface.

- Simple Network Management Protocol (SNMP). [Chapter 18, “Configuring SNMP,”](#) explains how to configure your access point for SNMP management.

Roaming Client Devices

If you have more than one access point in your wireless LAN, wireless client devices can roam seamlessly from one access point to another. The roaming functionality is based on signal quality, not proximity. When a client’s signal quality drops, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client’s signal to a distant access point remains strong and the signal quality is high, the client will not roam to a closer access point. Checking constantly for closer access points would be inefficient, and the extra radio traffic would slow throughput on the wireless LAN.

Using CCKM and an access point acting as a subnet context manager, client devices can roam from one access point to another so quickly that there is no perceptible delay in voice or other time-sensitive applications.

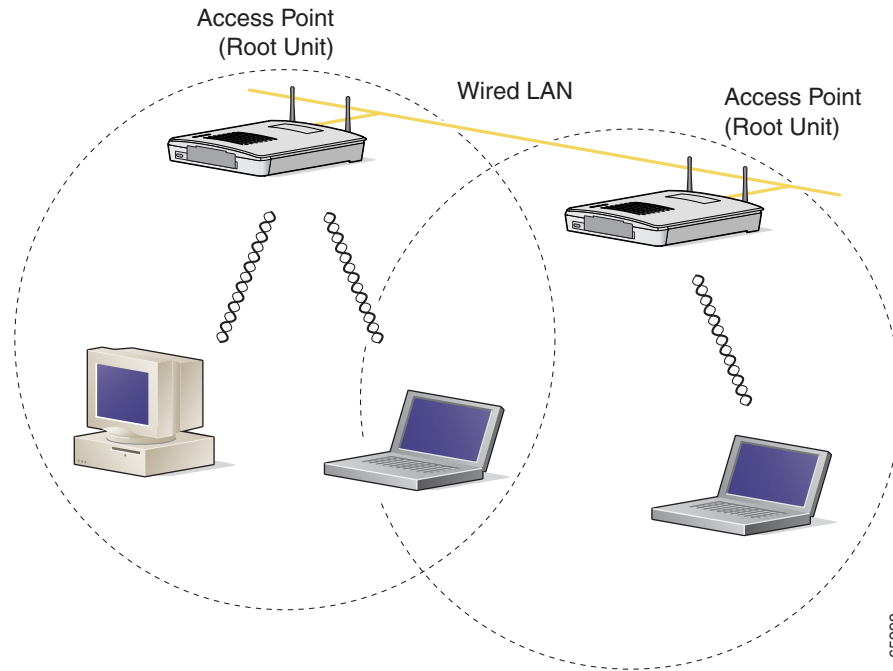
Network Configuration Examples

This section describes the access point’s role in three common wireless network configurations. The 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.

Root Unit on a Wired LAN

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

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



Repeater Unit that Extends Wireless Range

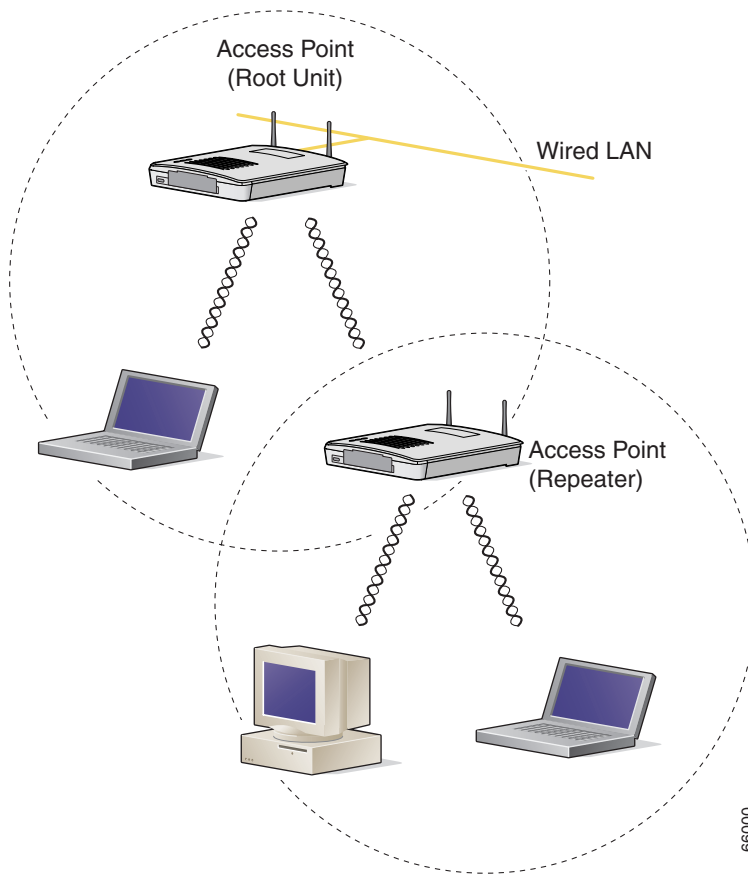
An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. [Figure 1-2](#) shows an access point acting as a repeater. Consult the [“Configuring a Repeater Access Point”](#) section on page 19-3 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 1-2 Access Point as Repeater



66000

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 1-3](#) shows an access point in an all-wireless network.

Figure 1-3 Access Point as Central Unit in All-Wireless Network

