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.

An 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 wireless device using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Each access point platform contains one or two radios:

- 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 1130AG series access point has integrated 802.11g and 802.11a radios and antennas.
- 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.
- The 1230AG series access point is pre-configured to include both an 802.11g and an 802.11a radio. It has antenna connectors for externally attached antennas for both radios.

This chapter provides information on the following topics:

Features

This section lists features supported on access points running Cisco IOS software.

Note The proxy Mobile-IP feature is not supported in Cisco IOS Releases 12.3(2)JA and later.

Features Introduced in This Release

- Support for Multiple BSSIDs—This feature permits a single access point to appear to the WLAN as multiple virtual access points. It does this by assigning an access point with multiple Basic Service Set IDs (MBSSIDs) or MAC addresses.

  To determine whether a radio supports multiple basic SSIDs, enter the **show controllers** command for the radio interface. The radio supports multiple basic SSIDs if the results include this line:

  ```
  Number of supported simultaneous BSSID on radio_interface: 8
  ```

- Support for Wi-Fi 802.11h and Dynamic Frequency Selection (DFS)—This feature allows Cisco Aironet access points configured at the factory for use in Europe and Singapore to detect radar signals such as military and weather sources and switch channels on the access points.
- Wireless IDS – Excess Management Frame Detection—This feature provides scanner access points the ability to detect that WLAN management and control frames exceeded a configurable threshold.
- Wireless IDS – Authentication Attack Detection—This feature requires Cisco Aironet access points to detect and report on excessive attempted or failed authentication attempts (Authentication failure detection and Excess EAPoL authentication).
- Frame Monitor Mode—This feature requires a Scan-only access point to forward all 802.11 frames seen to a protocol analysis station for network troubleshooting from remote sites via partner applications and/or partner Intrusion Detection companies.
- Location Based Services (LBS)—This feature allows a Cisco Aironet access point to detect frames from LBS tags and send them to a pre-configured IP destination, such as a third-party LBS server.
- SNMPv3—This feature enables SNMPv3 support on Cisco Aironet access points to provide an additional level of security.
- WGB Mode on 1200 Series Access Points—This feature allows 1200 series access points to support Work Group Bridge (WGB) functionality on either the 802.11b/g or 802.11a radio.

Existing 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 the wireless device 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
  - RADIUS accounting list identifier
  - A separate SSID for infrastructure devices such as repeaters and workgroup bridges
- VLANs—Assign VLANs to the SSIDs on the wireless device (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™.
- 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 the wireless device.
- 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 Light Extensible Authentication Protocol (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 Temporal Key Integrity Protocol (TKIP) 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 authentication 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 up to 50 LEAP-enabled wireless client devices and allow them to join your network. Access points running Cisco IOS Release 12.2(15)JA also can provide backup MAC-address authentication service for up to 50 addresses.

- Client ARP caching—To reduce traffic on the wireless LAN, you can configure access points running Cisco IOS Release 12.2(13)JA or later 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 or later 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 or later to include these attributes in all RADIUS accounting and authentication requests.
- Support for 802.11g radios—Cisco IOS Releases 12.2(13)JA or later support the 802.11g, 2.4-GHz 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.
- Radio management features on 802.11a, 802.11b, and 802.11g radios—Access points running Cisco IOS Release 12.2(15)JA can participate in radio management using 802.11a, b, or g radios. Access points configured for WDS interact with the WDS device on your wireless LAN. The WDS device forwards radio data to and from the WLSE device or wireless network manager on your network. Radio management includes these features, which are configured on your WLSE device:
  - Rogue access point detection, including the rogue device's IP and MAC addresses, SSID, and, if it is connected to a Cisco device, the switch port to which the rogue is connected
  - Self-healing wireless LAN; if an access point fails, nearby access points increase their transmit power to cover the gap in your wireless LAN
  - Client tracking to identify the access point to which each client device is associated
- Scanning-only mode—Access points running Cisco IOS Release 12.2(15)JA can act as scanners to detect rogue access points and monitor radio traffic on your wireless LAN. Access points configured as scanners participate in radio management but do not accept client associations.
- HTTPS - HTTP with SSL 3.0—This feature supports a Secure Sockets Layer (SSL)/Secure Hypertext Transfer Protocol (HTTPS) method of managing Cisco Aironet access points through a Web browser.
- Support for Cisco Aironet IEEE 802.11a Radio Part Numbers AIR-RM21A and AIR-RM22A—Cisco IOS Release 12.3(2)JA introduces support for the Cisco Aironet 1200 series access point IEEE 802.11a radio part numbers AIR-RM21A and AIR-RM22A. These new IEEE 802.11a radios support all access point features introduced in Cisco IOS Release 12.3(2)JA as well as all Cisco IOS software access point features supported by 1200 series access points in Cisco IOS Release 12.2(15)XR and earlier.
- AES-CCMP—This feature supports Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security.
- IEEE 802.1X Local Authentication Service for EAP-FAST—This feature expands wireless domain services (WDS) IEEE 802.1X local authentication to include support for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). IEEE 802.1X local authentication was introduced in Cisco IOS Release 12.2(11)JA.

- Wi-Fi Multimedia (WMM) Required Elements—This feature supports the required elements of WMM. WMM is designed to improve the user experience for audio, video, and voice applications over a Wi-Fi wireless connection. WMM is a subset of the IEEE 802.11e Quality of Service (QoS) draft standard. WMM supports QoS prioritized media access via the Enhanced Distributed Channel Access (EDCA) method. Optional elements of the WMM specification including call admission control using traffic specifications (TSPEC) are not supported in this release.
- VLAN Assignment By Name—This feature allows the RADIUS server to assign a client to a virtual LAN (VLAN) identified by its VLAN name. In releases before Cisco IOS Release 12.3(2)JA, the RADIUS server identified the VLAN by ID. This feature is important for deployments where VLAN IDs are not used consistently throughout the network.
- Microsoft WPS IE SSIDL—This feature allows the Cisco Aironet access point to broadcast a list of configured SSIDs (the SSIDL) in the Microsoft Wireless Provisioning Services Information Element (WPS IE). A client with the ability to read the SSIDL can alert the user to the availability of the SSIDs. This feature provides a bandwidth-efficient, software-upgradeable alternative to multiple broadcast SSIDs (MB/SSIDs).
- HTTP Web Server v1.1—This feature provides a consistent interface for users and applications by implementing the HTTP 1.1 standard (see RFC 2616). In previous releases, Cisco software supported only a partial implementation of HTTP 1.0. The integrated HTTP Server API supports server application interfaces. When combined with the HTTPS and HTTP 1.1 Client features, provides a complete, secure solution for HTTP services to and from Cisco devices.
- IP-Redirect—This features provides the capability to redirect traffic intended for a particular destination to another IP address specified by the administrator.

Management Options

You can use the wireless device management system through the following interfaces:

- The Cisco IOS command-line interface (CLI), which you use through a console port or Telnet session. Use the **interface dot11radio** global configuration command to place the wireless device into the radio configuration mode. 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 17, "Configuring SNMP," explains how to configure the wireless device for SNMP management.

Roaming Client Devices

If you have more than one wireless device in your wireless LAN, wireless client devices can roam seamlessly from one wireless device 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 a device providing WDS, 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.

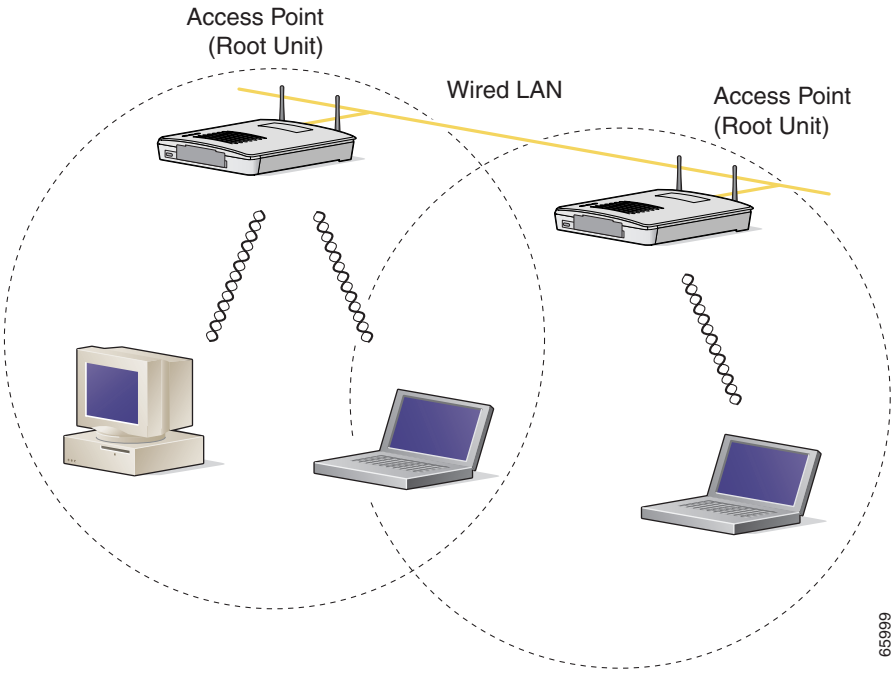
Network Configuration Examples

This section describes the access point's role in 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

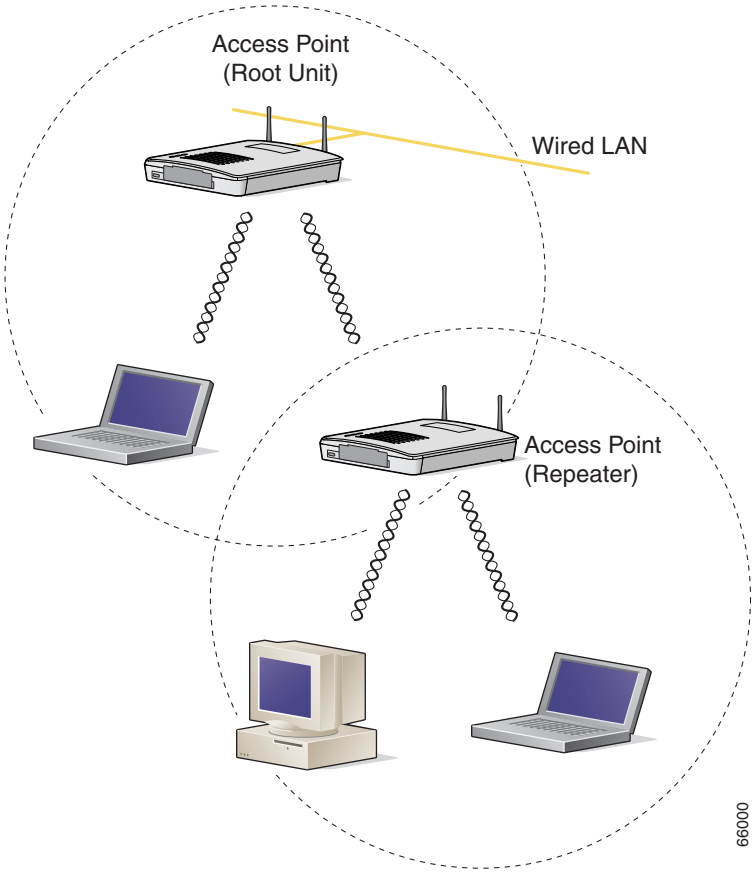


Repeater Unit that Extends Wireless Range

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 18-3 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



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